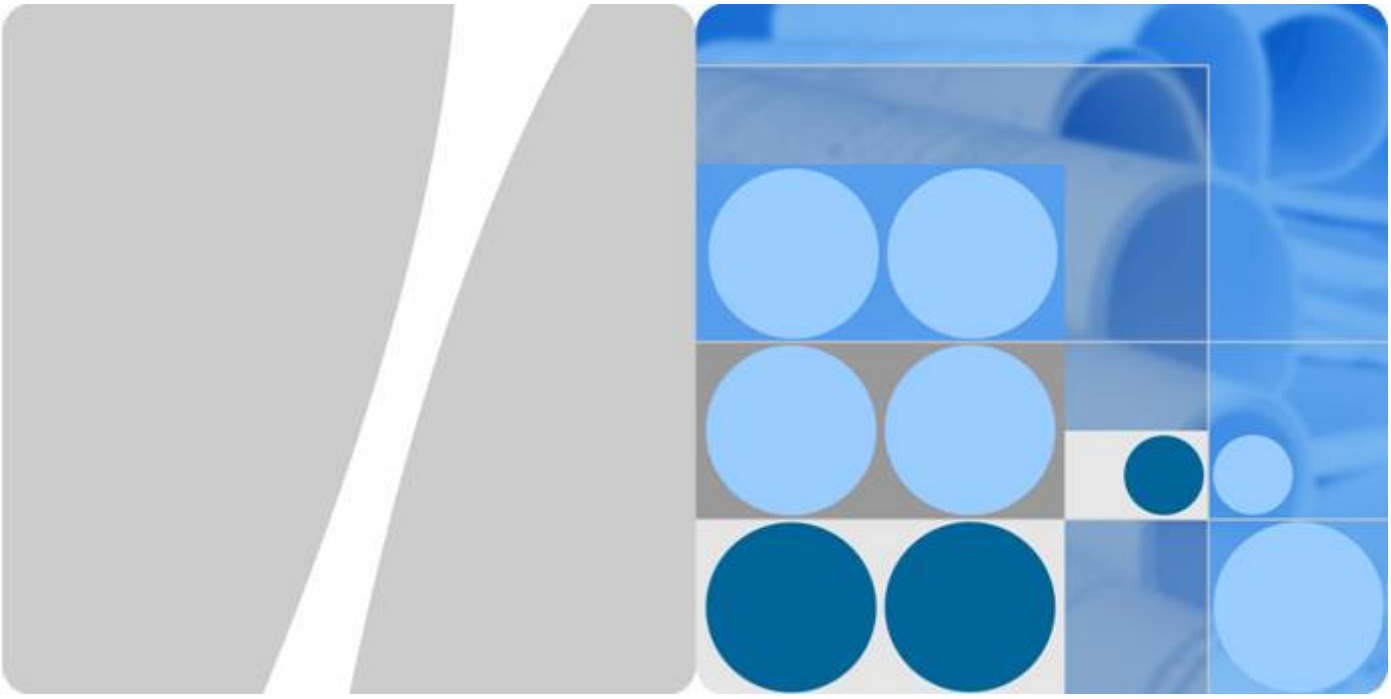


S2700&S3700 系列以太网交换机

V100R006C05

配置指南-IP 组播

文档版本　05

发布日期　2017-03-30

华为技术有限公司

HUAWEI

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://e.huawei.com

前 言

读者对象

本文档介绍了S2700&S3700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	用于警示紧急的危险情形，若不避免，将会导致人员死亡或严重的人身伤害。
 警告	用于警示潜在的危险情形，若不避免，可能会导致人员死亡或严重的人身伤害。
 小心	用于警示潜在的危险情形，若不避免，可能会导致中度或轻微的人身伤害。
 注意	用于传递设备或环境安全警示信息，若不避免，可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “注意”不涉及人身伤害。

符号	说明
说明	用于突出重要/关键信息、最佳实践和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

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&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。

密码配置约定

- 配置明文模式的密码时，密码将会以明文形式保存在配置文件中，这种模式具有较高安全风险，配置时请尽量选择密文模式。为了充分保证设备安全，请定期修改密码。
- 配置密文模式的密码时，如果输入以“%$%$....%$%$”为起始和结束符的合法密文（本设备可以解密的密文），查看设备上的配置文件时会显示与配置相同的密文。请不要采用此种方式直接配置密码。

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 05 (2017-03-30)

修正了资料中的一些错误。

文档版本 04 (2016-03-31)

该版本的更新如下：

修正了资料中的一些错误。

文档版本 03 (2014-01-20)

该版本的更新如下：

资料随产品更新。

文档版本 02 (2013-04-20)

该版本的更新如下：

新增：

- **3.9.2 配置IGMP SSM Mapping后没有生成（S，G）表项**
- **4.14.3 源DR在接收到组播数据报文后仍不向RP发送注册报文**
- **4.14.4 源DR向RP发送了注册报文之后，注册出接口一直存在**
- **5.8.2 组播转发表项入接口不正确**
- **8.5.1 收到IGMPv2 Report报文后无法生成表项**

文档版本 01 (2013-02-08)

第一次正式发布。

目 录

前 言 ii
1 交换机支持的 IP 组播特性概述 1
2 IP 组播配置指导 2
2.1 IP 组播介绍 3
2.2 IPv4 组播相关概念 5
2.3 在 IPv4 网络中部署组播 9
3 IGMP 配置 12
3.1 IGMP 概述 14
3.2 设备支持的 IGMP 特性 14
3.3 缺省配置 15
3.4 配置 IGMP 基本功能 16
3.4.1 使能 IGMP 功能 16
3.4.2 配置 IGMP 版本 17
3.4.3 （可选）配置静态组播组 17
3.4.4 （可选）配置接口加入的组播组范围 18
3.4.5 检查配置结果 18
3.5 调整 IGMP 性能 19
3.5.1 配置 Router-Alert 选项 19
3.5.2 配置 IGMP 查询器参数 20
3.5.3 配置 IGMP 快速离开 22
3.5.4 配置 IGMP On-Demand 23
3.5.5 检查配置结果 24
3.6 配置 IGMP SSM Mapping 24
3.7 维护 IGMP 25
3.7.1 清除 IGMP 组信息 25
3.7.2 监控 IGMP 运行状况 26
3.8 配置举例 26
3.8.1 配置 IGMP 基本功能示例 26
3.8.2 配置静态加入组播组示例 31
3.8.3 配置 IGMP SSM Mapping 示例 35
3.9 常见配置错误 40
3.9.1 IGMP 表项无法正常建立 41

3.9.2 配置 IGMP SSM Mapping 后没有生成（S，G）表项.....41
4 PIM-SM（IPv4）配置.....43
4.1 PIM-SM（IPv4）概述.....45
4.2 设备支持的 PIM-SM（IPv4）特性.....47
4.3 缺省配置.....49
4.4 配置 ASM 模型的 PIM-SM.....49
4.4.1 使能 PIM-SM.....49
4.4.2 配置 RP.....50
4.4.3 （可选）配置 BSR 管理域.....52
4.4.4 （可选）配置 RPT 不向 SPT 切换.....53
4.4.5 （可选）调整注册控制参数.....53
4.4.6 （可选）调整 C-RP 控制参数.....54
4.4.7 （可选）调整 C-BSR 控制参数.....55
4.4.8 检查配置结果.....56
4.5 配置 SSM 模型的 PIM-SM.....57
4.5.1 使能 PIM-SM.....57
4.5.2 （可选）配置 SSM 组策略.....57
4.5.3 检查配置结果.....58
4.6 调整组播源控制参数.....58
4.7 调整邻居控制参数.....59
4.8 调整 DR 竞选控制参数.....61
4.9 调整加入和剪枝控制参数.....62
4.9.1 调整 Join-Prune 报文的时间控制参数.....62
4.9.2 调整剪枝延迟时间.....63
4.9.3 检查配置结果.....64
4.10 调整断言控制参数.....65
4.11 配置 PIM BFD.....66
4.12 维护 PIM-SM.....67
4.12.1 清除 PIM 控制报文统计信息.....67
4.12.2 监控 PIM 的运行状况.....68
4.13 配置举例.....68
4.13.1 配置 ASM 的 PIM-SM 网络示例.....69
4.13.2 配置 SSM 的 PIM-SM 网络示例.....77
4.13.3 配置 PIM BFD 示例.....85
4.14 常见配置错误.....88
4.14.1 PIM-SM 网络中 RPT 无法正常转发数据.....88
4.14.2 PIM-SM 网络中 SPT 无法正常转发数据.....90
4.14.3 源 DR 在接收到组播数据报文后仍不向 RP 发送注册报文.....93
4.14.4 源 DR 向 RP 发送了注册报文之后，注册出接口一直存在.....94
5 组播路由管理（IPv4）配置.....95
5.1 组播路由管理（IPv4）概述.....96
5.2 缺省配置.....96

5.3 改变 RPF 检查规则 97
5.3.1 配置组播静态路由 97
5.3.2 配置组播路由最长匹配 98
5.3.3 配置组播负载分担 98
5.3.4 检查配置结果 99
5.4 配置组播转发边界 99
5.5 配置组播转发表控制参数 100
5.5.1 限制组播转发表项数量 100
5.5.2 配置组播转发表项最大下行节点数 101
5.5.3 检查配置结果 101
5.6 维护组播路由管理 102
5.6.1 使用 Ping 检测组播业务性能 102
5.6.2 使用 Tracert 检测组播业务性能 102
5.6.3 清除组播转发表项和路由表项 103
5.6.4 监控组播路由和转发的状况 103
5.7 配置举例 104
5.7.1 配置组播静态路由改变 RPF 路由示例 104
5.7.2 配置组播静态路由衔接 RPF 路由示例 109
5.7.3 配置组播负载分担示例 114
5.8 常见配置错误 121
5.8.1 组播静态路由建立失败 121
5.8.2 组播转发表项入接口不正确 121
6 IGMP Snooping 配置 123
6.1 IGMP Snooping 概述 125
6.2 设备支持的 IGMP Snooping 特性 126
6.3 缺省配置 127
6.4 配置 IGMP Snooping 基本功能 128
6.4.1 使能 IGMP Snooping 功能 128
6.4.2 配置 IGMP Snooping 版本 129
6.4.3 （可选）配置静态路由器端口 129
6.4.4 （可选）配置静态成员端口 130
6.4.5 （可选）配置 IGMP Snooping 查询器 130
6.4.6 （可选）配置 Report 和 Leave 报文抑制 133
6.4.7 （可选）配置 Router-Alert 选项 134
6.4.8 （可选）配置 IGMP Snooping 抑制动态加入 134
6.4.9 检查配置结果 135
6.5 配置 IGMP Snooping Proxy 135
6.6 配置 IGMP Snooping 策略 136
6.6.1 配置组播组过滤策略 137
6.6.2 配置接口下组播数据过滤 137
6.6.3 配置丢弃未知组播流 138
6.6.4 配置接口学习的组播表项数量限制 139

6.6.5 检查配置结果 139
6.7 配置成员关系快速刷新 140
6.7.1 配置动态成员端口老化时间 140
6.7.2 配置动态路由器端口老化时间 141
6.7.3 配置成员端口快速离开 142
6.7.4 配置网络拓扑变化时发送 Query 报文 142
6.7.5 检查配置结果 143
6.8 配置 IGMP Snooping SSM Mapping 143
6.8.1 （可选）配置 SSM 组策略 143
6.8.2 配置 IGMP Snooping SSM Mapping 144
6.8.3 检查配置结果 145
6.9 维护 IGMP Snooping 145
6.9.1 清除 IGMP Snooping 表项 145
6.9.2 清除 IGMP Snooping 统计信息 146
6.9.3 监控 IGMP Snooping 的运行状况 146
6.10 配置举例 147
6.10.1 配置 IGMP Snooping 示例 147
6.10.2 配置使用静态端口实现二层组播示例 150
6.10.3 配置 IGMP Snooping 查询器示例 152
6.10.4 配置 IGMP Snooping Proxy 示例 156
6.10.5 配置 IGMP Snooping SSM Mapping 功能示例 159
6.11 常见配置错误 161
6.11.1 二层组播流量不通 162
6.11.2 配置的组播组策略不生效 163
7 组播 VLAN 配置 164
7.1 组播 VLAN 概述 165
7.2 设备支持的组播 VLAN 特性 166
7.3 缺省配置 168
7.4 配置基于用户 VLAN 的组播 VLAN 一对多 169
7.4.1 配置用户 VLAN 169
7.4.2 配置组播 VLAN 169
7.4.3 配置接口加入 VLAN 170
7.4.4 检查配置结果 171
7.5 配置基于用户 VLAN 的组播 VLAN 多对多 171
7.5.1 配置用户 VLAN 172
7.5.2 配置组播 VLAN 172
7.5.3 配置接口加入 VLAN 173
7.5.4 检查配置结果 173
7.6 配置基于接口的组播 VLAN 功能 174
7.6.1 配置组播 VLAN 174
7.6.2 配置用户 VLAN 绑定组播 VLAN 175
7.6.3 配置接口加入 VLAN 175

7.6.4 检查配置结果 175
7.7 配置举例 175
7.7.1 配置基于用户 VLAN 的组播 VLAN 一对多功能示例 176
7.7.2 配置基于用户 VLAN 的组播 VLAN 多对多功能示例 178
7.7.3 配置基于接口的组播 VLAN 功能示例 181
7.8 常见配置错误 184
7.8.1 用户 VLAN 下用户主机接收不到组播数据 184
8 可控组播配置 185
8.1 可控组播概述 186
8.2 基本概念 186
8.3 配置可控组播功能 187
8.3.1 配置组播组 187
8.3.2 配置组播列表 188
8.3.3 配置组播模板 188
8.3.4 VLAN 上应用组播模板 189
8.3.5 检查配置结果 190
8.4 配置举例 190
8.4.1 配置可控组播示例 190
8.5 常见配置错误 194
8.5.1 收到 IGMPv2 Report 报文后无法生成表项 194
9 MLD Snooping 配置 195
9.1 MLD Snooping 概述 197
9.2 设备支持的 MLD Snooping 特性 198
9.3 缺省配置 199
9.4 配置 MLD Snooping 基本功能 199
9.4.1 使能 MLD Snooping 199
9.4.2 配置 MLD Snooping 版本 200
9.4.3 （可选）配置静态路由器端口 201
9.4.4 （可选）配置静态成员端口 201
9.4.5 （可选）配置 MLD Snooping 查询器 202
9.4.6 （可选）配置 Router-Alert 选项 204
9.4.7 检查配置结果 205
9.5 配置 MLD Snooping 策略 205
9.5.1 配置组播组过滤策略 205
9.5.2 配置接口下组播数据过滤 206
9.5.3 配置丢弃未知组播流 207
9.5.4 配置接口学习的组播表项数量限制 208
9.5.5 检查配置结果 208
9.6 配置成员关系快速刷新 208
9.6.1 配置动态成员端口老化时间 209
9.6.2 配置动态路由器端口老化时间 210
9.6.3 配置成员端口快速离开 210

9.6.4 配置网络拓扑变化时发送 Query 报文 211
9.6.5 检查配置结果 211
9.7 维护 MLD Snooping 211
9.7.1 清除 MLD Snooping 表项 211
9.7.2 清除 MLD Snooping 统计信息 212
9.7.3 监控 MLD Snooping 的运行状况 212
9.8 配置举例 213
9.8.1 配置 MLD Snooping 示例 213
9.8.2 配置使用静态端口实现二层组播示例 215
9.8.3 配置 MLD Snooping 查询器示例 218
9.8.4 配置成员端口快速离开示例 222
9.8.5 配置 MLD Snooping 响应网络拓扑变化示例 224
9.9 常见配置错误 229
9.9.1 二层组播不生效 229
9.9.2 配置的 IPv6 组播组策略不生效 230

1 交换机支持的 IP 组播特性概述

以下表格列出了组播特性在交换机各系列上的支持情况。

交换机不同形态对组播特性的支持情况如表1所示。

表 1-1 交换机支持的组播特性

特性名称	S2700SI	S2710SI	S2700EI	S3700SI	S3700EI
IGMP	不支持	不支持	不支持	不支持	支持
PIM-DM（IPv4）	不支持	不支持	不支持	不支持	不支持
PIM-SM（IPv4）	不支持	不支持	不支持	不支持	支持
组播路由管理（IPv4）	不支持	不支持	不支持	不支持	支持
IGMP Snooping	支持	支持	支持	支持	支持
组播VLAN	不支持	不支持	支持	支持	支持
可控组播	不支持	不支持	支持	支持	支持
MLD Snooping	不支持	不支持	支持	支持	支持

2 IP 组播配置指导

关于本章

本章介绍IP组播的基本概念和相关协议、特性，并提供典型的组播网络场景。

2.1 IP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。

2.2 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。

2.3 在IPv4网络中部署组播
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。

2.1 IP 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。

说明

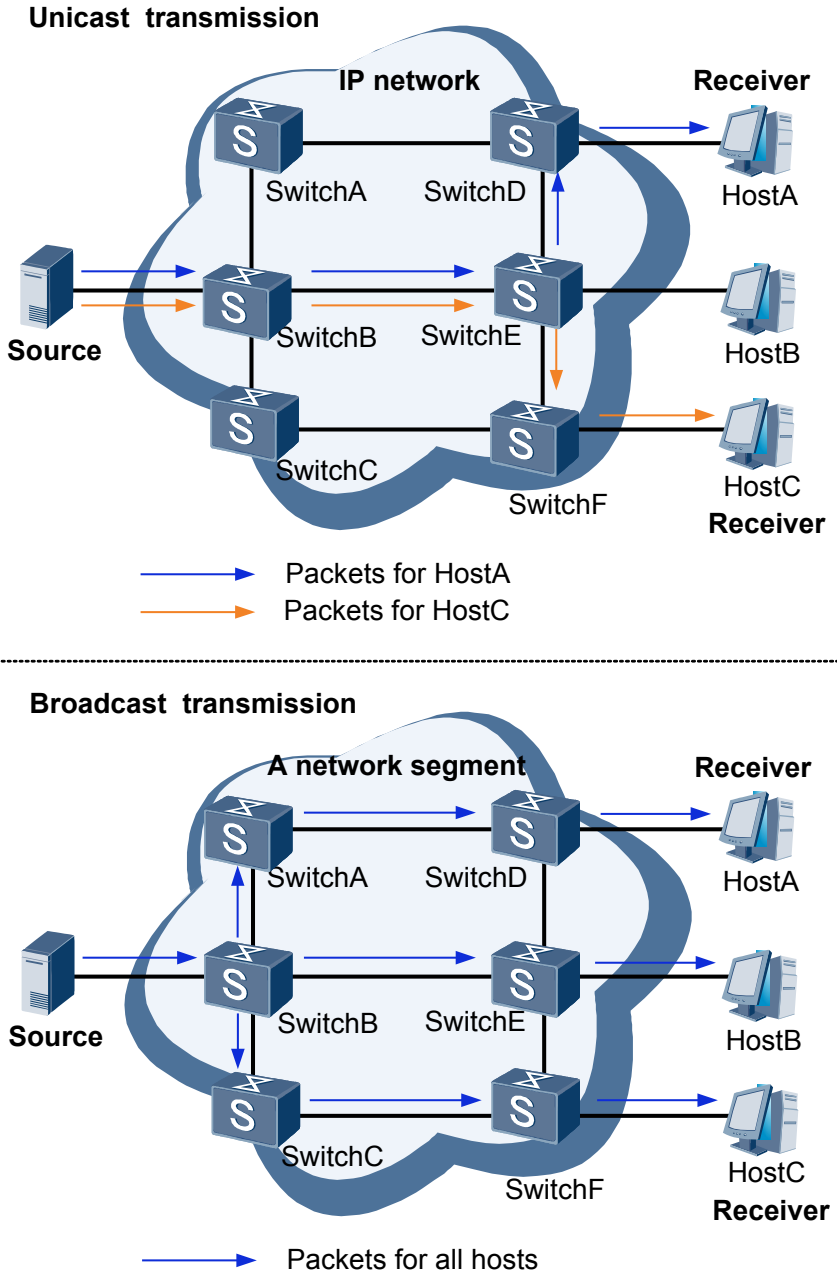
本文中出现的路由器，指代一般意义的路由器和三层交换机。S2700&S3700支持IP组播路由功能，可以用作组播路由器。

组播产生原因

传统的IP通信有两种方式：单播（Unicast），信息源为每个需要信息的主机都发送一份独立的报文；广播（Broadcast），信息源将信息发送给该网段中的所有主机，而不管其是否需要该信息。

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2-1**所示。

图 2-1 采用单播和广播方式进行点对多点传输数据示意图

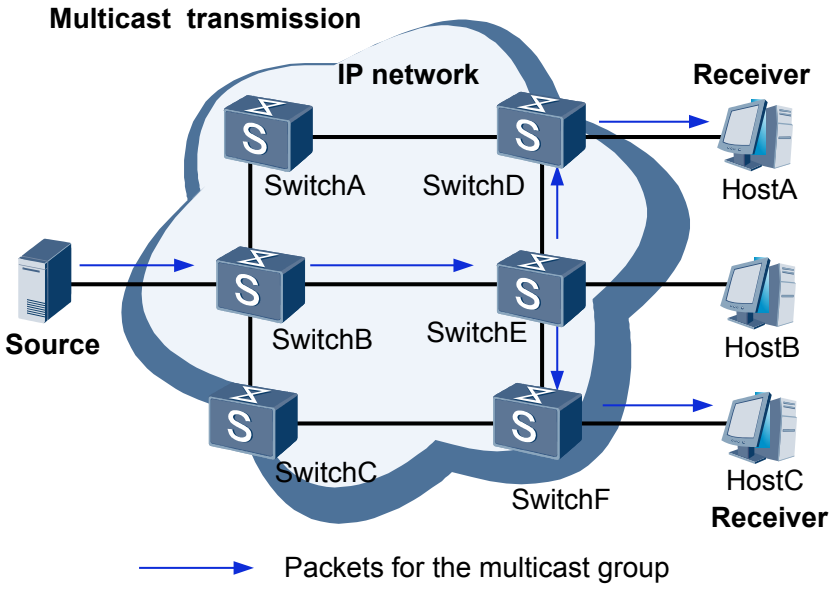


- 采用单播方式时，网络中传输的信息量与需要该信息的用户量成正比。当需要该信息的用户数量较大时，信息源需要将多份内容相同的信息发送给不同的用户，这对信息源以及网络带宽都将造成巨大的压力。由此可以看出，该传输方式不利于信息的批量发送，只适用于用户稀少的网络。
- 采用广播方式时，不需要信息的主机也将收到该信息，这样不仅信息的安全性得不到保障，而且会造成同一网段中信息泛滥。由此可见，该传输方式不利于与特定对象进行数据交互，并且还浪费了大量的带宽。

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2-2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（HostA、HostC）可以接收该数据，网络中其他主机（HostB）不能收到该数据。

图 2-2 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。

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。

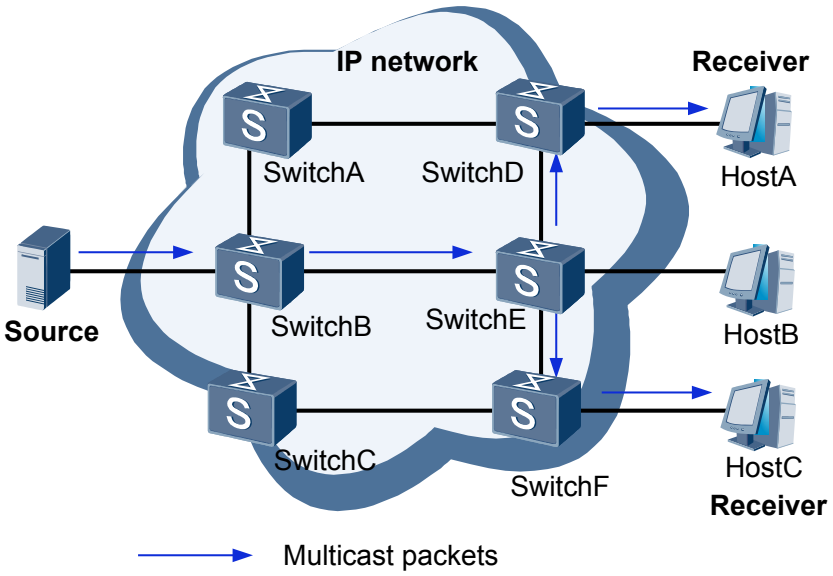
2.2 IPv4 组播相关概念

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2-3所示，网络中存在信息发送者Source，对Source的信息感兴趣的主机提出信息需求，网络采用组播方式传输信息。

图 2-3 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2-3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2-3中的Receiver。组播组中的成员是动态的，主机可以在任何时刻加入或离开组播组。组播组成员可以广泛地分布在网络中的任何地方。
- 组播路由器：支持三层组播功能的路由器或交换机，如图2-3中的各个Switch。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：ASM模型仅针对组地址提供组播分发。一个组播组地址作为一个网络服务的集合，任何源发布到该组地址的数据得到同样的服务。接收者主机加入组播组以后可以接收到任意源发送到该组的数据。
- SSM（Source-Specific Multicast）指定源组播模型：SSM模型针对特定源和组的绑定数据流提供服务，接收者主机在加入组播组时，可以指定只接收哪些源的数据。加入组播组以后，主机只会收到指定源发送到该组的数据。

而且为了便于接收者进行区分，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。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2-1。

表 2-1 IPv4 组播地址的范围及含义

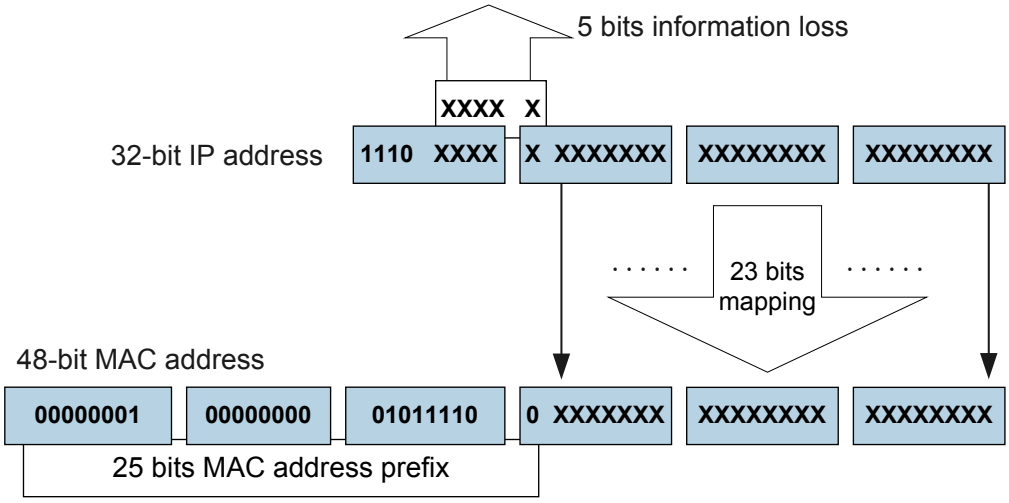
D类地址范围	含义
224.0.0.0～224.0.0.255	本地链路的保留组地址。IANA为路由协议预留的组播地址（也称为永久组地址），用于标识一组特定的网络设备，不用于组播转发。
224.0.1.0～231.255.255.255 233.0.0.0～238.255.255.255	ASM组播地址，全网范围内有效。
232.0.0.0～232.255.255.255	缺省情况下的SSM组播地址，全网范围内有效。
239.0.0.0～239.255.255.255	管理范围组地址。缺省的BSR管理域组地址范围，仅在BSR管理域内有效，属于私有地址。在不同的BSR管理域内使用相同的地址不会冲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

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2-4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 2-4 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 2-2 IPv4 组播协议

协议	功能	备注
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。
PIM（Protocol Independent Multicast）-IPv4协议无关组播	PIM-IPv4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组播设备上，从而实现组播数据的路由查找与转发。PIM协议包括PIM-SM（Protocol Independent Multicast Sparse Mode）协议无关组播-稀疏模式和PIM-DM（Protocol Independent Multicast Dense Mode）协议无关组播－密集模式。PIM-SM适合规模较大、组成员相对比较分散的网络；PIM-DM适合规模较小、组播组成员相对比较集中的网络。 **说明** S3700EI仅支持PIM-SM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。

协议	功能	备注
IGMP Snooping & IGMP Snooping Proxy	IGMP Snooping功能可以使交换机工作在二层时，通过侦听上游的三层设备和用户主机之间发送的IGMP报文来建立组播数据报文的二层转发表，管理和控制组播数据报文的转发，进而有效抑制组播数据在二层网络中扩散。 IGMP Snooping Proxy功能在IGMP Snooping的基础上使交换机代替上游三层设备向下游主机发送IGMP Query报文和代替下游主机向上游设备发送IGMP Report和Leave报文，这样能够有效的节约上游设备和本设备之间的带宽。	与IGMP对应，IGMP Snooping就是IGMP协议在二层设备中的延伸协议，可以通过配置IGMP Snooping的版本使交换机可以处理不同IGMP版本的报文。

2.3 在 IPv4 网络中部署组播

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。

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。

单 PIM 域内组播

在一个小型网络中，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2-5所示。

图 2-5 PIM 域内组播业务的基本部署示意图

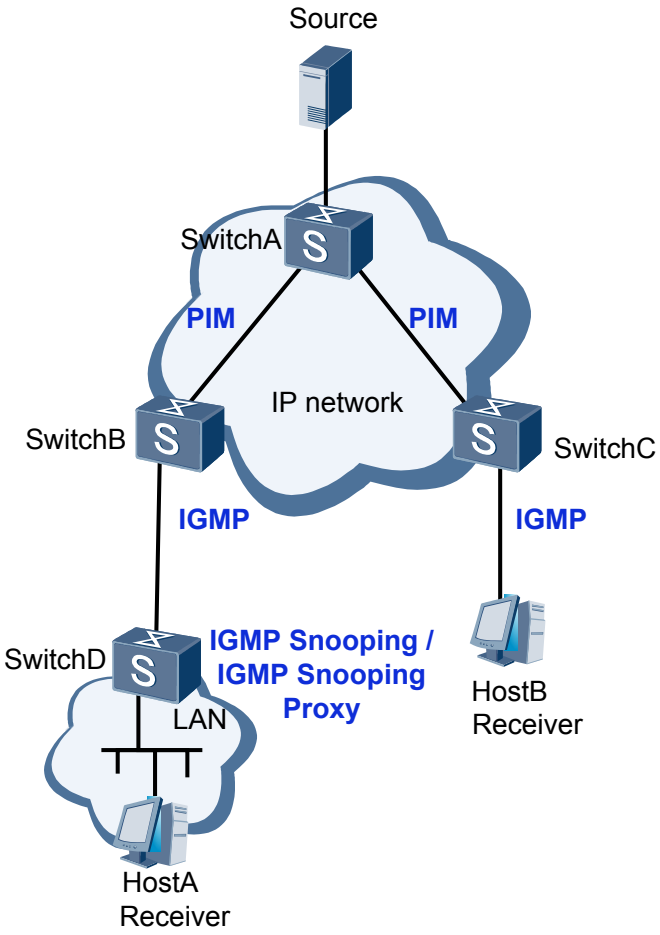


表 2-3 PIM 域内组播业务的各设备应用组播协议

部署协议	应用位置	目的
PIM （必选）	组播域内的设备所有接口，包括SwitchA、SwitchB、SwitchC的所有接口。 具体配置请参见**4 PIM-SM（IPv4）配置**。	将组播数据流从组播源Source发送到与有组播需求的用户相连的SwitchB和SwitchC上。
IGMP （必选）	三层组播设备与用户连接侧接口，包括SwitchB、SwitchC的用户侧接口。 具体配置请参见**3 IGMP配置**。	实现组播组成员Host加入与离开组播组，SwitchB和SwitchC维护与管理组成员。

部署协议	应用位置	目的
IGMP Snooping & IGMP Snooping Proxy （可选）	三层组播设备与用户主机之间的交换机SwitchD的VLAN内。 具体配置请参见**6 IGMP Snooping配置**。	IGMP Snooping通过侦听SwitchB和HostA之间发送的IGMP报文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。 IGMP Snooping Proxy代替SwitchB发送IGMP Query报文，代替HostA发送IGMP Report和Leave报文。

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（Internet Group Management Protocol）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。

3.2 设备支持的IGMP特性
设备支持的IGMP特性包括：IGMP基本功能、调整IGMP性能、IGMP SSM Mapping等。

3.3 缺省配置
介绍缺省情况下，IGMP的配置信息。

3.4 配置IGMP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。

3.5 调整IGMP性能
IGMP使能后，缺省情况下可以正常工作。同时根据安全性和网络性能优化的要求，可以适当调整相关参数。

3.6 配置IGMP 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或IGMPv2。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 维护IGMP
IGMP的维护包括：清除IGMP的组信息、监控IGMP运行状况。

3.8 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，分别提供配置举例。

3.9 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。

3.1 IGMP 概述

IGMP（Internet Group Management Protocol）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。

要使组播数据最终能够到达接收者，需要将接收者接入IP组播网络，并加入到相应的组播组中。通过在接收者主机和与其在共享网段的组播路由器之间运行IGMP，可以实现主机动态加入组播组和组播路由器对本地网络组成员信息的管理。

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则需要与SSM Mapping技术相结合才能实现。

图 3-1 IGMP 基本组网图

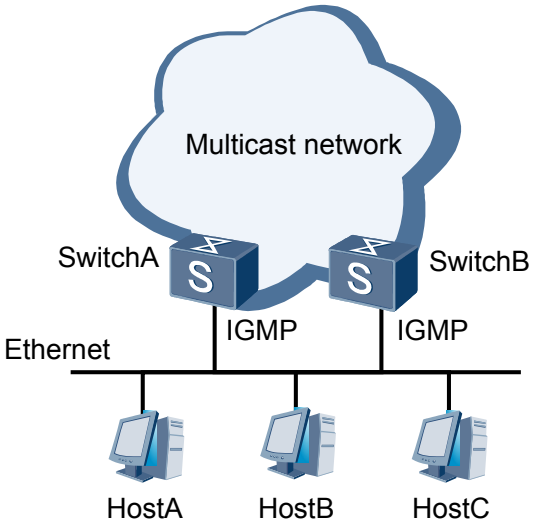


图3-1所示为IGMP的基本组网图，在接收者主机和共享网段的组播路由器上配置IGMP。

- 当用户主机网段上连接多台路由器时，从中选出一台作为查询路由器（简称查询器），负责向该网段周期发送查询报文。
- 查询器定时发送Query报文并接收主机反馈的Report报文和Leave报文，了解接口连接的网段上有哪些组播组存在接收者，也就是组成员。如果出现组成员，路由器应将组播数据转发到这个网段；如果没有成员则不转发。
- 主机发送Report报文加入组播组，发送Leave报文宣告离开组播组（只在IGMPv2和IGMPv3时），自主决定接收哪些组播组的数据。

3.2 设备支持的 IGMP 特性

设备支持的IGMP特性包括：IGMP基本功能、调整IGMP性能、IGMP SSM Mapping等。

说明

S2700&S3700支持IGMP的接口为VLANIF接口、Loopback接口。在本章配置中，如无特殊说明，接口的配置一般选择VLANIF接口。使用VLANIF接口前需要先将物理接口加入该VLAN。

在IGMP协议报文（不包括IGMPv3）默认的CPCAR值下，设备最多能够同时处理大约150个组播用户的点播需求。

IGMP 基本功能

设备支持的IGMP基本功能有：

- 支持IGMPv1、IGMPv2和IGMPv3，版本可配置。由于不同版本的IGMP协议报文不相同，因此需要为路由器和成员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）。
- 支持静态加入组播组。当网络中存在稳定的组播组成员时，通过配置接口静态加入组播组，可以实现组播数据的快速、稳定转发。
- 允许配置接口加入的组播组范围。通过在对应接口上设置一个ACL规则作为过滤器，以限制接口所服务的组播组范围，从而提高IGMP的安全性。

调整 IGMP 性能

出于安全性或网络性能优化考虑，可以在路由器上配置以下功能：

- Router-Alert选项：可以配置设备仅接收包含Router-Alert选项的IGMP报文，提高安全性。
- 查询器：对查询器的参数进行合理配置，既可以使成员关系得到及时的更新维护，又可以避免报文发送过多造成网络拥塞。
- 快速离开：配置快速离开可以使路由器快速响应成员主机的Leave报文，还可以节省网络带宽。
- IGMP On-Demand：根据成员的需求维护组成员关系，减少了报文交互，降低网络流量。

IGMP SSM Mapping

SSM（Source-Specific Multicast）提供了一种能够在成员端指定组播源的传输服务，需要IGMPv3的支持。有些情况下，成员端只能运行IGMPv1或IGMPv2，可以通过在路由器上配置IGMP SSM Mapping功能，向运行IGMPv1或IGMPv2的成员提供SSM服务。

IGMP-CPCAR 注意事项

CPCAR通过对上送控制平面的不同业务的协议报文分别进行限速，来保护控制平面的安全。设备针对每类协议报文都有缺省的CPCAR值，部分协议报文的CPCAR值需要根据实际业务规模和具体的用户网络环境进行调整。

调整CPCAR不当将会影响网络业务，如果需要调整IGMP报文的CPCAR，建议联系华为工程师处理。

3.3 缺省配置

介绍缺省情况下，IGMP的配置信息。

表3-1列出了IGMP的缺省配置。

表 3-1 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

3.4 配置 IGMP 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。

前置任务

在配置IGMP基本功能之前，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。

配置流程

IGMP配置在成员主机和与之相连的交换机上。本文介绍如何在交换机上配置IGMP。

3.4.1 使能IGMP功能和3.4.2 配置IGMP版本为必选配置，其他为可选配置，请根据需要选配。

3.4.1 使能 IGMP 功能

背景信息

配置组播协议之前，必须先使能IP组播路由功能。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，组播所有相关配置将无法生效。

IGMP应该配置在与组成员相连的接口上。

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IP组播路由功能。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 执行命令**igmp enable**，使能IGMP功能。

说明

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

----结束

3.4.2 配置 IGMP 版本

背景信息

运行IGMP高版本的交换机可以识别低版本的成员报告，但是低版本的交换机不能识别高版本的成员报告。为了保证IGMP的正常运行，建议在交换机上配置和成员主机相同或高于成员主机的版本。

如果在主机侧共享网段上有多个交换机，由于不同版本的IGMP协议报文结构不同，为了保证IGMP的正常运行，必须在所有交换机接口配置相同的IGMP版本。

说明

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

- 配置全局的IGMP版本
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**igmp**，进入IGMP视图。
  c. 执行命令**version** { **1** | **2** | **3** }，配置全局的IGMP版本。

     缺省情况下，IGMP协议运行的是IGMPv2版本。
- 配置接口的IGMP版本
  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 version** { **1** | **2** | **3** }，配置IGMP版本。

----结束

3.4.3 （可选）配置静态组播组

背景信息

在某些应用场景中，可以在交换机的用户侧接口上配置静态组播组。比如：

- 网络中存在稳定的组播组成员，为了实现组播数据的快速、稳定转发，可以在用户侧接口配置静态组播组。
- 某网段内没有组播组成员或主机无法发送Report报文，但是又需要将组播数据转发到该网段，可以在接口上配置静态组播组，将组播数据“拉”到接口。

在接口上配置静态组播组后，交换机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。

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。

如果在Loopback接口上配置静态加入组播组或组播源组，组播交换机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。接口会立即转发。

缺省情况下，接口未配置任何静态组播组。

----结束

3.4.4 （可选）配置接口加入的组播组范围

背景信息

为了让接口所在网段的成员主机加入指定的组播组，并接收这些组的报文，可以在该接口上设置ACL规则，对收到的成员Report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《S2700&S3700 系列以太网交换机 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* [**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

3.4.5 检查配置结果

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

- 使用命令**display igmp interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]查看接口上的IGMP配置和运行信息。

- 使用命令**display igmp group** [*group-address* | **interface** *interface-type interface-number*]* [**verbose**]查看动态加入的IGMP组播组成员信息。
- 使用命令**display igmp group** [*group-address*] **static** [**up** | **down**] [**verbose**]查看静态IGMP组播组的成员信息。

----结束

3.5 调整 IGMP 性能

IGMP使能后，缺省情况下可以正常工作。同时根据安全性和网络性能优化的要求，可以适当调整相关参数。

前置任务

3.4 配置IGMP基本功能

配置流程

以下任务没有顺序关系，可以根据需要选择执行下面的配置任务。

3.5.1 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。这样就会存在一个问题，如果协议报文的目的地址不为本设备的接口地址，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，当前交换机在收到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，也可以配置交换机丢弃未携带Router-Alert选项的IGMP报文。

交换机在发送IGMP报文时，也可以选择是否需要携带Router-Alert选项。缺省情况下，组播设备发送的IGMP报文中携带Router-Alert选项。

说明

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Router-Alert选项
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**igmp**，进入IGMP视图。

c. 执行命令**require-router-alert**，配置设备检查Router-Alert选项，即丢弃未包含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。

- 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**，配置设备丢弃未包含Router-Alert选项的IGMP报文。

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

----结束

3.5.2 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设备时，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，缺省情况下这些参数可以正常工作。同时根据需要，也可以通过命令行进行调整。

查询器参数	参数说明	缺省值	支持的版本
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，本参数定义了发送该报文的时间间隔	60s	IGMPv1、IGMPv2、IGMPv3

查询器参数	参数说明	缺省值	支持的版本
IGMP健壮系数	健壮系数用来规定以下两个值： ● 当IGMP查询器启动时发送“健壮系数”次的“普遍组查询报文”，发送时间间隔为“IGMP普遍组查询报文发送间隔”的1/4 ● 当组播设备收到Leave报文后，发送“健壮系数”次的“IGMP特定组查询报文”，发送间隔为“IGMP特定组查询报文发送间隔”	2	IGMPv1、IGMPv2、IGMPv3
IGMP查询报文的最大响应时间	组播组成员接收到一个IGMP查询报文后，会在最大响应时间内发送Report报文	10s	IGMPv2、IGMPv3
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	“其他IGMP查询器存活时间”＝“普遍组查询报文发送间隔”*“健壮系数”+“最大响应时间”*（1/2）。当等式右边的参数都取缺省值时，“其他IGMP查询器存活时间”的值为125s	IGMPv2、IGMPv3
IGMP特定组查询报文的发送间隔	当查询器收到主机退出某组播组的Leave报文时，会连续发送特定组查询报文，询问该组播组是否还存在成员。本参数定义了发送该报文的时间间隔	1s	IGMPv2、IGMPv3

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间隔”<“其他IGMP查询器存活时间”。

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**，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健壮系数。
  e. 执行命令**max-response-time** *interval*，配置IGMP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特定组查询报文的时间间隔。
- 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*，配置设备发送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健壮系数。
  e. 执行命令**igmp max-response-time** *interval*，配置IGMP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*，配置设备发送IGMP特定组查询报文的时间间隔。

----结束

3.5.3 配置 IGMP 快速离开

背景信息

在某些应用中，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Leave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版本。

说明

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

- 配置全局的IGMP快速离开
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**igmp**，进入IGMP视图。
  c. 执行命令**prompt-leave** [**group-policy** *acl-number*]，配置IGMP快速离开。

     缺省情况下，交换机在收到Leave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。
- 配置接口的IGMP快速离开
  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 prompt-leave** [**group-policy** *acl-number*]，配置接口快速离开功能。

----结束

3.5.4 配置 IGMP On-Demand

背景信息

IGMP On-Demand意为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。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Report和Leave报文来了解组播组成员信息，组成员收到查询时都会进行回应。为了减少这个过程中的报文交互，降低网络流量，可以在查询器上配置IGMP On-Demand功能。

交换机配置了IGMP On-Demand特性后：

- 接口不再发送IGMP查询报文。
- 收到Report报文后创建组表项，且表项永不超时。
- 在收到Leave报文后，会立即删除对应的组表项。

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，接口发送查询报文，参与查询器选举。

----结束

3.5.5 检查配置结果

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 group** [*group-address* | **interface** *interface-type interface-number*] * [**static**] [**verbose**]，查看IGMP组播组的成员信息。
- 执行命令**display igmp 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 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

3.6 配置 IGMP 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或IGMPv2。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。

前置任务

已完成**3.4.1 使能IGMP功能**。

背景信息

SSM Mapping通过给SSM组地址映射一个或多个源地址，将IGMPv1或IGMPv2的Report报文中（*，G）信息转换为一组（S，G）信息。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**4.5.2 （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**igmp**，进入IGMP视图。

步骤3 执行命令**ssm-mapping** *group-address* { *group-mask* | *group-mask-length* } *source-address*，配置组到源的映射。

步骤4 执行命令**quit**，返回系统视图。

步骤5 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤6 执行命令**igmp ssm-mapping enable**，使能SSM Mapping功能。

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，建议在交换机的接口上运行IGMPv3。

----结束

检查配置结果

配置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SSM Mapping是否使能。

- 使用命令**display igmp 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。
- 使用命令**display igmp ssm-mapping** { **group** [*group-address*] | **interface** [*interface-type interface-number*] }查看配置的映射关系、接口上SSM Mapping是否使能。

3.7 维护 IGMP

IGMP的维护包括：清除IGMP的组信息、监控IGMP运行状况。

3.7.1 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，使用命令**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* }]] } } 清除接口动态加入的组播组。
- 在接口视图下，使用命令**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。

----结束

3.7.2 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

- 使用命令**display igmp group** [*group-address* | **interface** *interface-type interface-number*] * [**static**] [**verbose**]查看IGMP组播组的成员信息。
- 使用命令**display igmp interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]查看接口上IGMP配置和运行信息。
- 使用命令**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*]]查看IGMP路由表信息。
- 使用命令**display igmp 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。
- 使用命令**display igmp ssm-mapping** { **group** [*group-address*] | **interface** [*interface-type interface-number*] }查看SSM Mapping中源和组的映射关系。
- 使用命令**display igmp control-message counters** [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]查看IGMP报文统计计数。

----结束

3.8 配置举例

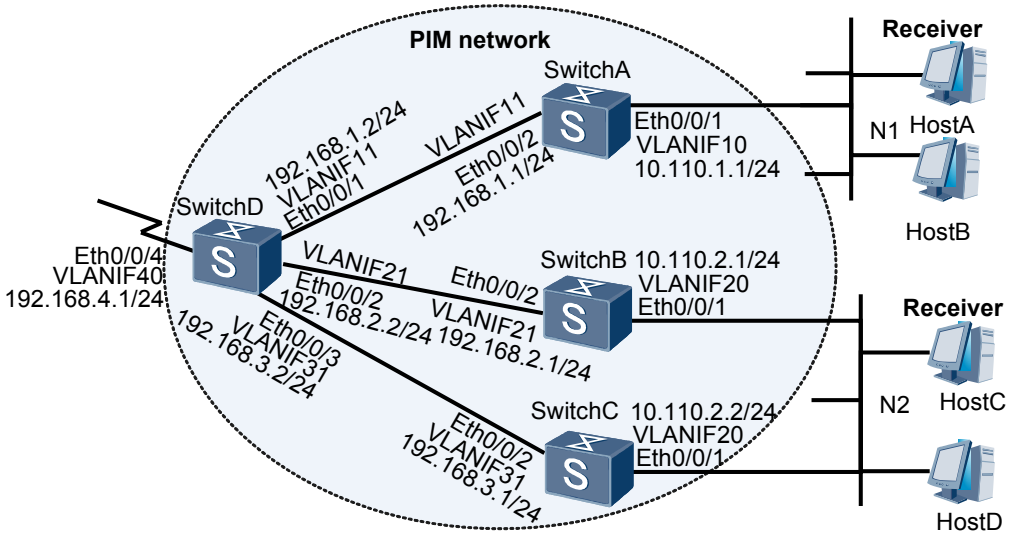
针对如何在组播网络中配置IGMP基本功能、静态加入组、IGMP SSM Mapping，分别提供配置举例。

3.8.1 配置 IGMP 基本功能示例

组网需求

如图3-2所示的网络中，接收者通过组播方式接收数据。在主机侧存在两个主机网段N1和N2，HostA和HostC分别为N1和N2中的接收者。网络中传播组播数据使用的组播组地址为225.1.1.1～225.1.1.5，接收者HostA只购买了组225.1.1.1对应的节目，HostC则没有限制。

图 3-2 配置 IGMP 的基本功能组网图



配置思路

配置IGMP的基本功能以及限制HostA所在接口加入的组播组范围，可以实现此需求。

1. 配置网络中的单播路由协议，实现网络层互通。为了实现这一步，需要在各Switch的接口配置IP地址和单播路由协议。单播路由正常是组播路由协议正常工作的基础。
2. 配置基本组播功能，实现组播数据可以在网络中转发。为了实现这一步，需要在各Switch上使能PIM-SM并配置RP，在Switch与接收者相连的接口上使能IGMP。
3. 配置对HostA能接收的组播数据进行限制。通过在连接HostA的SwitchA接口上配置ACL，可以实现对组播数据的过滤。

操作步骤

步骤1 配置各Switch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Switch之间采用OSPF进行互连，确保网络中各Switch间能够在网络层互通，并且能够借助单播路由协议实现动态路由更新。具体配置过程略。

步骤2 使能组播功能，并在所有接口上使能PIM-SM功能。

在SwitchA上使能组播功能，在所有接口上使能PIM-SM功能，配置SwitchD的VLANIF40为静态RP。SwitchB、SwitchC和SwitchD上的配置过程与此类似，配置过程略。

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] pim sm
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 11
[SwitchA-Vlanif11] pim sm
[SwitchA-Vlanif11] quit
[SwitchA] pim
```

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

步骤3 在SwitchA、SwitchB、SwitchC接收者侧接口上使能IGMP功能。

在SwitchA的VLANIF10接口上使能IGMP功能。SwitchB和SwitchC上的配置过程与此类似，配置过程略。

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] igmp enable
[SwitchA-Vlanif10] quit
```

步骤4 配置SwitchA的VLANIF10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SwitchA的VLANIF10接口上应用该策略。

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 225.1.1.1 0
[SwitchA-acl-basic-2001] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] igmp group-policy 2001
[SwitchA-Vlanif10] quit
```

步骤5 验证配置结果。

通过使用**display igmp interface**命令可以查看各接口上IGMP的配置和运行情况。例如SwitchA的VLANIF10接口上IGMP的显示信息如下：

```
<SwitchA> display igmp interface vlanif 10
Interface information
Vlanif 10(10.110.1.1):
  IGMP is enabled
  Current IGMP version is 2
  IGMP state: up
  IGMP group policy: 2001
  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
```

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10 11
#
multicast routing-enable
#
acl number 2001
 rule 5 permit source 225.1.1.1 0
#
interface Vlanif10
 ip address 10.110.1.1 255.255.255.0
 pim sm
 igmp enable
 igmp group-policy 2001
#
interface Vlanif11
```

```
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 11
 port hybrid untagged vlan 11
#
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
```

- SwitchB的配置文件

```
#
sysname SwitchB
#
vlan batch 20 21
#
multicast routing-enable
#
interface Vlanif20
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif21
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/2
 port hybrid pvid vlan 21
 port hybrid untagged vlan 21
#
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
```

- SwitchC的配置文件

```
#
sysname SwitchC
#
vlan batch 20 31
#
multicast routing-enable
#
interface Vlanif20
 ip address 10.110.2.2 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif31
```

```
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/2
 port hybrid pvid vlan 31
 port hybrid untagged vlan 31
#
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
```

- SwitchD的配置文件

```
#
sysname SwitchD
#
vlan batch 11 21 31 40
#
multicast routing-enable
#
interface Vlanif11
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlanif21
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface Vlanif31
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface Vlanif40
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 11
 port hybrid untagged vlan 11
#
interface Ethernet0/0/2
 port hybrid pvid vlan 21
 port hybrid untagged vlan 21
#
interface Ethernet0/0/3
 port hybrid pvid vlan 31
 port hybrid untagged vlan 31
#
interface Ethernet0/0/4
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
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
```

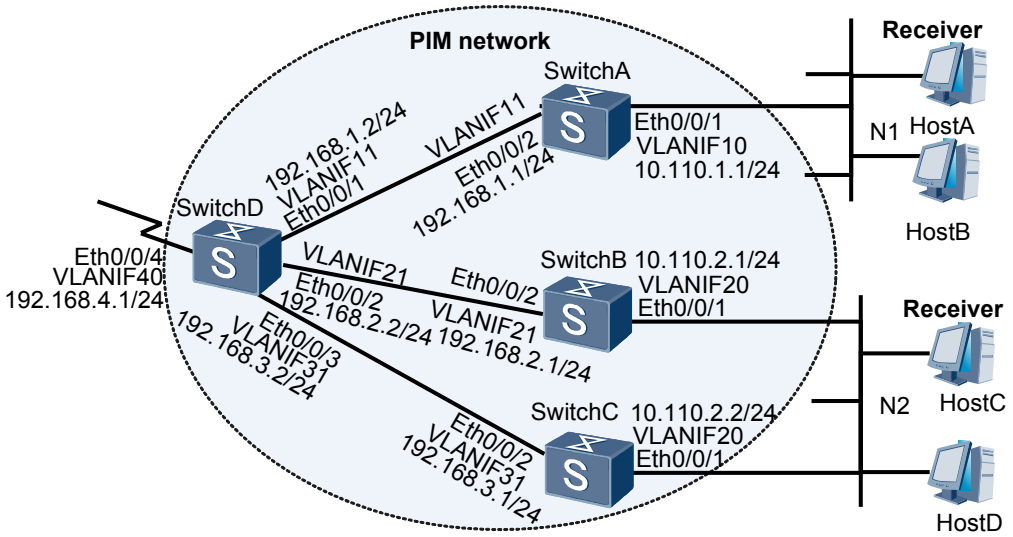
```
#
return
```

3.8.2 配置静态加入组播组示例

组网需求

如图3-3所示的网络中，接收者通过组播方式接收数据。在主机侧存在两个主机网段N1和N2，N1中有一个接收者HostA，N2中HostC和HostD都是接收者。HostA希望长期稳定地接收组播组225.1.1.3的数据，HostC和HostD对组播组没有这样的需求。

图 3-3 配置静态加入组播组组网图



配置思路

配置HostA所在接口静态加入组播组，可以实现此需求。

1. 配置网络中的单播路由协议，实现网络层互通。为了实现这一步，需要在各Switch的接口配置IP地址和单播路由协议。单播路由正常是组播路由协议正常工作的基础。
2. 配置基本组播功能，实现组播数据可以在网络中转发。为了实现这一步，需要在各Switch上使能PIM-SM并配置RP，在Switch与接收者相连的接口上使能IGMP。
3. 配置对HostA可以稳定接收225.1.1.3的数据。通过在连接HostA的SwitchA接口上配置静态加入组播组，可以实现此功能。

操作步骤

步骤1 配置各Switch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Switch之间采用OSPF进行互连，确保网络中各Switch间能够在网络层互通，并且能够借助单播路由协议实现动态路由更新。具体配置过程略。

步骤2 使能组播功能，并在所有接口上使能PIM-SM功能。

在SwitchA上使能组播功能，在所有接口上使能PIM-SM功能，配置SwitchD的VLANIF40为静态RP。SwitchB、SwitchC和SwitchD上的配置过程与此相似，配置过程略。

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] pim sm
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 11
[SwitchA-Vlanif11] pim sm
[SwitchA-Vlanif11] quit
[SwitchA] pim
[SwitchA-pim] static-rp 192.168.4.1
[SwitchA-pim] quit
```

步骤3 配置SwitchA、SwitchB和SwitchC的接收者侧接口使能IGMP。

配置SwitchA的VLANIF10接口使能IGMP，SwitchB和SwitchC的配置与此类似，配置过程略。

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] igmp enable
[SwitchA-Vlanif10] quit
```

步骤4 配置SwitchA的VLANIF10接口静态加入组播组225.1.1.3。

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] igmp static-group 225.1.1.3
[SwitchA-Vlanif10] quit
```

步骤5 验证配置结果。

通过使用**display igmp group static**命令可以查看接口上静态加入的组播组。

```
<SwitchA> display igmp group static
Static join group information
 Total 1 entry
  Group Address   Source Address  Interface            State     Expires
  225.1.1.3       0.0.0.0         Vlanif10             UP        never
```

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10 11
#
multicast routing-enable
#
interface Vlanif10
 ip address 10.110.1.1 255.255.255.0
 pim sm
 igmp enable
 igmp static-group 225.1.1.3
#
interface Vlanif11
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
```

```
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 11
 port hybrid untagged vlan 11
#
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
```

- SwitchB的配置文件

```
#
sysname SwitchB
#
vlan batch 20 21
#
multicast routing-enable
#
interface Vlanif20
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif21
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/2
 port hybrid pvid vlan 21
 port hybrid untagged vlan 21
#
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
```

- SwitchC的配置文件

```
#
sysname SwitchC
#
vlan batch 20 31
#
multicast routing-enable
#
interface Vlanif20
 ip address 10.110.2.2 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif31
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
```

```
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/2
 port hybrid pvid vlan 31
 port hybrid untagged vlan 31
#
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
```

- SwitchD的配置文件

```
#
sysname SwitchD
#
vlan batch 11 21 31 40
#
multicast routing-enable
#
interface Vlanif11
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlanif21
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface Vlanif31
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface Vlanif40
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 11
 port hybrid untagged vlan 11
#
interface Ethernet0/0/2
 port hybrid pvid vlan 21
 port hybrid untagged vlan 21
#
interface Ethernet0/0/3
 port hybrid pvid vlan 31
 port hybrid untagged vlan 31
#
interface Ethernet0/0/4
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
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
```

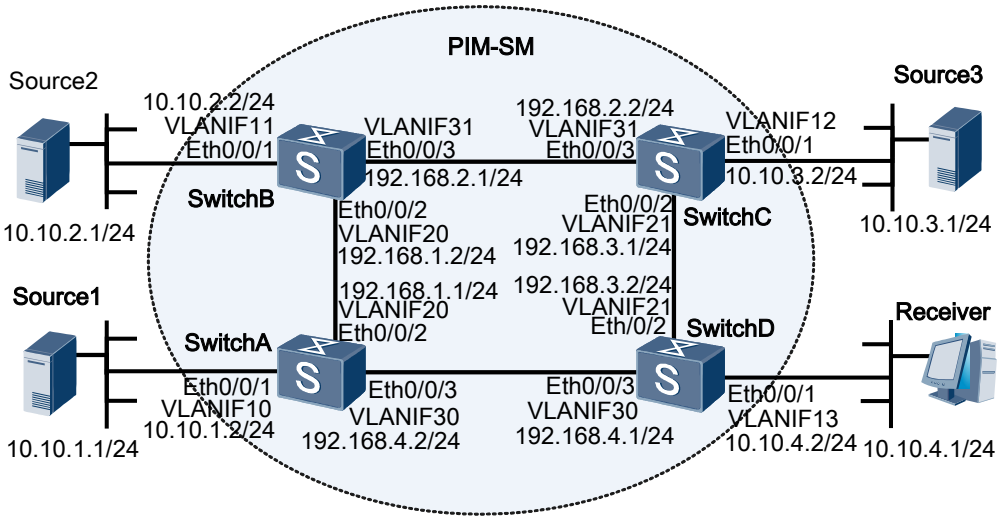
3.8.3 配置 IGMP SSM Mapping 示例

组网需求

已知如图3-4所示的组播网络中，运行PIM-SM协议，同时采用ASM和SSM模式提供组播服务。与主机Receiver相连的Switch接口上运行IGMPv3，Receiver上的IGMP的版本为v2，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。而Receiver只想接收来自Source1和Source3的组播数据。

图 3-4 配置 SSM Mapping 功能组网图



配置思路

配置组播基本功能后，在SwitchD上配置SSM Mapping功能，可以实现此需求。

1. 配置网络中的单播路由协议，实现网络层互通。为了实现这一步，需要在各Switch的接口配置IP地址和单播路由协议。单播路由正常是组播路由协议正常工作的基础。
2. 配置基本组播功能，实现组播数据可以在网络中转发。为了实现这一步，需要在各Switch上使能PIM-SM并配置RP，在Switch与接收者相连的接口上使能IGMP。
3. 配置SSM Mapping功能，使Receiver可以对组播源进行选择。为了实现这一步，需要在连接主机的SwitchD接口上使能SSM Mapping功能并配置Mapping规则。

操作步骤

步骤1 配置IP地址和单播路由协议。

按照图3-4配置各接口的IP地址和掩码，并配置各Switch之间采用OSPF进行互连，确保网络中各Switch间能够在网络层互通，并且能够借助单播路由协议实现动态路由更新。具体配置过程略。

步骤2 使能IP组播路由，并配置PIM-SM和IGMP。

在SwitchD上使能IP组播路由，在各接口上使能PIM-SM，在主机侧接口VLANIF13上使能IGMP，配置版本为IGMPv3。

```
[SwitchD] multicast routing-enable
[SwitchD] interface vlanif 13
[SwitchD-Vlanif13] pim sm
[SwitchD-Vlanif13] igmp enable
[SwitchD-Vlanif13] igmp version 3
[SwitchD-Vlanif13] quit
[SwitchD] interface vlanif 21
[SwitchD-Vlanif21] pim sm
[SwitchD-Vlanif21] quit
[SwitchD] interface vlanif 30
[SwitchD-Vlanif30] pim sm
[SwitchD-Vlanif30] quit
```

在SwitchA上使能IP组播路由，并在各接口上使能PIM-SM。SwitchB和SwitchC的配置与SwitchA类似，配置过程略。

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] pim sm
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] pim sm
[SwitchA-Vlanif20] quit
[SwitchA] interface vlanif 30
[SwitchA-Vlanif30] pim sm
[SwitchA-Vlanif30] quit
```

将SwitchD的VLANIF30配置为静态RP。SwitchB、SwitchC和SwitchD的配置与SwitchA类似，配置过程略。

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

步骤3 使能主机侧接口的SSM Mapping功能。

在SwitchD的VLANIF13上使能SSM Mapping功能。

```
[SwitchD] interface vlanif 13
[SwitchD-Vlanif13] igmp ssm-mapping enable
[SwitchD-Vlanif13] quit
```

步骤4 在所有Switch上配置SSM组播组地址范围。

在SwitchA上配置SSM组播组地址范围为232.1.1.0/24。SwitchB、SwitchC和SwitchD上的配置过程与SwitchA上的配置类似，配置过程略。

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

步骤5 在连接主机的Switch上配置SSM Mapping映射规则。

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

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

步骤6 验证配置结果。

查看Switch上源和组的映射关系。

```
<SwitchD> display igmp ssm-mapping group
IGMP SSM-Mapping conversion table
 Total 2 entries    2 entries matched

 00001. (10.10.1.1, 232.1.1.0)

 00002. (10.10.3.1, 232.1.1.0)

 Total 2 entries matched
```

Receiver加入组232.1.1.1。

通过使用**display igmp group ssm-mapping**命令，可以查看Switch特定源组地址的信息。SwitchD上特定源/组地址信息显示如下：

```
<SwitchD> display igmp group ssm-mapping
IGMP SSM mapping interface group report information

  Vlanif13 (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

<SwitchD> display igmp group ssm-mapping verbose
Interface group report information
  Vlanif13 (10.10.4.2):
  Total entry on this interface: 1
    Total 1 IGMP SSM-Mapping Group reported
   Group: 232.1.1.1
     Uptime: 00:01:52
     Expires: 00:00:18
     Last reporter: 10.10.4.1
     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: 00:01:55
```

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

```
<SwitchD> 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: Vlanif30
         Upstream neighbor: 192.168.4.2
         RPF prime neighbor: 192.168.4.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif13
             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: Vlanif21
         Upstream neighbor: 192.168.3.1
         RPF prime neighbor: 192.168.3.1
     Downstream interface(s) information:
     Total number of downstreams: 1
```

```
    1: Vlanif13
        Protocol: ssm-map, UpTime: 00:19:40, Expires: -
```

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10 20 30
#
multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif10
 ip address 10.10.1.2 255.255.255.0
 pim sm
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Vlanif30
 ip address 192.168.4.2 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
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
 static-rp 192.168.4.2
 ssm-policy 2000
#
return
```

- SwitchB的配置文件

```
#
sysname SwitchB
#
vlan batch 11 20 31
#
multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif11
 ip address 10.10.2.2 255.255.255.0
 pim sm
```

```
#
interface Vlanif20
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlanif31
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 11
 port hybrid untagged vlan 11
#
interface Ethernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/3
 port hybrid pvid vlan 31
 port hybrid untagged vlan 31
#
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
 static-rp 192.168.4.2
 ssm-policy 2000
#
return
```

- SwitchC的配置文件

```
#
 sysname SwitchC
#
vlan batch 12 21 31
#
multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif12
 ip address 10.10.3.2 255.255.255.0
 pim sm
#
interface Vlanif21
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Vlanif31
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 12
 port hybrid untagged vlan 12
#
interface Ethernet0/0/2
 port hybrid pvid vlan 21
 port hybrid untagged vlan 21
#
interface Ethernet0/0/3
 port hybrid pvid vlan 31
 port hybrid untagged vlan 31
#
ospf 1
 area 0.0.0.0
```

```
  network 10.10.3.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
pim
 static-rp 192.168.4.2
 ssm-policy 2000
#
return
```

- SwitchD的配置文件

```
#
sysname SwitchD
#
vlan batch 13 21 30
#
multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif13
 ip address 10.10.4.2 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
 igmp ssm-mapping enable
#
interface Vlaniaf21
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface Vlanif30
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 13
 port hybrid untagged vlan 13
#
interface Ethernet0/0/2
 port hybrid pvid vlan 21
 port hybrid untagged vlan 21
#
interface Ethernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
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
 static-rp 192.168.4.2
 ssm-policy 2000
#
return
```

3.9 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。

3.9.1 IGMP 表项无法正常建立

故障现象

IGMP配置完成后，有主机点播组播组G的数据，离该主机最近的组播设备上却没有生成IGMP组表项。

操作步骤

步骤1 检查用户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 Report报文，设备不会处理，因此也不会生成IGMP Group表项。

步骤2 执行**display interface** *interface-type interface-number*命令，指定设备上与主机网段直连的接口，查看接口状态是否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**命令使能组播路由。

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 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。需要修改该ACL规则，允许设备接收该组播组的Report报文。

----结束

3.9.2 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 Report报文，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）Report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**ssm-policy** *basic-acl-number*，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232.0.0.0/8。

----结束

4 PIM-SM（IPv4）配置

关于本章

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

注意事项

端口作为VPLS AC侧的接入端口时，如果该端口同时还作为组播流入接口，会导致对应组播数据无法正常转发。

4.1 PIM-SM（IPv4）概述
介绍PIM-SM的适用范围及基本原理。

4.2 设备支持的PIM-SM（IPv4）特性
设备支持的PIM-SM特性有：PIM-SM for ASM、PIM-SM for SSM、PIM BFD。

4.3 缺省配置
介绍缺省情况下，PIM-SM的配置信息。

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

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

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

4.7 调整邻居控制参数
PIM设备之间通过交互Hello报文建立邻居关系。

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

4.9 调整加入和剪枝控制参数

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

4.10 调整断言控制参数

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

4.11 配置PIM BFD

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

4.12 维护PIM-SM

PIM-SM的维护包括：清除PIM控制报文统计信息、监控PIM的运行状况。

4.13 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。

4.14 常见配置错误

介绍常见配置错误及定位思路。

4.1 PIM-SM（IPv4）概述

介绍PIM-SM的适用范围及基本原理。

PIM-SM（Protocol Independent Multicast-Sparse Mode）称为协议无关组播－稀疏模式，属于稀疏模式的域内组播路由协议。PIM-SM不会将组播数据扩散到全网，而只将组播数据传输到有组成员的网络，所以一般用于规模较大、组成员分布稀疏的组播网络。

PIM-SM对于ASM模型和SSM模型都适用。

PIM-SM for ASM

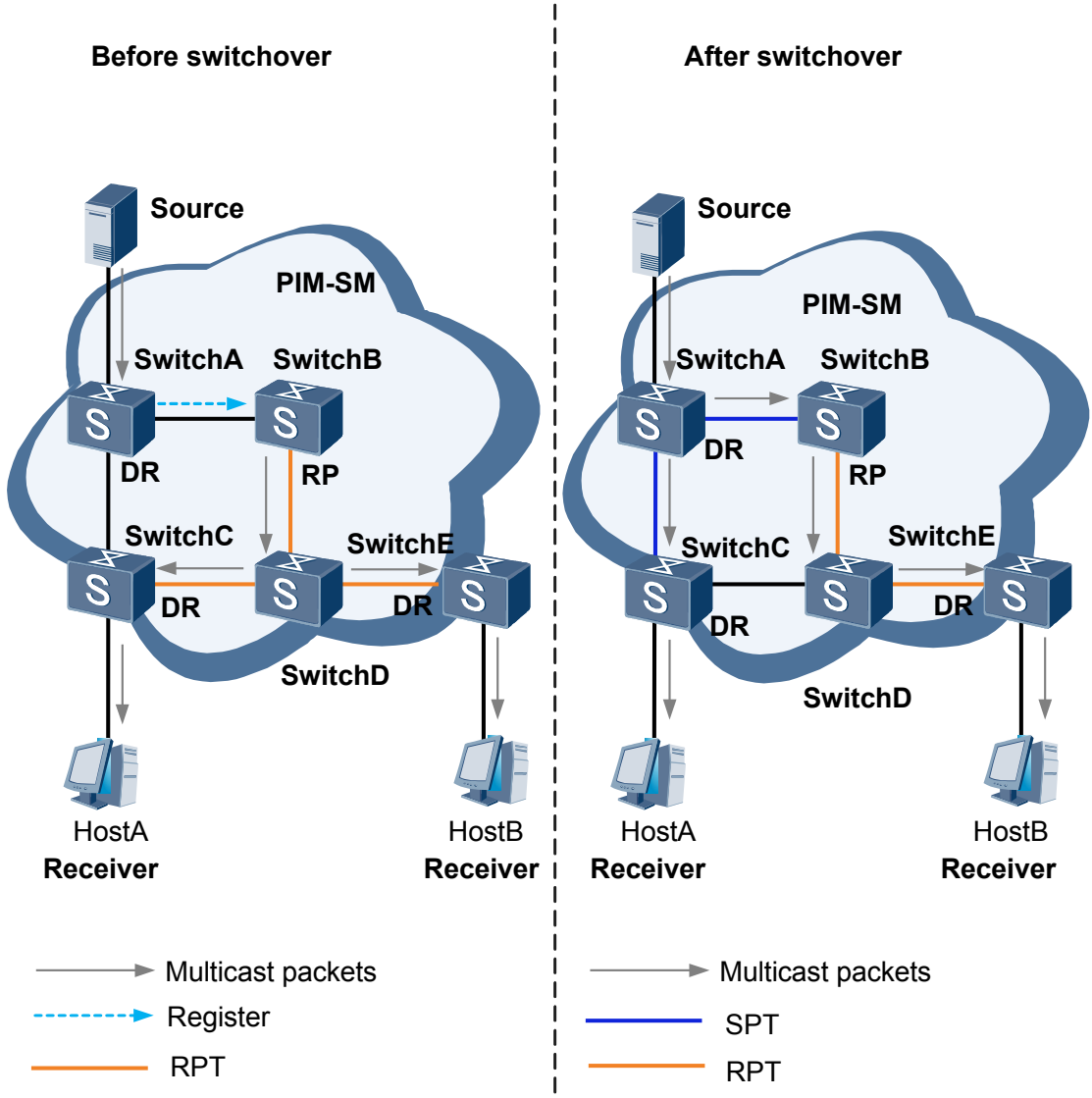
在ASM模型中，RP（Rendezvous Point）是网络的转发核心，网络中所有PIM路由器都知道RP的位置。当网络中出现组成员时，最后一跳路由器向RP方向发送Join信息，逐跳创建（*，G）表项，生成一棵以RP为根的RPT（RP Tree）；当网络中出现活跃的组播源时，第一跳路由器将组播信息封装在Register报文中发往RP，在RP上创建（S，G）表项，注册源信息。然后，RP会将注册信息中的组播信息解封装，沿着RPT转发到有组成员的网段。

如果当前RP负担较重，可通过SPT（Shortest Path Tree）切换减轻压力：

- RP向组播源方向发送Join信息，构建“源-RP”的SPT。
- 组成员端DR向组播源方向发送Join信息，构建“源-组成员”的SPT。

如图4-1所示，SwitchB、SwitchC都向源方向进行了SPT切换。

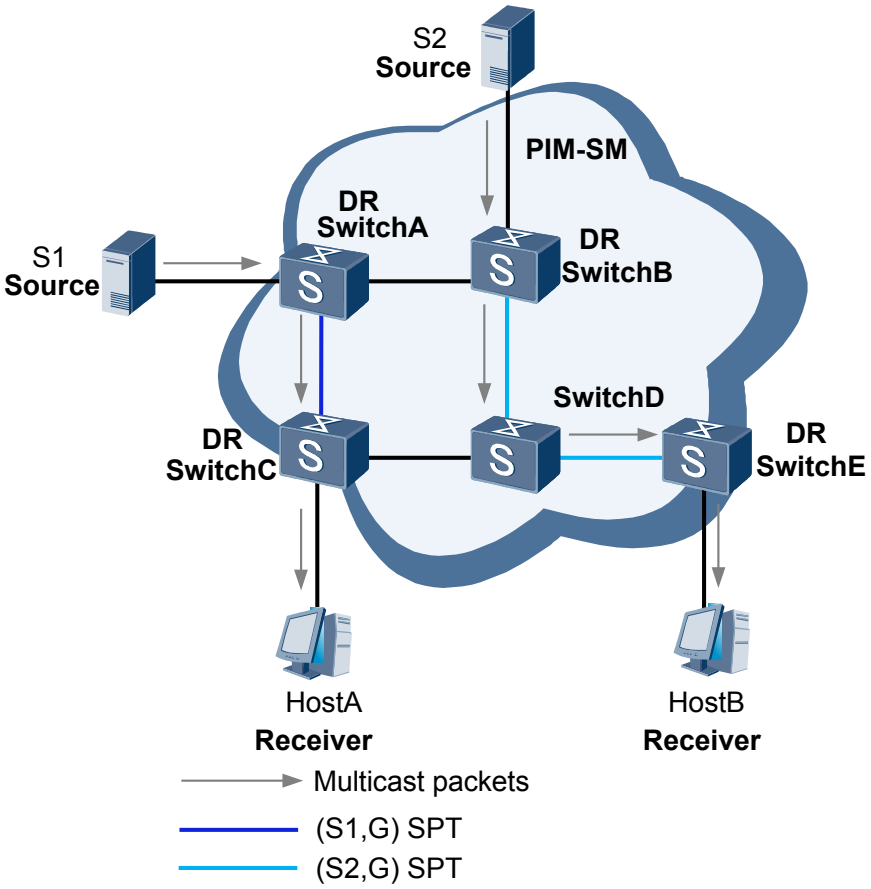
图 4-1 ASM 模型 SPT 切换前后对比示意图



PIM-SM for SSM

在SSM模型中，网络用户能够预先知道组播源的具体位置。因此用户在加入组播组时，可以明确指定从哪些源接收信息。组成员端DR了解到用户的需求后，直接向组播源方向发送Join信息。Join信息逐跳向上传输，在源与组成员之间建立SPT。它只是借助PIM-SM的部分技术和IGMPv3来实现，无需维护RP、无需构建RPT、无需注册组播源。如图4-2所示，HostA、HostB都已经加入了组播组G，HostA需要接收S1的组播数据，HostB需要接收S2的组播数据，组成员端DR分别向各自源方向发送Join信息，构建SPT。

图 4-2 SSM 模型中 SPT 构建示意图



4.2 设备支持的 PIM-SM（IPv4）特性

设备支持的PIM-SM特性有：PIM-SM for ASM、PIM-SM for SSM、PIM BFD。

说明

S2700&S3700支持PIM-SM的接口为VLANIF接口、Loopback接口。在本章配置中，如无特殊说明，接口的配置一般选择VLANIF接口。使用VLANIF接口前需要先将物理接口加入该VLAN。

在PIM（IPv4）协议报文默认的CPCAR值下，设备最多能够同时处理大约190个组播用户的点播需求。

PIM-SM for ASM

ASM模型中，设备使能PIM-SM并配置RP后即可以提供ASM服务。RP可以静态指定也可以通过BSR（BootStrap Router）机制选举。此外，为了实现更好的管理，设备还提供以下功能：

- BSR管理域：将PIM域划分为多个BSR管理域和一个Global域，便于更有效的管理。
- SPT切换条件的配置：SPT切换用于减轻RP的压力，可以通过设置组播速率阈值来触发SPT切换或者不发起SPT切换。

- 源注册控制参数的调整：源端DR收到组播源发送的数据后，将其封装在注册报文中转发给RP。可以在RP或源端DR上对注册报文的时间参数、地址范围等进行调整。
- 动态RP的参数调整：调整C-RP、C-BSR的参数，可以控制RP和BSR的选举以及服务范围。

PIM-SM for SSM

SSM模型中，设备支持通过配置SSM组策略来指定SSM组地址范围。

调整 PIM-SM 控制参数

在配置ASM或SSM的PIM-SM基本功能后，通过设备提供的缺省值，PIM-SM域就可以正常工作，将组播源发出的组播数据分发到组成员网段。根据实际需要，设备也支持调整如表4-1所示的PIM-SM控制参数。

表 4-1 PIM-SM 控制参数

参数	说明
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。
邻居控制参数	设备间通过交互Hello报文建立PIM邻居关系，协商各类控制参数，所以可以基于Hello报文来控制邻居间的关系。
DR竞选控制参数	无论是与组播源相连的网络，还是与组成员相连的网络，都需要选举DR，由DR负责转发组播源或组成员发来的组播报文。可以根据实际需要调整设备上DR的优先级。
加入和剪枝控制参数	设备向上游发送Join信息请求转发组播数据，发送Prune信息请求停止转发组播数据。可根据实际需要调整加入或剪枝过程的控制参数，达到控制组播报文转发的目的。
断言控制参数	当设备从下游接口接收到组播数据时，说明该网段中还存在其他的上游设备。设备从该接口发出Assert报文，参与竞选唯一上游的转发者。可根据实际需要调整发送断言的间隔，来控制断言竞选的周期。

PIM BFD

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

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

4.3 缺省配置

介绍缺省情况下，PIM-SM的配置信息。

表4-2列出了PIM-SM（IPv4）的缺省配置。

表 4-2 PIM-SM（IPv4）的缺省配置

参数	缺省值
组播路由功能	未使能
PIM-SM	未使能
静态RP地址	未配置
C-RP接口	未指定
C-BSR接口	未指定
DR优先级	1
SPT切换条件	RP或组成员端DR接收到第一个组播数据报文时就进行SPT切换
SSM组地址范围	232.0.0.0/8
PIM BFD	未使能

4.4 配置 ASM 模型的 PIM-SM

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

前置任务

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

配置流程

配置ASM模型的PIM-SM必选步骤如下：

1. 使能PIM-SM
2. 配置RP

配置SPT切换条件、调整源注册控制参数为可选步骤，可根据实际需要进行选配。

4.4.1 使能 PIM-SM

背景信息

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

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

操作步骤

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**，使能组播路由功能。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 执行命令**pim sm**，使能PIM-SM功能。

----结束

4.4.2 配置 RP

背景信息

配置RP有手工静态配置和BSR机制动态选举两种方式。手工方式静态配置RP，可以避免C-RP与BSR之间频繁的信息交互而占用带宽。通过BSR机制动态选举RP，可以避免手工配置的繁琐；同时配置了多台C-RP也可以保证组播数据转发的可靠性。

注意

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

缺省配置

表4-3列出了C-BSR、C-RP部分参数的缺省配置。

表 4-3 C-BSR、C-RP 部分参数的缺省配置

参数	缺省值
C-BSR优先级	0
C-BSR携带的哈希掩码长度	30
BSR报文分片功能	未使能
静态RP组播组策略	没有组播组策略，即允许接收任意组地址的组播报文
C-RP组播组策略	没有组播组策略，即允许接收任意组地址的组播报文
C-RP优先级	0

参数	缺省值
C-RP的宣告报文发送间隔	60s
C-RP的宣告报文保持时间	150s

操作步骤

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

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

     说明

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

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

     说明

     使能BSR报文分片功能后，可以解决IP分片时分片信息丢失而导致所有分片不可用的问题。但是必须要保证所有设备都要使能，否则会导致未使能的设备接收到的RP信息不完整。
  b. 配置C-RP
     i. 执行命令**system-view**，进入系统视图。
     ii. 执行命令**pim**，进入PIM视图。
     iii. 执行命令**c-rp** *interface-type interface-number* [**group-policy** *basic-acl-number* | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] *，指定C-RP所在接口。

     建议在组播数据流量汇聚的设备上配置C-RP。
  c. （可选）配置BSR边界
     i. 执行命令**system-view**，进入系统视图。
     ii. 执行命令**interface** *interface-type interface-number*，进入接口视图。
     iii. 执行命令**pim bsr-boundary**，配置BSR服务边界。

说明

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

建议在规划的PIM-SM域的边缘接口配置BSR服务边界。

----结束

4.4.3 （可选）配置 BSR 管理域

背景信息

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

说明

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

操作步骤

步骤1 在PIM域内所有设备上使能BSR管理域功能

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

步骤2 在每个BSR管理域的边缘接口上配置边界

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

   说明

   限定了组地址范围后，该范围内的组播报文将无法通过此接口进行转发。

步骤3 在每个BSR管理域的C-BSR上配置服务的组地址范围

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

步骤4 配置Global域的C-BSR

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

----结束

4.4.4 （可选）配置 RPT 不向 SPT 切换

背景信息

缺省情况下，组成员端DR在接收到第一份组播数据报文后都会向源方向发起SPT切换。如果不希望组成员端DR发起SPT切换，一直用RPT传输组播数据，可配置此功能。

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**pim**，进入PIM视图。

步骤3 执行命令**spt-switch-threshold infinity**，在组成员端DR上配置不发起SPT切换。

----结束

4.4.5 （可选）调整注册控制参数

背景信息

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

在源端DR上可进行如下调整：

- 配置注册Register抑制时间。源端DR在收到RP发来的注册停止Register-stop报文后，在注册抑制时间内，会停止向RP发送注册报文。超时后，如果源端DR没有收到后续的注册停止报文，则恢复相应注册报文的转发。
- 配置发送空注册报文时间间隔。如果注册抑制时间过大或过小，都会影响组播数据的正常转发。通过在抑制期间发空注册报文，可以改善这种影响。
- 配置仅根据注册报文头来计算校验和，可减少计算校验和的时间，提高注册报文封装组播数据的效率。

在RP上可进行如下调整：

- 配置过滤注册报文的规则，可限定注册报文的地址范围，提高网络安全性。

缺省配置

表4-4列出了注册控制参数的缺省配置。

表 4-4 注册控制参数的缺省配置

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

参数	缺省值
发送空注册报文时间间隔	5s

操作步骤

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

     说明

     probe-interval的值必须小于**register-suppression-timeout**值的二分之一。
  e. 执行命令**register-header-checksum**，配置根据注册报文头信息计算校验和，未通过校验的Register注册报文将被丢弃。
- 在RP上配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim**，进入PIM视图。
  c. 执行命令**register-policy** *advanced-acl-number*，配置过滤注册报文的规则。

     说明

     在定义ACL的**rule**时，通过**permit**参数配置设备仅接收指定地址范围的注册报文。如果ACL未定义**rule**，则设备默认过滤掉所有的注册报文。

----结束

4.4.6 （可选）调整 C-RP 控制参数

背景信息

在接口上配置了C-RP后，C-RP会周期性地向BSR发送Advertisement报文（以下称宣告报文），报文携带C-RP优先级、宣告报文的保持时间。BSR在收到该报文后，启动C-RP超时定时器，时间设为宣告报文的保持时间。在超时前，BSR将宣告报文中携带的C-RP信息汇总成RP-Set信息，封装在自举报文中向PIM域中的所有PIM设备发送。超时后，如果BSR没有收到来自C-RP后续的宣告报文，则认为目前网络中的C-RP失效或不可达。所以C-RP发送宣告报文时间间隔必须要小于宣告报文的保持时间。

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

说明

有关宣告报文携带的参数的缺省值，可参见**4.4.2 配置RP**。

操作步骤

- 在C-RP上配置宣告报文携带的参数。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim**，进入PIM视图。
  c. 执行命令**c-rp priority** *priority*，配置C-RP优先级。
  d. 执行命令**c-rp advertisement-interval** *interval*，配置C-RP发送宣告报文的间隔时间。
  e. 执行命令**c-rp holdtime** *interval*，配置保持来自C-RP的宣告报文的时间。
- 在BSR上限定合法的C-RP地址范围。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim**，进入PIM视图。
  c. 执行命令**crp-policy** *advanced-acl-number*，限定合法的C-RP地址范围及其服务的组播组地址范围。

  说明

  在定义ACL的**rule**时，通过**permit**参数配置设备仅接收指定地址范围的宣告报文。如果ACL未定义**rule**，则设备默认过滤掉所有的宣告报文。

----结束

4.4.7 （可选）调整 C-BSR 控制参数

背景信息

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

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

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

缺省配置

表4-5列出了C-BSR部分参数的缺省配置。

表 4-5 C-BSR 部分参数的缺省配置

参数	缺省值
发送自举报文的时间间隔	60s

参数	缺省值
自举报文的保持时间	130s

说明

有关C-BSR其他参数的缺省值，可参见**4.4.2 配置RP**。

操作步骤

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

  说明

  在定义ACL的**rule**时，通过**permit**参数配置设备仅接收指定地址范围的自举报文。如果ACL未定义**rule**，则设备默认过滤掉所有地址范围的自举报文。

----结束

4.4.8 检查配置结果

前提条件

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

操作步骤

- 使用命令**display pim bsr-info**，查看BSR的信息。
- 使用命令**display pim rp-info** [*group-address*]，查看RP信息。
- 使用命令**display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]，查看接口上的PIM信息。
- 使用命令**display pim neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *，查看PIM邻居信息。
- 使用命令**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 { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]，查看PIM路由表。

----结束

4.5 配置 SSM 模型的 PIM-SM

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

前置任务

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

配置流程

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

4.5.1 使能 PIM-SM

背景信息

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

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

操作步骤

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**，使能组播路由功能。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 执行命令**pim sm**，使能PIM-SM功能。

----结束

4.5.2 （可选）配置 SSM 组策略

背景信息

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

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pim**，进入PIM视图。

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

说明

确保网络内所有PIM设备上配置的SSM组地址范围都一致。

----结束

4.5.3 检查配置结果

前提条件

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

操作步骤

- 使用命令**display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]查看接口上的PIM信息。
- 使用命令**display pim neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *查看PIM邻居信息。
- 使用命令**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** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]，查看PIM路由表。

----结束

4.6 调整组播源控制参数

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

前置任务

在调整组播源控制参数之前，需完成以下任务：

- 配置单播路由协议，保证网络内单播路由畅通。
- 使能PIM-SM。

背景信息

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

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

缺省配置

表4-6列出了组播源控制参数的缺省配置。

表 4-6 组播源控制参数的缺省配置

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

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pim**，进入PIM视图。

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

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

- 如果配置的是基本ACL，通过与**rule**中的**source**参数配合，只转发源地址属于过滤规则允许范围的组播报文。
- 如果配置的是高级ACL，通过与**rule**中的**source**和**destination**参数配合，只转发源地址和组地址都属于过滤规则允许范围内的组播报文。

说明

- 执行此命令后，如果指定ACL没有配置过滤规则，则不转发任何源地址发送的组播报文。
- 如果当前PIM表项是通过学习静态配置指定（S，G）的IGMP组信息而生成的，执行此命令后，不过滤对应PIM表项的组播报文。

----结束

检查配置结果

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

使用命令**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** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]，查看PIM路由表。

4.7 调整邻居控制参数

PIM设备之间通过交互Hello报文建立邻居关系。

前置任务

在调整邻居控制参数之前，需完成以下任务：

- 配置单播路由协议，保证网络内单播路由畅通。

- 使能PIM-SM。

背景信息

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

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

有时候为了保证设备相连的都是正常工作的PIM邻居，可配置拒绝接收无Generation ID的Hello报文。

说明

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

触发Hello报文的最大延迟时间、拒绝接收无Generation ID的Hello报文只能在接口上配置。

缺省配置

表4-7列出了邻居控制参数的缺省配置。

表 4-7 邻居控制参数的缺省配置

参数	缺省值
发送Hello报文的时间间隔	30s
Hello报文的保持时间	105s
触发Hello报文的最大延迟时间	5s
对无Generation ID的Hello报文的处理方式	接收

操作步骤

- 全局配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pim**，进入PIM视图。
  c. 执行命令**timer hello** *interval*，配置发送Hello报文的时间间隔。
  d. 执行命令**hello-option holdtime** *interval*，配置Hello报文的保持时间。
- 接口配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

c. 执行命令**pim timer hello** *interval*，配置发送Hello报文的时间间隔。

d. 执行命令**pim hello-option holdtime** *interval*，配置Hello报文的保持时间。

e. 执行命令**pim triggered-hello-delay** *interval*，配置触发Hello报文的最大延迟。

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

----结束

后续处理

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。

- 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。

4.8 调整 DR 竞选控制参数

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

前置任务

在调整DR竞选控制参数之前，需完成以下任务：

- 配置单播路由协议，保证网络内单播路由畅通。
- 使能PIM-SM。

背景信息

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

说明

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

缺省配置

表4-8列出了DR优先级的缺省配置。

表 4-8 DR 优先级的缺省配置

参数	缺省值
DR优先级	1

操作步骤

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

----结束

后续处理

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

- 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。

4.9 调整加入和剪枝控制参数

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

前置任务

在调整加入和剪枝控制参数之前，需完成以下任务：

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

配置流程

Join-Prune报文的时间控制参数、剪枝延迟时间配置时并无先后顺序，用户可根据实际需要进行调整。

4.9.1 调整 Join-Prune 报文的时间控制参数

背景信息

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

- 若未收到的Join-Prune报文携带有加入某组播组信息，则抑制相应组播组下游接口的转发；

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

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

说明

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

缺省配置

表4-9列出了Join-Prune报文时间参数的缺省配置。

表 4-9 Join-Prune 报文时间参数的缺省配置

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

操作步骤

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

----结束

4.9.2 调整剪枝延迟时间

背景信息

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

说明

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

缺省配置

表4-10列出了剪枝延迟时间参数的缺省配置。

表 4-10 剪枝延迟时间参数的缺省配置

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

操作步骤

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

----结束

4.9.3 检查配置结果

前提条件

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

操作步骤

- 使用命令**display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]，查看接口上的PIM信息。
- 使用以下命令查看PIM发送和接收的PIM控制报文的数目信息：
  - **display pim control-message counters message-type** { **probe** | **register** | **register-stop** }

- **display pim control-message counters** [**message-type** { **assert** | **hello** | **join-prune** } | **interface** *interface-type interface-number*] *

- 使用命令**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** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]，查看PIM路由表。

----结束

4.10 调整断言控制参数

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

前置任务

在调整断言控制参数之前，需完成以下任务：

- 配置单播路由协议，保证网络内单播路由畅通。
- 使能PIM-SM。

背景信息

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

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

说明

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

缺省配置

表4-11列出了断言参数的缺省配置。

表 4-11 断言参数的缺省配置

参数	缺省值
保持Assert状态的时间	180s

操作步骤

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

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

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

----结束

检查配置结果

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

- 使用命令**display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]查看接口上的PIM信息。
- 使用命令**display pim neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *查看PIM邻居信息。
- 使用命令**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** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]，查看PIM路由表。

4.11 配置 PIM BFD

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

前置任务

在配置PIM-BFD之前，需完成以下任务：

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

背景信息

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

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

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

缺省配置

表4-12列出了PIM BFD检测报文控制参数的缺省配置。

表 4-12 PIM BFD 检测报文控制参数的缺省配置

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

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

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

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

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

----结束

检查配置结果

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

- **display pim bfd session statistics**
- **display pim bfd session** [**interface** *interface-type interface-number* | **neighbor** *neighbor-address*] *

4.12 维护 PIM-SM

PIM-SM的维护包括：清除PIM控制报文统计信息、监控PIM的运行状况。

4.12.1 清除 PIM 控制报文统计信息

背景信息

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

注意

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

操作步骤

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

----结束

4.12.2 监控 PIM 的运行状况

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解PIM的运行状况。

操作步骤

- 使用命令**display pim claimed-route** [*source-address*]，查看PIM使用的单播路由信息。
- 使用命令**display pim bfd session** [**interface** *interface-type interface-number* | **neighbor** *neighbor-address*] *，查看PIM BFD session的信息。
- 使用命令**display pim bsr-info**，查看PIM-SM域中BSR的信息。
- 使用以下命令，查看发送和接收PIM控制报文的数目信息。
  - **display pim control-message counters message-type** { **probe** | **register** | **register-stop** }
  - **display pim control-message counters** [**message-type** { **assert** | **hello** | **join-prune** | **bsr** } | **interface** *interface-type interface-number*] *
- 使用命令**display pim interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]，查看接口上的PIM信息。
- 使用命令**display pim neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *，查看PIM邻居信息。
- 使用命令**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** { **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]，查看PIM路由表。
- 使用命令**display pim rp-info** [*group-address*]命令，查看组播组对应的RP信息。

----结束

4.13 配置举例

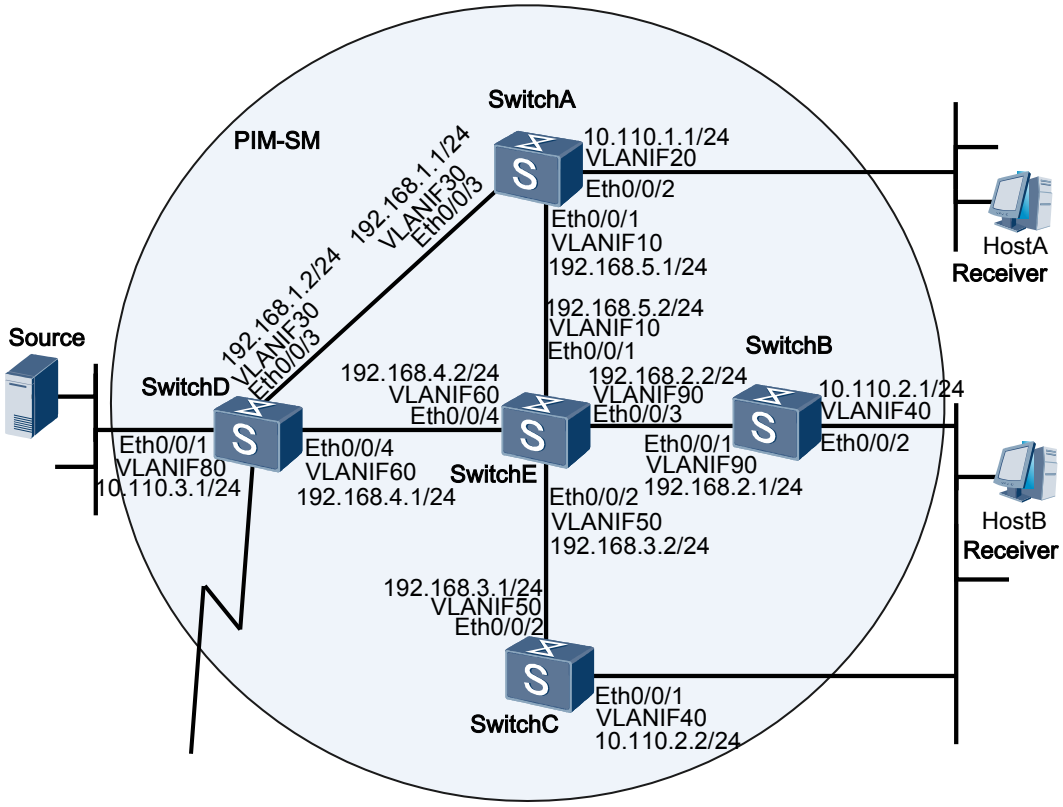
通过配置举例，可以了解如何构建基本的PIM-SM网络、配置PIM-SM常用功能。

4.13.1 配置 ASM 的 PIM-SM 网络示例

组网需求

如图4-3所示，该网络接入了Internet，用户主机HostA、HostB希望能够接收到Source发送的组播数据。

图 4-3 配置 ASM 模型的 PIM-SM 域内组播组网图



配置思路

通过在交换机配置PIM-SM协议，为网络中的用户主机提供ASM服务，使得加入同一组播组的所有用户主机能够接收任意源发往该组的组播数据。

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

说明

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

5. 配置RP。在PIM-SM域中，RP是提供ASM服务的核心，是转发组播数据的中转站。建议RP的位置配置在组播流量分支较多的交换机上，如本图中的SwitchE的位置。

操作步骤

步骤1 配置各接口的IP地址和单播路由协议。

按照图4-3配置各交换机接口的IP地址和掩码，配置各交换机间采用OSPF进行互连，确保网络中各交换机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。SwitchB、SwitchC、SwitchD和SwitchE上的配置过程与SwitchA上的配置相似，配置过程略。

```
[SwitchA] vlan batch 10 20 30
[SwitchA] interface ethernet0/0/1
[SwitchA-Ethernet0/0/1] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/1] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/1] quit
[SwitchA] interface ethernet0/0/2
[SwitchA-Ethernet0/0/2] port hybrid pvid vlan 20
[SwitchA-Ethernet0/0/2] port hybrid untagged vlan 20
[SwitchA-Ethernet0/0/2] quit
[SwitchA] interface ethernet0/0/3
[SwitchA-Ethernet0/0/3] port hybrid pvid vlan 30
[SwitchA-Ethernet0/0/3] port hybrid untagged vlan 30
[SwitchA-Ethernet0/0/3] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 192.168.5.1 24
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ip address 10.110.1.1 24
[SwitchA-Vlanif20] quit
[SwitchA] interface vlanif 30
[SwitchA-Vlanif30] ip address 192.168.1.1 24
[SwitchA-Vlanif30] quit
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.110.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.5.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

步骤2 使能组播功能，在各接口上使能PIM-SM功能。

在所有交换机使能组播功能，在各接口上使能PIM-SM功能。SwitchB、SwitchC、SwitchD和SwitchE上的配置过程与SwitchA上的配置相似，配置过程略。

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] pim sm
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] pim sm
[SwitchA-Vlanif20] quit
[SwitchA] interface vlanif 30
[SwitchA-Vlanif30] pim sm
[SwitchA-Vlanif30] quit
```

步骤3 在连接用户主机的接口上使能IGMP功能。

在SwitchA连接用户主机的接口上使能IGMP功能。SwitchB和SwitchC上的配置过程与SwitchA上的配置相似，配置过程略。

```
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] igmp enable
```

步骤4 配置RP。

说明

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

本实例同时配置两种RP，默认优选动态RP，静态RP作为备份。

配置动态RP。需要将PIM-SM域的一个或多个交换机上配置为C-RP和C-BSR。本例中指定SwitchE同时为C-RP和C-BSR，在SwitchE上配置RP服务的组地址范围，及C-BSR和C-RP所在接口位置。

```
[SwitchE] acl number 2008
[SwitchE-acl-basic-2008] rule permit source 225.1.1.0 0.0.0.255
[SwitchE-acl-basic-2008] quit
[SwitchE] pim
[SwitchE-pim] c-bsr vlanif 90
[SwitchE-pim] c-rp vlanif 90 group-policy 2008
```

配置静态RP。需要在所有交换机上指定静态RP的地址，在SwitchA上配置如下。SwitchB、SwitchC、SwitchD和SwitchE上的配置过程与SwitchA上的配置相似，配置过程略。

说明

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

```
[SwitchA] pim
[SwitchA-pim] static-rp 192.168.4.2
```

步骤5 在SwitchD与Internet相连的接口上配置BSR边界。

```
[SwitchD] interface vlanif 70
[SwitchD-Vlanif70] pim bsr-boundary
[SwitchD-Vlanif70] quit
```

步骤6 验证配置结果。

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

```
<SwitchC> display pim interface
VPN-Instance: public net
Interface      State   NbrCnt   HelloInt   DR-Pri     DR-Address
Vlanif40        up      1         30         1         10.110.2.2    (local)
Vlanif50        up      1         30         1         192.168.3.2
```

通过使用**display pim bsr-info**命令可以查看交换机上BSR选举的信息。例如SwitchA和SwitchE上BSR信息分别如下（SwitchE上还显示C-BSR信息）：

```
<SwitchA> display pim bsr-info
VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 192.168.2.2
     Priority: 0
     Hash mask length: 30
     State: Accept Preferred
     Scope: Not scoped
     Uptime: 01:40:40
     Expires: 00:01:42
     C-RP Count: 1

<SwitchE> display pim bsr-info
VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 192.168.2.2
     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: 192.168.2.2
    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Switch上获取的RP信息。例如SwitchA上RP信息如下：

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

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

说明

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

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

(*, 225.1.1.1)
    RP: 192.168.2.2
    Protocol: pim-sm, Flag: WC
    UpTime: 00:13:46
    Upstream interface: Vlanif10,
        Upstream neighbor: 192.168.5.2
        RPF prime neighbor: 192.168.5.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif20
            Protocol: igmp, UpTime: 00:13:46, Expires:-

(10.110.3.100, 225.1.1.1)
    RP: 192.168.2.2
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 00:00:42
    Upstream interface: Vlanif30
        Upstream neighbor: 192.168.1.2
        RPF prime neighbor: 192.168.1.2
   Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif20
            Protocol: pim-sm, UpTime: 00:00:42, Expires:-
[SwitchB] display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
```

```
    RP: 192.168.2.2
    Protocol: pim-sm, Flag: WC
    UpTime: 00:10:12
    Upstream interface: Vlanif90,
        Upstream neighbor: 192.168.2.2
        RPF prime neighbor: 192.168.2.2
    Downstream interface(s) information:
    Total number of downstreams: None

(10.110.3.100, 225.1.1.1)
    RP: 192.168.2.2
    Protocol: pim-sm, Flag: ACT
    UpTime: 00:00:42
    Upstream interface: Vlanif90
        Upstream neighbor: 192.168.2.2
        RPF prime neighbor: 192.168.2.2
   Downstream interface(s) information:
    Total number of downstreams: None

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

 (*, 225.1.1.1)
    RP: 192.168.2.2
    Protocol: pim-sm, Flag: WC
    UpTime: 00:01:25
    Upstream interface: Vlanif50
        Upstream neighbor: 192.168.3.2
        RPF prime neighbor: 192.168.3.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif40
            Protocol: igmp, UpTime: 00:01:25, Expires:-

 (10.110.3.100, 225.1.1.1)
    RP: 192.168.2.2
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 00:01:25
    Upstream interface: Vlanif50
        Upstream neighbor: 192.168.3.2
        RPF prime neighbor: 192.168.3.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif40
            Protocol: pim-sm, UpTime: 00:01:25, Expires:-

[SwitchD] display pim routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

 (10.110.3.100, 225.1.1.1)
    RP: 192.168.2.2
    Protocol: pim-sm, Flag: SPT LOC ACT
    UpTime: 00:00:42
    Upstream interface: Vlanif80
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 2
        1: Vlanif30
            Protocol: pim-sm, UpTime: 00:01:22, Expires:-
        2: Vlanif60
            Protocol: pim-sm, UpTime: 00:00:42, Expires:-

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

```
 (*, 225.1.1.1)
     RP: 192.168.2.2 (local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:13:16
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 2
         1: Vlanif10
             Protocol: pim-sm, UpTime: 00:12:13, Expires: 00:02:21
         2: Vlanif50
             Protocol: pim-sm, UpTime: 00:13:16, Expires: 00:03:22

(10.110.3.100, 225.1.1.1)
     RP: 192.168.2.2
     Protocol: pim-sm, Flag: SPT ACT
     UpTime: 00:01:22
     Upstream interface: Vlanif60
         Upstream neighbor: 192.168.4.1
         RPF prime neighbor: 192.168.4.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif50
             Protocol: pim-sm, UpTime: 00:01:22, Expires:-
```

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10 20 30
#
multicast routing-enable
#
interface Vlanif10
 ip address 192.168.5.1 255.255.255.0
 pim sm
#
interface Vlanif20
 ip address 10.110.1.1 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif30
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
```

```
#
pim
 static-rp 192.168.4.2
#
return
```

- SwitchB的配置文件

```
#
 sysname SwitchB
#
 multicast routing-enable
#
vlan batch 40 90
#
interface Vlanif40
 ip address 10.110.2.1 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif90
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 90
 port hybrid untagged vlan 90
#
interface Ethernet0/0/2
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
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
```

- SwitchC的配置文件

```
#
 sysname SwitchC
#
 vlan batch 40 50
#
 multicast routing-enable
#
interface Vlanif40
 ip address 10.110.2.2 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif50
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface Ethernet0/0/2
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
```

```
#
pim
 static-rp 192.168.2.2
#
return
```

- SwitchD的配置文件

```
#
 sysname SwitchD
#
 vlan batch 30 60 80
#
 multicast routing-enable
#
interface Vlanif30
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlanif60
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
interface Vlanif80
 ip address 10.110.3.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 80
 port hybrid untagged vlan 80
#
interface Ethernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface Ethernet0/0/4
 port hybrid pvid vlan 60
 port hybrid untagged vlan 60
#
ospf 1
 area 0.0.0.0
  network 10.110.3.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 static-rp 192.168.4.2
#
return
```

- SwitchE的配置文件

```
#
 sysname SwitchE
#
 vlan batch 10 50 60 90
#
 multicast routing-enable
#
acl number 2008
 rule 5 permit source 225.1.1.0 0.0.0.255
#
interface Vlanif10
 ip address 192.168.5.2 255.255.255.0
 pim sm
#
interface Vlanif50
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface Vlanif60
 ip address 192.168.4.2 255.255.255.0
```

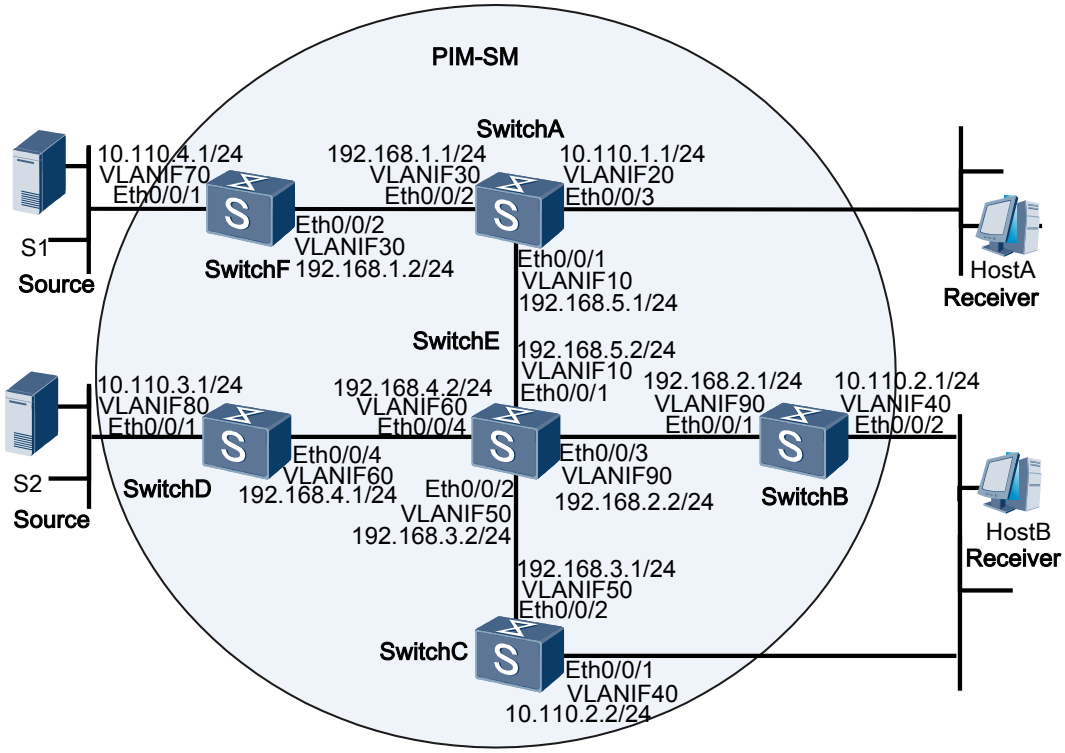
```
 pim sm
#
interface Vlanif90
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface Ethernet0/0/3
 port hybrid pvid vlan 90
 port hybrid untagged vlan 90
#
interface Ethernet0/0/4
 port hybrid pvid vlan 60
 port hybrid untagged vlan 60
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
#
pim
 c-bsr Vlanif90
 c-rp Vlanif90 group-policy 2008
 static-rp 192.168.4.2
#
return
```

4.13.2 配置 SSM 的 PIM-SM 网络示例

组网需求

如图4-4所示，HostA希望能够接收到S1、S2发送的组播数据，而HostB希望能够接收S2发送的组播数据。

图 4-4 配置 SSM 模型的 PIM-SM 域内组播组网图



配置思路

通过在交换机配置PIM-SM协议，为网络中的用户主机提供SSM服务，使得用户主机在加入组播组的同时，能够接收到自己所指定的组播源的组播数据。

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

   说明

   如果用户主机侧需同时配置PIM-SM和IGMP，必须先使能PIM-SM，再使能IGMP。
5. 在各交换机上设置SSM组地址范围。使PIM-SM域内的交换机为特定组地址范围内的SSM服务，实现可控组播。

   说明

   各交换机上设置SSM组地址范围必须相同。

操作步骤

步骤1 配置各接口的IP地址和单播路由协议。

按照图4-4配置各交换机接口的IP地址和掩码，配置各交换机间采用OSPF进行互连，确保网络中各交换机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。SwitchB、SwitchC、SwitchD、SwitchE和SwitchF上的配置过程与SwitchA上的配置相似，配置过程略。

```
[SwitchA] vlan batch 10 20 30
[SwitchA] interface ethernet0/0/1
[SwitchA-Ethernet0/0/1] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/1] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/1] quit
[SwitchA] interface ethernet0/0/2
[SwitchA-Ethernet0/0/2] port hybrid pvid vlan 20
[SwitchA-Ethernet0/0/2] port hybrid untagged vlan 20
[SwitchA-Ethernet0/0/2] quit
[SwitchA] interface ethernet0/0/3
[SwitchA-Ethernet0/0/3] port hybrid pvid vlan 30
[SwitchA-Ethernet0/0/3] port hybrid untagged vlan 30
[SwitchA-Ethernet0/0/3] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 192.168.5.1 24
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ip address 10.110.1.1 24
[SwitchA-Vlanif20] quit
[SwitchA] interface vlanif 30
[SwitchA-Vlanif30] ip address 192.168.1.1 24
[SwitchA-Vlanif30] quit
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.110.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.5.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

步骤2 使能组播功能，在各接口上使能PIM-SM功能。

在所有交换机使能组播功能，在各接口上使能PIM-SM功能。SwitchB、SwitchC、SwitchD、SwitchE和SwitchF上的配置过程与SwitchA上的配置相似，配置过程略。

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] pim sm
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] pim sm
[SwitchA-Vlanif20] quit
[SwitchA] interface vlanif 30
[SwitchA-Vlanif30] pim sm
[SwitchA-Vlanif30] quit
```

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

在SwitchA连接用户主机的接口上使能IGMP功能。SwitchB和SwitchC上的配置过程与SwitchA上的配置相似，配置过程略。

```
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] igmp enable
[SwitchA-Vlanif20] igmp version 3
```

步骤4 在SwitchA接口上使能PIM silent。

```
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] pim silent
```

步骤5 配置SSM组播组地址范围。

在所有交换机配置SSM组播组地址范围为232.1.1.0/24。SwitchB、SwitchC、SwitchD、SwitchE和SwitchF上的配置过程与SwitchA上的配置完全相同，配置过程略。

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

步骤6 验证配置结果。

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

```
<SwitchC> display pim interface
VPN-Instance: public net
Interface      State   NbrCnt   HelloInt   DR-Pri     DR-Address
Vlanif40        up      1         30         1         10.110.2.2    (local)
Vlanif50        up      1         30         1         192.168.3.2
```

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

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

(10.110.3.100, 232.1.1.1)
     Protocol: pim-ssm, Flag: SG_RCVCR
     UpTime: 00:13:46
     Upstream interface: Vlanif10,
         Upstream neighbor: 192.168.5.2
         RPF prime neighbor: 192.168.5.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif20
             Protocol: igmp, UpTime: 00:13:46, Expires:-

(10.110.4.100, 232.1.1.1)
     Protocol: pim-ssm, Flag: SG_RCVCR
     UpTime: 00:00:42
     Upstream interface: Vlanif30
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
    Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif20
             Protocol: igmp, UpTime: 00:00:42, Expires:-
[SwitchB] display pim routing-table
 VPN-Instance: public net
 Total 1 (S, G) entry

(10.110.3.100, 232.1.1.1)
     Protocol: pim-ssm, Flag: SG_RCVCR
     UpTime: 00:10:12
     Upstream interface: Vlanif90,
         Upstream neighbor: 192.168.2.2
         RPF prime neighbor: 192.168.2.2
     Downstream interface(s) information:
     Total number of downstreams: None

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

```
 (10.110.3.100, 232.1.1.1)
     Protocol: pim-ssm, Flag:
     UpTime: 00:01:25
     Upstream interface: Vlanif50
         Upstream neighbor: 192.168.3.2
         RPF prime neighbor: 192.168.3.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif40
             Protocol: pim-ssm, UpTime: 00:01:25, Expires:-

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

 (10.110.3.100, 232.1.1.1)
     Protocol: pim-ssm, Flag: LOC
     UpTime: 00:00:42
     Upstream interface: Vlanif80
         Upstream neighbor: 10.110.3.100
         RPF prime neighbor: 10.110.3.100
     Downstream interface(s) information:
     Total number of downstreams: 2
         1: Vlanif60
             Protocol: pim-ssm, UpTime: 00:00:42, Expires:-

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

 (10.110.3.100, 232.1.1.1)
     Protocol: pim-ssm, Flag: LOC
     UpTime: 00:13:16
     Upstream interface: Vlanif 60
         Upstream neighbor: 192.168.4.1
         RPF prime neighbor: 192.168.4.1
     Downstream interface(s) information:
     Total number of downstreams: 3
         1: Vlanif10
             Protocol: pim-ssm, UpTime: 00:13:16, Expires: 00:02:21
         2: Vlanif50
             Protocol: pim-ssm, UpTime: 00:13:16, Expires: 00:04:23
         3: Vlanif90
             Protocol: pim-ssm, UpTime: 00:13:16, Expires: 00:03:22

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

 (10.110.4.100, 232.1.1.1)
     Protocol: pim-ssm, Flag: LOC
     UpTime: 00:13:16
     Upstream interface: Vlanif 70
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif30
             Protocol: pim-ssm, UpTime: 00:15:28, Expires: 00:05:21
```

----结束

配置文件

- SwitchA的配置文件

```
#
 sysname SwitchA
```

```
#
 vlan batch 10 20 30
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif10
 ip address 192.168.5.1 255.255.255.0
 pim sm
#
interface Vlanif20
 ip address 10.110.1.1 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
#
interface vlanif 30
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ospf 1
 area 0.0.0.0
  network 10.110.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- SwitchB的配置文件

```
#
 sysname SwitchB
#
 multicast routing-enable
#
vlan batch 40 90
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif40
 ip address 10.110.2.1 255.255.255.0
 pim sm
#
interface Vlanif90
 ip address 192.168.2.1 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
#
interface Ethernet0/0/1
 port hybrid pvid vlan 90
 port hybrid untagged vlan 90
#
```

```
interface Ethernet0/0/2
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- SwitchC的配置文件

```
#
 sysname SwitchC
#
 vlan batch 40 50
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif40
 ip address 10.110.2.2 255.255.255.0
 pim sm
 igmp enable
 igmp version 3
#
interface Vlanif50
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface Ethernet0/0/2
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
ospf 1
 area 0.0.0.0
  network 10.110.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- SwitchD的配置文件

```
#
 sysname SwitchD
#
 vlan batch 60 80
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif60
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
interface Vlanif80
 ip address 10.110.3.1 255.255.255.0
```

```
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 80
 port hybrid untagged vlan 80
#
interface Ethernet0/0/4
 port hybrid pvid vlan 60
 port hybrid untagged vlan 60
#
ospf 1
 area 0.0.0.0
  network 10.110.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

- SwitchE的配置文件

```
#
 sysname SwitchE
#
 vlan batch 10 50 60 90
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif10
 ip address 192.168.5.2 255.255.255.0
 pim sm
#
interface Vlanif50
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface Vlanif60
 ip address 192.168.4.2 255.255.255.0
 pim sm
#
interface Vlanif90
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface Ethernet0/0/3
 port hybrid pvid vlan 90
 port hybrid untagged vlan 90
#
interface Ethernet4/0/0
 port hybrid pvid vlan 60
 port hybrid untagged vlan 60
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
#
```

```
pim
 ssm-policy 2000
#
return
```

- SwitchF的配置文件

```
#
 sysname SwitchF
#
 vlan batch 30 70
#
 multicast routing-enable
#
acl number 2000
 rule 5 permit source 232.1.1.0 0.0.0.255
#
interface Vlanif30
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlanif70
 ip address 10.110.4.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 70
 port hybrid untagged vlan 70
#
interface Ethernet0/0/4
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ospf 1
 area 0.0.0.0
  network 10.110.4.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
#
pim
 ssm-policy 2000
#
return
```

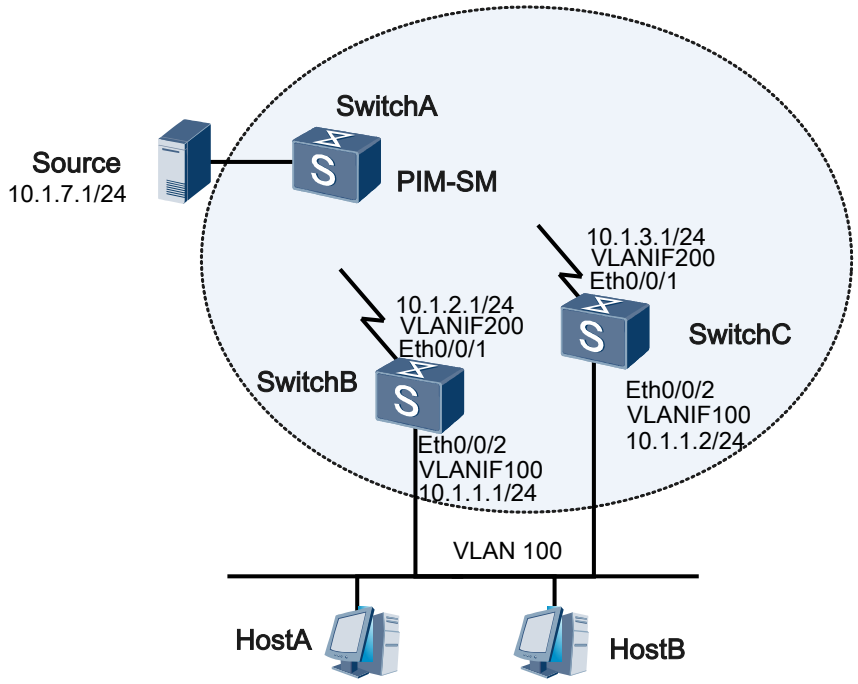
4.13.3 配置 PIM BFD 示例

组网需求

在图4-5所示的组播网络中，Switch之间已完成PIM-SM基本配置，用户主机正常接收来自组播源Source的组播数据。SwitchA是组播源端DR，SwitchB和SwitchC同时连接用户主机网段。要求当组成员端DR变化时，能够快速响应。

解决方案：在用户主机网段建立BFD Session，快速响应DR变化。

图 4-5 配置共享网段应用 PIM BFD 组网图



配置思路

采用如下的思路配置PIM BFD的基本功能：

1. 在Switch接用户主机网段的接口上配置PIM BFD功能。

说明

配置步骤中，只列出了与PIM-SM BFD配置相关的命令。

操作步骤

步骤1 使能全局BFD，在接口下配置PIM BFD。

在SwitchB和SwitchC上全局使能BFD，并在连接用户主机网段的接口上使能PIM BFD功能，配置PIM BFD参数。SwitchC的配置过程与SwitchB相似，配置过程略。

```
[SwitchB] bfd
[SwitchB-bfd] quit
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] pim bfd enable
[SwitchB-Vlanif100] pim bfd min-tx-interval 100 min-rx-interval 100 detect-multiplie 3
```

步骤2 验证配置结果。

使用**display pim interface verbose**命令，可以查看PIM接口上的详细信息。SwitchB上的PIM接口信息表明用户主机网段的DR为SwitchC，接口使能了PIM BFD。

```
<SwitchB> display pim interface vlanif100 verbose
VPN-Instance: public net
 Interface: Vlanif100, 10.1.1.1
     PIM version: 2
     PIM mode: Sparse
```

```
    PIM state: up
    PIM DR: 10.1.1.2
    PIM DR Priority (configured): 1
    PIM neighbor count: 1
    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 generation ID: 0XF5712241
    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: enabled
    PIM BFD min-tx-interval: 100 ms
    PIM BFD min-rx-interval: 100 ms
    PIM BFD detect-multiplier: 3
    Number of routers on link not using DR priority: 0
    Number of routers on link not using LAN delay: 0
```

使用**display pim bfd session**显示各Switch的BFD Session信息，查看BFD Session是否建立。

```
<SwitchB> display pim bfd session
VPN-Instance: public net
Total 1 BFD session Created

Vlanif100 (10.1.1.1): Total 1 BFD session Created

Neighbor     ActTx(ms)     ActRx(ms)     ActMulti     Local/Remote     State
10.1.1.2     100           100           3            8192/8192        Up
```

使用**display pim routing-table**命令可以查看PIM路由表。SwitchC作为DR，存在（S，G）和（*，G）表项。显示信息如下：

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

(*, 225.1.1.1)
    RP: 10.1.5.2
    Protocol: pim-sm, Flag: WC
    UpTime: 00:13:46
    Upstream interface: Vlanif200,
        Upstream neighbor: 10.1.2.2
        RPF prime neighbor: 10.1.2.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif100,
            Protocol: pim-sm, UpTime: 00:13:46, Expires:-
(10.1.7.1, 225.1.1.1)
    RP: 10.1.5.2
    Protocol: pim-sm, Flag: SPT ACT
    UpTime: 00:00:42
    Upstream interface: Vlanif200
        Upstream neighbor: 10.1.2.2
        RPF prime neighbor: 10.1.2.2
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif100
            Protocol: pim-sm, UpTime: 00:00:42, Expires:-
```

----结束

配置文件

- SwitchA只需配置PIM SM的基本功能，在本例中不重点关注，配置文件略。
- SwitchB的配置文件如下。SwitchC的配置文件与SwitchB相似，内容略。

```
#
 sysname SwitchB
#
 vlan batch 100 200
#
 multicast routing-enable
#
bfd
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
 pim sm
 pim bfd enable
 pim bfd min-tx-interval 100 min-rx-interval 100
 igmp enable
#
interface Vlanif200
 ip address 10.1.2.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface Ethernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
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
#
return
```

4.14 常见配置错误

介绍常见配置错误及定位思路。

4.14.1 PIM-SM 网络中 RPT 无法正常转发数据

故障现象

为ASM提供服务的RPT建立不正常，用户主机不能接收到组播数据。

原因分析

本类故障的常见原因主要包括：

- 组播设备到RP的单播路由不通
- 各组播设备的RP地址不一致
- 组播设备的下游接口没有收到（*,G）加入
- 接口没有使能PIM-SM

- 到RP的RPF路由不正确（举例：单播路由环路）
- 配置问题（举例：MTU或组播边界配置不当等）

操作步骤

步骤1 检查PIM路由表中是否存在正确的（*,G）表项

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

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

步骤2 检查上游设备的下游接口是否收到Join信息

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

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

步骤3 检查接口是否使能PIM-SM

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

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

步骤4 检查RP信息是否正确

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

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

步骤5 检查是否存在到达RP的RPF路由

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

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

步骤6 检查转发组播数据的接口是否为组成员端DR

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

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

步骤7 检查接口是否配置组播边界

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

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

步骤8 检查是否配置了source-policy

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

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

----结束

4.14.2 PIM-SM 网络中 SPT 无法正常转发数据

故障现象

SPT建立不正常，用户主机不能接收到组播数据。

原因分析

本类故障的常见原因主要包括：

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

操作步骤

步骤1 检查PIM路由表中是否存在正确的（S,G）表项

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

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

  在组成员端DR上执行**display current-configuration configuration pim**命令，查看PIM视图下的当前配置信息。如果显示信息中出现“spt-switch-threshold infinity”，请执行**undo spt-switch-threshold infinity**命令删除配置信息

  。
- 如果存在，且标志位为SPT，请执行**display multicast forwarding-table**命令查看转发表中的（S,G）表项并且查看显示信息中的“Matched”计数是否保持增长。执行**display multicast forwarding-table**命令后，由于计数更新比较慢，请等待几分钟。
  - 如果“Matched”计数保持增长，则表明上游设备到当前设备的组播数据转发正常，但是由于某种原因导致组播数据无法向下游设备转发。
  - 如果“Matched”计数停止，当前设备不是源DR，表明当前设备没有收到组播数据，故障可能出在上游设备，请检查上游设备的PIM路由表中是否存在正确的（S,G）表项。
- 如果PIM路由表中不存在正确的（S,G）表项，请执行步骤2。

步骤2 检查下游接口是否收到Join信息

说明

如果当前设备是组成员端DR，请跳过此步骤。

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

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

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

- 如果计数没有增加，则下游设备有问题，请排查下游设备的故障。

- 如果下游接口收到的Join-Prune报文计数增加，请执行步骤3。

步骤3 检查接口是否使能PIM-SM

到达组播源的RPF接口没有使能PIM-SM是常见的故障原因。

说明

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

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

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

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

- 如果设备的所有接口均已使能PIM-SM，请执行步骤4。

步骤4 检查是否存在到达组播源的RPF路由

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

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

步骤5 检查转发组播数据的接口是否为组成员端DR

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

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

步骤6 检查接口是否配置组播边界

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

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

步骤7 检查是否配置了source-policy

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

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

----结束

4.14.3 源 DR 在接收到组播数据报文后仍不向 RP 发送注册报文

故障现象

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

操作步骤

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

只有是源DR的设备才会负责向RP注册。例如：

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

 (172.168.0.12, 225.0.0.1)
     RP: 2.2.2.2
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: Vlanif 10
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif 20
             Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

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

例如查看上一步骤中入接口VLANIF10的Peer地址：

```
<Quidway> display rm interface vlanif 10
Name: vlanif10
Physical IF Info:
 IfnetIndex: 0x6
 State: DOWN P2P MULT
 Hardware Address: 286E-D4D4-4F54
 Slot: 0(Logic Slot: 0)
 IntType: 3, PriLog: 0, MTU: 1500, Reference Count 1
 Bandwidth: 0, 64000
 Baudrate: 0, 64000
 Delay: 0, Reliability: 0, Load: 0
 LDP-ISIS sync capability: disabled
 LDP-OSPF sync capability: disabled
 InstanceID: 0, Instance Name: Public
 Age: 1236sec
Logical IF Info:
 IfnetIndex: 0x3E, PhyIndex: 21 Logical Index : 3,
```

```
Dest: 172.168.0.12, Mask: 255.255.255.0
State: UP PRM BCA MULT , Reference Count 3
Age: 1623973sec
```

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

----结束

4.14.4 源 DR 向 RP 发送了注册报文之后，注册出接口一直存在

故障现象

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

原因分析

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

操作步骤

步骤1 确认源DR和RP之间单播路由正确，且能够ping通。

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

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

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

----结束

5 组播路由管理（IPv4）配置

关于本章

设备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。

5.1 组播路由管理（IPv4）概述
组播路由管理主要介绍如何进行组播路由的创建或更改来控制组播报文的转发，以及组播转发路径的检测和维护。

5.2 缺省配置
介绍缺省情况下，组播路由管理的配置信息。

5.3 改变RPF检查规则
在不同的组播场景中，有时候默认的RPF检查规则无法满足要求。此时，可通过如下方法来改变RPF检查规则。

5.4 配置组播转发边界
通过配置组播转发边界，可以限制组播报文转发范围。

5.5 配置组播转发表控制参数
在组播路由与转发中，组播转发表直接控制组播报文的转发。通过配置组播转发表控制参数，间接的就控制了组播报文的转发。

5.6 维护组播路由管理
组播路由管理的维护包括：使用Ping/Tracert检测组播业务性能、清除组播转发表项和路由表项、监控组播路由和转发状况。

5.7 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。

5.8 常见配置错误
介绍常见配置错误及定位思路。

5.1 组播路由管理（IPv4）概述

组播路由管理主要介绍如何进行组播路由的创建或更改来控制组播报文的转发，以及组播转发路径的检测和维护。

说明

S2700&S3700支持组播路由管理（IPv4）的接口为VLANIF接口、Loopback接口。在本章配置中，如无特殊说明，接口的配置一般选择VLANIF接口。使用VLANIF接口前需要先将物理接口加入该VLAN。

在组播设备中，用于指导组播报文转发的主要有三种表：组播协议路由表（Multicast Protocol Routing-Table）、组播路由表（Multicast Routing-Table）、组播转发表（Multicast Forwarding-Table）。

组播报文的路由和转发过程与单播报文的路由和转发过程类似。首先每个组播路由协议都建立并维护了一张协议自身的路由表，比如由PIM协议生成的路由表（PIM Routing-Table）。各组播路由协议的组播路由信息经过综合形成一个总的组播路由表（Multicast Routing-Table）。最后，设备根据组播路由和转发策略，从组播路由表中选出最优的组播路由，并下发到组播转发表（Multicast Forwarding-Table），用于控制组播数据的转发。

为了实现组播转发过程的控制，设备提供了一系列如表5-1所示的组播路由管理功能。

表 5-1 组播路由管理功能

功能	说明
RPF（Reverse Path Forwarding）检查	用于保证组播数据沿正确的转发路径进行传输。当设备收到组播报文，满足一定条件后，就会自动触发RPF检查机制，无需手工配置。
RPF检查规则的改变	用于支持不同组播场景的选路策略。
组播转发边界	用于限制组播报文转发范围。
组播转发表项控制参数的调整	用于调整组播转发表项数量、下行节点数等。
组播Ping	用于促进组播转发树的建立和检测网络中的保留组成员。
组播Tracert	用于沿着组播转发树追踪某一接收者。

5.2 缺省配置

介绍缺省情况下，组播路由管理的配置信息。

表5-2列出了组播路由管理的缺省配置。

表 5-2 组播路由管理（IPv4）的缺省配置

参数	缺省值
组播路由最长匹配	未配置，RPF检查时会先根据路由优先级选取路由。
组播负载分担	未配置，RPF检查会根据一定规则只选取出一条最优路由转发组播报文。
组播转发边界	未配置

5.3 改变 RPF 检查规则

在不同的组播场景中，有时候默认的RPF检查规则无法满足要求。此时，可通过如下方法来改变RPF检查规则。

前置任务

在配置改变RPF检查规则的各种方法之前，需要完成以下任务：

- 配置单播路由协议，确保单播路由畅通。
- 在系统视图下执行命令**multicast routing-enable**，全局使能三层组播路由功能。

配置流程

以下任务是并列关系，可以根据实际需要进行选配。

5.3.1 配置组播静态路由

背景信息

通过配置组播静态路由，可以为来自特定组播源的组播报文指定RPF接口或RPF邻居，主要应用于两个场景：

- 改变RPF路由

  如果设备希望特定组播源发来的数据报文从指定接口接收，但是RPF检查时发现该接口不是RPF接口，此时可配置组播静态路由，指定该接口为RPF接口。当设备接收到特定源发来的组播数据报文后，会以该路由为RPF路由来执行RPF检查，不是通过指定接口发来的报文在RPF检查时将不通过。
- 衔接RPF路由

  在单播路由被阻断的网段，比如相邻两台设备配置不同的路由协议，并且路由没有相互引入，设备上会由于没有RPF路由而无法进行报文转发。此时通过配置组播静态路由，指定RPF接口来完成RPF检查，便可实现组播报文的转发。

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**ip rpf-route-static** *source-address* { *mask* | *mask-length* } [**isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **bgp** | **static**] [**route-policy** *route-policy-name*] { *gateway-address* | *interface-type interface-number* } [**preference** *preference*] [**order** *order-number*]，配置组播静态路由。

注意

配置组播静态路由时，如果下一跳接口为点对点接口，则可选择*gateway-address* | *interface-type interface-number*的*interface-type interface-number*参数，指定出接口；如果下一跳接口为点到多点接口，则必须选择*gateway-address*参数，指定下一跳地址。

----结束

5.3.2 配置组播路由最长匹配

背景信息

缺省情况下，在进行RPF检查时，设备会根据路由优先级来选取路由。可通过配置组播路由最长匹配，改变默认RPF检查规则，在选取RPF路由时首先按照路由的掩码长度来比较，然后再比较路由优先级。

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 longest-match**，配置按照最长匹配来选择路由。

----结束

5.3.3 配置组播负载分担

背景信息

缺省情况下，如果存在多条到达源的等价路由，设备在进行RPF检查时，针对不同的情况会有不同的选路规则：

- 如果这几条等价路由都是来自同一张路由表项，比如单播路由表、组播静态路由表中的一种，则选取下一跳地址最大的路由作为RPF路由。
- 如果这几条等价路由来自不同的路由表，首先会比较路由优先级，再比较掩码长度。如果上述都相同，则设备会根据一定的函数计算选取出一条路由作为RPF路由。

无论上述何种情况，根据RPF检查规则，设备只会选取一条路由作为RPF路由。配置了组播负载分担之后，当存在多条等价的最优路由时，组播数据将不会按照RPF检查规则只选一条路由作为RPF路由进行转发，而是在这多条路径上按照一定的策略进行分流转发。这样，在一定程度上优化了组播数据在网络上的传输质量。

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**multicast load-splitting** { **source** | **group** | **source-group** }，配置组播负载分担。

命令中不同的参数对应着不同组播负载分担策略：

- **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。

----结束

5.3.4 检查配置结果

背景信息

改变RPF检查规则的方法配置成功后，查看组播静态路由表、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

- 使用命令**display multicast routing-table static** [**config**] [*source-address* { *mask* | *mask-length* }]，查看组播静态路由表信息。
- 使用命令**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*]]，查看组播路由表信息。
- 使用命令**display multicast rpf-info** *source-address* [*group-address*] [**rpt** | **spt**]，查看指定组播源的RPF路由信息。

----结束

5.4 配置组播转发边界

通过配置组播转发边界，可以限制组播报文转发范围。

前置任务

在配置组播转发边界之前，需要完成以下任务：

- 配置单播路由协议，确保单播路由畅通。
- 在系统视图下执行命令**multicast routing-enable**，全局使能三层组播路由功能。

背景信息

在组播网络中，有时候希望发往某个组播组的组播报文只在一个范围内进行转发，此时可在接口配置针对该组播组的转发边界。设备在接收到该组的组播报文时，组播报文将无法通过边界接口进行转发。

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**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

检查配置结果

组播转发边界配置成功后，查看组播路由表、接口的组播边界信息，确保组播网络正常运行。

- 使用命令**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*]]，查看组播路由表信息。
- 使用命令**display multicast boundary** [*group-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*]，查看接口的组播边界信息。

5.5 配置组播转发表控制参数

在组播路由与转发中，组播转发表直接控制组播报文的转发。通过配置组播转发表控制参数，间接的就控制了组播报文的转发。

前置任务

在配置改变RPF检查规则的各种方法之前，需要完成以下任务：

- 配置单播路由协议，确保单播路由畅通。
- 在系统视图下执行命令**multicast routing-enable**，全局使能三层组播路由功能。

配置流程

以下任务是并列关系，可以根据实际需要进行选配。

5.5.1 限制组播转发表项数量

背景信息

过量的组播转发表项可能会耗尽设备内存，设备允许用户限制组播转发表项数量。

缺省配置

表5-3列出了组播转发表项数量限制值的缺省值。

表 5-3 组播转发表项数量限制值的缺省值

参数	缺省值
组播转发表项数量限制值	1024

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 forwarding-table route-limit** *limit*，配置组播转发表项数量限制值。

----结束

5.5.2 配置组播转发表项最大下行节点数

背景信息

在组播报文转发过程中，设备为组播转发表项的每一个下行节点复制一份组播报文。根据实际组网情况，设备允许用户对单个转发表项的最大下行节点数进行适当限制，从而缓解设备的处理压力。

缺省配置

表5-4列出了组播转发表项最大下行节点数的缺省值。

表 5-4 组播转发表项最大下行节点数的缺省值

参数	缺省值
组播转发表项最大下行节点数	128

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 forwarding-table downstream-limit** *limit*，配置单个组播转发表项的最大下行节点数目。

----结束

5.5.3 检查配置结果

背景信息

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

- 使用命令**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**] *查看组播转发表信息。

----结束

5.6 维护组播路由管理

组播路由管理的维护包括：使用Ping/Tracert检测组播业务性能、清除组播转发表项和路由表项、监控组播路由和转发状况。

5.6.1 使用 Ping 检测组播业务性能

背景信息

在选择支持组播的网络设备时，用户不仅仅要求设备支持组播转发和组播路由协议，还要求支持组播故障诊断工具。伴随着组播业务的开展，组播维护和故障定位自然成为必要的需求。

MPing主要有以下几种用途：

- 发起普通组播组的MPing。
- 通过查看交换机上的组播路由表信息，检查协议运行状态是否正常，确认组播分发树是否正确建立。
- 通过对目的主机反馈的ICMP Echo Reply报文进行统计处理，计算从MPing发起者到组播组成员的TTL、响应时间等。
- 按照一定时间间隔连续执行多次MPing，计算网络时延和路由抖动。
- 发起保留组播组的MPing检测网络中的保留组成员。

操作步骤

步骤1 执行命令**ping multicast** [**-c** *count* | **-h** *ttl-value* | **-i** *interface-type interface-number* | **-m** *time* | **-p** *pattern* | **-q** | **-s** *packetsize* | **-t** *timeout* | **-tos** *tos-value* | **-v**] * *host*，监控组播业务性能。

通过执行目的地址为保留组的MPing命令可以检查与指定接口直连的交换机上的接口是否使能相应协议，加入相应的保留组播组。

说明

当目的地址为保留组播组时必须指定**-i**参数；当目的地址为一般组播地址时不能指定**-i**参数。

----结束

5.6.2 使用 Tracert 检测组播业务性能

背景信息

在组播故障处理和日常维护中使用**mtrace**命令在追踪过程中收集流量信息，有助于定位故障结点、减少配置错误，循环执行追踪过程，可以统计组播流速率。

操作步骤

- 执行命令**mtrace** [**-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | [**-mr** | **-ur** *resp-dest*] | **-q** *nqueries* | **-tr** *ttl* | **-ts** *ttl* | **-v** | **-w** *timeout*] * **source** *source-address*，检测从组播源到查询者的RPF路径。
- 执行命令**mtrace -g** *group* [**-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | [**-mr** | **-ur** *resp-dest*] | **-q** *nqueries* | **-tr** *ttl* | **-ts** *ttl* | **-v** | **-w** *timeout*] * **source** *source-address*，检测从组播源到查询者的组播路径。

- 执行命令**mtrace** { **-gw** *last-hop-router* | **-d** } **-r** *receiver* [**-a** *source-ip-address* | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | [**-mr** | **-ur** *resp-dest*] | **-q** *nqueries* | **-tr** *ttl* | **-ts** *ttl* | **-v** | **-w** *timeout*] * **source** *source-address*，检测从组播源到目的主机的RPF路径。
- 执行命令**mtrace** { **-gw** *last-hop-router* | **-b** | **-d** } **-r** *receiver* **-g** *group* [**-a** *source-ip-address* | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | [**-mr** | **-ur** *resp-dest*] | **-q** *nqueries* | **-tr** *ttl* | **-ts** *ttl* | **-v** | **-w** *timeout*] * **source** *source-address*，检测从组播源到目的主机的组播路径。

----结束

后续处理

使用**mtrace**检测后，可以使用**display mtrace statistics**命令查看报文统计信息。但是进行多次检测后，大量的测试报文统计信息已经不便于进行结果分析，这时可以使用**reset mtrace statistics**命令用来清除mtrace的统计信息。

5.6.3 清除组播转发表项和路由表项

背景信息

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。

注意

执行reset命令将清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。清除组播路由表中的路由项后，相应组播转发项也将被清除。

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

5.6.4 监控组播路由和转发的状况

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，了解组播转发表和路由表的运行状况。

操作步骤

- 使用命令**display multicast boundary** [*group-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*]，查看接口上配置的组播边界信息。
- 使用命令**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**] *，查看组播转发表信息。
- 使用命令**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*]]查看组播路由表信息。
- 使用命令**display multicast routing-table static** [**config**] [*source-address* { *mask-length* | *mask* }]，查看组播静态路由信息。
- 使用命令**display multicast rpf-info** *source-address* [*group-address*] [**rpt** | **spt**]，查看RPF（Reverse Path Forwarding）路由信息。

----结束

5.7 配置举例

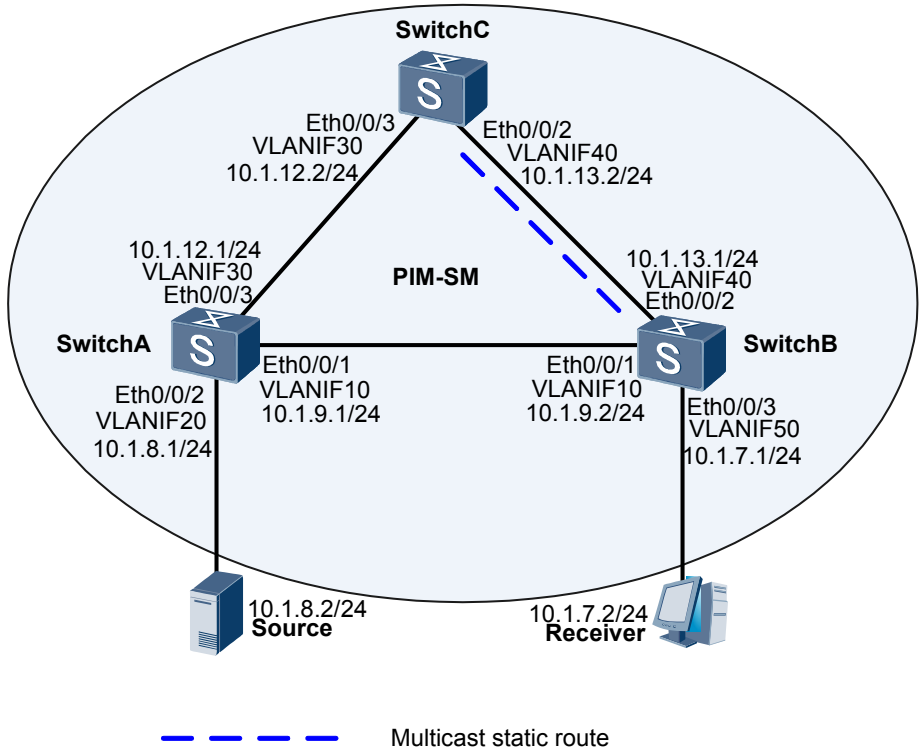
针对如何在组播网络中配置组播静态路由和组播负载分担，分别提供配置举例。

5.7.1 配置组播静态路由改变 RPF 路由示例

组网需求

如图5-1所示，SwitchA、SwitchB和SwitchC之间运行OSPF协议，并且接口上都使能了PIM-SM，组播源Source发出的数据能够沿SwitchA→SwitchB正常的发往Receiver。要求：组播数据沿SwitchA→SwitchC→SwitchB进行传输，减轻SwitchA→SwitchB这条链路同时承载单播业务和组播业务的负担。

图 5-1 配置组播静态路由改变 RPF 路由组网图



配置思路

通过配置组播静态路由，改变接收组播数据的RPF接口，可实现图5-1中所示的组播业务与单播业务分离，通过两条链路进行传输，减轻单链路传输的负担。具体配置思路如下：

1. 配置各Switch接口IP地址和OSPF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. 使能组播功能，在所有交换机的各三层接口上使能PIM-SM并配置静态RP，在与主机相连的接口上使能IGMP。配置了组播协议的基本功能之后，通过设备提供的缺省值，就可以正常建立组播分发树，组播数据沿组播分发树传给Receiver。
3. 在SwitchB上配置RPF组播静态路由，指定RPF邻居为SwitchC，改变组播转发路径。

操作步骤

步骤1 配置各Switch接口IP地址和单播路由协议。

在各交换机上创建VLAN，并将二层物理接口加入VLAN。其他交换机的配置过程与SwitchB上的配置相似，配置过程略。

```
[SwitchB] vlan batch 10 40 50
[SwitchB] interface ethernet0/0/1
[SwitchB-Ethernet0/0/1] port hybrid pvid vlan 10
[SwitchB-Ethernet0/0/1] port hybrid untagged vlan 10
[SwitchB-Ethernet0/0/1] quit
[SwitchB] interface ethernet0/0/2
[SwitchB-Ethernet0/0/2] port hybrid pvid vlan 40
```

```
[SwitchB-Ethernet0/0/2] port hybrid untagged vlan 40
[SwitchB-Ethernet0/0/2] quit
[SwitchB] interface ethernet0/0/3
[SwitchB-Ethernet0/0/3] port hybrid pvid vlan 50
[SwitchB-Ethernet0/0/3] port hybrid untagged vlan 50
[SwitchB-Ethernet0/0/3] quit
```

在各交换机的三层VLANIF接口配置IP地址和掩码。其他交换机的配置过程与SwitchB上的配置相似，配置过程略。

```
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] ip address 10.1.9.2 24
[SwitchB-Vlanif10] quit
[SwitchB] interface vlanif 40
[SwitchB-Vlanif40] ip address 10.1.13.1 24
[SwitchB-Vlanif40] quit
[SwitchB] interface vlanif 50
[SwitchB-Vlanif50] ip address 10.1.7.1 24
[SwitchB-Vlanif50] quit
```

在各交换机上配置单播路由协议OSPF。其他交换机的配置过程与SwitchB上的配置相似，配置过程略。

```
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.7.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.9.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.13.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

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

在所有Switch启动组播功能，并在各接口上使能PIM-SM功能，主机侧接口上使能IGMP功能。其他交换机的配置过程与SwitchB上的配置相似，配置过程略。

```
[SwitchB] multicast routing-enable
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] pim sm
[SwitchB-Vlanif10] quit
[SwitchB] interface vlanif 40
[SwitchB-Vlanif40] pim sm
[SwitchB-Vlanif40] quit
[SwitchB] interface vlanif 50
[SwitchB-Vlanif50] pim sm
[SwitchB-Vlanif50] igmp enable
[SwitchB-Vlanif50] quit
```

将SwitchC的VLANIF30接口IP地址配置为静态RP地址。其他交换机的配置过程与SwitchB上的配置相似，配置过程略。

```
[SwitchB] pim
[SwitchB-pim] static-rp 10.1.12.2
[SwitchB] quit
```

在SwitchB上执行**display multicast rpf-info**命令，查看Source的RPF路由信息。发现当前RPF路由来源于单播，RPF邻居是SwitchA。信息显示如下：

```
[SwitchB] display multicast rpf-info 10.1.8.2
VPN-Instance: public net
RPF information about source 10.1.8.2:
     RPF interface: Vlanif10, RPF neighbor: 10.1.9.1
     Referenced route/mask: 10.1.8.0/24
     Referenced route type: unicast
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

步骤3 配置组播静态路由。

在SwitchB上配置RPF组播静态路由，到Source的RPF邻居为SwitchC。

```
[SwitchB] ip rpf-route-static 10.1.8.0 255.255.255.0 10.1.13.2
```

步骤4 验证配置结果。

在SwitchB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。

```
[SwitchB] display multicast rpf-info 10.1.8.2
VPN-Instance: public net
RPF information about source 10.1.8.2:
     RPF interface: Vlanif40, RPF neighbor: 10.1.13.2
     Referenced route/mask: 10.1.8.0/24
     Referenced route type: mstatic
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

----结束

配置文件

- SwitchA的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 20 30
#
 multicast routing-enable
#
interface Vlanif10
 ip address 10.1.9.1 255.255.255.0
 pim sm
#
interface Vlanif20
 ip address 10.1.8.1 255.255.255.0
 pim sm
#
interface Vlanif30
 ip address 10.1.12.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ospf 1
 area 0.0.0.0
  network 10.1.8.0 0.0.0.255
  network 10.1.9.0 0.0.0.255
  network 10.1.12.0 0.0.0.255
#
pim
 static-rp 10.1.12.2
#
return
```

- SwitchB的配置文件

```
#
 sysname SwitchB
```

```
#
 vlan batch 10 40 50
#
 multicast routing-enable
#
interface Vlanif10
 ip address 10.1.9.2 255.255.255.0
 pim sm
#
interface Vlanif40
 ip address 10.1.13.1 255.255.255.0
 pim sm
#
interface Vlanif50
 ip address 10.1.7.1 255.255.255.0
 pim sm
 igmp enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface Ethernet0/0/3
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
ospf 1
 area 0.0.0.0
  network 10.1.7.0 0.0.0.255
  network 10.1.9.0 0.0.0.255
  network 10.1.13.0 0.0.0.255
#
pim
 static-rp 10.1.12.2
#
ip rpf-route-static 0.1.8.0 24 10.1.13.2
#
return
```

- SwitchC的配置文件

```
#
 sysname SwitchC
#
 vlan batch 30 40
#
 multicast routing-enable
#
interface Vlanif30
 ip address 10.1.12.2 255.255.255.0
 pim sm
#
interface Vlanif40
 ip address 10.1.13.2 255.255.255.0
 pim sm
#
interface Ethernet0/0/2
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface Ethernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ospf 1
 area 0.0.0.0
  network 10.1.12.0 0.0.0.255
```

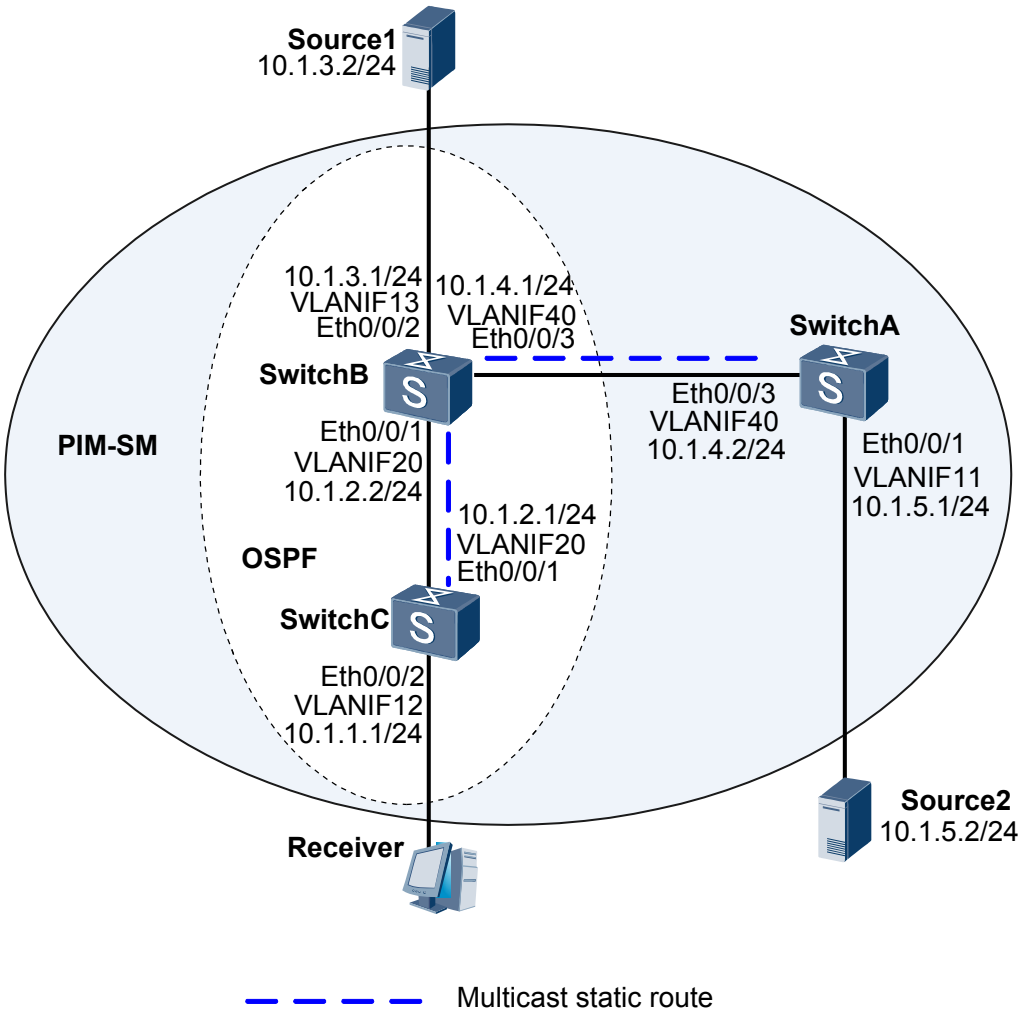
```
 network 10.1.13.0 0.0.0.255
#
pim
 static-rp static-rp 10.1.12.2
#
return
```

5.7.2 配置组播静态路由衔接 RPF 路由示例

组网需求

如图5-2所示，SwitchB和SwitchC之间运行OSPF协议，与SwitchA单播路由隔离，并且每台交换机的接口上都使能了PIM-SM，Receiver能够正常接收组播源Source1的信息。要求使Receiver也能够接收组播源Source2的信息。

图 5-2 配置组播静态路由衔接 RPF 路由组网图



配置思路

通过配置组播静态路由，沿SwitchC→SwitchB→SwitchA这条路径建立能够到达组播源Source2的RPF路由。具体配置思路如下：

1. 配置各交换机接口的IP地址，在SwitchB、SwitchC上配置OSPF路由协议，与SwitchA单播路由隔离。
2. 使能组播功能，在所有交换机的各三层接口上使能PIM-SM并配置静态RP，在与主机相连的接口上使能IGMP。配置了组播协议的基本功能之后，通过设备提供的缺省值，就可以正常建立组播分发树，组播数据沿组播分发树传给Receiver。
3. 在SwitchB、SwitchC上配置到达组播源Source2的组播静态路由。

操作步骤

步骤1 配置各Switch接口IP地址和单播路由协议。

在各交换机上创建VLAN，并将二层物理接口加入VLAN。其他交换机的配置过程与SwitchB上的配置相似，配置过程略。

```
[SwitchB] vlan batch 13 20 40
[SwitchB] interface ethernet0/0/1
[SwitchB-Ethernet0/0/1] port hybrid pvid vlan 20
[SwitchB-Ethernet0/0/1] port hybrid untagged vlan 20
[SwitchB-Ethernet0/0/1] quit
[SwitchB] interface ethernet0/0/2
[SwitchB-Ethernet0/0/2] port hybrid pvid vlan 13
[SwitchB-Ethernet0/0/2] port hybrid untagged vlan 13
[SwitchB-Ethernet0/0/2] quit
[SwitchB] interface ethernet0/0/3
[SwitchB-Ethernet0/0/3] port hybrid pvid vlan 40
[SwitchB-Ethernet0/0/3] port hybrid untagged vlan 40
[SwitchB-Ethernet0/0/3] quit
```

在各交换机的三层VLANIF接口配置IP地址和掩码。其他交换机的配置过程与SwitchB上的配置相似，配置过程略。

```
[SwitchB] interface vlanif 13
[SwitchB-Vlanif13] ip address 10.1.3.1 24
[SwitchB-Vlanif13] quit
[SwitchB] interface vlanif 20
[SwitchB-Vlanif20] ip address 10.1.2.2 24
[SwitchB-Vlanif20] quit
[SwitchB] interface vlanif 40
[SwitchB-Vlanif40] ip address 10.1.4.1 24
[SwitchB-Vlanif40] quit
```

在SwitchB、SwitchC上配置单播路由协议OSPF。SwitchC的配置过程与SwitchB上的配置相似，配置过程略。

```
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

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

在所有Switch启动组播功能，并在各接口上使能PIM-SM功能，主机侧接口上使能IGMP功能。其他交换机的配置过程与SwitchA上的配置相似，配置过程略。

配置SwitchA

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif11
[SwitchA-Vlanif11] pim sm
[SwitchA-Vlanif11] quit
[SwitchA] interface vlanif 40
[SwitchA-Vlanif40] pim sm
[SwitchA-Vlanif40] quit
```

配置SwitchB

```
[SwitchB] multicast routing-enable
[SwitchB] interface vlanif 20
[SwitchB-Vlanif20] pim sm
[SwitchB-Vlanif20] quit
[SwitchB] interface vlanif 13
[SwitchB-Vlanif13] pim sm
[SwitchB-Vlanif13] quit
[SwitchB] interface vlanif 40
[SwitchB-Vlanif40] pim sm
[SwitchB-Vlanif40] quit
```

配置SwitchC

```
[SwitchC] multicast routing-enable
[SwitchC] interface vlanif 20
[SwitchC-Vlanif20] pim sm
[SwitchC-Vlanif20] quit
[SwitchC] interface vlanif 12
[SwitchC-Vlanif12] pim sm
[SwitchC-Vlanif12] igmp enable
[SwitchC-Vlanif12] quit
```

将SwitchB的VLANIF20接口IP地址配置为静态RP地址。其他交换机的配置过程与SwitchA上的配置相似，配置过程略。

```
[SwitchB] pim
[SwitchB-pim] static-rp 10.1.2.2
[SwitchB] 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SwitchB和SwitchC上执行**display multicast rpf-info 10.1.5.2**命令，没有显示信息。说明交换机没有到Source2的RPF路由。

步骤3 配置组播静态路由。

在SwitchB上配置RPF组播静态路由，到Source2的RPF邻居为SwitchA。

```
[SwitchB] ip rpf-route-static 10.1.5.0 255.255.255.0 10.1.4.2
```

在SwitchC上配置RPF组播静态路由，到Source2的RPF邻居为SwitchB。

```
[SwitchC] ip rpf-route-static 10.1.5.0 255.255.255.0 10.1.2.2
```

步骤4 验证配置结果。

分别在SwitchB和SwitchC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。

```
[SwitchB] display multicast rpf-info 10.1.5.2
VPN-Instance: public net
RPF information about source: 10.1.5.2
     RPF interface: vlanif40, 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: disable
[SwitchC] display multicast rpf-info 10.1.5.2
VPN-Instance: public net
RPF information about source 10.1.5.2:
     RPF interface: vlanif20, 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: disable
```

在SwitchC上执行**display pim routing-table**命令，查看路由表信息。SwitchC上存在Source2的组播表项。Receiver正常接收来自Source2的组播数据。

```
[SwitchC] display pim routing-table
VPN-Instance: public net
 Total 1 (*, G) entry; 2 (S, G) entries

 (*, 225.1.1.1)
     RP: 10.1.2.2
     Protocol: pim-sm, 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: Vlanif12
             Protocol: pim-sm, UpTime: 01:38:19, Expires: never

(10.1.3.2, 225.1.1.1)
     RP: 10.1.2.2
     Protocol: pim-sm, Flag: ACT
     UpTime: 00:00:44
     Upstream interface: Vlanif20
         Upstream neighbor: 10.1.2.2
         RPF prime neighbor: 10.1.2.2
     Downstream interface(s) information:
     Total number of downstreams: 1
          1: Vlanif12
              Protocol: pim-sm, UpTime: 00:00:44, Expires: never

(10.1.5.2, 225.1.1.1)
     RP: 10.1.2.2
     Protocol: pim-sm, Flag: ACT
     UpTime: 00:00:44
     Upstream interface: Vlanif20
         Upstream neighbor: 10.1.2.2
         RPF prime neighbor: 10.1.2.2
     Downstream interface(s) information:
     Total number of downstreams: 1
          1: Vlanif12
              Protocol: pim-sm, UpTime: 00:00:44, Expires: never
```

----结束

配置文件

- SwitchA的配置文件

```
#
 sysname SwitchA
#
 multicast routing-enable
#
 vlan batch 11 40
#
interface Vlanif11
 ip address 10.1.5.1 255.255.255.0
 pim sm
#
interface Vlanif40
 ip address 10.1.4.2 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 11
```

```
 port hybrid untagged vlan 11
#
interface Ethernet0/0/3
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
pim
 static-rp 10.1.2.2
#
return
```

- SwitchB的配置文件

```
#
 sysname SwitchB
#
 vlan batch 13 20 40
#
 multicast routing-enable
#
interface Vlanif13
 ip address 10.1.3.1 255.255.255.0
 pim sm
#
interface Vlanif20
 ip address 10.1.2.2 255.255.255.0
 pim sm
#
interface Vlanif40
 ip address 10.1.4.1 255.255.255.0
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/2
 port hybrid pvid vlan 13
 port hybrid untagged vlan 13
#
interface Ethernet0/0/3
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
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
#
pim
 static-rp 10.1.2.2
#
ip rpf-route-static 10.1.5.0 24 10.1.4.2
#
return
```

- SwitchC的配置文件

```
#
 sysname SwitchC
#
 vlan batch 12 20
#
 multicast routing-enable
#
interface Vlanif12
 ip address 10.1.1.1 255.255.255.0
 pim sm
 igmp enable
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
```

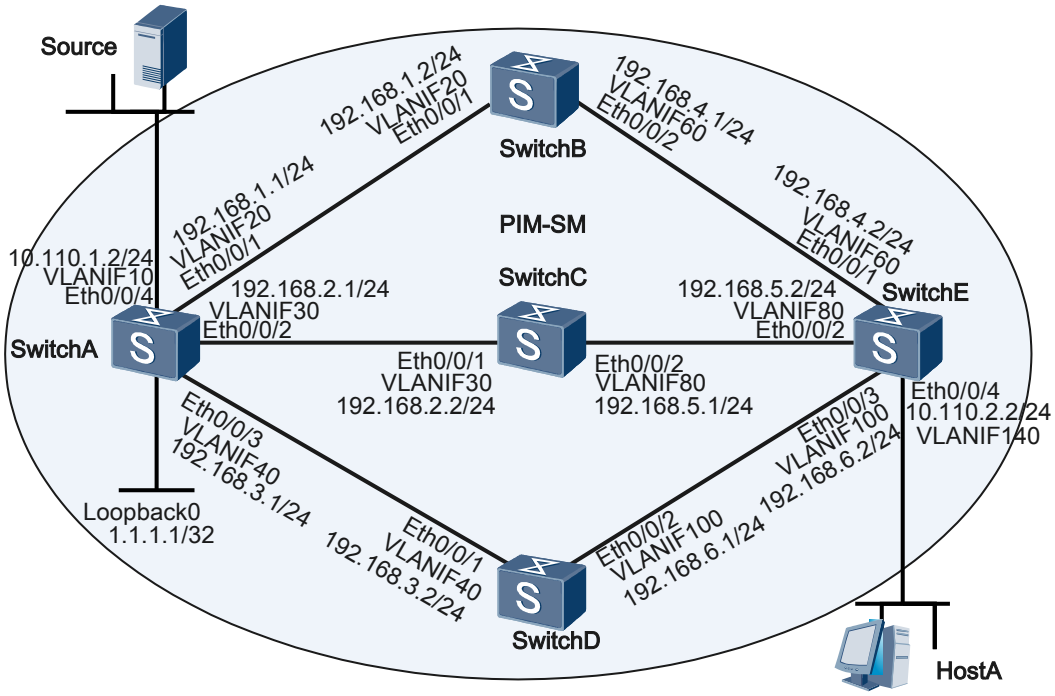
```
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/2
 port hybrid pvid vlan 12
 port hybrid untagged vlan 12
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
#
pim
 static-rp 10.1.2.2
#
ip rpf-route-static 10.1.5.0 24 10.1.2.2
#
return
```

5.7.3 配置组播负载分担示例

组网需求

如图5-3所示，与HostA相连的SwitchE到组播源Source之间存在3条等价路由。默认的RPF检查规则会选取其中的一条进行组播数据的传输，若组播流量过大，可能会出现网络拥塞，影响组播业务。要求通过配置组播负载分担，实现组播数据可以在多条等价路由上进行分流。

图 5-3 配置组播负载分担组网图



配置思路

采用如下的思路配置组播负载分担：

- 配置各交换机的接口IP地址。
- 配置单播路由协议IS-IS，使所有交换机单播互通，且所有路由开销相同。
- 在所有交换机上使能组播路由功能，并在各接口上使能PIM-SM，将SwitchA的环回接口配置为RP。
- 在SwitchE上配置根据组播组地址进行组播负载分担，实现组播数据在多条等价路径上进行分流。
- HostA需要长期接收某些组播组的数据。配置SwitchE的主机侧接口以静态方式批量加入组播组。

操作步骤

步骤1 配置各交换机接口的IP地址。

在各交换机上创建VLAN，并将二层物理接口加入VLAN。以下为SwitchA的配置示例，SwitchB、SwitchC、SwitchD和SwitchE上的配置与SwitchA相似，配置过程略。

```
[SwitchA] vlan batch 10 20 30 40
[SwitchA] interface ethernet0/0/4
[SwitchA-Ethernet0/0/4] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/4] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/4] quit
[SwitchA] interface ethernet0/0/1
[SwitchA-Ethernet0/0/1] port hybrid pvid vlan 20
[SwitchA-Ethernet0/0/1] port hybrid untagged vlan 20
[SwitchA-Ethernet0/0/1] quit
[SwitchA] interface ethernet0/0/2
[SwitchA-Ethernet0/0/2] port hybrid pvid vlan 30
[SwitchA-Ethernet0/0/2] port hybrid untagged vlan 30
[SwitchA-Ethernet0/0/2] quit
[SwitchA] interface ethernet0/0/3
[SwitchA-Ethernet0/0/3] port hybrid pvid vlan 40
[SwitchA-Ethernet0/0/3] port hybrid untagged vlan 40
[SwitchA-Ethernet0/0/3] quit
```

在各交换机的三层接口配置IP地址和掩码。以下为SwitchA的配置示例，SwitchB、SwitchC、SwitchD和SwitchE上的配置与SwitchA相似，配置过程略。

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 10.110.1.2 24
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ip address 192.168.1.1 24
[SwitchA-Vlanif20] quit
[SwitchA] interface vlanif 30
[SwitchA-Vlanif30] ip address 192.168.2.1 24
[SwitchA-Vlanif30] quit
[SwitchA] interface vlanif 40
[SwitchA-Vlanif40] ip address 192.168.3.1 24
[SwitchA-Vlanif40] quit
[SwitchA] interface loopback0
[SwitchA-LoopBack0] ip address 1.1.1.1 32
[SwitchA-LoopBack0] quit
```

步骤2 配置IS-IS协议，使所有交换机单播互通，且所有路由开销相同。

以下为SwitchA的配置示例，SwitchB、SwitchC、SwitchD和SwitchE上的配置与SwitchA相似，配置过程略。

```
[SwitchA] isis
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
```

```
[SwitchA-isis-1] quit
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] isis enable
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] isis enable
[SwitchA-Vlanif20] quit
[SwitchA] interface vlanif 30
[SwitchA-Vlanif30] isis enable
[SwitchA-Vlanif30] quit
[SwitchA] interface vlanif 40
[SwitchA-Vlanif40] isis enable
[SwitchA-Vlanif40] quit
[SwitchA] interface loopback0
[SwitchA-LoopBack0] isis enable
[SwitchA-LoopBack0] quit
```

步骤3 在所有交换机上使能组播功能，并在各接口上使能PIM-SM

以下为SwitchA的配置示例，SwitchB、SwitchC、SwitchD和SwitchE上的配置与SwitchA相似，配置过程略。

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] pim sm
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] pim sm
[SwitchA-Vlanif20] quit
[SwitchA] interface vlanif 30
[SwitchA-Vlanif30] pim sm
[SwitchA-Vlanif30] quit
[SwitchA] interface vlanif 40
[SwitchA-Vlanif40] pim sm
[SwitchA-Vlanif40] quit
[SwitchA] interface loopback 0
[SwitchA-LoopBack0] pim sm
[SwitchA-LoopBack0] quit
```

步骤4 在所有交换机上将SwitchA的Loopback0接口的IP地址指定为静态RP地址。

以下为SwitchA的配置示例，SwitchB、SwitchC、SwitchD和SwitchE上的配置与SwitchA相似，配置过程略。

```
[SwitchA] pim
[SwitchA-pim] static-rp 1.1.1.1
[SwitchA-pim] quit
```

步骤5 在SwitchE上配置根据组播组地址进行组播负载分担。

```
[SwitchE] multicast load-splitting group
```

步骤6 配置SwitchE的主机侧接口以静态方式批量加入组播组

配置接口VLANIF140以静态方式加入组播组225.1.1.1～225.1.1.3。

```
[SwitchE] interface Vlanif140
[SwitchE-Vlanif140] igmp static-group 225.1.1.1 inc-step-mask 32 number 3
[SwitchE-Vlanif140] quit
```

步骤7 验证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SwitchE上查看PIM路由表信息。

```
<SwitchE> display pim routing-table
 VPN-Instance: public net
 Total 3 (*, G) entries; 3 (S, G) entries
  (*, 225.1.1.1)
```

```
   RP: 1.1.1.1
   Protocol: pim-sm, Flag: WC
   UpTime: 3d:20h
   Upstream interface: Vlanif100
       Upstream neighbor: 192.168.6.1
       RPF prime neighbor: 192.168.6.1
   Downstream interface (s)  information:
   Total number of downstreams: 1
       1: Vlanif140
           Protocol: static, UpTime: 3d:20h, Expires: -
(10.110.1.1, 225.1.1.1)
   RP: 1.1.1.1
   Protocol: pim-sm, Flag: SPT ACT
   UpTime: 00:00:11
   Upstream interface: Vlanif100
       Upstream neighbor: 192.168.6.1
       RPF prime neighbor: 192.168.6.1
   Downstream interface (s)  information:
   Total number of downstreams: 1
       1: Vlanif140
           Protocol: pim-sm, UpTime: 00:00:11, Expires: -
(*, 225.1.1.2)
   RP: 1.1.1.1
   Protocol: pim-sm, Flag: WC
   UpTime: 01:06:42
   Upstream interface: Vlanif80
       Upstream neighbor: 192.168.5.1
       RPF prime neighbor: 192.168.5.1
   Downstream interface (s)  information:
   Total number of downstreams: 1
       1: Vlanif140
           Protocol: static, UpTime: 01:06:42, Expires: -
(10.110.1.1, 225.1.1.2)
   RP: 1.1.1.1
   Protocol: pim-sm, Flag: SPT ACT
   UpTime: 00:00:11
   Upstream interface: Vlanif80
       Upstream neighbor: 192.168.5.1
       RPF prime neighbor: 192.168.5.1
   Downstream interface (s)  information:
   Total number of downstreams: 1
       1: Vlanif140
           Protocol: pim-sm, UpTime: 00:00:11, Expires: -
(*, 225.1.1.3)
   RP: 1.1.1.1
   Protocol: pim-sm, Flag: WC
   UpTime: 01:06:42
   Upstream interface: Vlanif60
       Upstream neighbor: 192.168.4.1
       RPF prime neighbor: 192.168.4.1
   Downstream interface (s)  information:
   Total number of downstreams: 1
       1: Vlanif140
           Protocol: static, UpTime: 01:06:42, Expires: -
(10.110.1.1, 225.1.1.3)
   RP: 1.1.1.1
   Protocol: pim-sm, Flag: SPT ACT
   UpTime: 00:00:10
   Upstream interface: Vlanif60
       Upstream neighbor: 192.168.4.1
       RPF prime neighbor: 192.168.4.1
   Downstream interface (s)  information:
   Total number of downstreams: 1
       1: Vlanif140
           Protocol: pim-sm, UpTime: 00:00:10, Expires: -
```

(*,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VLANIF100、VLANIF80和VLANIF60。

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。

----结束

配置文件

- SwitchA的配置文件

```
#
 sysname SwitchA
#
 vlan batch 10 20 30 40
#
 multicast routing-enable
#
isis 1
 network-entity 10.0000.0000.0001.00
#
interface Vlanif10
 ip address 10.110.1.2 255.255.255.0
 isis enable 1
 pim sm
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
 isis enable 1
 pim sm
#
interface Vlanif30
 ip address 192.168.2.1 255.255.255.0
 isis enable 1
 pim sm
#
interface Vlanif40
 ip address 192.168.3.1 255.255.255.0
 isis enable 1
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/2
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface Ethernet0/0/3
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface Ethernet0/0/4
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
 pim sm
#
pim
 static-rp 1.1.1.1
#
return
```

- SwitchB的配置文件

```
#
 sysname SwitchB
```

```
#
 vlan batch 20 60
#
 multicast routing-enable
#
isis 1
 network-entity 10.0000.0000.0002.00
#
interface Vlanif20
 ip address 192.168.1.2 255.255.255.0
 isis enable 1
 pim sm
#
interface Vlanif60
 ip address 192.168.4.1 255.255.255.0
 isis enable 1
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/2
 port hybrid pvid vlan 60
 port hybrid untagged vlan 60
#
pim
 static-rp 1.1.1.1
#
return
```

- SwitchC的配置文件

```
#
 sysname SwitchC
#
 vlan batch 30 80
#
 multicast routing-enable
#
isis 1
 network-entity 10.0000.0000.0003.00
#
interface Vlanif30
 ip address 192.168.2.2 255.255.255.0
 isis enable 1
 pim sm
#
interface Vlanif80
 ip address 192.168.5.1 255.255.255.0
 isis enable 1
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface Ethernet0/0/2
 port hybrid pvid vlan 80
 port hybrid untagged vlan 80
#
pim
 static-rp 1.1.1.1
#
return
```

- SwitchD的配置文件

```
#
 sysname SwitchD
#
 vlan batch 40 100
```

```
#
 multicast routing-enable
#
isis 1
 network-entity 10.0000.0000.0004.00
#
interface Vlanif40
 ip address 192.168.3.2 255.255.255.0
 isis enable 1
 pim sm
#
interface Vlanif100
 ip address 192.168.6.1 255.255.255.0
 isis enable 1
 pim sm
#
interface Ethernet0/0/1
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface Ethernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
pim
 static-rp 1.1.1.1
#
return
```

- SwitchE的配置文件

```
#
 sysname SwitchE
#
 vlan batch 60 80 100 140
#
 multicast routing-enable
 multicast load-splitting group
#
isis 1
 network-entity 10.0000.0000.0005.00
#
interface Vlanif60
 ip address 192.168.4.2 255.255.255.0
 isis enable 1
 pim sm
#
interface Vlanif80
 ip address 192.168.5.2 255.255.255.0
 isis enable 1
 pim sm
#
interface Vlanif100
 ip address 192.168.6.2 255.255.255.0
 isis enable 1
 pim sm
#
interface Vlanif140
 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
#
interface Ethernet0/0/1
 port hybrid pvid vlan 60
 port hybrid untagged vlan 60
#
interface Ethernet0/0/2
 port hybrid pvid vlan 80
 port hybrid untagged vlan 80
#
```

```
interface Ethernet0/0/3
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface Ethernet0/0/4
 port hybrid pvid vlan 140
 port hybrid untagged vlan 140
#
pim
 static-rp 1.1.1.1
#
return
```

5.8 常见配置错误

介绍常见配置错误及定位思路。

5.8.1 组播静态路由建立失败

故障现象

设备没有配置动态路由协议，接口的物理状态与链路层协议状态都显示为up；但是组播静态路由建立失败，组播数据无法转发到用户主机。

操作步骤

步骤1 检查是否正确配置了对应的静态路由并汇总到组播路由表中。

使用命令**display multicast routing-table static**查看设备配置的组播静态路由是否正确。

如果没有正确配置或更新与当前网络情况相匹配的组播静态路由，则组播路由表中不存在此路由项以及组播静态路由的配置信息。此时需要执行命令**ip rpf-route-static**重新配置与当前网络情况相匹配的组播静态路由。

步骤2 检查组播静态路由是否匹配指定的路由协议。

如果配置组播静态路由时指定了协议，使用命令**display ip routing-table**查看单播路由表中指定的协议是否添加了相同的路由。如果没有，则需要在指定的协议中配置相应的路由。

步骤3 检查组播静态路由是否匹配指定的路由策略。

如果配置组播静态路由时指定了路由策略，则使用命令**display route-policy**查看指定的路由策略信息是否与配置的组播静态路由相匹配。如果不匹配，则需要执行命令**route-policy**改变相应的匹配规则，使配置的组播静态路由能够匹配规则，允许其通过。

----结束

5.8.2 组播转发表项入接口不正确

故障现象

组播路由协议配置完成后，能正常创建PIM路由表项，但是组播转发表项入接口不正确，组播数据无法发送到用户网段。

操作步骤

步骤1 执行**display multicast forwarding-table**命令，检查组播转发表项，查看入接口是否为Loopback接口。

如果是Loopback接口，原因通常是组播数据报文的源IP地址与当前设备的VLANIF接口地址相同。此时可修改组播源IP地址或者VLANIF接口地址，保证两者在相同网段，但不能相同。

----结束

6 IGMP Snooping 配置

关于本章

IGMP Snooping配置在二层组播设备上，通过对上游三层设备和下游用户之间的IGMP报文进行分析，建立和维护二层组播转发表，实现组播数据报文在数据链路层的按需分发。

注意事项

端口作为VPLS AC侧的接入端口时，如果该端口同时还作为组播流入接口，会导致对应组播数据无法正常转发。

6.1 IGMP Snooping概述
IGMP Snooping (Internet Group Management Protocol Snooping)是一种IPv4二层组播协议，通过侦听三层组播设备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接口信息，从而管理和控制组播数据报文在数据链路层的转发。

6.2 设备支持的IGMP Snooping特性
设备支持的IGMP Snooping特性包括：IGMP Snooping基本功能、IGMP Snooping Proxy功能、IGMP Snooping策略、成员关系快速刷新以及IGMP Snooping SSM Mapping等。

6.3 缺省配置
介绍缺省情况下，IGMP Snooping的配置信息。

6.4 配置IGMP Snooping基本功能
配置IGMP Snooping基本功能，设备可以建立并维护二层组播转发表，实现组播数据报文在数据链路层的按需分发。

6.5 配置IGMP Snooping Proxy
IGMP Snooping Proxy功能在IGMP Snooping的基础上使交换机代替上游三层设备向下游主机发送IGMP Query报文和代替下游主机向上游设备发送IGMP Report和Leave报文，这样能够有效的节约上游设备和本设备之间的带宽。

6.6 配置IGMP Snooping策略
通过配置IGMP Snooping策略，可以控制用户对组播节目的点播，提高二层组播网络的可控性和安全性。

6.7 配置成员关系快速刷新
配置成员关系快速刷新，使组播组成员加入或者离开组播组时设备能够快速响应成员变化，可以提高组播业务运行效率和用户体验。

6.8 配置IGMP Snooping SSM Mapping
在二层网络中，如果某些用户主机只能运行IGMPv1或IGMPv2，但是这些用户希望享受SSM服务，就需要在设备上配置IGMP Snooping SSM Mapping功能。

6.9 维护IGMP Snooping
IGMP Snooping的维护，包括清除IGMP Snooping表项、清除IGMP Snooping的统计数据、监控IGMP Snooping运行状态。

6.10 配置举例
针对如何配置基于VLAN的IGMP Snooping基本功能、静态端口、IGMP Snooping查询器、IGMP Snooping Proxy、二层组播SSM Mapping，分别提供配置举例。

6.11 常见配置错误
介绍了常见配置错误导致的故障现象以及处理步骤。

6.1 IGMP Snooping 概述

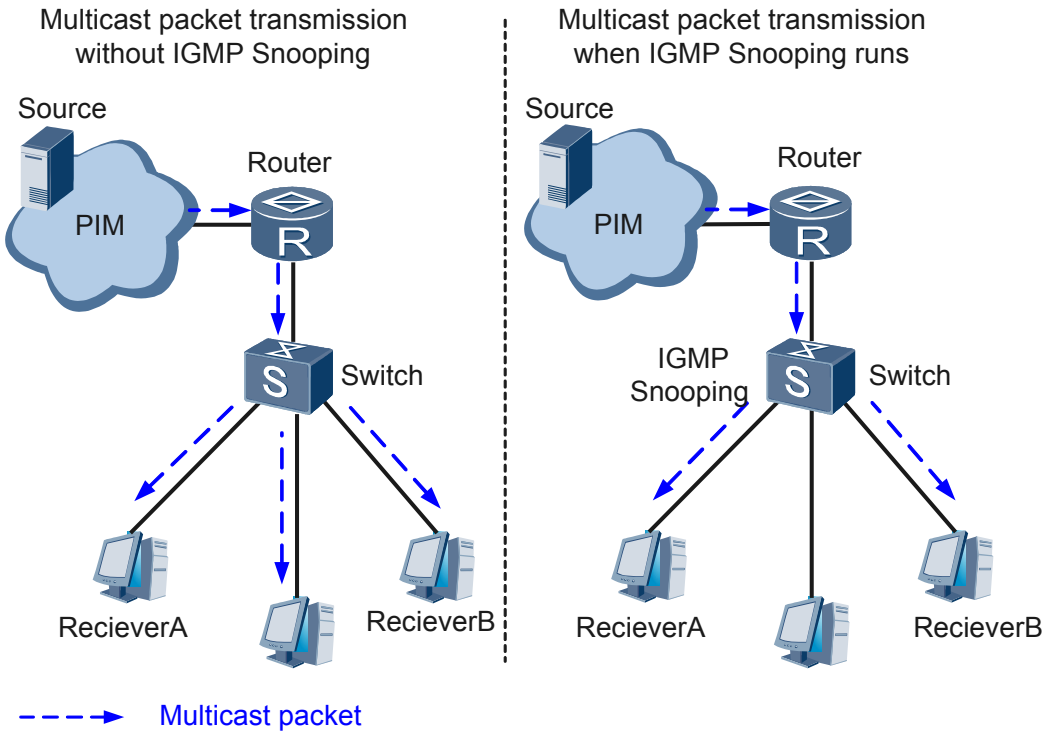
IGMP Snooping (Internet Group Management Protocol Snooping)是一种IPv4二层组播协议，通过侦听三层组播设备和用户主机之间发送的组播协议报文来维护组播报文的出接口信息，从而管理和控制组播数据报文在数据链路层的转发。

IGMP Snooping 功能

在IPv4组播网络中，当上游设备将组播数据报文转发下来以后，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6-1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。

在二层设备（如图6-1中的Switch）上配置IGMP Snooping后，Switch会侦听上游设备和下游主机之间交互的IGMP报文，通过分析报文中携带的信息，建立二层组播转发表项，从而指导组播数据在数据链路层按需转发。

图 6-1 二层设备运行 IGMP Snooping 前后对比



IGMP Snooping 优势

配置了IGMP Snooping的设备能够将组播数据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数据广播，节约了带宽。
- 实现组播数据在二层按需分发，增强了信息安全性。

6.2 设备支持的 IGMP Snooping 特性

设备支持的IGMP Snooping特性包括：IGMP Snooping基本功能、IGMP Snooping Proxy功能、IGMP Snooping策略、成员关系快速刷新以及IGMP Snooping SSM Mapping等。

说明

IGMP Snooping作为一个二层组播特性，本章中涉及到接口的配置，都是在二层物理接口（包括Eth-Trunk接口）下进行配置。

在IGMP协议报文（不包括IGMPv3）默认的CPCAR值下，S2700SI、S2710SI、S2700EI最多能够同时处理大约60个组播用户的点播需求；S3700EI最多能够同时处理大约150个组播用户的点播需求。

IGMP Snooping 基本功能

交换机支持配置基于VLAN的IGMP Snooping功能。IGMP Snooping的基本功能有：

- 支持IGMPv1、IGMPv2和IGMPv3，版本可配置。由于不同版本的IGMP协议报文不相同，因此需要为交换机配置和上游三层设备相同的版本。
- 支持配置静态路由器端口和静态成员端口，实现组播数据快速稳定转发。
- 支持配置IGMP Snooping查询器功能，当上游设备没有启用IGMP查询器时，交换机可以代替上游设备发送IGMP查询报文。
- 支持IGMP Snooping报文抑制功能，对成员主机上送的IGMP Report和Leave报文进行抑制，从而降低上游设备的报文交互数量，提升系统性能。
- 支持配置Router-Alert选项，提高设备性能以及网络安全性。
- 支持配置抑制动态加入，禁止VLAN内收到的IGMP Report和Leave报文向配置有静态组的上游三层设备转发。

IGMP Snooping Proxy 功能

通过在二层设备上配置IGMP Snooping Proxy功能，可以同时具备报文抑制功能和查询器功能。配置了IGMP Snooping Proxy功能的交换机，在其上游设备看来，相当于一台主机；而在其下游主机看来，则相当于一台查询器。

IGMP Snooping 策略

根据不同的场景要求，可以在交换机上进行一些配置，对组播报文进行过滤。

- 通过配置组播组过滤策略，可以限制用户加入的组播组范围。
- 通过配置接口可以学习的最大组播转发表项数量，可以控制接口上的组播数据流量。
- 通过配置接口下组播数据过滤，可以拒绝从该接口收到的指定VLAN的组播数据。
- 通过配置丢弃未知组播报文，使未知组播报文不在VLAN内广播。

成员关系快速刷新

成员关系快速刷新，即成员加入或者离开组播组时交换机快速响应成员变化，可以提高组播业务运行效率和用户体验。主要包括以下几个功能：

- 调整动态成员端口老化时间。

- 调整动态路由器端口老化时间。
- 成员端口快速离开。
- 二层网络拓扑变化时发送查询报文。

IGMP Snooping SSM Mapping

SSM（Source-Specific Multicast）提供了一种能够在成员端指定组播源的传输服务，需要IGMPv3的支持。如果某些接收者主机只能运行IGMPv1或IGMPv2，可以在交换机上配置IGMP Snooping 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，将IGMPv1或IGMPv2报文中所包含的（*，G）信息映射为（S，G）信息，提供SSM组播服务。

IGMP Snooping-CPCAR 注意事项

CPCAR通过对上送控制平面的不同业务的协议报文分别进行限速，来保护控制平面的安全。设备针对每类协议报文都有缺省的CPCAR值，部分协议报文的CPCAR值需要根据实际业务规模和具体的用户网络环境进行调整。

调整CPCAR不当将会影响网络业务，如果需要调整IGMP报文的CPCAR，建议联系华为工程师处理。

6.3 缺省配置

介绍缺省情况下，IGMP Snooping的配置信息。

表 6-1 IGMP Snooping 缺省配置

参数	缺省值
IGMP Snooping功能	未使能
IGMP Snooping版本	IGMP Snooping使能后，默认的版本为IGMPv2
VLAN内组播数据转发模式	● S2700按MAC模式转发组播数据 ● S3700按IP模式转发组播数据
IGMP Snooping端口学习功能	IGMP Snooping使能后，该功能默认使能
IGMP Snooping查询器	未使能
IGMP Snooping普遍组查询间隔	125s
IGMP Snooping报文抑制	未使能
IGMP Snooping Proxy	未使能
IGMP Snooping SSM Mapping	未使能

6.4 配置 IGMP Snooping 基本功能

配置IGMP Snooping基本功能，设备可以建立并维护二层组播转发表，实现组播数据报文在数据链路层的按需分发。

前置任务

在配置IGMP Snooping基本功能之前，需创建VLAN。

配置流程

6.4.1 使能IGMP Snooping功能和6.4.2 配置IGMP Snooping版本为必选配置，其他为可选配置，请根据需要选配。

6.4.1 使能 IGMP Snooping 功能

背景信息

使能全局IGMP Snooping功能，是进行其他IGMP Snooping配置的前提。VLAN下使能IGMP Snooping功能，是VLAN下其他IGMP Snooping配置生效的前提。

缺省情况下，交换机的全局IGMP Snooping功能未使能。

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**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 （可选）执行命令**l2-multicast forwarding-mode** { **ip** | **mac** }，配置VLAN中组播数据是按IP地址还是MAC地址转发。

缺省情况下，S2700按MAC模式转发组播数据，S3700按IP模式转发组播数据。

注意

- 配置VLAN中组播数据转发模式需要在没有使能该VLAN的IGMP Snooping功能时进行。配置完成后需要使能VLAN内IGMP Snooping功能才会生效。
- 如果当前设备按MAC模式转发组播数据，在网络中规划组播IP地址时，请避免选择为协议预留的组播IP地址映射成相同组播MAC地址的组播IP地址。否则，可能造成使用保留组地址发送协议报文的协议无法正常运行。比如：OSPF协议使用224.0.0.5发送协议报文，映射后的组播MAC地址为01-00-5E-00-00-05。如果当前组播数据按MAC模式转发，并且使用的组播IP地址是225.0.0.5，就会造成OSPF协议不能正常运行。

说明

只有S3700EI支持通过此命令改变默认组播数据转发模式，其他设备不支持。

步骤5 执行命令**igmp-snooping enable**，使能VLAN的IGMP Snooping功能。

说明

可以在系统视图下使用**igmp-snooping enable** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]命令，使能多个VLAN的IGMP Snooping功能。

IGMP Snooping功能不能和N:1（N大于1） VLAN Mapping功能配合使用。

S2700的IGMP Snooping功能不能和全局的VLAN Mapping功能配合使用。

----结束

6.4.2 配置 IGMP Snooping 版本

背景信息

IGMP协议用于组成员关系管理，运行于三层组播设备和成员主机之间的网段，有v1、v2、v3三个版本。在二层设备上配置IGMP Snooping版本，设备可以处理相应版本的IGMP报文。一般二层设备上配置和三层组播设备一致的版本。如果三层组播设备没有启用IGMP，则在二层设备上配置和成员主机相同或高于成员主机的版本。

同一VLAN内必须运行同一个版本的IGMP协议。如果VLAN内存在支持不同版本的主机，需要配置IGMP Snooping版本，使设备可以处理所有主机的报文。

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 version** *version*，配置IGMP Snooping可以处理的IGMP版本。

缺省情况下，设备可以处理IGMPv1和IGMPv2的报文，但无法处理IGMPv3的报文。

说明

如果配置IGMP Snooping可以处理的IGMP版本为IGMPv3:

- 则不能改变设备默认的二层组播转发模式。
- S2700按MAC模式转发组播数据。

----结束

6.4.3 （可选）配置静态路由器端口

背景信息

路由器端口一般是二层设备上朝向上游三层组播设备（组播路由器或三层交换机）的接口。VLAN内使能IGMP Snooping功能后，加入该VLAN的接口会从组播协议报文中学习表项。当一个接口接收到IGMP Query报文或PIM Hello报文时，二层设备会标识该接口为动态路由器端口。路由器端口主要有两个功能：

- 接收上游的组播数据。
- 指导IGMP Report/Leave报文转发。当VLAN内收到IGMP Report/Leave报文后，仅会向该VLAN内的路由器端口转发。

动态路由器端口会定时老化，当动态路由器端口在其老化时间超时前没有收到IGMP Query或者PIM Hello报文，设备将把该接口从路由器端口列表中删除。如果希望某接口

长期稳定的转发IGMP Report/Leave报文到上游IGMP查询器，可配置该接口为静态路由器端口。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 （可选）执行命令**vlan** *vlan-id*，进入VLAN视图。

步骤3 （可选）执行命令**undo igmp-snooping router-learning**，禁止动态学习路由器端口。

缺省情况下，VLAN的路由器端口动态学习功能处于使能状态。

步骤4 （可选）执行命令**quit**，退出VLAN视图。

步骤5 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤6 执行命令**igmp-snooping static-router-port vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，配置接口为静态路由器端口。

----结束

6.4.4 （可选）配置静态成员端口

背景信息

成员端口一般是设备上朝向接收者主机的接口，表示该接口下有组播组成员，可以通过组播协议动态学习或静态配置。VLAN内使能IGMP Snooping功能后，加入该VLAN的接口会从组播协议报文中学习表项。当一个接口收到IGMP Report报文时，设备会标识该接口为动态成员端口。动态成员端口会定时老化。

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，成为静态成员端口。静态成员端口不会老化。

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**interface** *interface-type interface-number*，进入接口视图。

步骤3 （可选）执行命令**undo igmp-snooping learning vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }，禁止动态学习组播成员端口。

缺省情况下，成员端口动态学习功能处于使能状态。禁止动态学习组播成员端口功能之后，如果要完成组播数据的转发，接口只能静态加入组播组。

步骤4 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，接口成为静态成员端口。也可以通过命令**l2-multicast static-group** [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id*将接口批量加入组播组。

----结束

6.4.5 （可选）配置 IGMP Snooping 查询器

背景信息

通过使能IGMP Snooping，二层设备就可以通过侦听IGMP查询器与用户主机间的IGMP协议报文，动态建立二层组播转发表项，实现二层组播。

但是当出现下面的情况时，即使二层设备运行了IGMP Snooping，也会由于侦听不到IGMP协议报文，而无法正常动态建立二层组播转发表项：

- 上游三层组播设备在接口上未运行IGMP协议，而是配置了静态组播组。
- 组播源和用户主机同属于一个二层网络，不需要三层组播设备。

此时，可通过在二层组播设备上配置IGMP Snooping查询器，代替三层组播设备向用户主机发送IGMP Query报文，从而解决此问题。

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IGMP Snooping查询器功能。

说明

- 如果与VLAN对应的三层VLANIF接口使能了IGMP功能，则不能在该VLAN内使能IGMP Snooping查询器功能。
- 使能IGMP Snooping查询器功能后，交换机会定时以广播的方式向VLAN内所有接口（包括路由器端口）发送IGMP Query报文，如果组播网络中已经存在IGMP查询器，可能会引起IGMP查询器重新选举。此时，建议不配置此功能；如果一定要配置IGMP Snooping查询器功能，请确保交换机的IP地址比上游IGMP查询器的IP地址大。
- 在同一VLAN内，IGMP Snooping查询器功能和IGMP Snooping Proxy功能不能同时配置。
- 如果设备上配置了组播VLAN复制功能，则不能在用户VLAN上使能IGMP Snooping查询器功能。

步骤4 （可选）配置查询器参数。

说明

在配置参数时，要确保“IGMP查询报文最大响应时间”<“IGMP普遍组查询报文发送间隔”。

查询器参数	配置命令	参数说明	缺省值	支持的版本
普遍组查询报文的发送间隔	**igmp-snooping query-interval** *query-interval*	查询器周期性的发送普遍组查询报文，维护VLAN内的组成员关系，本参数定义了发送该报文的时间间隔。	125秒	IGMPv1、IGMPv2、IGMPv3

查询器参数	配置命令	参数说明	缺省值	支持的版本
IGMP健壮系数	**igmp-snooping robust-count** *robust-count*	健壮系数用来规定以下两个值： ● 当查询器启动时发送“健壮系数”次的“普遍组查询报文”，发送时间间隔为“普遍组查询报文发送间隔”的1/4。 ● 当设备收到Leave报文后，发送“健壮系数”次的“IGMP特定组查询报文”，发送间隔为“特定组查询报文发送间隔”。	2	IGMPv1、IGMPv2、IGMPv3
IGMP查询报文的最大响应时间	**igmp-snooping max-response-time** *max-response-time*	当交换机收到主机的IGMP Report报文后，成员端口老化时间设置为：普遍组查询报文的发送间隔 × IGMP健壮系数 + 最大响应时间。 组播组成员接收到一个IGMP查询报文后，会在最大响应时间内发送Report报文。	10秒	IGMPv2、IGMPv3

查询器参数	配置命令	参数说明	缺省值	支持的版本
特定组查询报文的发送间隔	**igmp-snooping lastmember-queryinterval** *lastmember-queryinterval*	当交换机收到主机退出某组播组的Leave报文时，重置成员端口老化时间为：特定组查询报文发送间隔 × IGMP健壮系数。即会连续发送“IGMP健壮系数”次特定组成员查询报文，询问该组播组是否还存在成员。本参数定义了发送该报文的时间间隔。	1秒	IGMPv2、IGMPv3

步骤5 （可选）执行命令**quit**，返回到系统视图。

步骤6 （可选）执行命令**igmp-snooping send-query source-address** *ip-address*，配置IGMP普遍组查询报文的源IP地址。

缺省情况下，IGMP Snooping查询器发送普遍组查询报文时源IP地址为192.168.0.1。当该地址已被网络中的其他设备占用时，可使用本命令配置为其他地址。

----结束

6.4.6 （可选）配置 Report 和 Leave 报文抑制

背景信息

IGMP协议通过周期性的查询和响应来维护组成员关系。在此过程中，如果多个成员加入了相同的组播组，会不断上送相同的Report报文给IGMP路由器。同时，当IGMPv2或IGMPv3的主机在离开某个组播组时，也会重复发送Leave报文。为了节约带宽，可以在二层设备上配置Report和Leave报文抑制功能。

当配置了对Report和Leave报文抑制后，针对每一个组播组，交换机会在第一次有成员加入需要建立组播表项，以及响应IGMP查询报文时，向上游转发一份Report报文；在最后一个组成员离开需要删除组播表项时，向上游转发一份Leave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**，配置对Report和Leave报文进行抑制。

说明

配置此功能需注意以下几点:

- 在某VLAN下配置了报文抑制功能后，不能在与之对应的三层VLANIF接口使能IGMP功能。
- 在同一VLAN内，Report和Leave报文抑制功能和IGMP Snooping Proxy不能同时配置。
- 如果设备上配置了组播VLAN复制功能，则不能在用户VLAN上配置Report和Leave报文抑制功能。
- 设备未使能报文抑制功能时，对重复的IGMPv1或IGMPv2成员关系报告报文也会进行抑制，默认的抑制时间为10秒，此时间可通过**igmp-snooping suppress-time** *suppress-time*命令来配置。如果将*suppress-time*设为0，表示对所有的成员关系报文都立即转发。

----结束

6.4.7 （可选）配置 Router-Alert 选项

背景信息

出于兼容性考虑，缺省情况下交换机不对Router-Alert选项进行检查，当收到IGMP报文时，不管其IP报头中是否携带Router-Alert选项，设备都会将其送给上层协议进行处理。为了提高系统性能、减少不必要的开支，同时出于协议安全性的考虑，可以配置对Router-Alert选项进行检查，当收到的IGMP报文中没有携带Router-Alert选项时，就丢弃该报文。

缺省情况下，交换机在发送的IGMP报文中携带Router-Alert选项。

有关Router-Alert选项的详细介绍，请参见RFC2113。

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**，配置设备对接收的IGMP报文进行Router-Alert检查。

步骤4 执行命令**igmp-snooping send-router-alert**，配置设备发送的IGMP报文中携带Router-Alert选项。

----结束

6.4.8 （可选）配置 IGMP Snooping 抑制动态加入

背景信息

当上游三层设备为其他厂商设备，并且在用户主机侧接口上配置了静态组播组，不允许下游用户主机动态加入或离开组播组时，可以在设备上配置IGMP Snooping抑制动态加入，禁止向上游设备转发包含静态组地址信息的Report和Leave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 static-group suppress-dynamic-join**，配置设备不转发包含静态组地址信息的Report和Leave报文。

缺省情况下，设备收到包含静态组地址信息的Report和Leave报文后会向路由器端口转发。

----结束

6.4.9 检查配置结果

背景信息

完成上述配置后，可以在任意视图下执行以下命令，查看IGMP Snooping的配置、转发表项等信息。

操作步骤

- 执行命令**display igmp-snooping** [**vlan** [*vlan-id*]] **configuration**，查看IGMP Snooping的配置信息。
- 执行命令**display igmp-snooping** [**vlan** [*vlan-id*]]，查看IGMP Snooping的运行参数信息。
- 执行命令**display igmp-snooping port-info** [**vlan** *vlan-id* [**group-address** *group-address*]] [**verbose**]，查看组播组的成员端口信息。
- 执行命令**display igmp-snooping router-port vlan** *vlan-id*，查看路由器端口信息。
- 执行命令**display l2-multicast forwarding-table vlan** *vlan-id* [[**source-address** *source-address*] **group-address** { *group-address* | **router-group** }]，查看VLAN内二层组播转发表信息。
- 执行命令**display l2-multicast forwarding-mode vlan** [*vlan-id*]，查看VLAN内组播数据转发模式。
- 使用命令**display igmp-snooping querier vlan** [*vlan-id*]，查看IGMP Snooping查询器使能信息。

----结束

6.5 配置 IGMP Snooping Proxy

IGMP Snooping Proxy功能在IGMP Snooping的基础上使交换机代替上游三层设备向下游主机发送IGMP Query报文和代替下游主机向上游设备发送IGMP Report和Leave报文，这样能够有效的节约上游设备和本设备之间的带宽。

前置任务

6.4.1 使能IGMP Snooping功能

背景信息

当三层设备没有启用IGMP时，例如只配置了静态组播组，网络中就不会有IGMP查询器来维护组成员关系。通过在二层设备上配置IGMP Snooping Proxy功能，可以使其发送Query报文，充当IGMP查询器。

当网络中运行了IGMP时，为了减少上游三层设备收到的IGMP Report报文和Leave报文的数量，可以在二层设备上部署IGMP Snooping Proxy功能，使其能够代理下游主机来向上游设备发送成员关系报告报文。

配置了IGMP Snooping Proxy功能的设备称为IGMP Snooping代理，在其上游设备看来，它就相当于一台主机；在其下游设备看来，它相当于一台查询器。

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 proxy**，使能IGMP Snooping Proxy功能。

说明

- 如果与VLAN对应的三层VLANIF接口使能了IGMP，则不能在该VLAN内使能IGMP Snooping Proxy功能。
- 在指定VLAN内，可同时配置查询器和报文抑制功能共同完成IGMP Snooping Proxy功能。如果配置了IGMP Snooping Proxy功能，不能再配置查询器或报文抑制功能。有关查询器和报文抑制功能的配置请参见**6.4.5（可选）配置IGMP Snooping查询器**和**6.4.6（可选）配置Report和Leave报文抑制**。
- 如果设备上配置了组播VLAN复制功能，则不能在用户VLAN上使能IGMP Snooping Proxy功能。

步骤4 （可选）执行命令**quit**，退回到系统视图。

步骤5 （可选）执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤6 （可选）执行命令**igmp-snooping proxy-uplink-port vlan** *vlan-id*，配置设备禁止向路由器端口转发IGMP Query报文。

启用IGMP Snooping Proxy功能后，交换机会定时以广播的方式向VLAN内所有接口（包括路由器端口）发送IGMP Query报文，可能会引起IGMP查询器重新选举。当上游已经启用IGMP时，配置此命令可以禁止交换机向路由器端口转发Query报文，避免查询器重新选举。

----结束

检查配置结果

配置完成后，在任意视图下执行**display igmp-snooping** [**vlan** [*vlan-id*]] **configuration**命令，可以查看到VLAN的IGMP Snooping Proxy的功能配置情况。

6.6 配置 IGMP Snooping 策略

通过配置IGMP Snooping策略，可以控制用户对组播节目的点播，提高二层组播网络的可控性和安全性。

前置任务

6.4 配置IGMP Snooping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。

6.6.1 配置组播组过滤策略

背景信息

组播组过滤策略主要用于对VLAN内的主机加入的组播组进行限制。本功能仅对动态加入的组生效，对静态组播组无效。本功能需要结合ACL使用，先创建ACL并在其规则中定义组播组过滤策略。ACL的配置方法，请参见《S2700&S3700 系列以太网交换机配置指南-安全》中的“ACL配置”。

说明

创建VLAN的组播组过滤策略的ACL时，默认ACL规则**permit**对所有组播组都适用，如果要配置只允许接收某个组的组播数据，需要结合**rule deny source any**命令一起使用。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 通过以下两种方式配置组播组过滤策略，来满足不同的生效范围：

- 配置VLAN内的组播组过滤策略。
  a. 执行命令**vlan** *vlan-id*，进入VLAN视图。
  b. 执行命令**igmp-snooping group-policy** *acl-number* [**version** *version-number*]，配置VLAN内的组播组过滤策略。
- 配置接口下的组播组过滤策略。
  a. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  b. 执行命令**igmp-snooping group-policy** *acl-number* [**version** *version-number*] **vlan** *vlan-id1* [**to** *vlan-id2*]，配置接口下的组播组过滤策略。

缺省情况下，VLAN内的主机可以加入任何组播组。如果不指定应用组播组过滤策略的IGMP报文版本，则交换机对接收到的所有IGMP报文都应用该组播组过滤策略。

如果接口视图和VLAN视图都配置了针对同一VLAN的组播组过滤策略，先根据接口视图上配置的过滤策略进行判断，再根据VLAN视图上配置的过滤策略进行判断。

----结束

6.6.2 配置接口下组播数据过滤

背景信息

当网络管理员希望拒绝某特定的组播数据报文时，可以在交换机接口下配置组播数据过滤，拒绝来自指定VLAN的组播数据报文。

产品	支持情况
S2700	S2700SI、S2710SI不支持
S3700	支持

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-source-deny vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，对指定VLAN内的组播数据进行过滤。

说明

执行本命令时指定的VLAN应该是接口已经加入的VLAN。否则配置没有意义。

使用此命令只过滤同时满足以下条件的组播数据报文：

- 报文目的MAC为IP组播MAC地址（即0x01005E开头的IPv4组播MAC地址或0x3333开头的IPv6组播MAC地址）。
- 报文封装的协议类型为UDP类型。

----结束

6.6.3 配置丢弃未知组播流

背景信息

未知组播流，是指组播转发表中不存在对应的可指导转发的表项的组播报文，也就是用户还没有点播的流量。这种流量可能是上游处于某种目的将流量静态“推”下来的，比如为提高点播的速度，到达交换机后，一般应将流量终结掉，不应该在VLAN内广播。

未使能二层组播时，交换机对未知组播流均采用广播方式。如果用户不需要接收组播流量，可以通过配置**multicast drop-unknown**命令，节省瞬时带宽占用率。

在使能了二层组播后：

- 对于S1720，S2700系列，S5700S-LI、S5700LI、S5710LI、S5700SI设备：

  无论当前二层组播转发模式为何种转发模式，未知组播流都会在VLAN内广播。配置**multicast drop-unknown**命令后，设备在接收到未知组播流后会将其丢弃。通过配置丢弃未知组播流，可以节省瞬时带宽占用率。
- 对于其他设备：
  - 如果当前二层组播转发模式为按IP转发，此时未知组播流不会在VLAN内广播，无论是否配置**multicast drop-unknown**命令，设备都不会接收未知组播流。
  - 如果当前二层组播转发模式为按MAC转发，此时未知组播流会在VLAN内广播。配置**multicast drop-unknown**命令后，设备在接收到未知组播流后会将其丢弃。

可以在VLAN视图下通过**l2-multicast forwarding-mode** { **ip** | **mac** }命令来配置转发模式。缺省情况下，VLAN内组播数据按IP地址模式转发。

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**vlan** *vlan-id*，进入VLAN视图。

步骤3 执行命令**multicast drop-unknown**，配置丢弃未知组播流。

说明

OSPF，VRRP，IPv6 RA message等部分协议报文的目的MAC和目的IP使用的是保留组播地址，没有组播转发表项。如果配置了此命令，这些协议报文将因没有组播转发表项而被丢弃，从而无法通过交换机转发出去。因此当交换机需要在VLAN内透传保留组播地址的协议报文时，VLAN内建议不要配置此命令。

S2700（S2710SI、S2700-52P-EI、S2700-52P-PWR-EI除外）在系统视图下配置此功能。

----结束

6.6.4 配置接口学习的组播表项数量限制

背景信息

通过配置接口可以学习的组播表项最大数量，可以限制用户点播组播节目的数量，控制接口上的数据流量。

如果当前组播表项数量已达到或超过配置值，设备上将无法再加入新的组播组。通过配置二层组播表项替换功能，可解决此问题。配置二层组播表项替换功能后，设备会记录组播用户信息。当某组播用户有加入新的组播组请求，先检查这个组播用户已经点播的所有节目，然后删除其中只有该用户在观看的表项，加入新的表项，实现替换功能。

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-snooping group-limit** *group-limit* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，配置接口可以学习的组播表项最大数量。

说明

在配置接口可以学习的组播表项最大数量时，如果当前接口上的表项数量已经超过了配置值，配置后当前接口上的组播表项数量不会改变，但是不允许接口再学习到新的组播表项。

步骤4 （可选）执行命令**quit**，退回到系统视图。

步骤5 （可选）执行命令**vlan** *vlan-id*，进入VLAN视图。

步骤6 （可选）执行命令**igmp-snooping limit-action**，配置当前VLAN的二层组播表项替换功能。

说明

- 如果当前接口静态加入了组播组，该接口上配置的二层组播表项替换功能将会失效。
- 如果当前组播组有其他组播用户或者为静态组播组时，新的组播表项不会替换该表项。
- 如果新的组播组请求为加入（S，G）的请求，则被替换的表项只能是（S，G）表项，不能是（*，G）表项；反之亦然。

----结束

6.6.5 检查配置结果

前提条件

完成IGMP Snooping策略配置以后，可以在任意视图下执行以下命令，查看策略的配置和应用情况。

操作步骤

- 执行命令**display igmp-snooping** [**vlan** [*vlan-id*]] **configuration**，查看IGMP Snooping的配置信息。

  通过查看IGMP Snooping的配置信息，可查看到VLAN下的IGMP Snooping策略的配置情况。
- 执行命令**display l2-multicast forwarding-table vlan** *vlan-id* [[**source-address** *source-address*] **group-address** { *group-address* | **router-group** }]，查看VLAN内的二层组播转发表信息。

  通过查看二层组播转发表项，可以检查IGMP Snooping策略的应用情况。

----结束

6.7 配置成员关系快速刷新

配置成员关系快速刷新，使组播组成员加入或者离开组播组时设备能够快速响应成员变化，可以提高组播业务运行效率和用户体验。

前置任务

6.4 配置IGMP Snooping基本功能

配置流程

以下功能是并列、可选的，可以根据需要进行配置。

6.7.1 配置动态成员端口老化时间

背景信息

设备在收到不同IGMP协议报文之后，会为成员端口启动不同时长的老化定时器：

- 当设备的成员端口收到下游主机的Report报文后，将接口老化时间设置为：健壮系数 × 普遍组查询报文发送时间间隔 + 最大响应时间。
- 当设备的成员端口收到下游主机的Leave报文后，将接口老化时间设置为：特定组查询报文发送时间间隔 × 健壮系数。

在部署二层组播网络时，要确保所有二层组播设备的用于计算动态成员端口老化时间的相关参数保持一致，尤其是IGMP Snooping普遍组查询时间间隔。否则可能造成二层组播业务运行不正常。

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 query-interval** *query-interval*，配置IGMP Snooping普遍组查询报文的时间间隔。

缺省情况下，IGMP Snooping普遍组查询时间间隔为125秒。

说明

RFC规定的普遍组查询间隔缺省值是125秒，目前并不是所有的厂商都是按照RFC标准实现的。尽量确保组播网络中所有设备的普遍组查询间隔（包括IGMP普遍组查询间隔和IGMP Snooping普遍组查询间隔）保持一致。

表6-2给出了华为S系列交换机普遍组查询间隔的缺省值。

表 6-2 普遍组查询间隔缺省值

特性	框式交换机缺省值	盒式交换机缺省值
IGMP	60s	60s
IGMP Snooping	60s	125s

步骤4 执行命令**igmp-snooping robust-count** *robust-count*，配置IGMP Snooping健壮系数。

缺省情况下，IGMP健壮系数为2。

步骤5 执行命令**igmp-snooping max-response-time** *max-response-time*，配置IGMP Snooping最大响应时间。

缺省情况下，IGMP Snooping的最大响应时间是10秒。

步骤6 执行命令**igmp-snooping lastmember-queryinterval** *lastmember-queryinterval*，配置IGMP Snooping特定组查询报文时间间隔。

缺省情况下，IGMP Snooping特定组查询时间间隔为1秒。

----结束

6.7.2 配置动态路由器端口老化时间

背景信息

路由器端口用来向上游三层设备发送Report/Leave报文和接收上游设备的组播数据报文。在配置IGMP Snooping功能后，设备可以动态学习路由器端口，实时监测上游组播数据的下发。当网络发生拥塞或者网络稳定性不佳时，动态路由器端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端口列表中删除，可能造成组播数据中断，此时可以将路由器端口老化时间值适当调大。

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 router-aging-time** *router-aging-time*，配置动态路由器端口老化时间。

缺省情况下，通过IGMP普遍组查询报文学到的路由器端口老化时间为180秒；通过PIM Hello报文学到的路由器端口老化时间为Hello报文中Holdtime值。

----结束

6.7.3 配置成员端口快速离开

背景信息

成员端口快速离开是指当交换机从成员端口接收到IGMP Leave报文时，不再重置老化定时器等待转发表项老化，而是立即将该成员端口在转发表项中删除。

说明

- 只有当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的成员端口快速离开功能。
- 只有当交换机在VLAN内可以处理IGMPv2或IGMPv3报文时，配置成员端口快速离开功能才有意义。

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 prompt-leave** [**group-policy** *acl-number*]，配置快速离开功能。

缺省情况下，不允许成员端口快速离开。

可以通过**group-policy**参数，对快速离开的组播组进行限制。此时需要创建ACL并配置规则。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。ACL的配置方法，请参见《S2700&S3700 系列以太网交换机 配置指南-安全》中“ACL配置”。

----结束

6.7.4 配置网络拓扑变化时发送 Query 报文

背景信息

当二层网络拓扑发生变化时，组播报文的转发路径可能发生变化。配置交换机在链路故障时主动发送IGMP Query报文，当组播组成员回应IGMP Report报文时，设备根据Report报文更新成员端口信息，将组播数据流迅速切换到新的转发路径上。

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**，配置设备在网络拓扑变化时发送IGMP普遍组查询报文。

缺省情况下，当网络拓扑变化时，设备不会主动发送IGMP普遍组查询报文。

配置本命令后，当设备感知二层网络拓扑发生变化时，会主动发送IGMP普遍组查询报文（报文源地址默认为192.168.0.1），保证设备能够快速更新端口信息，减少下游组成员接收组播数据中断时间。

步骤3 （可选）执行命令**igmp-snooping send-query source-address** *ip-address*，配置IGMP普遍组查询报文的源IP地址。

缺省情况下，响应拓扑变化时发送的普遍组查询报文源地址为192.168.0.1。当该地址已被网络中的其他设备占用时，可使用本命令配置为其他地址。

----结束

6.7.5 检查配置结果

前提条件

完成成员关系快速刷新配置以后，可以在任意视图下执行以下命令，查看IGMP Snooping配置和转发表项信息。

操作步骤

- 执行命令**display igmp-snooping** [**vlan** [*vlan-id*]] **configuration**，查看IGMP Snooping的配置信息。
- 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内二层组播转发表信息。

----结束

6.8 配置 IGMP Snooping SSM Mapping

在二层网络中，如果某些用户主机只能运行IGMPv1或IGMPv2，但是这些用户希望享受SSM服务，就需要在设备上配置IGMP Snooping SSM Mapping功能。

前置任务

已完成**6.4.1 使能IGMP Snooping功能**。

配置流程

一般情况下**6.8.2 配置IGMP Snooping SSM Mapping**即可，如果需要改变SSM组地址范围，可以选配**6.8.1 （可选）配置SSM组策略**。

6.8.1 （可选）配置 SSM 组策略

背景信息

缺省情况下，SSM组范围是232.0.0.0～232.255.255.255。如果用户加入的组播组地址不在SSM组范围内，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。SSM组策略需要结合ACL使用，ACL的配置方法，请参见《S2700&S3700 系列以太网交换机 配置指南-安全》中的“ACL配置”。

说明

创建SSM策略的ACL时，默认ACL规则**deny**对所有组播组都适用，如果要配置某个组地址在SSM组地址范围之外，需要结合**rule permit source any**命令一起使用。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**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。

配置SSM组策略后，该策略允许的组播组都将作为SSM范围内的组对待。

----结束

6.8.2 配置 IGMP Snooping SSM Mapping

背景信息

- 配置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。
- 配置VLAN内IGMP Snooping的版本为3，才能支持SSM Mapping功能。
- 如果配置了组播VLAN复制功能，只需在组播VLAN内配置SSM Mapping即可。
- 虽然配置SSM-Mapping时，需要在VLAN下指定IGMP的版本号为3，但是在向路由器端口转发IGMPv2协议报文时，并不会将其转换为Version 3版本。此时可以通过在交换机上配置IGMP Snooping Proxy或者IGMP Snooping Report Suppress功能将其转换为Version 3的协议报文向上游发送。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**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，VLAN内SSM Mapping功能未使能。

步骤5 执行命令**igmp-snooping ssm-mapping** *group-address* { *group-mask* | *mask-length* } *source-address*，配置组播组地址与源地址映射。

组播组地址为SSM组策略范围内的组播组地址。如果需要修改SSM组地址的范围，其方法请参见**6.8.1 （可选）配置SSM组策略**。

说明

配置了组播组地址与源地址映射关系后：

- S2700按MAC模式转发组播数据。

----结束

6.8.3 检查配置结果

背景信息

完成IGMP Snooping SSM Mapping功能配置以后，可以在任意视图下执行以下命令，查看SSM组映射信息。

操作步骤

- 执行命令**display igmp-snooping port-info** [**vlan** *vlan-id* [**group-address** *group-address*]] [**verbose**]，查看端口表项信息。

----结束

6.9 维护 IGMP Snooping

IGMP Snooping的维护，包括清除IGMP Snooping表项、清除IGMP Snooping的统计数据、监控IGMP Snooping运行状态。

6.9.1 清除 IGMP Snooping 表项

背景信息

IGMP Snooping表项包括静态表项和动态表项，两者的清除方法不一样。

注意

静态表项被清除后无法自动恢复，直到再次执行命令配置静态成员端口。

清除动态表项后，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 Report报文，设备重新生成转发表项后，主机才能再收到组播流。

操作步骤

- 在接口视图下执行命令**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。

  也可以通过以下命令批量取消接口上加入的组播组地址。

  - **undo l2-multicast static-group** [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id*
  - **undo l2-multicast static-group** [**source-address** *source-ip-address*] **group-address all vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }
- 在用户视图下执行命令**reset igmp-snooping group** { **all** | **vlan** { **all** | *vlan-id* } }，清除动态组表项。

----结束

6.9.2 清除 IGMP Snooping 统计信息

背景信息

IGMP Snooping的统计信息主要包括VLAN内接收到的Report、Leave、Query等协议报文的数量，通过该命令可以将这些统计计数置0，便于重新统计。

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

- 在用户视图下执行命令**reset igmp-snooping statistics** { **all** | **vlan** { *vlan-id* | **all** } }，清除IGMP Snooping统计信息。

----结束

6.9.3 监控 IGMP Snooping 的运行状况

背景信息

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

操作步骤

- 执行命令**display igmp-snooping** [**vlan** [*vlan-id*]]，查看VLAN内IGMP Snooping的运行参数信息。
- 执行命令**display igmp-snooping** [**vlan** [*vlan-id*]] **configuration**，查看VLAN内IGMP Snooping的配置信息。
- 执行命令**display igmp-snooping port-info** [**vlan** *vlan-id* [**group-address** *group-address*]] [**verbose**]，查看成员端口信息。
- 执行命令**display igmp-snooping router-port vlan** *vlan-id*，查看路由器端口信息。
- 执行命令**display igmp-snooping querier vlan** [*vlan-id*]，查看IGMP Snooping查询器信息。
- 执行命令**display igmp-snooping statistics vlan** [*vlan-id*]，查看IGMP Snooping的统计信息。
- 执行命令**display l2-multicast forwarding-mode vlan** [*vlan-id*]，查看二层组播的转发模式。
- 执行命令**display l2-multicast forwarding-table vlan** *vlan-id* [[**source-address** *source-address*] **group-address** { *group-address* | **router-group** }]，查看VLAN内二层组播转发表信息。

----结束

6.10 配置举例

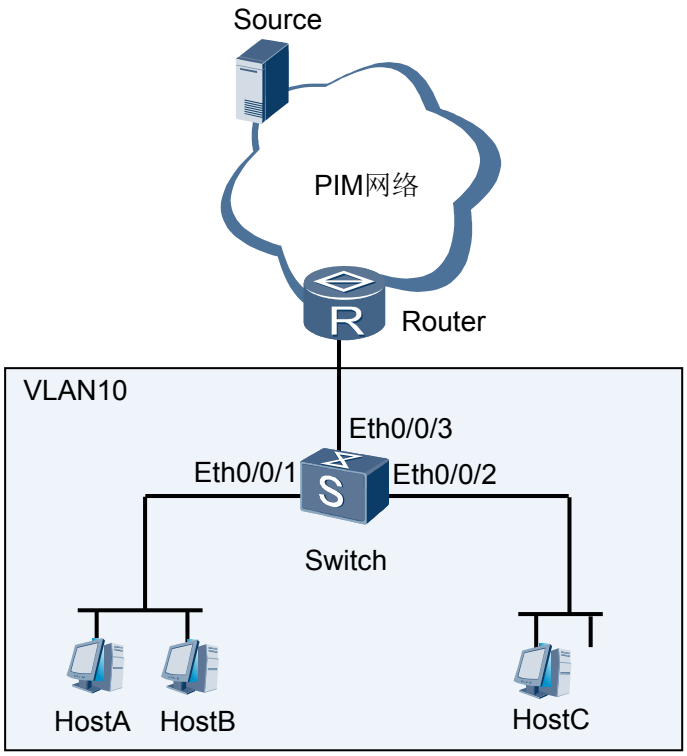
针对如何配置基于VLAN的IGMP Snooping基本功能、静态端口、IGMP Snooping查询器、IGMP Snooping Proxy、二层组播SSM Mapping，分别提供配置举例。

6.10.1 配置 IGMP Snooping 示例

组网需求

如图6-2所示组播网络中，路由器Router通过二层设备Switch连接用户网络，Router上运行IGMPv2版本。组播源Source向组播组225.1.1.1～225.1.1.5发送数据，网络中有HostA、HostB、HostC三个接收者，他们只对225.1.1.1～225.1.1.3的数据感兴趣。

图 6-2 配置 IGMP Snooping 组网图



配置思路

在二层设备上配置IGMP Snooping基本功能以及组播组过滤策略，可以实现此需求。

1. 在Switch上创建VLAN并将接口加入VLAN。
2. 使能全局和VLAN的IGMP Snooping功能。
3. 配置组播组过滤策略，并在VLAN内应用此策略。

操作步骤

步骤1 创建VLAN，配置接口加入VLAN。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] port hybrid pvid vlan 10
[Switch-Ethernet0/0/1] port hybrid untagged vlan 10
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/2
[Switch-Ethernet0/0/2] port hybrid pvid vlan 10
[Switch-Ethernet0/0/2] port hybrid untagged vlan 10
[Switch-Ethernet0/0/2] quit
[Switch] interface ethernet 0/0/3
[Switch-Ethernet0/0/3] port hybrid pvid vlan 10
[Switch-Ethernet0/0/3] port hybrid untagged vlan 10
[Switch-Ethernet0/0/3] quit
```

步骤2 使能IGMP Snooping功能。

使能全局的IGMP Snooping功能。

```
[Switch] igmp-snooping enable
```

使能VLAN10的IGMP Snooping功能。

```
[Switch] vlan 10
[Switch-vlan10] igmp-snooping enable
[Switch-vlan10] quit
```

说明

配置完成后，Switch就可以通过侦听IGMP协议报文生成二层组播转发表项。确保Switch与上游三层设备Router的普遍组查询间隔保持一致，以防止Switch的二层组播转发表项被错误老化，导致组播流量不通。如果Switch默认的普遍组查询间隔与Router不一致，可在VLAN10内执行命令**igmp-snooping query-interval** *query-interval*进行调整。

步骤3 配置并应用组播组过滤策略。

配置组播组过滤策略。

```
[Switch] acl 2000
[Switch-acl-basic-2000] rule deny source 225.1.1.4 0
[Switch-acl-basic-2000] rule deny source 225.1.1.5 0
[Switch-acl-basic-2000] quit
```

在VLAN10内应用组播组过滤策略。

```
[Switch] vlan 10
[Switch-vlan10] igmp-snooping group-policy 2000
[Switch-vlan10] quit
```

步骤4 验证配置结果。

查看Switch上的端口信息。

```
<Switch> display igmp-snooping port-info vlan 10
 ----------------------------------------------------------------------
                   (Source, Group)  Port                          Flag
 Flag: S:Static     D:Dynamic     M: Ssm-mapping
 ----------------------------------------------------------------------
VLAN 10, 3 Entry(s)
                    (*, 225.1.1.1)  Eth0/0/1                       -D-
                                    Eth0/0/2                       -D-
                                              2 port(s)
                    (*, 225.1.1.2)  Eth0/0/1                       -D-
                                    Eth0/0/2                       -D-
```

```
                                          2 port(s)
                    (*, 225.1.1.3)  Eth0/0/1                        -D-
                                    Eth0/0/2                        -D-
                                          2 port(s)
 ----------------------------------------------------------------------
```

由显示信息可知，组225.1.1.1～225.1.1.3已在Switch上动态生成的成员端口为Eth0/0/1和Eth0/0/2。

查看Switch上二层组播转发表。

```
<Switch> display l2-multicast forwarding-table vlan 10
VLAN ID : 10, Forwarding Mode : IP
----------------------------------------------------------------------
                    (Source, Group)    Interface               Out-Vlan
----------------------------------------------------------------------
                       Router-port     Ethernet0/0/3             10
                     (*, 225.1.1.1)    Ethernet0/0/1             10
                                       Ethernet0/0/2             10
                                       Ethernet0/0/3             10
                     (*, 225.1.1.2)    Ethernet0/0/1             10
                                       Ethernet0/0/2             10
                                       Ethernet0/0/3             10
                     (*, 225.1.1.3)    Ethernet0/0/1             10
                                       Ethernet0/0/2             10
                                       Ethernet0/0/3             10
----------------------------------------------------------------------
Total Group(s) : 3
```

由显示信息可知，转发表中只有225.1.1.1～225.1.1.3的组播数据。225.1.1.4～225.1.1.5的数据不会转发给Host。

----结束

配置文件

- Switch的配置文件

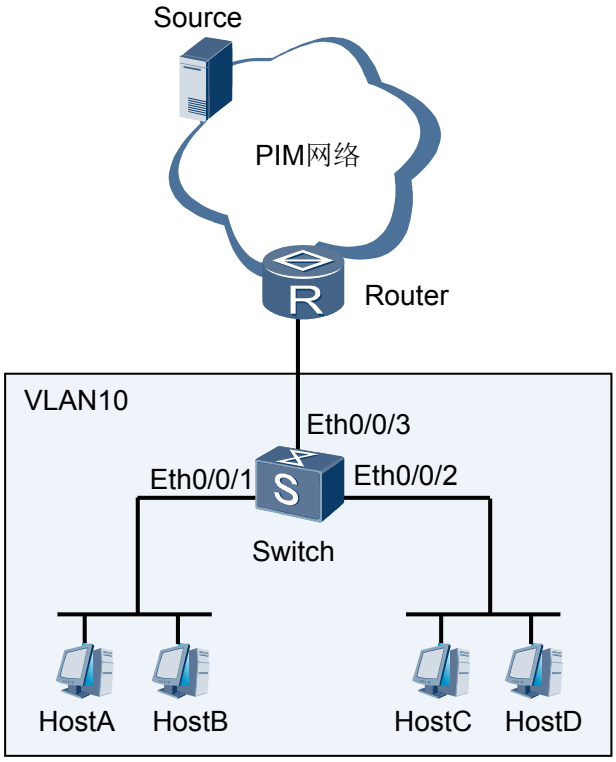
```
#
sysname Switch
#
vlan batch 10
#
igmp-snooping enable
#
acl number 2000
 rule 5 deny source 225.1.1.4 0
 rule 10 deny source 225.1.1.5 0
#
vlan 10
 igmp-snooping enable
 igmp-snooping group-policy 2000
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

6.10.2 配置使用静态端口实现二层组播示例

组网需求

如图6-3所示组播网络中，路由器Router通过二层设备Switch连接用户网络，Router的用户侧三层VLANIF接口配置了225.1.1.1～225.1.1.5的IGMP静态组，没有运行IGMP协议。网络中有HostA、HostB、HostC、HostD四个接收者，其中HostA和HostB希望长期稳定接收225.1.1.1～225.1.1.3的数据，HostC和HostD希望长期稳定接收225.1.1.4～225.1.1.5的数据。

图 6-3 配置静态端口实现二层组播组网图



配置思路

在二层设备上配置IGMP Snooping的静态路由器端口和静态成员端口，可以实现此需求。

1. 在Switch上创建VLAN并将接口加入VLAN。
2. 使能全局和VLAN的IGMP Snooping功能。
3. 配置静态路由器端口。
4. 配置静态成员端口。

操作步骤

步骤1 创建VLAN，配置接口加入VLAN。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] port hybrid pvid vlan 10
[Switch-Ethernet0/0/1] port hybrid untagged vlan 10
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/2
[Switch-Ethernet0/0/2] port hybrid pvid vlan 10
[Switch-Ethernet0/0/2] port hybrid untagged vlan 10
[Switch-Ethernet0/0/2] quit
[Switch] interface ethernet 0/0/3
[Switch-Ethernet0/0/3] port hybrid pvid vlan 10
[Switch-Ethernet0/0/3] port hybrid untagged vlan 10
[Switch-Ethernet0/0/3] quit
```

步骤2 使能IGMP Snooping功能。

使能全局的IGMP Snooping功能。

```
[Switch] igmp-snooping enable
```

使能VLAN10的IGMP Snooping功能。

```
[Switch] vlan 10
[Switch-vlan10] igmp-snooping enable
[Switch-vlan10] quit
```

步骤3 配置静态路由器端口。

```
[Switch] interface ethernet 0/0/3
[Switch-Ethernet0/0/3] igmp-snooping static-router-port vlan 10
[Switch-Ethernet0/0/3] quit
```

步骤4 配置静态成员端口。

```
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] l2-multicast static-group group-address 225.1.1.1 to 225.1.1.3 vlan 10
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/2
[Switch-Ethernet0/0/2] l2-multicast static-group group-address 225.1.1.4 to 225.1.1.5 vlan 10
[Switch-Ethernet0/0/2] quit
```

步骤5 验证配置结果。

查看Switch上的路由器端口信息。

```
<Switch> display igmp-snooping router-port vlan 10
 Port Name                       UpTime        Expires       Flags
 ----------------------------------------------------------------------
 VLAN 10, 1 router-port(s)
 Eth0/0/3                         00:20:09      --            STATIC
```

由显示信息可知，Eth0/0/3已成为静态路由器端口。

查看Switch上的成员端口信息。

```
<Switch> display igmp-snooping port-info vlan 10
 ----------------------------------------------------------------------
                    (Source, Group)  Port                          Flag
  Flag: S:Static     D:Dynamic     M: Ssm-mapping
 ----------------------------------------------------------------------
 VLAN 10, 5 Entry(s)
                     (*, 225.1.1.1)  Eth0/0/1                       S--
                                              1 port(s)
                     (*, 225.1.1.2)  Eth0/0/1                       S--
                                              1 port(s)
                     (*, 225.1.1.3)  Eth0/0/1                       S--
                                              1 port(s)
                     (*, 225.1.1.4)  Eth0/0/2                       S--
```

```
                                          1 port(s)
                    (*, 225.1.1.5)  Eth0/0/2                        S--
                                          1 port(s)
 ------------------------------------------------------------------------
```

由显示信息可知，组225.1.1.1～225.1.1.3在Switch上有静态成员端口Eth0/0/1，组225.1.1.4～225.1.1.5在Switch上有静态成员端口Eth0/0/2。

查看Switch上二层组播转发表。

```
<Switch> display l2-multicast forwarding-table vlan 10
VLAN ID : 10, Forwarding Mode : IP
------------------------------------------------------------------------------
                     (Source, Group)    Interface                    Out-Vlan
------------------------------------------------------------------------------
                        Router-port     Ethernet0/0/3                  10
                      (*, 225.1.1.1)    Ethernet0/0/1                  10
                                        Ethernet0/0/3                  10
                      (*, 225.1.1.2)    Ethernet0/0/1                  10
                                        Ethernet0/0/3                  10
                      (*, 225.1.1.3)    Ethernet0/0/1                  10
                                        Ethernet0/0/3                  10
                      (*, 225.1.1.4)    Ethernet0/0/2                  10
                                        Ethernet0/0/3                  10
                      (*, 225.1.1.5)    Ethernet0/0/2                  10
                                        Ethernet0/0/3                  10
------------------------------------------------------------------------------
Total Group(s) : 5
```

由显示信息可知，组225.1.1.1～225.1.1.5在Switch上已生成转发表。

----结束

配置文件

- Switch的配置文件

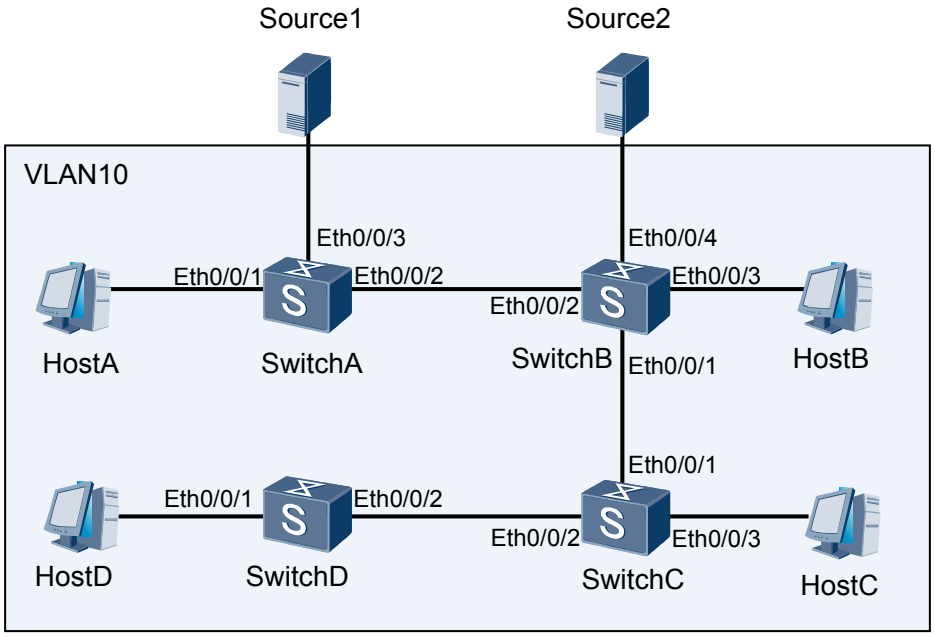
```
#
sysname Switch
#
vlan batch 10
#
igmp-snooping enable
#
vlan 10
 igmp-snooping enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 l2-multicast static-group group-address 225.1.1.1 to 225.1.1.3 vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 l2-multicast static-group group-address 225.1.1.4 to 225.1.1.5 vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 igmp-snooping static-router-port vlan 10
#
return
```

6.10.3 配置 IGMP Snooping 查询器示例

组网需求

如图6-4所示，在一个没有三层设备纯二层网络环境中，组播源Source1和Source2分别向组播组224.1.1.1和225.1.1.1发送组播数据，HostA和HostC希望接收组播组224.1.1.1的数据，HostB和HostD希望接收组播组225.1.1.1的数据。所有接收者运行IGMPv2。

图 6-4 配置 IGMP Snooping 查询器组网图



配置思路

在网络中各Switch上使能IGMP Snooping功能，并配置某一台Switch为IGMP Snooping查询器，可以实现此需求。同时为防止设备在没有二层组播转发表项时将组播数据在VLAN内广播，在所有Switch上都使能丢弃未知组播报文功能。

1. 根据图6-4在所有Switch上创建VLAN并将接口加入VLAN。
2. 在所有Switch上使能全局和VLAN的IGMP Snooping功能。
3. 选择距离组播源较近的SwitchA为IGMP Snooping查询器。
4. 在所有Switch上使能丢弃未知组播报文功能。

操作步骤

步骤1 在所有Switch上创建VLAN并将接口加入VLAN。

配置SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface ethernet 0/0/1
[SwitchA-Ethernet0/0/1] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/1] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/1] quit
[SwitchA] interface ethernet 0/0/2
[SwitchA-Ethernet0/0/2] port hybrid pvid vlan 10
```

```
[SwitchA-Ethernet0/0/2] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/2] quit
[SwitchA] interface ethernet 0/0/3
[SwitchA-Ethernet0/0/3] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/3] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/3] quit
```

SwitchB、SwitchC、SwitchD的配置与此类似，配置过程略。

步骤2 在所有Switch上使能全局和VLAN的IGMP Snooping功能。

配置SwitchA。

```
[SwitchA] igmp-snooping enable
[SwitchA] vlan 10
[SwitchA-vlan10] igmp-snooping enable
[SwitchA-vlan10] quit
```

SwitchB、SwitchC、SwitchD的配置与此类似，配置过程略。

步骤3 配置SwitchA为查询器。

```
[SwitchA] vlan 10
[SwitchA-vlan10] igmp-snooping querier enable
[SwitchA-vlan10] quit
```

步骤4 在所有Switch上使能丢弃未知组播报文功能。

配置SwitchA。

说明

S2700（S2710SI、S2700-52P-EI、S2700-52P-PWR-EI除外）在系统视图下配置此命令。

```
[SwitchA] vlan 10
[SwitchA-vlan10] multicast drop-unknown
[SwitchA-vlan10] quit
```

SwitchB、SwitchC、SwitchD的配置与此类似，配置过程略。

步骤5 验证配置结果。

当IGMP Snooping查询器开始工作之后，除查询器以外的所有设备都能收到IGMP普遍组查询报文。可以通过命令查看IGMP报文的统计信息，例如查看SwitchB上收到的IGMP报文统计信息。

```
<SwitchB> display igmp-snooping statistics vlan 10
 IGMP Snooping Packets Counter
   Statistics for VLAN 10
     Recv V1 Report          0
     Recv V2 Report          32
     Recv V3 Report          0
     Recv V1 Query           0
     Recv V2 Query       30
     Recv V3 Query           0
     Recv Leave              0
     Recv Pim Hello          0
     Send Query(S=0)         0
     Send Query(S!=0)        0
     Suppress Report         0
     Suppress Leave          0
     Proxy Send General Query               0
     Proxy Send Group-Specific Query        0
     Proxy Send Group-Source-Specific Query 0
```

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10
#
igmp-snooping enable
#
vlan 10
 multicast drop-unknown
 igmp-snooping enable
 igmp-snooping querier enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SwitchB的配置文件

```
#
sysname SwitchB
#
vlan batch 10
#
igmp-snooping enable
#
vlan 10
 multicast drop-unknown
 igmp-snooping enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/4
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SwitchC的配置文件

```
#
sysname SwitchC
#
vlan batch 10
#
igmp-snooping enable
#
vlan 10
 multicast drop-unknown
```

```
 igmp-snooping enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SwitchD的配置文件

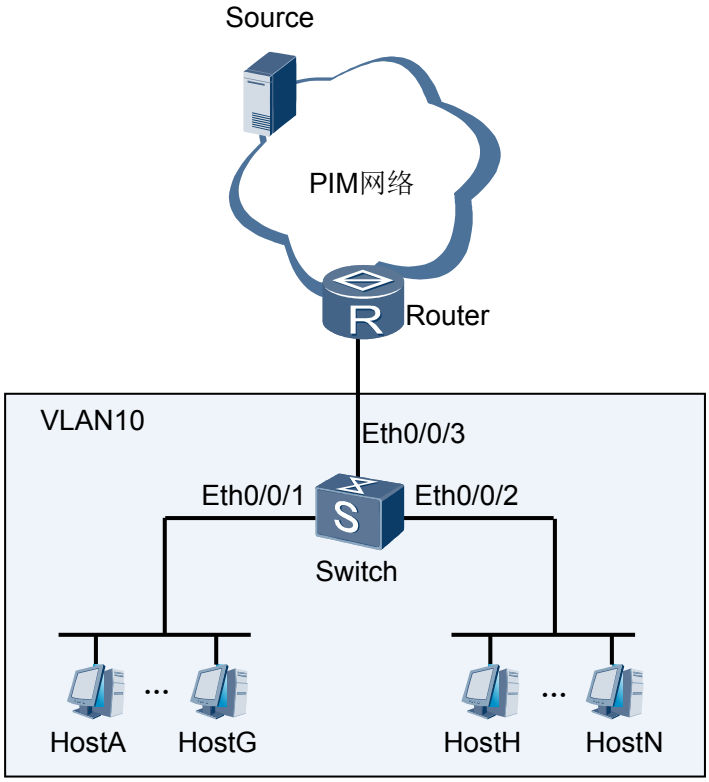
```
#
sysname SwitchD
#
vlan batch 10
#
igmp-snooping enable
#
vlan 10
 multicast drop-unknown
 igmp-snooping enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

6.10.4 配置 IGMP Snooping Proxy 示例

组网需求

如图6-5所示为一个IPv4组播网络，路由器Router通过二层设备Switch连接用户网络，Router运行IGMPv3。网络中接收者主机较多，管理员希望主机在接收组播数据的同时，众多IGMP报文交互不会对Router形成压力。

图 6-5 配置 IGMP Snooping Proxy 功能组网图



配置思路

在Switch上配置IGMP Snooping Proxy，可以实现此需求。

1. 创建VLAN，配置接口加入VLAN。
2. 使能全局和VLAN的IGMP Snooping功能，实现用户接收组播数据。
3. 配置IGMP Snooping Proxy，实现IGMP报文代理功能，减少Switch和Router之间报文交互。
4. 配置Switch不向上游接口发送Query报文，避免引起查询器选举。

操作步骤

步骤1 创建VLAN，配置接口加入VLAN。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] port hybrid pvid vlan 10
[Switch-Ethernet0/0/1] port hybrid untagged vlan 10
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/2
[Switch-Ethernet0/0/2] port hybrid pvid vlan 10
[Switch-Ethernet0/0/2] port hybrid untagged vlan 10
[Switch-Ethernet0/0/2] quit
[Switch] interface ethernet 0/0/3
[Switch-Ethernet0/0/3] port hybrid pvid vlan 10
```

```
[Switch-Ethernet0/0/3] port hybrid untagged vlan 10
[Switch-Ethernet0/0/3] quit
```

步骤2 使能IGMP Snooping功能。

使能全局的IGMP Snooping功能。

```
[Switch] igmp-snooping enable
```

使能VLAN10的IGMP Snooping功能。

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

配置IGMP Snooping版本为v3，使设备可以处理所有版本的IGMP报文。

```
[Switch-vlan10] igmp-snooping version 3
```

步骤3 使能IGMP Snooping Proxy功能。

```
[Switch-vlan10] igmp-snooping proxy
[Switch-vlan10] quit
```

步骤4 配置Switch不向上游接口发送Query报文。

```
[Switch] interface ethernet 0/0/3
[Switch-Ethernet0/0/3] igmp-snooping proxy-uplink-port vlan 10
[Switch-Ethernet0/0/3] quit
```

步骤5 验证配置结果。

查看Switch上IGMP报文统计信息。

```
<Switch> display igmp-snooping statistics vlan 10
 IGMP Snooping Packets Counter
   Statistics for VLAN 10
     Recv V1 Report  0
     Recv V2 Report  121
     Recv V3 Report  0
     Recv V1 Query   0
     Recv V2 Query   0
     Recv V3 Query   0
     Recv Leave      82
     Recv Pim Hello  0
     Send Query(S=0) 0
     Send Query(S!=0)0
     Suppress Report         0
     Suppress Leave          0
     Proxy Send General Query          135
     Proxy Send Group-Specific Query        95
     Proxy Send Group-Source-Specific Query 0
```

由显示信息可知，Switch作为Proxy发送了普遍组查询报文，IGMP Snooping Proxy功能已生效。

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 10
#
igmp-snooping enable
#
vlan 10
 igmp-snooping enable
```

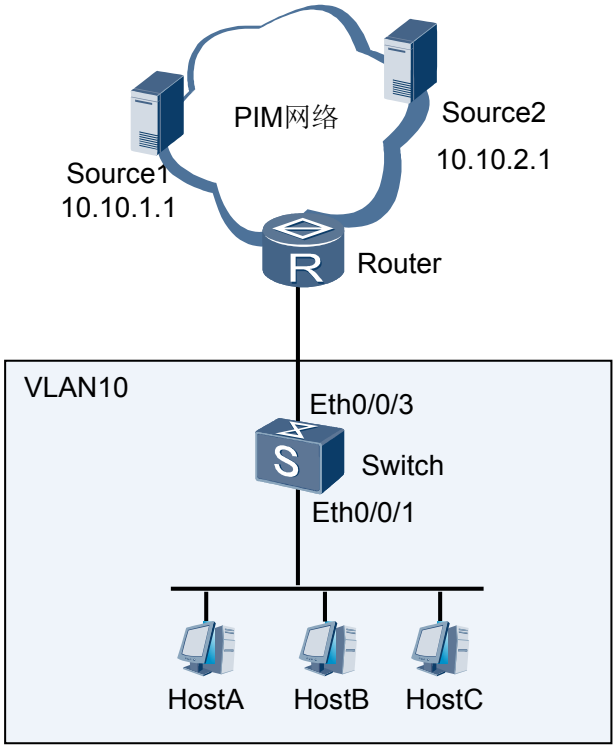
```
 igmp-snooping version 3
 igmp-snooping proxy
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 igmp-snooping proxy-uplink-port vlan 10
#
return
```

6.10.5 配置 IGMP Snooping SSM Mapping 功能示例

组网需求

如图6-6所示组播网络中，路由器Router通过二层设备Switch连接用户网络。Router上运行IGMPv3版本，同时采用ASM和SSM模式提供组播服务。网络中用户主机HostA、HostB、HostC的IGMP版本为IGMPv2，不能升级到IGMPv3。组播源Source1和Source2同时往组播组225.1.1.1发送组播数据，用户主机只想接收Source1发送的数据。

图 6-6 配置 IGMP Snooping SSM Mapping 功能组网图



配置思路

在Switch上配置IGMP Snooping SSM Mapping功能，可以实现此需求。

1. 在Switch上创建VLAN，配置接口加入VLAN。
2. 使能全局和VLAN的IGMP Snooping功能，实现用户接收组播数据。
3. 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。
4. 配置IGMP Snooping SSM Mapping功能，实现用户接收指定组播源数据。

操作步骤

步骤1 创建VLAN，配置接口加入VLAN。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] port hybrid pvid vlan 10
[Switch-Ethernet0/0/1] port hybrid untagged vlan 10
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/3
[Switch-Ethernet0/0/3] port hybrid pvid vlan 10
[Switch-Ethernet0/0/3] port hybrid untagged vlan 10
[Switch-Ethernet0/0/3] quit
```

步骤2 使能IGMP Snooping功能。

使能全局的IGMP Snooping功能。

```
[Switch] igmp-snooping enable
```

使能VLAN10的IGMP Snooping功能。

```
[Switch] vlan 10
[Switch-vlan10] igmp-snooping enable
[Switch-vlan10] quit
```

步骤3 配置IGMP Snooping的SSM组策略。

创建ACL，配置其规则为允许组225.1.1.1的数据通过。

```
[Switch] acl number 2008
[Switch-acl-basic-2008] rule 5 permit source 225.1.1.1 0
[Switch-acl-basic-2008] quit
```

在VLAN下应用SSM Mapping策略，将组225.1.1.1作为SSM范围的组地址对待。

```
[Switch] vlan 10
[Switch-vlan10] igmp-snooping ssm-policy 2008
```

步骤4 配置SSM Mapping功能。

配置Switch上运行IGMPv3版本，使能SSM Mapping功能，并配置映射关系为组225.1.1.1对应的源地址为10.10.1.1。

```
[Switch-vlan10] igmp-snooping version 3
[Switch-vlan10] igmp-snooping ssm-mapping enable
[Switch-vlan10] igmp-snooping ssm-mapping 225.1.1.1 32 10.10.1.1
[Switch-vlan10] quit
```

步骤5 验证配置结果。

查看VLAN内IGMP Snooping的配置情况。

```
<Switch> 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 225.1.1.1 255.255.255.255 10.10.1.1
```

可见VLAN10内已配置了SSM Mapping策略。

查看二层组播转发表。

```
<Switch> display l2-multicast forwarding-table vlan 10
VLAN ID : 10, Forwarding Mode : IP
--------------------------------------------------------------------------------
                     (Source, Group)    Interface                     Out-Vlan
--------------------------------------------------------------------------------
                         Router-port    Ethernet0/0/3                   10
              (10.10.1.1, 225.1.1.1)    Ethernet0/0/1                   10
                                        Ethernet0/0/3                   10
              (10.10.2.1, 225.1.1.1)    Stream                          10
                                        Ethernet0/0/3                   10
--------------------------------------------------------------------------------
Total Group(s) : 1
```

由显示信息可知，Switch上生成(10.10.1.1, 225.1.1.1)表项，是Source1发送的数据。

说明

上面的Stream表项是由于用户主机没有对组播源10.10.2.1的点播需求而形成的未知流表项。

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 10
#
igmp-snooping enable
#
acl number 2008
 rule 5 permit source 225.1.1.1 0
#
vlan 10
 igmp-snooping enable
 igmp-snooping ssm-mapping enable
 igmp-snooping version 3
 igmp-snooping ssm-policy 2008
 igmp-snooping ssm-mapping 225.1.1.1 255.255.255.255 10.10.1.1
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

6.11 常见配置错误

介绍了常见配置错误导致的故障现象以及处理步骤。

6.11.1 二层组播流量不通

故障现象

未配置IGMP Snooping时，组播转发正常，配置了IGMP Snooping功能后，发现用户无法收到组播数据。

操作步骤

步骤1 检查是否配置的IGMP Snooping Version较低。

如果配置的IGMP Snooping Version比用户主机的IGMP版本低，设备在收到IGMP Report报文后，只会向路由器端口转发，不会生成成员端口和转发表项。

执行**display igmp-snooping configuration**命令查看配置信息。如果IGMP Snooping Version比用户主机的IGMP版本低，执行命令**igmp-snooping version** *version*，配置与用户主机的IGMP版本保持一致。

步骤2 检查是否配置的普遍组查询间隔不一致。

如果当前IGMP Snooping设备的普遍组查询间隔比上游IGMP查询器或者IGMP Snooping设备的数值小，很容易造成当前IGMP Snooping设备的IGMP Snooping表项提前老化，无法转发上游发送过来的组播数据。

执行**display igmp-snooping**命令查看IGMP Snooping运行参数信息。如果普遍组查询间隔比上游IGMP查询器或者IGMP Snooping设备的数值小，执行命令**igmp-snooping query-interval** *query-interval*，重新调整IGMP Snooping普遍组查询间隔。建议调整的数值与上下游设备保持一致。

表6-3给出了华为S系列交换机普遍组查询间隔的缺省值。

表 6-3 普遍组查询间隔缺省值

特性	框式交换机缺省值	盒式交换机缺省值
IGMP	60s	60s
IGMP Snooping	60s	125s

步骤3 检查是否禁止了路由器端口动态学习功能。

如果配置了禁止VLAN的路由器端口动态学习功能，VLAN不再侦听IGMP Query报文，无法生成路由器端口。

执行**display igmp-snooping configuration**命令查看配置信息，如果有“undo igmp-snooping router-learning”，在VLAN下执行**igmp-snooping router-learning**命令使能VLAN的路由器端口动态学习功能。

步骤4 检查是否配置了成员端口快速离开功能。

当接口下仅有一个成员主机时，才能配置快速离开功能。如果接口下不止一个接收主机，而在VLAN配置了成员端口快速离开功能，则当交换机从成员端口收到IGMP Leave报文时，不发送特定组查询报文，立即将该接口的转发表项从设备的组播转发表中删除，导致流量不通。

执行**display igmp-snooping configuration**命令查看配置信息，如果有“igmp-snooping prompt-leave”，在VLAN视图下，执行**undo igmp-snooping prompt-leave**命令，取消成员端口快速离开功能。

步骤5 检查是否配置了检查Router-Alert选项功能。

如果配置了对Router-Alert选项进行检查，则交换机会检查IGMP报文中的Option字段，对于未携带Router-Alert选项的报文做丢弃处理。

执行**display igmp-snooping configuration**命令查看配置信息，如果有“igmp-snooping require-router-alert”，在VLAN视图下，执行**undo igmp-snooping require-router-alert**命令，取消相关配置。

步骤6 检查是否配置了组播组过滤策略。

如果配置了组播组过滤策略，可能限制了VLAN下的主机加入组播组的范围，可以执行**display igmp-snooping configuration**命令，查看组播组策略限制是否正确。如果配置了ACL规则，再执行**display acl**命令查看对应的ACL规则是否正确。

步骤7 检查是否配置了接口下的二层组播数据过滤功能。

如果设备接口下配置了二层组播数据过滤功能，会对来自某VLAN的UDP报文进行过滤，导致二层组播流量不通。

进入物理接口视图，执行**undo multicast-source-deny**命令，取消接口下的二层组播数据过滤功能。

----结束

6.11.2 配置的组播组策略不生效

故障现象

在设备上配置了组播组策略，只允许主机加入某些特定的组播组，但主机仍然可以收到发往其他组播组的组播数据。

操作步骤

步骤1 执行**display acl**命令查看配置的ACL规则，检查其是否匹配想要执行的组播组过滤策略。

步骤2 执行**display igmp-snooping configuration**命令查看VLAN下是否应用了正确的组播组策略。如果没有，则使用**igmp-snooping group-policy**命令应用正确的组播组策略。

步骤3 执行**display current-configuration | include drop-unknown**命令查看是否已使能丢弃未知组播数据报文的功能。如果没有使能，则使用**multicast drop-unknown**命令使能丢弃未知组播数据报文功能。

----结束

7 组播 VLAN 配置

关于本章

组播VLAN复制功能可以使三层设备只需把组播数据传送给该组播VLAN，而不必再为每个用户VLAN都复制一份组播报文，减少带宽浪费。

7.1 组播VLAN概述
组播VLAN一般部署于设备的网络侧来实现组播流汇聚，然后将组播报文在用户VLAN内复制分发。

7.2 设备支持的组播VLAN特性
设备支持基于用户VLAN和基于接口两种方式配置组播VLAN复制功能，可根据不同的应用场景来选择基于何种方式配置组播VLAN复制功能。

7.3 缺省配置
介绍缺省情况下，组播VLAN的配置信息。

7.4 配置基于用户VLAN的组播VLAN一对多
通过配置基于用户VLAN的组播VLAN一对多，可以实现组播数据在不同用户VLAN间复制分发，减少上游带宽浪费。

7.5 配置基于用户VLAN的组播VLAN多对多
通过配置基于用户VLAN的组播VLAN多对多，能够使单个用户VLAN绑定到多个组播VLAN，弥补了组播VLAN一对多中一个用户VLAN只能加入一个组播VLAN的不足。

7.6 配置基于接口的组播VLAN功能
通过配置基于接口的组播VLAN功能，可以实现同一用户VLAN中不同用户之间的组播业务隔离，增强了对组播业务流量的控制。

7.7 配置举例
介绍组播VLAN复制功能的配置举例。

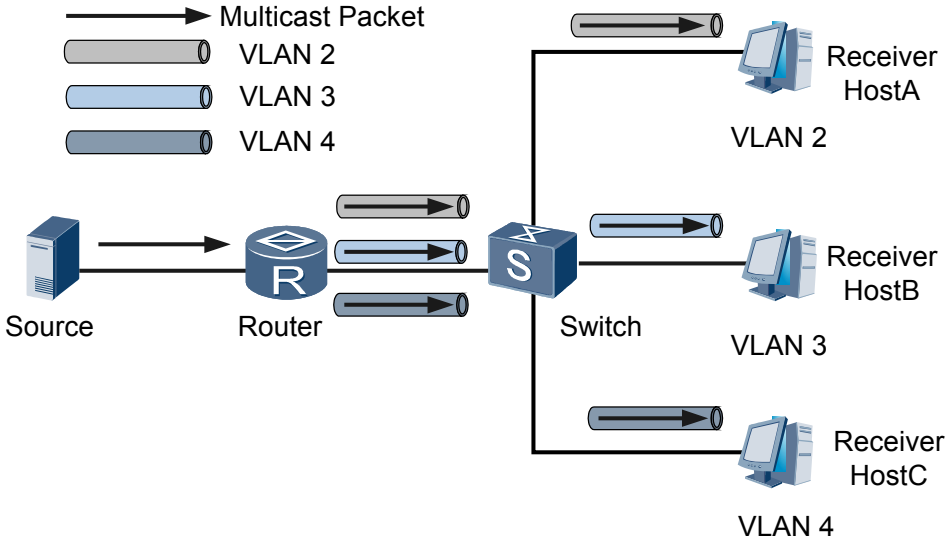
7.8 常见配置错误
介绍了常见的配置错误的故障现象以及处理步骤。

7.1 组播 VLAN 概述

组播VLAN一般部署于设备的网络侧来实现组播流汇聚，然后将组播报文在用户VLAN内复制分发。

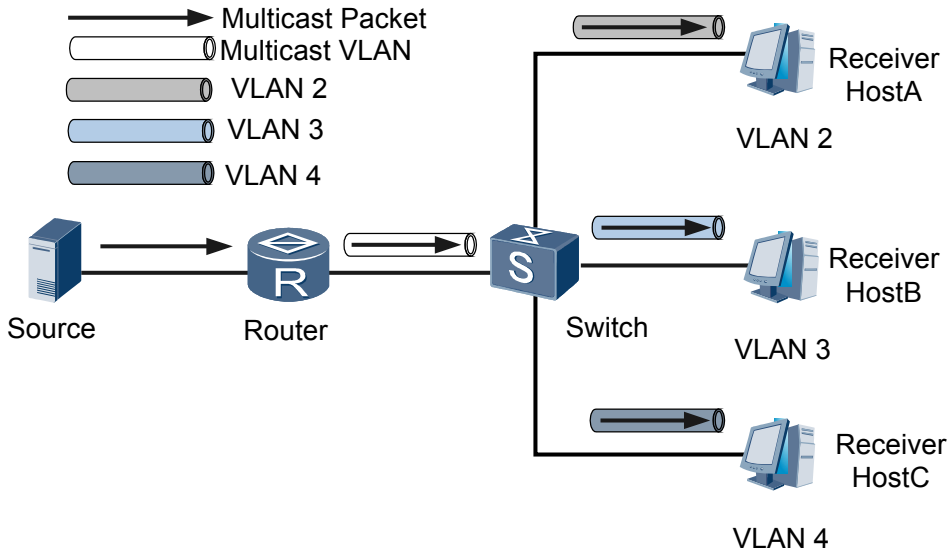
如图7-1所示，在传统的组播点播方式下，当属于不同VLAN的主机HostA、HostB和HostC同时点播同一组播组时，三层设备（Router）需要把组播数据在每个用户VLAN（即主机所属的VLAN）内都复制一份发送给二层设备（Switch）。这样既造成了带宽的浪费，也给三层设备增加了额外的负担。

图 7-1 未运行组播 VLAN 时的组播数据传输



可以使用组播VLAN功能解决这个问题。图7-2所示，在二层设备上配置了组播VLAN后，三层设备（Router）只需把组播数据在组播VLAN内复制一份发送给二层设备（Switch），而不必在每个用户VLAN内都复制一份，从而节省了网络带宽，也减轻了三层设备的负担。

图 7-2 运行组播 VLAN 时的组播数据传输



7.2 设备支持的组播 VLAN 特性

设备支持基于用户VLAN和基于接口两种方式配置组播VLAN复制功能，可根据不同的应用场景来选择基于何种方式配置组播VLAN复制功能。

说明

组播VLAN作为一个二层组播特性，本章中涉及到接口的配置，都是在二层物理接口（包括Eth-Trunk接口）下进行配置。

建议对组播源发出的组播数据报文设置一个合理的TTL值，保证设备通过组播VLAN接收到该报文时，其TTL值大于1。否则可能造成无法向用户VLAN正常转发。

基于用户 VLAN 的组播 VLAN 功能

交换机支持将用户VLAN与组播VLAN进行绑定，实现在不同的用户VLAN间进行组播报文复制，并且包含以下两种方式。

- 组播VLAN一对多

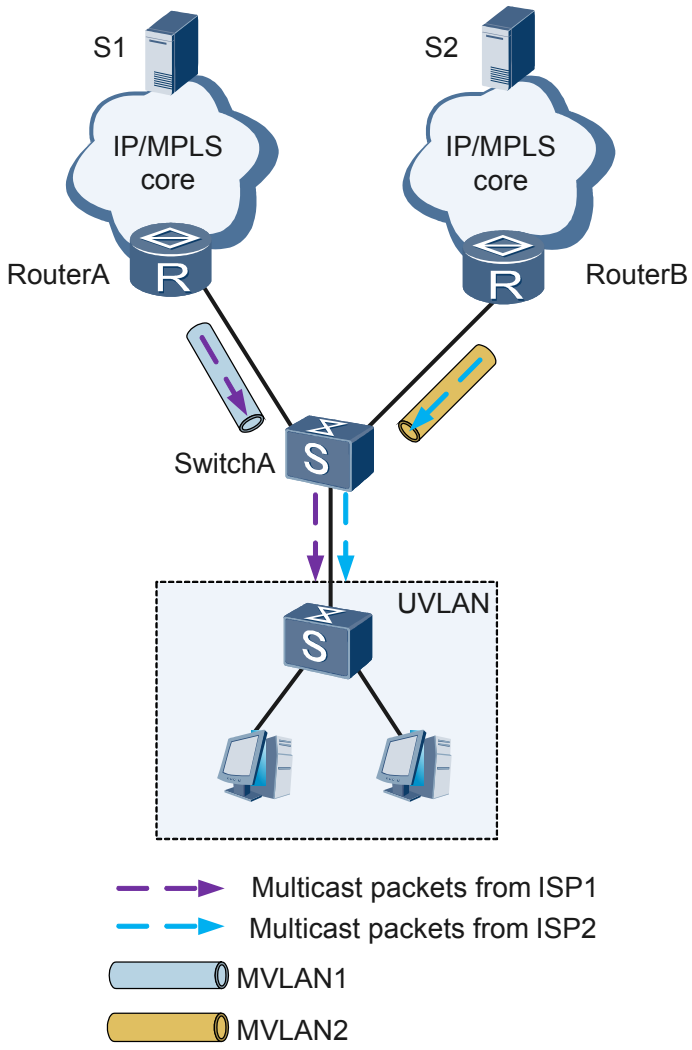
  组播VLAN一对多为传统的基于用户VLAN的组播VLAN复制方式，即多个用户VLAN可以加入一个组播VLAN，但是一个用户VLAN不能加入多个组播VLAN。组播VLAN一对多提供了组播VLAN复制功能中最核心的功能：上游设备只需要向配置了组播VLAN的交换机上发送一份组播数据，然后交换机再将其复制分发到有相同组播需求的不同用户VLAN中，从而减少了上游设备与交换机之间的带宽浪费，即如**7.1 组播VLAN概述**中的**图7-2**所示。

- 组播VLAN多对多

  组播VLAN多对多为组播VLAN一对多的扩展，通过配置静态组播流，实现一个用户VLAN能够加入多个组播VLAN的目的。

  如**图7-3**所示，用户VLAN（UVLAN）中的用户同时定制了多个ISP提供的组播业务。为了便于区分不同ISP的组播业务，可以使用不同的组播VLAN（MVLAN）来标识不同的ISP。然后通过配置组播VLAN多对多功能，用户又可以接收来自不同ISP的组播数据。

图 7-3 组播 VLAN 多对多的示意图

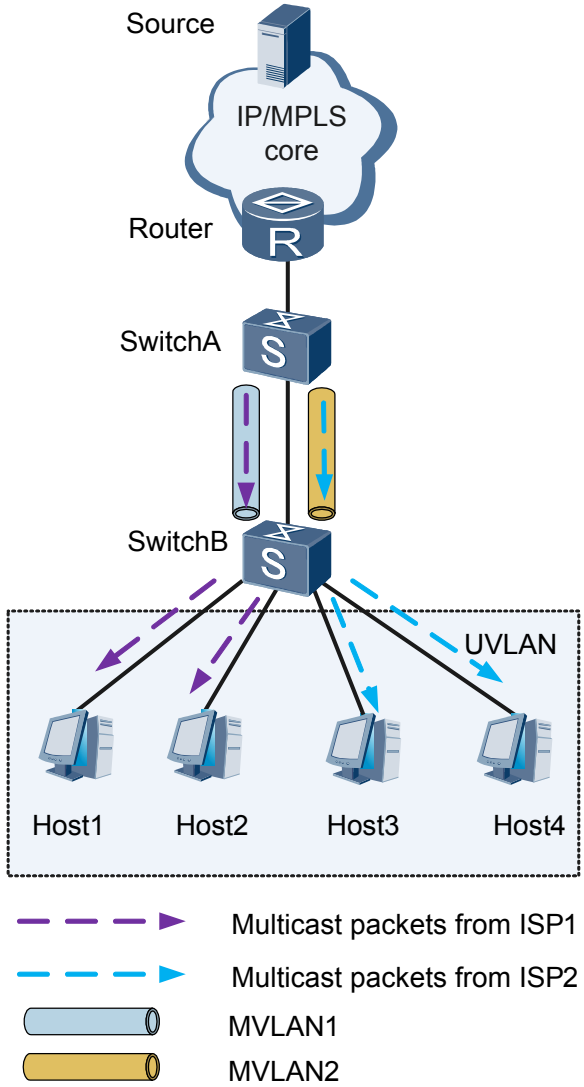


基于接口的组播 VLAN 功能

交换机支持在用户侧接口下配置用户VLAN与组播VLAN进行绑定，不仅能够实现组播数据在不同用户VLAN间进行复制，还可以实现同一用户VLAN中基于接口的组播业务隔离。

同一VLAN中的不同接口绑定不同的组播VLAN，就可以实现同一VLAN中基于接口的组播业务隔离。如图7-4所示，组播业务批发给了ISP1、ISP2两个服务商，用户VLAN（UVLAN）中的Host1、Host2定制的是ISP1提供的服务，Host3、Host4定制的是ISP2提供的。为了使两个ISP提供的组播数据不会发送到所有的用户主机上，给ISP1、ISP2分别分配一个组播VLAN（MVLAN1、MVLAN2），在Hos1、Host2接入接口上配置UVLAN与MVLAN1绑定，Host3、Host4接入接口上配置UVLAN与MVLAN2绑定。这样，ISP1提供的组播数据只向Host1、Host2发送，ISP2提供的组播数据只向Host3、Host4发送。

图 7-4 基于接口的组播 VLAN 示意图



7.3 缺省配置

介绍缺省情况下，组播VLAN的配置信息。

表7-1列出了组播VLAN的缺省配置。

表 7-1 组播 VLAN 缺省配置

参数	缺省值
基于用户VLAN的组播VLAN功能	未使能
静态组播流触发功能	未使能

7.4 配置基于用户 VLAN 的组播 VLAN 一对多

通过配置基于用户VLAN的组播VLAN一对多，可以实现组播数据在不同用户VLAN间复制分发，减少上游带宽浪费。

配置流程

说明

目前交换机在IPv4网络和IPv6网络都支持配置组播VLAN一对多。两种网络在配置时并无差异，都需要结合二层组播侦听功能（IPv4网络为IGMP Snooping，IPv6网络为MLD Snooping）来实现，下面是IPv4网络的配置流程。

按如下配置顺序进行配置：

7.4.1 配置用户 VLAN

背景信息

配置基于用户VLAN的组播VLAN一对多功能时，需要在用户VLAN下使能二层组播侦听功能。

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

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

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

----结束

7.4.2 配置组播 VLAN

背景信息

组播VLAN是实现组播VLAN复制功能的基础，它的主要作用就是用来汇聚网络侧的组播流，然后将组播流在其对应的用户VLAN内复制分发。同时，在配置基于用户VLAN的组播VLAN功能时，组播VLAN也需要使能二层组播侦听功能。

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

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

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

步骤5 （可选）执行命令**igmp-snooping querier enable**，使能VLAN的IGMP Snooping查询器功能。

说明

建议在组播VLAN视图下配置步骤5。如果上游设备作为网关，使能了IGMP功能，就可以不用配置步骤5。

步骤6 执行命令**multicast-vlan enable**，使能组播VLAN功能，将当前VLAN配置为组播VLAN。

步骤7 执行命令**multicast-vlan user-vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，配置组播VLAN和用户VLAN的对应关系，将用户VLAN绑定到组播VLAN。

说明

配置组播VLAN和用户VLAN的对应关系时，一个用户VLAN只能绑定到一个组播VLAN。

步骤8 （可选）执行命令**multicast-vlan send-query prune-source-port**，禁止组播VLAN收到通用查询报文后，通过用户VLAN从上行接口回传。

缺省情况下，如果上行接口加入组播VLAN的同时，也加入了用户VLAN，组播VLAN收到通用查询报文后，允许查询报文通过用户VLAN从上行接口转发回去。如果不希望上游设备收到回传的查询报文，可以配置该命令避免查询报文从上行接口转发回去。

----结束

7.4.3 配置接口加入 VLAN

背景信息

组播VLAN和用户VLAN配置完成后，网络侧接口需要加入组播VLAN，用户侧接口需要加入用户VLAN。

说明

S2700EI在配置组播VLAN时，用户侧接口必须以相同方式同时加入组播VLAN和用户VLAN。如果单个用户侧接口加入了两个或者两个以上的用户VLAN，只有第一个上送Report报文的用户VLAN才会实现组播VLAN复制功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 将网络侧接口加入组播VLAN。详细配置过程请参见基于接口划分VLAN。

注意

如果S2700EI的网络侧接口同时加入了用户VLAN，则需要在网络侧接口入方向使用流量策略禁止发送到用户VLAN的IGMP报文上送到CPU，否则可能会导致CPU负载过高。例如：用户VLAN为VLAN100和VLAN200，组播VLAN为VLAN1000，网络侧接口为GE0/0/1,则可以进行以下配置：

```
<Quidway> system-view
[Quidway] acl 3000
[Quidway-acl-adv-3000] rule 5 permit igmp
[Quidway-acl-adv-3000] quit
[Quidway] traffic classifier uvlan operator and
[Quidway-classifier-uvlan] if-match vlan-id 100
[Quidway-classifier-uvlan] if-match vlan-id 200
[Quidway-classifier-uvlan] if-match acl 3000
[Quidway-classifier-uvlan] quit
[Quidway] traffic behavior uvlan
[Quidway-behavior-uvlan] deny
[Quidway-behavior-uvlan] quit
[Quidway] traffic classifier mvlan operator and
[Quidway-classifier-mvlan] if-match vlan-id 1000
[Quidway-classifier-mvlan] if-match acl 3000
[Quidway] traffic behavior mvlan
[Quidway-behavior-mvlan] permit
[Quidway-behavior-mvlan] quit
[Quidway] traffic policy igmp
[Quidway-trafficpolicy-igmp] classifier mvlan behavior mvlan
[Quidway-trafficpolicy-igmp] classifier uvlan behavior uvlan
[Quidway] interface gigabitethernet0/0/1
[Quidway-GigabitEthernet0/0/1] traffic-policy igmp inbound
```

步骤3 将用户侧接口加入用户VLAN。详细配置过程请参见基于接口划分VLAN。

----结束

7.4.4 检查配置结果

前提条件

已经完成组播VLAN功能的配置。

操作步骤

- 使用命令**display multicast-vlan vlan** [*vlan-id*]，查看组播VLAN的信息。
- 使用命令**display user-vlan vlan** [*vlan-id*]，查看用户VLAN信息。

----结束

7.5 配置基于用户 VLAN 的组播 VLAN 多对多

通过配置基于用户VLAN的组播VLAN多对多，能够使单个用户VLAN绑定到多个组播VLAN，弥补了组播VLAN一对多中一个用户VLAN只能加入一个组播VLAN的不足。

产品	支持情况
S2700	不支持

产品	支持情况
S3700	支持

配置流程

说明

目前交换机在IPv4网络和IPv6网络都支持配置组播VLAN多对多。两种网络在配置时并无差异，都需要结合二层组播侦听功能（IPv4网络为IGMP Snooping，IPv6网络为MLD Snooping）来实现，下面是IPv4网络的配置步骤。

按如下配置顺序进行配置：

7.5.1 配置用户 VLAN

背景信息

配置基于用户VLAN的组播VLAN多对多功能时，在用户VLAN下不仅需要使能二层组播侦听功能，还需要使能组播流触发功能。

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

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

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

步骤5 执行命令**multicast flow-trigger enable**，使能VLAN的组播流触发功能。

----结束

7.5.2 配置组播 VLAN

背景信息

在配置基于用户VLAN的组播VLAN多对多功能时，除了需要在组播VLAN下使能二层组播侦听功能，将用户VLAN绑定到组播VLAN之外，还需要在组播VLAN配置静态流。通过在用户VLAN和组播VLAN之间建立基于（UVLAN，Source，Group）的映射关系，在用户VLAN向该组播VLAN发起点播请求时生成组播表项，实现用户VLAN和组播VLAN的多对多映射。

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*，创建VLAN并进入VLAN视图。

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

步骤5 （可选）执行命令**igmp-snooping querier enable**，使能VLAN的IGMP Snooping查询器功能。

说明

建议在组播VLAN视图下配置步骤5。如果上游设备作为网关，使能了IGMP功能，就可以不用配置步骤5。

步骤6 执行命令**multicast-vlan enable**，使能组播VLAN功能，将当前VLAN配置为组播VLAN。

步骤7 执行命令**multicast-vlan user-vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，配置组播VLAN和用户VLAN的对应关系，将用户VLAN绑定到组播VLAN。

步骤8 执行命令**multicast static-flow** *ipv4-group-address* [**source** *ipv4-source-address*]，配置组播VLAN静态流。

配置组播静态流之后，用户VLAN下的用户可以加入组播静态流指定的组播组，并接收其组播数据。

说明

所有组播VLAN的静态流不能重复，组播组相同但源IP不同的两条流被视为两条不同的静态流。

步骤9 （可选）执行命令**multicast-vlan send-query prune-source-port**，禁止组播VLAN收到通用查询报文后，通过用户VLAN从上行接口回传。

缺省情况下，如果上行接口加入组播VLAN的同时，也加入了用户VLAN，组播VLAN收到通用查询报文后，允许查询报文通过用户VLAN从上行接口转发回去。如果不希望上游设备收到回传的查询报文，可以配置该命令避免查询报文从上行接口转发回去。

----结束

7.5.3 配置接口加入 VLAN

背景信息

组播VLAN和用户VLAN配置完成后，网络侧接口需要加入组播VLAN，用户侧接口需要加入用户VLAN。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 将网络侧接口加入组播VLAN。详细配置过程请参见基于接口划分VLAN。

步骤3 将用户侧接口加入用户VLAN。详细配置过程请参见基于接口划分VLAN。

----结束

7.5.4 检查配置结果

前提条件

已经完成基于用户VLAN的组播VLAN多对多功能的配置。

操作步骤

- 使用命令**display multicast-vlan vlan** [*vlan-id*]，查看组播VLAN的信息。

- 使用命令**display user-vlan vlan** [*vlan-id*]，查看用户VLAN信息。
- 使用命令**display multicast static-flow** [**vlan** *vlan-id*]，查看组播VLAN下配置的静态流。

----结束

7.6 配置基于接口的组播 VLAN 功能

通过配置基于接口的组播VLAN功能，可以实现同一用户VLAN中不同用户之间的组播业务隔离，增强了对组播业务流量的控制。

产品	支持情况
S2700	不支持
S3700	支持

配置流程

说明

目前交换机仅支持在IPv4网络配置基于接口的组播VLAN功能。在配置时需要结合IGMP Snooping功能来实现，但是与配置基于用户VLAN的组播VLAN功能有所不同的是，用户VLAN不需要使能IGMP Snooping功能，只需使用命令**vlan** *vlan-id*创建用户VLAN。

按如下配置顺序进行配置：

7.6.1 配置组播 VLAN

背景信息

配置基于接口的组播VLAN功能时，只需要在组播VLAN下使能二层组播侦听功能，不需要使能组播VLAN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**igmp-snooping enable**，使能全局IGMP Snooping功能。

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

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

步骤5 （可选）执行命令**igmp-snooping querier enable**，使能VLAN的IGMP Snooping查询器功能。

说明

建议在组播VLAN视图下配置步骤5。如果上游设备作为网关，使能了IGMP功能，就可以不用配置步骤5。

----结束

7.6.2 配置用户 VLAN 绑定组播 VLAN

背景信息

用户VLAN绑定组播VLAN主要在用户侧接口下进行配置，并且在同一接口下用户VLAN不能绑定到多个组播VLAN。

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**l2-multicast-bind vlan** *vlan-id1* [**to** *vlan-id2*] **mvlan** *mvlan-id*，在接口下配置用户VLAN绑定组播VLAN。

----结束

7.6.3 配置接口加入 VLAN

背景信息

组播VLAN和用户VLAN配置完成后，网络侧接口需要加入组播VLAN，用户侧接口需要加入用户VLAN。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 将网络侧接口加入组播VLAN。详细配置过程请参见基于接口划分VLAN。

步骤3 将用户侧接口加入用户VLAN。详细配置过程请参见基于接口划分VLAN。

----结束

7.6.4 检查配置结果

前提条件

已经完成基于接口的组播VLAN功能的配置。

操作步骤

- 使用命令**display l2-multicast-bind** [**mvlan** *vlan-id*]，查看接口上用户VLAN与组播VLAN的绑定信息。

----结束

7.7 配置举例

介绍组播VLAN复制功能的配置举例。

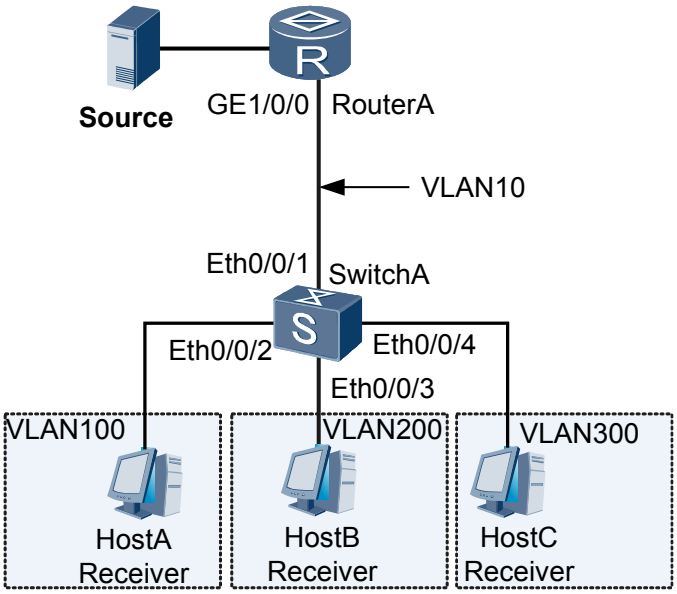
7.7.1 配置基于用户 VLAN 的组播 VLAN 一对多功能示例

组网需求

如图7-5所示，RouterA和SwitchA之间用于传输组播数据的业务VLAN为VLAN 10，而下游用户主机HostA、HostB和HostC分别属于VLAN 100、VLAN 200和VLAN 300，并且都需要接收组播Source的组播数据。

要求通过配置基于用户VLAN的组播VLAN一对多功能，对于不同用户主机多份相同的组播需求，RouterA只需要向VLAN 10发送一份组播数据，减少RouterA与SwitchA之间的带宽浪费。

图 7-5 配置基于用户 VLAN 的组播 VLAN 一对多功能组网图



配置思路

采用如下的思路配置基于用户VLAN的组播VLAN一对多功能：

1. 在系统视图下使能IGMP Snooping。
2. 创建用户VLAN，并在用户VLAN下使能IGMP Snooping。
3. 创建组播VLAN，并在组播VLAN下使能IGMP Snooping。
4. 在组播VLAN下面绑定用户VLAN。
5. 将接口分别以Hybrid方式加入VLAN。

操作步骤

步骤1 在系统视图下使能IGMP Snooping。

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

步骤2 创建用户VLAN，并在用户VLAN下使能IGMP Snooping功能。

```
[SwitchA] vlan 100
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
```

```
[SwitchA] vlan 200
[SwitchA-vlan200] igmp-snooping enable
[SwitchA-vlan200] quit
[SwitchA] vlan 300
[SwitchA-vlan300] igmp-snooping enable
[SwitchA-vlan300] quit
```

步骤3 创建组播VLAN，并在组播VLAN下使能IGMP Snooping功能和IGMP Snooping查询器功能。

说明

建议在组播VLAN视图下配置**igmp-snooping querier enable**。如果上游RouterA作为网关，使能了IGMP功能，就可以不用配置**igmp-snooping querier enable**命令。

```
[SwitchA] vlan 10
[SwitchA-vlan10] igmp-snooping enable
[SwitchA-vlan10] igmp-snooping querier enable
[SwitchA-vlan10] multicast-vlan enable
```

步骤4 在组播VLAN10下面绑定用户VLAN 100、VLAN 200和VLAN 300。

```
[SwitchA-vlan10] multicast-vlan user-vlan 100 200 300
[SwitchA-vlan10] quit
```

步骤5 把接口以Hybrid方式加入VLAN。

把Eth0/0/1接口加入组播VLAN 10。

```
[SwitchA] interface ethernet 0/0/1
[SwitchA-Ethernet0/0/1] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/1] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/1] quit
```

把Eth0/0/2、Eth0/0/3、Eth0/0/4接口分别加入用户VLAN 100、VLAN 200、VLAN 300。

说明

对于S2700EI交换机，用户侧接口在加入用户VLAN的同时，还需要以相同方式加入组播VLAN。

```
[SwitchA] interface ethernet 0/0/2
[SwitchA-Ethernet0/0/2] port hybrid pvid vlan 100
[SwitchA-Ethernet0/0/2] port hybrid untagged vlan 100
[SwitchA-Ethernet0/0/2] quit
[SwitchA] interface ethernet 0/0/3
[SwitchA-Ethernet0/0/3] port hybrid pvid vlan 200
[SwitchA-Ethernet0/0/3] port hybrid untagged vlan 200
[SwitchA-Ethernet0/0/3] quit
[SwitchA] interface ethernet 0/0/4
[SwitchA-Ethernet0/0/4] port hybrid pvid vlan 300
[SwitchA-Ethernet0/0/4] port hybrid untagged vlan 300
[SwitchA-Ethernet0/0/4] quit
```

步骤6 验证配置结果，在SwitchA可以查看到组播VLAN和用户VLAN的信息。

```
[SwitchA] display multicast-vlan vlan
Total multicast vlan   1
 multicast-vlan     user-vlan number     snooping-state
 ------------------------------------------------------------------------
 10                 3                    IGMP Enable /MLD Disable
[SwitchA] display user-vlan vlan
 Total user vlan   3
 user-vlan  snooping-state            multicast-vlan  snooping-state
 ------------------------------------------------------------------------------
 100        IGMP Enable /MLD Disable  10              IGMP Enable /MLD Disable
 200        IGMP Enable /MLD Disable  10              IGMP Enable /MLD Disable
 300        IGMP Enable /MLD Disable  10              IGMP Enable /MLD Disable
```

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10 100 200 300
#
igmp-snooping enable
#
vlan 10
 igmp-snooping enable
 igmp-snooping querier enable
 multicast-vlan enable
 multicast-vlan user-vlan 100 200 300
#
vlan 100
 igmp-snooping enable
vlan 200
 igmp-snooping enable
vlan 300
 igmp-snooping enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface Ethernet0/0/3
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface Ethernet0/0/4
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
return
```

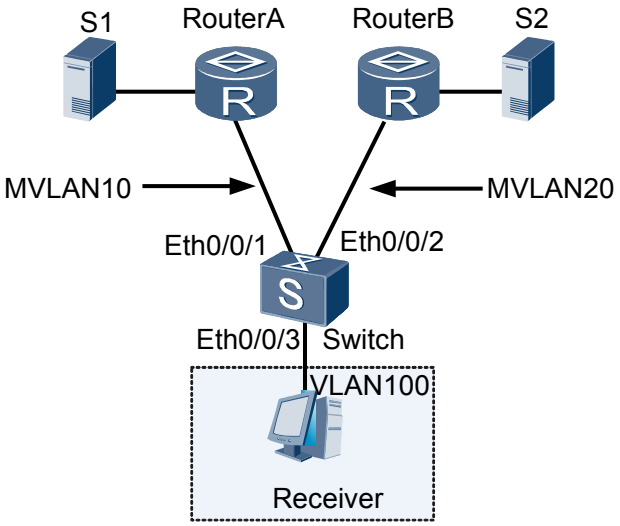
7.7.2 配置基于用户 VLAN 的组播 VLAN 多对多功能示例

组网需求

如图7-6所示，交换机通过Eth0/0/1接口和RouterA相连，通过Eth0/0/2接口和RouterB相连，通过Eth0/0/3连接用户主机；组播源S1、S2为不同ISP提供的组播源。

要求通过配置基于用户VLAN的组播VLAN多对多功能，用不同的组播VLAN标识不同的ISP，并且用户主机能够同时接收S1发往组播组225.1.1.1、S2发往组播组225.1.2.1的组播数据。

图 7-6 配置基于用户 VLAN 的组播 VLAN 多对多组网图



配置思路

采用如下的思路配置基于用户VLAN的组播VLAN多对多：

1. 在系统视图下使能IGMP Snooping。
2. 创建用户VLAN，并在用户VLAN下使能IGMP Snooping，并在用户VLAN下使能组播流触发功能。
3. 创建组播VLAN，并在组播VLAN下使能IGMP Snooping。
4. 用户VLAN加入多个组播VLAN，并且在组播VLAN下配置静态组播流。
5. 将接口分别以Hybrid方式加入VLAN。

操作步骤

步骤1 在系统视图下使能IGMP Snooping。

```
<Switch> system-view
[Switch] igmp-snooping enable
```

步骤2 创建用户VLAN100，在用户VLAN下使能IGMP Snooping功能，并在用户VLAN下使能组播流触发功能。

```
[Switch] vlan 100
[Switch-vlan100] igmp-snooping enable
[Switch-vlan100] multicast flow-trigger enable
[Switch-vlan100] quit
```

步骤3 创建组播VLAN10和组播VLAN20，并在组播VLAN下使能IGMP Snooping功能和IGMP Snooping查询器功能。

说明

建议在组播VLAN视图下配置**igmp-snooping querier enable**。如果上游RouterA和RouterB作为网关，都使能了IGMP功能，就可以不用配置**igmp-snooping querier enable**命令。

```
[Switch] vlan 10
[Switch-vlan10] igmp-snooping enable
[Switch-vlan10] igmp-snooping querier enable
[Switch-vlan10] multicast-vlan enable
[Switch-vlan10] quit
[Switch] vlan 20
[Switch-vlan20] igmp-snooping enable
[Switch-vlan20] igmp-snooping querier enable
```

```
[Switch-vlan20] multicast-vlan enable
[Switch-vlan20] quit
```

步骤4 用户VLAN100加入组播VLAN10和组播VLAN20，并且在组播VLAN下配置静态组播流。

```
[Switch] vlan 10
[Switch-vlan10] multicast-vlan user-vlan 100
[Switch-vlan10] multicast static-flow 225.1.1.1
[Switch-vlan10] quit
[Switch] vlan 20
[Switch-vlan20] multicast-vlan user-vlan 100
[Switch-vlan20] multicast static-flow 225.1.2.1
[Switch-vlan20] quit
```

步骤5 把接口以Hybrid方式加入VLAN。

把Eth0/0/1接口加入组播VLAN10，Eth0/0/2接口加入组播VLAN20。

```
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] port hybrid pvid vlan 10
[Switch-Ethernet0/0/1] port hybrid untagged vlan 10
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/2
[Switch-Ethernet0/0/2] port hybrid pvid vlan 20
[Switch-Ethernet0/0/2] port hybrid untagged vlan 20
[Switch-Ethernet0/0/2] quit
```

把Eth0/0/3接口加入用户VLAN100。

```
[Switch] interface ethernet 0/0/3
[Switch-Ethernet0/0/3] port hybrid pvid vlan 100
[Switch-Ethernet0/0/3] port hybrid untagged vlan 100
[Switch-Ethernet0/0/3] quit
```

步骤6 验证配置结果

在Switch使用**display user-vlan vlan**命令可以查看到用户VLAN同时就加入到了组播VLAN10和组播VLAN20。

```
[Switch] display user-vlan vlan
 Total user vlan   2
 user-vlan  snooping-state           multicast-vlan  snooping-state
 ------------------------------------------------------------------------------
 100        IGMP Enable /MLD Disable  10             IGMP Enable /MLD Disable
 100        IGMP Enable /MLD Disable  20             IGMP Enable /MLD Disable
```

使用**display multicast static-flow**命令可以查看到组播VLAN下面配置的组播静态流信息，说明用户VLAN下用户可以加入指定的组播组。

```
[Switch] display multicast static-flow
 ------------------------------------------------------------------
 Vlan                                      (Source, Group)
 ------------------------------------------------------------------
  10                                        (*, 225.1.1.1)
  20                                        (*, 225.1.2.1)
 ------------------------------------------------------------------
 Total Table(s) : 2
```

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 10 20 100
```

```
#
igmp-snooping enable
#
vlan 10
 igmp-snooping enable
 igmp-snooping querier enable
 multicast-vlan enable
 multicast static-flow 225.1.1.1
 multicast-vlan user-vlan 100
#
vlan 20
 igmp-snooping enable
 igmp-snooping querier enable
 multicast-vlan enable
 multicast static-flow 225.1.2.1
 multicast-vlan user-vlan 100
#
vlan 100
 multicast flow-trigger enable
 igmp-snooping enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/3
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

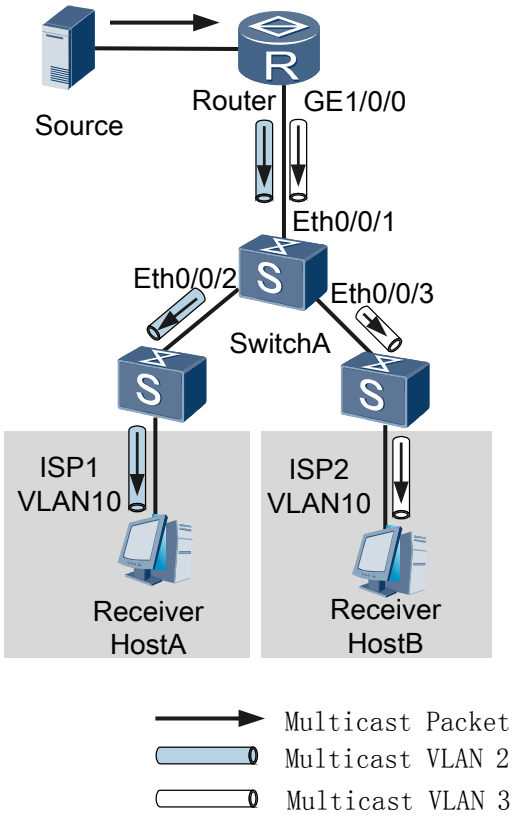
7.7.3 配置基于接口的组播 VLAN 功能示例

组网需求

在如图7-7所示的网络中，SwitchA上的Eth0/0/1接口连接路由器，Eth0/0/2和Eth0/0/3接口下的业务分别批发给ISP1和ISP2，ISP1和ISP2分别通过组播VLAN 2和组播VLAN 3传输组播数据。Eth0/0/2和Eth0/0/3接口下用户VLAN重复，都为VLAN 10。

为了防止不同ISP的组播报文会发送到不属于此ISP的用户，影响到ISP的利益，要求通过基于接口的组播VLAN功能，指定属于本ISP的组播数据只转发到连接本ISP用户的接口。

图 7-7 配置基于接口的组播 VLAN 功能组网图



配置思路

采用如下的思路配置基于接口组播VLAN功能：

1. 在系统视图下使能IGMP Snooping功能。
2. 创建用户VLAN 10。
3. 创建组播VLAN 2和组播VLAN 3，并在组播VLAN下使能IGMP Snooping。
4. 在Eth0/0/2接口和Eth0/0/3接口下对组播VLAN和用户VLAN分别进行绑定。
5. 将接口分别以Hybrid方式加入VLAN。

操作步骤

步骤1 创建用户VLAN 10。

```
<SwitchA> system-view
[SwitchA] vlan batch 10
```

步骤2 配置组播VLAN 2和组播VLAN 3，并在组播VLAN下使能IGMP Snooping功能和IGMP Snooping查询器功能。

说明

建议在组播VLAN视图下配置**igmp-snooping querier enable**。如果上游Router作为网关，使能了IGMP功能，就可以不用配置**igmp-snooping querier enable**命令。

```
[SwitchA] igmp-snooping enable
[SwitchA] vlan 2
[SwitchA-vlan2] igmp-snooping enable
[SwitchA-vlan2] igmp-snooping querier enable
[SwitchA-vlan2] quit
[SwitchA] vlan 3
```

```
[SwitchA-vlan3] igmp-snooping enable
[SwitchA-vlan3] igmp-snooping querier enable
[SwitchA-vlan3] quit
```

步骤3 在Eth0/0/2接口和Eth0/0/3接口下分别对组播VLAN和用户VLAN进行绑定。

```
[SwitchA] interface ethernet 0/0/2
[SwitchA-Ethernet0/0/2] l2-multicast-bind vlan 10 mvlan 2
[SwitchA-Ethernet0/0/2] quit
[SwitchA] interface ethernet 0/0/3
[SwitchA-Ethernet0/0/3] l2-multicast-bind vlan 10 mvlan 3
[SwitchA-Ethernet0/0/3] quit
```

步骤4 将Eth0/0/1接口加入组播VLAN，将Eth0/0/2和Eth0/0/3加入用户VLAN。

以Trunk方式把Eth0/0/1加入组播VLAN 2和组播VLAN 3。

```
[SwitchA] interface ethernet 0/0/1
[SwitchA-Ethernet0/0/1] port link-type trunk
[SwitchA-Ethernet0/0/1] port trunk allow-pass vlan 2 3
[SwitchA-Ethernet0/0/1] quit
```

把Eth0/0/2、Eth0/0/3接口分别以Hybrid方式加入用户VLAN 10。

```
[SwitchA] interface ethernet 0/0/2
[SwitchA-Ethernet0/0/2] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/2] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/2] quit
[SwitchA] interface ethernet 0/0/3
[SwitchA-Ethernet0/0/3] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/3] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/3] quit
```

步骤5 验证配置结果。

在SwitchA上是使用**display l2-multicast-bind**命令查看接口下用户VLAN与组播VLAN的绑定信息。

```
[SwitchA] display l2-multicast-bind
 ------------------------------------------------------------------------------
Port                            Startvlan        Endvlan         Mvlan
 ------------------------------------------------------------------------------
Ethernet0/0/2                       10             --             2
Ethernet0/0/3                       10             --             3
 ------------------------------------------------------------------------------
Total Table(s) : 2
```

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 2 to 3 10
#
igmp-snooping enable
#
vlan 2
 igmp-snooping enable
 igmp-snooping querier enable
vlan 3
 igmp-snooping enable
 igmp-snooping querier enable
#
interface Ethernet0/0/1
 port link-type trunk
```

```
 port trunk allow-pass vlan 2 to 3
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 l2-multicast-bind vlan 10 mvlan 2
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 l2-multicast-bind vlan 10 mvlan 3
#
return
```

7.8 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。

7.8.1 用户 VLAN 下用户主机接收不到组播数据

故障现象

配置了基于用户VLAN的组播VLAN功能后，用户VLAN下的用户主机接收不到组播数据。

操作步骤

- 检查组播VLAN配置是否正确。

  执行**display multicast-vlan vlan** *vlan-id*命令，查看用户VLAN是否绑定了正确的组播VLAN。

  - 如果组播VLAN与用户VLAN的绑定关系不正确，请执行**multicast-vlan user-vlan**命令正确配置。
  - 如果组播VLAN与用户VLAN的绑定关系正确，请检查是否与二层组播其他配置存在冲突，导致流量不通。

    如下所示组播VLAN10和用户VLAN100、VLAN200的绑定关系正确。

    ```
    [Quidway] display multicast-vlan vlan 10
     Multicast-vlan         : 10
     User-vlan Number       : 2
     IGMP snooping state    : Enable
     MLD  snooping state    : Disable
     Prune-source-port state: Disable
     User-vlan              Snooping-state
     ----------------------------------------------
     100                     IGMP Enable /MLD Disable
     200                     IGMP Enable /MLD Disable
    ```

----结束

8 可控组播配置

关于本章

通过配置可控组播，可以灵活控制用户加入组播组的权限，满足IPTV业务灵活可控的需求。

8.1 可控组播概述
可控组播全称Controllable Multicast，主要通过组播组、组播组列表、组播模板在内的三级控制机制来灵活的配置用户的组播权限。

8.2 基本概念
介绍可控组播中组播组、组播组列表、组播模板三个基本概念。

8.3 配置可控组播功能
当需要对用户加入组播组的权限进行控制时，可以配置可控组播。

8.4 配置举例
介绍可控组播功能的配置举例。

8.5 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。

8.1 可控组播概述

可控组播全称Controllable Multicast，主要通过组播组、组播组列表、组播模板在内的三级控制机制来灵活的配置用户的组播权限。

传统的组播业务是不可控的，用户可以通过发送IGMP/MLD Report报文来加入某个组播组，从而接收该组播组的组播报文。随着IPTV业务的逐步开展，这种不可控的组播业务已经无法适应运营需求。IPTV业务是以盈利为目的的电信业务，用户只有通过缴纳费用才能收看某个节目（加入组播组），如果不能对用户进行鉴权，则无法满足IPTV的运营需求。可控组播正是在这种背景下提出的，其核心思想就是控制用户加入某个组播组的权限。当用户请求加入某个组播组时，交换机设备必须对这个请求进行鉴权，拒绝非法或越权的请求。

交换机的可控组播通过拦截IGMP/MLD Report报文，控制二层组播转发表项的生成来达到组播控制目的。当收到用户的IGMP/MLD Report报文后，根据报文所属的VLAN找到其使用的模板，如果组播组不在模板的列表下，则认为用户对该组没有权限，拦截此IGMP/MLD Report报文，不让其生成转发表项，从而使用户接收不到该组播组的数据流。如果组播组在模板的列表下，则看列表以哪种方式加入模板，如果列表以观看方式加入模板，则让IGMP/MLD Report报文通过。如果列表以预览方式加入模板，也让IGMP/MLD Report报文通过，但同时启动一个定时器，当预览时间超时就删除该组播组的转发表项，并拦截该组播组后续的IGMP/MLD Report报文。从而实现预览功能。

8.2 基本概念

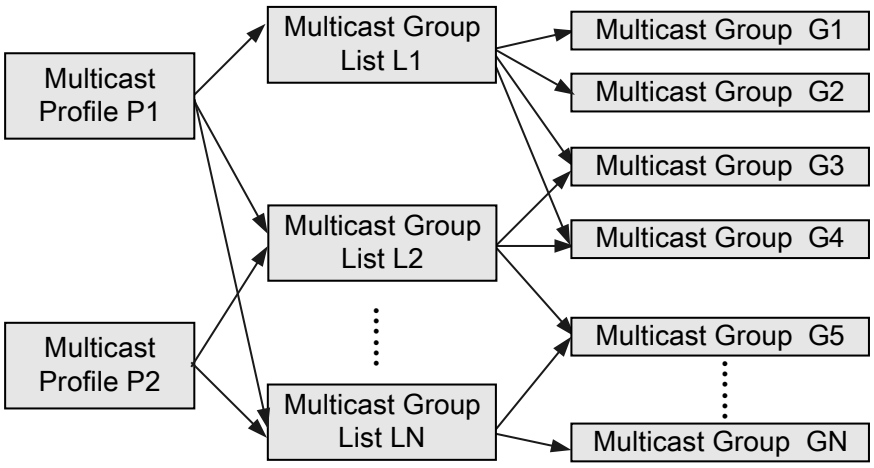
介绍可控组播中组播组、组播组列表、组播模板三个基本概念。

说明

可控组播作为一个二层组播特性，本章中涉及到接口的配置，都是在二层物理接口（包括Eth-Trunk接口）下进行配置。

交换机提供了基于VLAN的可控组播机制，通过配置组播模板（Multicast Profile）来实现对用户组播权限的控制。为了更灵活的配置用户的组播权限，交换机提供了包括组播组、组播组列表、组播模板在内的三级控制机制，如图8-1所示。

图 8-1 可控组播的分级控制机制



组播组

一个组播组对应一个组播地址，例如224.1.1.1。可理解为IPTV的一个频道（Channel）或者节目（Program）。

组播组列表

组播组列表是一系列组播组的集合。一个组播组列表可包含若干个组播组，例如图8-1中，组播组列表L1包含了组播组G1、G2、G3、G4。一个组播组也可以被若干个组播组列表包含，例如组播组G3被组播组列表L1、L2所包含。

组播模板

组播模板定义了用户组播权限的框架，它是一系列组播组列表的集合。一个组播模板可包含若干个组播组列表，例如图8-1中，组播模板P1包含了组播组列表L1、L2、L3。一个组播组列表也可以被若干个组播模板包含，例如组播组列表L2被组播模板P1、P2所包含。加入模板的列表都有其属性（观看或预览），如果列表是以观看属性加入模板，则模板的用户可观看列表下的所有组播组；如果列表是以预览属性加入模板，则模板的用户只能预览列表下的所有组播组。

8.3 配置可控组播功能

当需要对用户加入组播组的权限进行控制时，可以配置可控组播。

前置任务

在配置可控组播之前，需先配置二层组播（IGMP/MLD Snooping），实现组播报文的正常转发。

配置流程

按如下配置顺序进行配置：

8.3.1 配置组播组

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**btv**，进入BTV视图。

步骤3 执行命令**multicast-group** *group-name* { **ip-address** *ipv4-group-address* [**source** *ipv4-source-address*] | **ipv6-address** *ipv6-group-address* [**source** *ipv6-source-address*] }，配置组播组。

说明

- 如果用户接入使用的是IGMPv1或者IGMPv2版本，不需要配置*ipv4-source-address*参数，如果使用的是IGMPv3版本，可以配置*ipv4-source-address*参数。
- 如果用户接入使用的是MLDv1版本，不需要配置*ipv6-source-address*参数，如果使用的是MLDv2版本，可以配置*ipv6-source-address*参数。
- 如果配置的组播组与已配置的组播组地址相同，只是*group-name*不同，执行该命令的作用是将原先配置的组播组名称修改为当前配置的组播组名称。

----结束

8.3.2 配置组播列表

背景信息

组播组配置完成后，需要将组播组引用到组播列表中。

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**btv**，进入BTV视图。

步骤3 执行命令**multicast-list** *list-name*，创建组播组列表并进入组播组列表视图。

步骤4 执行命令**add multicast-group** { **name** *group-name* | **index** *start-index* **to** *end-index* }，引用组播组。

----结束

8.3.3 配置组播模板

背景信息

组播列表配置完成后，需要将组播列表引用到组播模板中。组播模板可引用预览和观看两种权限的组播列表。如果引用的组播列表具有预览权限，则表示用户在观看了一段时间之后，就不能再观看节目；如果引用的组播列表具有观看权限，则表示用户可以一直观看节目。

说明

S2700目前不支持节目预览功能。

缺省配置

表8-1列出了组播模板相关的缺省配置。

表 8-1 组播模板相关的缺省配置

参数	缺省值
用户同时接收的组播组最大个数	8
用户预览组播组的时间间隔	5min
用户每次预览组播组的时间长度	5min
用户每天可预览组播组的次数	10

操作步骤

- 配置组播模板引用只具备预览权限的组播列表。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**btv**，进入BTV视图。
  c. 执行命令**multicast-profile** *profile-name*，创建组播模板并进入组播模板视图。
  d. 执行命令**add multicast-list** { **name** *list-name* | **index** *start-index* **to** *end-index* } **preview**，引用只具备预览权限的组播组列表。
  e. （可选）执行命令**max-program-num** *max-value*，配置用户同时接收的组播组最大个数。
  f. （可选）执行命令**multicast-preview interval** *interval*，配置用户预览组播组的时间间隔。
  g. （可选）执行命令**multicast-preview minutes** *minutes*，配置用户每次预览组播组的时间长度。
  h. （可选）执行命令**multicast-preview times** *times*，配置用户每天可预览组播组的次数。
- 配置组播模板引用可观看的组播列表。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**btv**，进入BTV视图。
  c. 执行命令**multicast-profile** *profile-name*，创建组播模板并进入组播模板视图。
  d. 执行命令**add multicast-list** { **name** *list-name* | **index** *start-index* **to** *end-index* } **watch**，引用可观看的组播组列表。
  e. （可选）执行命令**max-program-num** *max-value*，配置用户同时接收的组播组最大个数。

----结束

8.3.4 VLAN 上应用组播模板

背景信息

组播模板配置完成后，整个可控组播的三级控制机制就已经配置完成，然后就需要在VLAN上应用，对VLAN内的用户请求进行鉴权。

说明

配置基于用户VLAN的组播VLAN时，如果需要应用组播模板，只能将组播模板绑定到用户VLAN上。

配置基于接口的组播VLAN时，如果需要应用组播模板，只能将组播模板绑定到组播VLAN上。

如果VLAN绑定了多个组播模板，但是模板中有相同组播组时，在实际应用中针对该相同的组播组先绑定的组播模板生效。

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**attach multicast-profile** *profile-name* [**interface** *interface-type interface-number* | **mac-address** *mac-address*] *，配置VLAN与组播模板的绑定关系。

一个VLAN下面可以绑定多个组播模板。

说明

可控组播配置支持“接口+VLAN”的控制方式，即将多个用户侧接口绑定在同一个VLAN中的控制方式，此时需要指定**interface** *interface-type interface-number*参数为这些接口分别指定组播模板。

步骤4 （可选）执行命令**max-program-num** *max-value* [**interface** *interface-type interface-number* | **mac-address** *mac-address*] *，配置用户同时接收的组播组最大个数。

说明

用户同时接收的组播组最大个数也可在组播模板视图下使用命令**max-program-num** *max-value*配置。如果在VLAN和该VLAN所绑定的组播模板上都配置了用户同时接收的组播组最大个数，仅VLAN上配置的生效；如果在VLAN上未配置用户同时接收的组播组最大个数:

- 若该VLAN只绑定了一个组播模板，组播模板上配置的生效。
- 若该VLAN绑定了多个组播模板，组播模板上配置的都不会生效，取缺省值8。

----结束

8.3.5 检查配置结果

操作步骤

- 使用命令**display multicast-group** [*group-name*]，查看组播组配置信息。
- 使用命令**display multicast-list** [*list-name*]，查看组播组列表配置信息。
- 使用命令**display multicast-profile** [*profile-name* [**verbose**]]，查看组播模板配置信息。
- 使用命令**display multicast-profile-apply**，查看VLAN应用的组播模板。

----结束

8.4 配置举例

介绍可控组播功能的配置举例。

8.4.1 配置可控组播示例

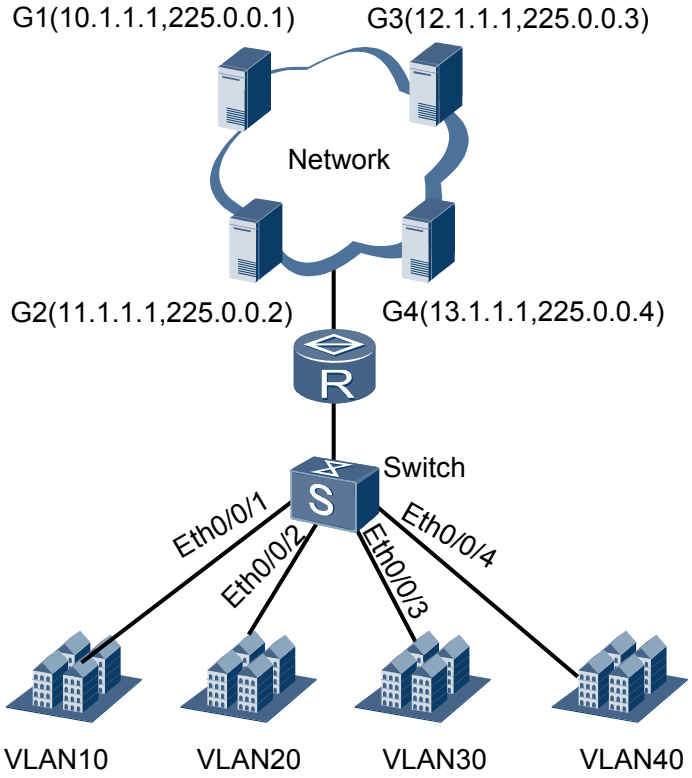
组网需求

如图8-2所示，路由器连接的网络上有组播组G1(225.0.0.1)、G2（225.0.0.2）、G3（225.0.0.3）和G4（225.0.0.4）。现在控制VlAN10和VLAN20的用户只能观看G1和G2；VlAN30和VlAN40的用户可观看所有的组播组。

说明

这里介绍IPv4网络中可控组播的配置示例。IPv6网络的配置示例和IPv4的配置示例类似，只需将配置IGMP Snooping换成配置MLD Snooping即可。

图 8-2 可控组播组网图



配置思路

在Switch上配置可控组播，可实现此需求。配置思路如下：

1. 配置IGMP Snooping。
2. 配置可控组播。
   - 配置两个组播列表L1（G1, G2）和L2（G3，G4）。
   - 配置两个模板P1和P2。

配置步骤

1. 配置用户VLAN，并将接口加入用户VLAN。

```
<Switch> system-view
[Switch] vlan batch 10 20 30 40
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] port hybrid untagged vlan 10
[Switch-Ethernet0/0/1] port hybrid pvid vlan 10
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/2
[Switch-Ethernet0/0/2] port hybrid untagged vlan 20
[Switch-Ethernet0/0/2] port hybrid pvid vlan 20
[Switch-Ethernet0/0/2] quit
[Switch] interface ethernet 0/0/3
[Switch-Ethernet0/0/3] port hybrid untagged vlan 30
[Switch-Ethernet0/0/3] port hybrid pvid vlan 30
[Switch-Ethernet0/0/3] quit
[Switch] interface ethernet 0/0/4
[Switch-Ethernet0/0/4] port hybrid untagged vlan 40
```

```
[Switch-Ethernet0/0/4] port hybrid pvid vlan 40
[Switch-Ethernet0/0/4] quit
```

2. 配置IGMP Snooping。

```
[Switch] igmp-snooping enable
[Switch] vlan 10
[Switch-vlan10] igmp-snooping enable
[Switch-vlan10] quit
[Switch] vlan 20
[Switch-vlan20] igmp-snooping enable
[Switch-vlan20] quit
[Switch] vlan 30
[Switch-vlan30] igmp-snooping enable
[Switch-vlan30] quit
[Switch] vlan 40
[Switch-vlan40] igmp-snooping enable
[Switch-vlan40] quit
```

3. 配置可控组播。

配置组播组。

```
[Switch] btv
[Switch-btv] multicast-group G1 ip-address 225.0.0.1
[Switch-btv] multicast-group G2 ip-address 225.0.0.2
[Switch-btv] multicast-group G3 ip-address 225.0.0.3
[Switch-btv] multicast-group G4 ip-address 225.0.0.4
```

配置组播组列表。

```
[Switch-btv] multicast-list L1
[Switch-btv-list-L1] add multicast-group name G1
[Switch-btv-list-L1] add multicast-group name G2
[Switch-btv-list-L1] quit
[Switch-btv] multicast-list L2
[Switch-btv-list-L2] add multicast-group name G3
[Switch-btv-list-L2] add multicast-group name G4
[Switch-btv-list-L2] quit
```

配置组播模板。

```
[Switch-btv] multicast-profile P1
[Switch-btv-profile-P1] add multicast-list name L1 watch
[Switch-btv-profile-P1] quit
[Switch-btv] multicast-profile P2
[Switch-btv-profile-P2] add multicast-list name L1 watch
[Switch-btv-profile-P2] add multicast-list name L2 watch
[Switch-btv-profile-P2] quit
[Switch-btv] quit
```

在VLAN下应用组播模板。

```
[Switch] vlan 10
[Switch-vlan10] attach multicast-profile P1
[Switch-vlan10] quit
[Switch] vlan 20
[Switch-vlan20] attach multicast-profile P1
[Switch-vlan20] quit
[Switch] vlan 30
[Switch-vlan30] attach multicast-profile P2
[Switch-vlan30] quit
[Switch] vlan 40
[Switch-vlan40] attach multicast-profile P2
[Switch-vlan40] quit
```

4. 检验配置结果。

```
[Switch] display multicast-profile-apply
-------------------------------------------------------------------------------
 Vlan-id  Port                      SMAC                              Max-Users
                    Index                Profile-name
-------------------------------------------------------------------------------
 Vlan10    --                        --                                    8
                     1                     P1
 Vlan20    --                        --                                    8
```

```
                        1                   P1
 Vlan30     --                       --                              8
                        2                   P2
 Vlan40     --                       --                              8
                        2                   P2

 Total: 4
[Switch] display multicast-profile
 ------------------------------------------------------------------------------
 Index        Profile-Name                    Multicast-list  Attach-User
 ------------------------------------------------------------------------------
  1             P1                               1             2
  2             P2                               2             2

 Total: 2
[Switch] display multicast-list
 ------------------------------------------------------------------------
 Index        Multicast-list-name             Multicast-group
 ------------------------------------------------------------------------
  1             L1                                   2
  2             L2                                   2

 Total: 2

[Switch] display multicast-group
-------------------------------------------------------------------------
 Index        Multicast-group-name             Address
 ------------------------------------------------------------------------
  1           G1                              225.0.0.1
  2           G2                              225.0.0.2
  3           G3                              225.0.0.3
  4           G4                              225.0.0.4

 Total: 4
```

配置文件

```
sysname Switch
#
vlan batch 10 20 30 40
#
igmp-snooping enable
#
btv
 multicast-group  G1 ip-address 225.0.0.1
 multicast-group  G2 ip-address 225.0.0.2
 multicast-group  G3 ip-address 225.0.0.3
 multicast-group  G4 ip-address 225.0.0.4
 multicast-list  L1
  add multicast-group name G1
  add multicast-group name G2
 multicast-list  L2
  add multicast-group name G3
  add multicast-group name G4
 multicast-profile  P1
  add  multicast-list name L1 watch
 multicast-profile  P2
  add  multicast-list name L1 watch
  add  multicast-list name L2 watch
#
vlan 10
 igmp-snooping enable
 attach multicast-profile P1
#
vlan 20
 igmp-snooping enable
 attach multicast-profile P1
#
```

```
vlan 30
 igmp-snooping enable
 attach multicast-profile P2
#
vlan 40
 igmp-snooping enable
 attach multicast-profile P2
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Ethernet0/0/3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface Ethernet0/0/4
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
return
```

8.5 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。

8.5.1 收到 IGMPv2 Report 报文后无法生成表项

故障现象

可控组播配置完成后，使用IGMPv2协议的用户主机点播组播组G的数据，设备上不能生成二层组播转发表项。

操作步骤

步骤1 执行**display multicast-group**命令，查看**Address**字段是否包含组播源地址信息。

如果包含组播源地址信息，说明通过命令**multicast-group**创建可控组播节目时，同时指定了组播节目的组地址和源地址。设备收到IGMP Report报文后，需要对报文内部的组地址和源地址都进行检查。如果用户主机发送的是IGMPv2报文，而IGMPv2报文没有指定源地址，则设备在进行检查时会检查失败，无法生成二层组播转发表项。

----结束

9 MLD Snooping 配置

关于本章

MLD Snooping配置在二层组播设备上，通过对上游三层设备和下游用户之间的MLD报文进行分析，建立和维护IPv6的二层组播转发表，实现组播数据报文在数据链路层的按需分发。

注意事项

端口作为VPLS AC侧的接入端口时，如果该端口同时还作为组播流入接口，会导致对应组播数据无法正常转发。

9.1 MLD Snooping概述
MLD Snooping (Multicast Listener Discovery Snooping)是一种IPv6二层组播协议，通过侦听三层组播设备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接口信息，从而管理和控制组播数据报文在数据链路层的转发。

9.2 设备支持的MLD Snooping特性
设备支持的MLD Snooping特性包括：MLD Snooping基本功能、MLD Snooping策略、成员快速刷新等。

9.3 缺省配置
介绍缺省情况下，MLD Snooping的配置信息。

9.4 配置MLD Snooping基本功能
配置MLD Snooping基本功能，设备可以建立并维护IPv6二层组播转发表，实现组播数据报文在数据链路层的按需分发。

9.5 配置MLD Snooping策略
通过配置MLD Snooping策略，可以控制用户对组播节目的点播，提高二层组播网络的可控性和安全性。

9.6 配置成员关系快速刷新
配置成员关系快速刷新，使组播组成员加入或者离开组播组时设备能够快速响应成员变化，可以提高组播业务运行效率和用户体验。

9.7 维护MLD Snooping
MLD Snooping的维护，包括清除MLD Snooping表项、清除MLD Snooping的统计信息、监控MLD Snooping运行状态。

9.8 配置举例
针对如何在IPv6组播网络中配置MLD Snooping基本功能、静态端口、MLD Snooping查询器、成员端口快速离开、响应拓扑变化发送查询报文，分别提供配置举例。

9.9 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。

9.1 MLD Snooping 概述

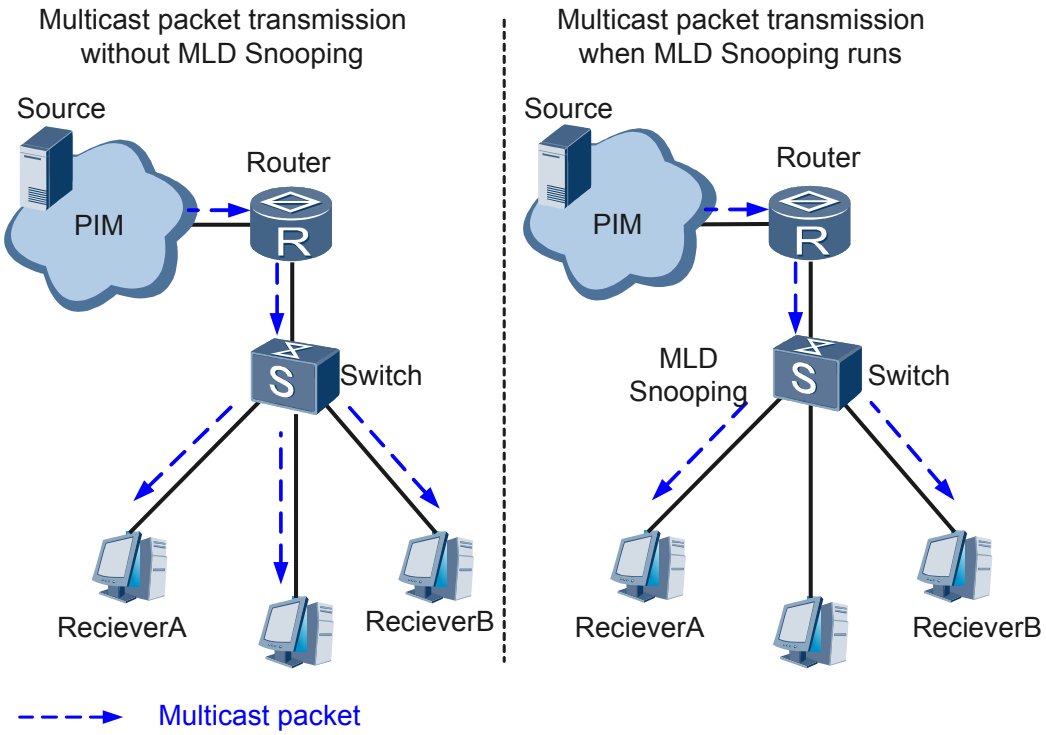
MLD Snooping (Multicast Listener Discovery Snooping)是一种IPv6二层组播协议，通过侦听三层组播设备和用户主机之间发送的组播协议报文来维护组播报文的出接口信息，从而管理和控制组播数据报文在数据链路层的转发。

MLD Snooping 功能

在IPv6组播网络中，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9-1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。

在二层设备（如图9-1中的Switch）上配置MLD Snooping后，Switch会侦听上游设备和下游主机之间交互的MLD报文，通过分析报文中携带的信息，建立二层组播转发表项，从而指导组播数据在数据链路层按需转发。

图 9-1 二层设备运行 MLD Snooping 前后的对比



MLD Snooping 优势

MLD 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数据广播，节约了带宽。
- 实现组播数据在二层按需分发，增强了信息安全性。

9.2 设备支持的 MLD Snooping 特性

设备支持的MLD Snooping特性包括：MLD Snooping基本功能、MLD Snooping策略、成员快速刷新等。

说明

MLD Snooping作为一个二层组播特性，本章中涉及到接口的配置，都是在二层物理接口（包括Eth-Trunk接口）下进行配置。

在MLD协议报文（不包括MLDv2），S2700EI最多能够同时处理大约60个组播用户的点播需求；S3700EI最多能够同时处理大约150个组播用户的点播需求。

MLD Snooping 基本功能

交换机支持配置基于VLAN的MLD Snooping功能。MLD Snooping的基本功能有：

- 支持MLDv1和MLDv2，版本可配置。由于不同版本的MLD协议报文不相同，因此需要为交换机配置和上游三层设备相同的版本。
- 支持配置静态路由器端口和成员端口，实现组播数据快速稳定转发。
- 支持配置MLD Snooping查询器功能，当上游没有启用MLD查询器时，交换机可以代替上游设备发送MLD查询报文。

MLD Snooping 策略

根据不同的场景要求，可以在交换机上进行一些配置，对组播数据进行过滤。

- 通过配置组播组过滤策略，可以限制用户加入的组播组范围。
- 通过配置接口下二层组播数据过滤，可以拒绝从指定VLAN收到的组播数据。
- 通过配置丢弃未知组播报文，使未知组播报文不在VLAN内广播。
- 通过配置接口可以学习的最大组播转发表项数量，可以控制接口上的组播数据流量。

成员快速刷新

成员快速刷新，即成员加入或者离开组播组时交换机快速响应成员变化，可以提高组播业务运行效率和用户体验。主要包括以下几个功能：

- 调整动态成员端口老化时间。
- 调整动态路由器端口老化时间。
- 成员端口快速离开。
- 二层网络拓扑变化时发送查询报文。

MLD Snooping-CPCAR 注意事项

CPCAR通过对上送控制平面的不同业务的协议报文分别进行限速，来保护控制平面的安全。设备针对每类协议报文都有缺省的CPCAR值，部分协议报文的CPCAR值需要根据实际业务规模和具体的用户网络环境进行调整。

调整CPCAR不当将会影响网络业务，如果需要调整MLD报文的CPCAR，建议联系华为工程师处理。

9.3 缺省配置

介绍缺省情况下，MLD Snooping的配置信息。

表9-1列出了MLD Snooping的缺省配置。

表 9-1 MLD Snooping 缺省配置

参数	缺省值
MLD Snooping功能	未使能
MLD Snooping版本	MLD Snooping使能后，默认的版本为MLDv1
MLD Snooping端口学习功能	MLD Snooping使能后，该功能默认使能
MLD Snooping查询器	未使能
MLD Snooping普遍组查询间隔	125s

9.4 配置 MLD Snooping 基本功能

配置MLD Snooping基本功能，设备可以建立并维护IPv6二层组播转发表，实现组播数据报文在数据链路层的按需分发。

前置任务

在配置MLD Snooping基本功能之前，需完成以下任务：

- 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。

配置流程

9.4.1 使能MLD Snooping和**9.4.2 配置MLD Snooping版本**为必选配置，其他为可选配置，请根据需要选配。

9.4.1 使能 MLD Snooping

背景信息

使能全局MLD Snooping功能，是进行其他MLD Snooping配置的前提。VLAN下使能MLD Snooping功能，是VLAN下其他MLD Snooping配置生效的前提。如果VLAN下未使能MLD Snooping，其他的配置成功但不生效，直至当前VLAN使能MLD Snooping功能，该配置才能生效。

缺省情况下，全局MLD Snooping功能未使能。

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**mld-snooping enable**，使能全局MLD Snooping功能。

步骤3 执行命令**vlan** *vlan-id*，进入VLAN视图。

步骤4 （可选）执行命令**l2-multicast forwarding-mode** { **ip** | **mac** }，配置VLAN中组播流是按IP地址还是MAC地址转发。

缺省情况下，S2700按MAC模式转发组播数据，S3700按IP模式转发组播数据。

注意

配置VLAN中组播数据转发模式需要在没有使能该VLAN的MLD Snooping功能时进行。配置完成后需要使能MLD Snooping功能才会生效。

如果当前设备按MAC模式转发组播数据，在网络中规划组播IP地址时，请避免选择为协议预留的组播IP地址映射成相同组播MAC地址的组播IP地址。否则，可能造成使用保留组地址发送协议报文的协议无法正常运行。比如：OSPFv3协议使用FF02::5发送协议报文，映射后的组播MAC地址为33-33-00-00-00-05。如果当前组播数据按MAC模式转发，并且使用的组播IP地址是FF13::5，就会造成OSPF协议不能正常运行。

说明

只有S3700EI支持通过此命令改变默认组播数据转发模式。

步骤5 执行命令**mld-snooping enable**，使能VLAN的MLD Snooping功能。

说明

可以在系统视图下使用**mld-snooping enable** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]命令，使能多个VLAN的MLD Snooping功能。

MLD Snooping功能不能和N:1（N大于1） VLAN Mapping功能配合使用。

S2700的MLD Snooping功能不能和全局的VLAN Mapping功能配合使用。

----结束

9.4.2 配置 MLD Snooping 版本

背景信息

MLD协议用于维护三层组播设备和主机之间的组成员关系，有v1、v2两个版本。在二层设备上配置MLD Snooping版本，设备可以处理相应版本的MLD报文。一般二层设备上配置和三层组播设备一致的版本。如果三层组播设备没有启用MLD，则在二层设备上配置和成员主机相同或高于成员主机的版本。

同一VLAN内必须运行同一个版本的MLD协议。如果VLAN内存在支持不同版本的主机，需要配置MLD Snooping版本为MLDv2，使设备可以处理所有主机的报文。

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**mld-snooping version** *version*，配置MLD Snooping可以处理的MLD版本。

缺省情况下，设备可以处理MLDv1报文，但无法处理MLDv2的报文。

说明

如果配置MLD Snooping可以处理的IGMP版本为MLDv2:

- 则不能改变设备默认的二层组播转发模式。
- S2700按MAC模式转发组播数据。

----结束

9.4.3 （可选）配置静态路由器端口

背景信息

路由器端口一般是二层设备上朝向上游三层组播设备（组播路由器或三层交换机）的接口。路由器端口从上游接收组播数据报文并向成员端口转发。VLAN内使能MLD Snooping功能后，加入该VLAN的接口默认会学习组播协议报文。当一个接口接收到MLD Query报文或PIM Hello报文时，二层设备会标识该接口为动态路由器端口。动态路由器端口会定时老化。

当需要长期稳定的从某接口接收和转发组播数据时，可以配置该接口为静态路由器端口。静态路由器端口不会老化，只能通过相应的**undo**命令删除。

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**mld-snooping static-router-port vlan** *vlan-id*，配置接口为静态路由器端口。

----结束

9.4.4 （可选）配置静态成员端口

背景信息

成员端口一般是二层设备上朝向接收者主机的接口，表示该接口下有组播组成员，可以通过组播协议动态学习或静态配置。VLAN内使能MLD Snooping功能后，加入该VLAN的接口默认会学习组播协议报文。当一个接口收到MLD Report报文时，设备会标识该接口为动态成员端口。动态成员端口会定时老化。

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，成为静态成员端口。静态成员端口不会老化。

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**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**mld-snooping static-group** *group-ipv6-address* [**source** *source-ipv6-address*] **vlan** *vlan-id*，配置接口静态加入组播组，接口成为静态成员端口。

----结束

9.4.5 （可选）配置 MLD Snooping 查询器

背景信息

通过使能MLD Snooping，二层设备就可以通过侦听MLD查询器与用户主机间的MLD协议报文，动态建立二层组播转发表项，实现二层组播。

但是当出现下面的情况时，即使二层设备运行了MLD Snooping，也会由于侦听不到MLD协议报文，而无法正常动态建立二层组播转发表项：

- 上游三层组播设备在接口上未运行MLD协议，而是配置了静态组播组。
- 组播源和用户主机同属于一个二层网络，不需要三层组播设备。

此时，可通过在二层组播设备上配置MLD Snooping查询器，代替三层组播设备向用户主机发送MLD Query报文，从而解决此问题。

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**mld-snooping querier enable**，使能MLD Snooping查询器功能。

说明

- 使能MLD Snooping查询器功能后，交换机会定时以广播的方式向VLAN内所有接口（包括路由器端口）发送MLD Query报文，如果组播网络中已经存在MLD查询器，可能会引起MLD查询器重新选举。此时，建议不配置此功能；如果一定要配置MLD Snooping查询器功能，请确保交换机的IPv6地址比上游MLD查询器的IPv6地址大。
- 如果设备上配置了组播VLAN复制功能，则不能在用户VLAN上使能MLD Snooping查询器功能。

步骤4 （可选）配置查询器参数。

说明

在配置参数时，要确保“MLD查询报文最大响应时间”<“MLD普遍组查询报文发送间隔”。

查询器参数	配置命令	参数说明	缺省值	支持的版本
普遍组查询报文的发送间隔	**mld-snooping query-interval** *query-interval*	查询器周期性的发送普遍组查询报文，维护VLAN内的组成员关系，本参数定义了发送该报文的时间间隔	125秒	MLDv1、MLDv2

查询器参数	配置命令	参数说明	缺省值	支持的版本
MLD健壮系数	**mld-snooping robust-count** *robust-count*	健壮系数用来规定以下两个值： ● 当查询器启动时发送“健壮系数”次的“普遍组查询报文”，发送时间间隔为“普遍组查询报文发送间隔”的1/4 ● 当设备收到Done报文后，发送“健壮系数”次的“MLD特定组查询报文”，发送间隔为“特定组查询报文发送间隔”	2	MLDv1、MLDv2
MLD查询报文的最大响应时间	**mld-snooping max-response-time** *max-response-time*	当交换机收到主机的MLD Report报文后，成员端口老化时间设置为：普遍组查询报文的发送间隔 × MLD健壮系数 + 最大响应时间 组播组成员接收到一个MLD查询报文后，会在最大响应时间内发送Report报文	10秒	MLDv2

查询器参数	配置命令	参数说明	缺省值	支持的版本
最后查询报文的发送间隔	**mld-snooping last-listener-query-interval** *query-interval*	当交换机收到主机退出某组播组的Done报文时，重置成员端口老化时间为：特定组查询报文发送间隔 × MLD健壮系数。即会连续发送“MLD健壮系数”次特定组成员查询报文，询问该组播组是否还存在成员。本参数定义了发送该报文的时间间隔	1秒	MLDv2

步骤5 （可选）执行命令**quit**，返回到系统视图。

步骤6 （可选）执行命令**mld-snooping send-query source-address** *ipv6-address*，配置MLD普遍组查询报文的源IPv6地址。

缺省情况下，MLD Snooping查询器发送普遍组查询报文时源IPv6地址为FE80::。当该地址已被网络中的其他设备占用时，可使用本命令配置为其他地址。

----结束

9.4.6 （可选）配置 Router-Alert 选项

背景信息

出于兼容性考虑，缺省情况下交换机不对Router-Alert选项进行检查，当收到MLD报文时，不管其IP报头中是否携带Router-Alert选项，设备都会将其送给上层协议进行处理。为了提高系统性能、减少不必要的开支，同时出于协议安全性的考虑，可以配置对Router-Alert选项进行检查，当收到的MLD报文中没有携带Router-Alert选项时，就丢弃该报文。

缺省情况下，交换机在发送的MLD报文中携带Router-Alert选项。

有关Router-Alert选项的详细介绍，请参见RFC2113。

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**mld-snooping require-router-alert**，配置设备对接收的MLD报文进行Router-Alert检查。

步骤4 执行命令**mld-snooping send-router-alert**，配置设备发送的MLD报文中携带Router-Alert选项。

----结束

9.4.7 检查配置结果

背景信息

完成上述配置后，可以在任意视图下执行以下命令，查看MLD Snooping的配置、成员端口、路由器端口等信息。

操作步骤

- 使用命令**display mld-snooping** [**vlan** *vlan-id*] **configuration**查看MLD Snooping的配置信息。
- 使用命令**display mld-snooping** [**vlan** *vlan-id*]查看MLD Snooping的运行参数信息。
- 使用命令**display mld-snooping port-info** [**vlan** *vlan-id* [**group** *ipv6-group-address* [**source-address** *ipv6-source-address*]]] [**verbose**]查看组播组的成员端口信息。
- 使用命令**display mld-snooping router-port** [**vlan** *vlan-id*]查看路由器端口信息。
- 使用命令**display l2-multicast forwarding-mode vlan** [*vlan-id*]查看VLAN内组播数据转发模式。

----结束

9.5 配置 MLD Snooping 策略

通过配置MLD Snooping策略，可以控制用户对组播节目的点播，提高二层组播网络的可控性和安全性。

前置任务

9.4 配置MLD Snooping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。

9.5.1 配置组播组过滤策略

背景信息

组播组过滤策略主要用于对VLAN内的主机加入的组播组进行限制。本功能仅对动态加入的组生效，对静态组播组无效。本功能需要结合ACL使用，先创建ACL并在其规则中定义组播组过滤策略。ACL的配置方法，请参见《配置指南-安全》中的“ACL配置”。

说明

创建VLAN的组播组过滤策略的ACL时，**rule**命令必须使用**deny**参数禁止VLAN内的主机访问全部或指定组播组，完成过滤组播组的目的。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 通过以下两种方式配置组播组过滤策略，来满足不同的生效范围：

- 配置VLAN内的组播组过滤策略。
  a. 执行命令**vlan** *vlan-id*，进入VLAN视图。
  b. 执行命令**mld-snooping group-policy** *acl6-number* [*mld-version*]，配置VLAN内的组播组过滤策略，禁止VLAN内的主机加入指定组播组。
- 配置接口下的组播组过滤策略。
  a. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  b. 执行命令**mld-snooping group-policy** *acl6-number* **vlan** *vlan-id* [*mld-version*]，配置接口下的组播组过滤策略，禁止VLAN内的主机加入指定组播组。

缺省情况下，VLAN内的主机可以加入任何组播组。如果不指定应用组播组过滤策略的MLD报文版本，则交换机对接收到的所有MLD报文都应用该组播组过滤策略。

如果接口视图和VLAN视图都配置了针对同一VLAN的组播组过滤策略，先根据接口视图上配置的过滤策略进行判断，再根据VLAN视图上配置的过滤策略进行判断。

----结束

9.5.2 配置接口下组播数据过滤

背景信息

当网络管理员希望拒绝某特定的组播数据报文时，可以在交换机接口下配置组播数据过滤，拒绝来自指定VLAN的组播数据报文。

产品	支持情况
S2700	S2700SI、S2710SI不支持
S3700	支持

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-source-deny vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，对指定VLAN内的组播数据进行过滤。

说明

执行本命令时指定的VLAN应该是接口已经加入的VLAN。否则配置没有意义。

使用此命令只过滤同时满足以下条件的组播数据报文:

- 报文目的MAC为IP组播MAC地址（即0x01005E开头的IPv4组播MAC地址或0x3333开头的IPv6组播MAC地址）。
- 报文封装的协议类型为UDP类型。

----结束

9.5.3 配置丢弃未知组播流

背景信息

未知组播流，是指组播转发表中不存在对应的可指导转发的表项的组播报文，也就是用户还没有点播的流量。这种流量可能是上游处于某种目的将流量静态“推”下来的，比如为提高点播的速度，到达交换机后，一般应将流量终结掉，不应该在VLAN内广播。

未使能二层组播时，交换机对未知组播流均采用广播方式。如果用户不需要接收组播流量，可以通过配置**multicast drop-unknown**命令，节省瞬时带宽占用率。

在使能了二层组播后：

- 对于S1720，S2700系列，S5700S-LI、S5700LI、S5710LI、S5700SI设备：

  无论当前二层组播转发模式为何种转发模式，未知组播流都会在VLAN内广播。配置**multicast drop-unknown**命令后，设备在接收到未知组播流后会将其丢弃。通过配置丢弃未知组播流，可以节省瞬时带宽占用率。
- 对于其他设备：
  - 如果当前二层组播转发模式为按IP转发，此时未知组播流不会在VLAN内广播，无论是否配置**multicast drop-unknown**命令，设备都不会接收未知组播流。
  - 如果当前二层组播转发模式为按MAC转发，此时未知组播流会在VLAN内广播。配置**multicast drop-unknown**命令后，设备在接收到未知组播流后会将其丢弃。

可以在VLAN视图下通过**l2-multicast forwarding-mode** { **ip** | **mac** }命令来配置转发模式。缺省情况下，VLAN内组播数据按IP地址模式转发。

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**vlan** *vlan-id*，进入VLAN视图。

步骤3 执行命令**multicast drop-unknown**，配置丢弃未知组播流。

说明

S2700（S2710SI、S2700-52P-EI、S2700-52P-PWR-EI除外）在系统视图下配置此功能。

OSPF，VRRP，IPv6 RA message等部分协议报文的目的MAC和目的IP使用的是保留组播地址，没有组播转发表项。如果配置了此命令，这些协议报文将因没有组播转发表项而被丢弃，从而无法通过交换机转发出去。因此当交换机需要在VLAN内透传保留组播地址的协议报文时，VLAN内建议不要配置此命令。

----结束

9.5.4 配置接口学习的组播表项数量限制

背景信息

如果限制用户点播组播节目的数量，可配置接口可以学习的组播表项最大数量，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。

步骤3 执行命令**mld-snooping table limit** *limit* **vlan** *vlan-id*，配置接口可以学习的组播表项最大数量。

说明

在配置接口可以学习的组播表项最大数量时，如果当前接口上的表项数量已经超过了配置值，配置后当前接口上的组播表项数量不会改变，但是不允许接口再学习到新的组播表项。

----结束

9.5.5 检查配置结果

前提条件

完成MLD Snooping策略配置以后，可以在任意试图下执行以下命令，查看策略的配置和应用情况。

操作步骤

- 使用命令**display mld-snooping** [**vlan** *vlan-id*] **configuration**查看MLD Snooping的配置信息。

  通过查看MLD Snooping的配置信息，可查看到VLAN下的MLD Snooping策略的配置情况。

----结束

9.6 配置成员关系快速刷新

配置成员关系快速刷新，使组播组成员加入或者离开组播组时设备能够快速响应成员变化，可以提高组播业务运行效率和用户体验。

前置任务

9.4 配置MLD Snooping基本功能

配置流程

以下功能是并列、可选的，可以根据需要进行配置，推荐使用缺省值。

9.6.1 配置动态成员端口老化时间

背景信息

设备在收到不同MLD协议报文之后，会为成员端口启动不同时长的老化定时器：

- 当设备的成员端口收到下游主机的Report报文后，将接口老化时间设置为：健壮系数 × 普遍组查询报文发送时间间隔 + 最大响应时间。
- 当设备的成员端口收到下游主机的Done报文后，将接口老化时间设置为：特定组查询报文发送时间间隔 × 健壮系数。

在部署二层组播网络时，要确保所有二层组播设备间用于计算动态成员端口老化时间的相关参数保持一致，尤其是MLD Snooping普遍组查询时间间隔。否则可能造成二层组播业务运行不正常。

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**mld-snooping query-interval** *query-interval*，配置MLD Snooping普遍组查询报文的时间间隔。

缺省情况下，普遍组查询时间间隔为125秒。

说明

RFC规定的普遍组查询间隔缺省值是125秒，目前并不是所有的厂商都是按照RFC标准实现的。尽量确保组播网络中所有设备的普遍组查询间隔（包括MLD普遍组查询间隔和MLD Snooping普遍组查询间隔）保持一致。

表9-2给出了华为S系列交换机普遍组查询间隔的缺省值。

表 9-2 普遍组查询间隔缺省值

特性	框式交换机缺省值	盒式交换机缺省值
MLD	125s	不涉及
MLD Snooping	60s	125s

步骤4 执行命令**mld-snooping robust-count** *robust-count*，配置MLD Snooping健壮系数。

缺省情况下，MLD Snooping健壮系数为2。

步骤5 执行命令**mld-snooping max-response-time** *max-response-time*，配置MLD Snooping最大响应时间。

缺省情况下，MLD Snooping最大响应时间是10秒。

步骤6 执行命令**mld-snooping last-listener-query-interval** *query-interval*，配置MLD Snooping特定组查询报文时间间隔。

缺省情况下，MLD Snooping特定组查询时间间隔为1秒。

----结束

9.6.2 配置动态路由器端口老化时间

背景信息

路由器端口用来向上游三层设备发送Report报文和接收上游设备的组播数据报文。在配置MLD Snooping功能后，设备可以动态学习路由器端口，实时监测上游组播数据的下发。当网络发生拥塞或者网络稳定性不佳时，动态路由器端口在其老化时间超时前没有收到MLD普遍组查询报文或者PIM Hello报文，设备将把该接口从路由器端口列表中删除，造成组播数据中断，此时可以将路由器端口老化时间值适当调大。

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**mld-snooping router-aging-time** *router-aging-time*，配置动态路由器端口老化时间。

缺省情况下，通过MLD普遍组查询报文学到的路由器端口老化时间为180秒；通过PIM Hello报文学到的路由器端口老化时间为Hello报文中Holdtime值。

----结束

9.6.3 配置成员端口快速离开

背景信息

成员端口快速离开是指当交换机从成员端口收到MLD Done报文时，不再启动老化定时器等待转发表项老化，而是立即将该接口对应的转发表项删除。

说明

只有当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的成员端口快速离开功能。

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**vlan** *vlan-id*，进入VLAN视图。

步骤3 执行命令**mld-snooping prompt-leave** [**group-policy** *acl6-number*]，配置接口快速离开。

缺省情况下，不允许成员端口快速离开。

可以通过**group-policy** *acl6-number*参数，对快速离开的组播组进行限制。此时需要先创建ACL，并配置规则。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。ACL的配置方法，请参见《配置指南-安全》中“ACL配置”。

----结束

9.6.4 配置网络拓扑变化时发送 Query 报文

背景信息

当二层网络拓扑发生变化时，组播报文的转发路径可能发生变化。配置交换机在链路故障时主动发送MLD Query报文，当组播组成员回应MLD Report报文时，设备根据Report报文更新成员端口信息，将组播数据流迅速切换到新的转发路径上。

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**mld-snooping send-query enable**，配置设备在网络拓扑变化时发送MLD普遍组查询报文。

缺省情况下，当网络拓扑变化时，设备不会主动发送MLD普遍组查询报文。

配置本命令后，当设备感知二层网络拓扑发生变化时，会主动发送MLD普遍组查询报文，保证设备能够快速更新端口信息，使下游组播组成员接收组播数据不中断。

步骤3 （可选）执行命令**mld-snooping send-query source-address** *ipv6-address*，配置MLD普遍组查询报文的源IPv6地址。

缺省情况下，MLD普遍组查询报文源IPv6地址为本地链路地址，即以FE80::开头的IPv6地址。当该地址已被网络中的其他设备占用时，可使用本命令配置为其他地址。

----结束

9.6.5 检查配置结果

前提条件

完成成员关系快速刷新配置以后，可以在任意试图下执行以下命令，查看MLD Snooping配置信息。

操作步骤

- 使用命令**display mld-snooping** [**vlan** *vlan-id*] **configuration**查看MLD Snooping的配置信息。

----结束

9.7 维护 MLD Snooping

MLD Snooping的维护，包括清除MLD Snooping表项、清除MLD Snooping的统计信息、监控MLD Snooping运行状态。

9.7.1 清除 MLD Snooping 表项

背景信息

MLD Snooping表项包括静态表项和动态表项，两者的清除方法不一样。

注意

静态表项被清除后无法自动恢复，直到再次执行命令配置静态成员端口。

清除动态表项后，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MLD Report报文，设备重新生成转发表项后，主机才能再收到组播流。

操作步骤

- 在接口视图下执行命令**undo mld-snooping static-group** { *group-ipv6-address* [**source** *source-ipv6-address*] **vlan** *vlan-id* | **all** }取消接口静态加入组播组的配置。
- 在用户视图下使用命令**reset mld-snooping group** { **vlan** { *vlan-id* | **all** } | **all** }清除动态组表项。

----结束

9.7.2 清除 MLD Snooping 统计信息

背景信息

MLD Snooping的统计信息主要包括VLAN内接收到的Report、Done、Query等协议报文的数量，通过该命令可以将这些统计计数置0，便于重新统计。

注意

清除MLD 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 mld-snooping statistics** [**vlan** *vlan-id*]清除MLD Snooping统计信息。

----结束

9.7.3 监控 MLD Snooping 的运行状况

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解MLD Snooping的运行状况。主要包括：查看配置信息、成员端口和路由器端口、组表项、报文统计计数等。

操作步骤

- 使用命令**display mld-snooping** [**vlan** *vlan-id*] **configuration**查看MLD Snooping的配置信息。
- 使用命令**display mld-snooping** [**vlan** *vlan-id*]查看MLD Snooping的运行参数信息。

- 使用命令**display mld-snooping port-info** [**vlan** *vlan-id* [**group** *ipv6-group-address* [**source-address** *ipv6-source-address*]]] [**verbose**]查看组播组的成员端口信息。
- 使用命令**display mld-snooping router-port** [**vlan** *vlan-id*]查看路由器端口信息。
- 使用命令**display l2-multicast forwarding-mode vlan** [*vlan-id*]查看VLAN内组播数据转发模式。
- 使用命令**display mld-snooping statistics** [**vlan** *vlan-id*]查看MLD Snooping的统计信息。

----结束

9.8 配置举例

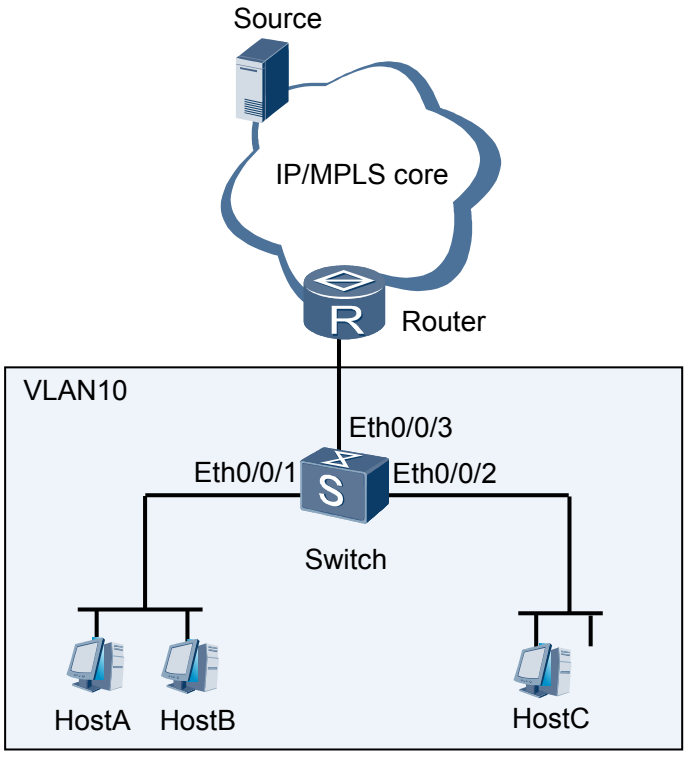
针对如何在IPv6组播网络中配置MLD Snooping基本功能、静态端口、MLD Snooping查询器、成员端口快速离开、响应拓扑变化发送查询报文，分别提供配置举例。

9.8.1 配置 MLD Snooping 示例

组网需求

如图9-2所示为一个IPv6组播网络，路由器Router通过二层设备Switch连接用户网络。组播源Source向组播组FF16::1～FF16::5发送数据，网络中有HostA、HostB、HostC三个接收者，他们只对FF16::1～FF16::3的数据感兴趣。

图 9-2 配置 MLD Snooping 组网图



配置思路

在二层设备上配置MLD Snooping基本功能以及组播组过滤策略，可以实现此需求。

1. 在Switch上创建VLAN并将接口加入VLAN。
2. 使能全局和VLAN的MLD Snooping功能。
3. 配置组播组过滤策略，并在VLAN内应用此策略。

操作步骤

步骤1 创建VLAN，配置接口加入VLAN。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] port hybrid pvid vlan 10
[Switch-Ethernet0/0/1] port hybrid untagged vlan 10
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/2
[Switch-Ethernet0/0/2] port hybrid pvid vlan 10
[Switch-Ethernet0/0/2] port hybrid untagged vlan 10
[Switch-Ethernet0/0/2] quit
[Switch] interface ethernet 0/0/3
[Switch-Ethernet0/0/3] port hybrid pvid vlan 10
[Switch-Ethernet0/0/3] port hybrid untagged vlan 10
[Switch-Ethernet0/0/3] quit
```

步骤2 使能MLD Snooping功能。

使能全局的MLD Snooping功能。

```
[Switch] mld-snooping enable
```

使能VLAN10的MLD Snooping功能。

```
[Switch] vlan 10
[Switch-vlan10] mld-snooping enable
[Switch-vlan10] quit
```

说明

配置完成后，Switch就可以通过侦听MLD协议报文生成二层组播转发表项。确保Switch与上游三层设备Router的普遍组查询间隔保持一致，以防止Switch的二层组播转发表项被错误老化，导致组播流量不通。如果Switch默认的普遍组查询间隔与Router不一致，可在VLAN10内执行命令**mld-snooping query-interval** *query-interval*进行调整。

步骤3 配置并应用组播组过滤策略。

配置组播组过滤策略。

```
[Switch] acl ipv6 2000
[Switch-acl6-basic-2000] rule deny source ff16::4 128
[Switch-acl6-basic-2000] rule deny source ff16::5 128
[Switch-acl6-basic-2000] quit
```

在VLAN10内应用组播组过滤策略。

```
[Switch] vlan 10
[Switch-vlan10] mld-snooping group-policy 2000
[Switch-vlan10] quit
```

步骤4 验证配置结果。

查看Switch上的端口信息。

```
<Switch> display mld-snooping port-info vlan 10
------------------------------------------------------------------------------
                    (Source, Group)  Port                            Flag
 Flag: S:Static     D:Dynamic     M: Ssm-mapping
------------------------------------------------------------------------------
VLAN 10, 3 Entry(s)
(              *, ff16:0:0:0:0:0:0:1)Eth0/0/3                     Router
                                     Eth0/0/1                       -D-
                                     Eth0/0/2                       -D-
                                                3 port(s)
(              *, ff16:0:0:0:0:0:0:2)Eth0/0/3                     Router
                                     Eth0/0/1                       -D-
                                     Eth0/0/2                       -D-
                                                3 port(s)
(              *, ff16:0:0:0:0:0:0:3)Eth0/0/3                     Router
                                     Eth0/0/1                       -D-
                                     Eth0/0/2                       -D-
                                                3 port(s)
------------------------------------------------------------------------------
```

由显示信息可知，组FF16::1～FF16::3已在Switch上动态生成的成员端口为Eth0/0/1和Eth0/0/2。

----结束

配置文件

- Switch的配置文件

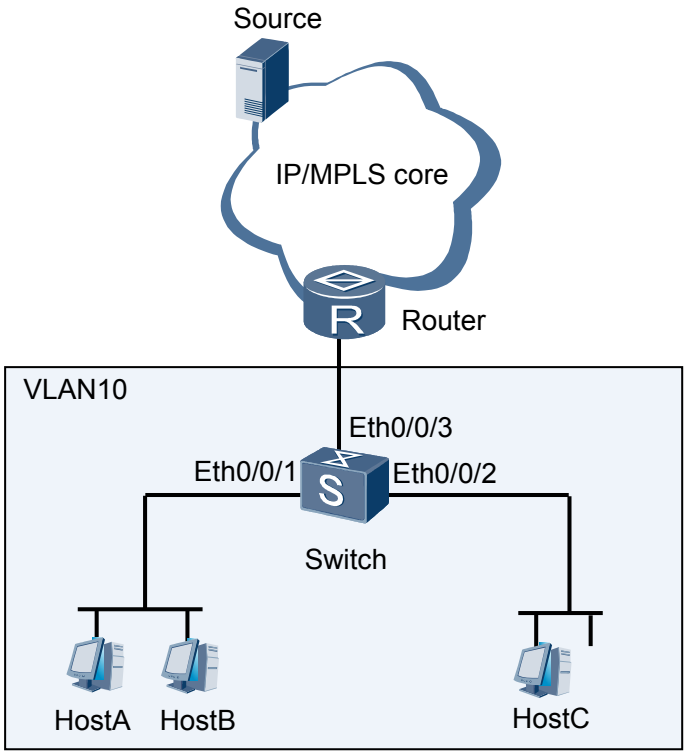
```
#
sysname Switch
#
vlan batch 10
#
mld-snooping enable
#
acl ipv6 number 2000
 rule 0 deny source FF16::4/128
 rule 1 deny source FF16::5/128
#
vlan 10
 mld-snooping enable
 mld-snooping group-policy 2000
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

9.8.2 配置使用静态端口实现二层组播示例

组网需求

如图9-3所示为一个IPv6组播网络，路由器Router通过二层设备Switch连接用户网络，Router的用户侧三层VLANIF接口配置了FF16::1～FF16::5的MLD静态组，没有运行MLD协议。网络中有HostA、HostB、HostC三个接收者，其中HostA和HostB希望长期稳定接收FF16::1～FF16::3的数据，HostC希望长期稳定接收FF16::4～FF16::5的数据。

图 9-3 配置静态端口实现二层组播组网图



配置思路

在Switch上配置MLD Snooping的静态路由器端口和静态成员端口，可以实现此需求。

1. 创建VLAN并将接口加入VLAN。
2. 使能全局和VLAN的MLD Snooping功能。
3. 配置静态路由器端口。
4. 配置静态成员端口。

操作步骤

步骤1 创建VLAN10，配置接口加入VLAN10。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] port hybrid pvid vlan 10
[Switch-Ethernet0/0/1] port hybrid untagged vlan 10
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/2
[Switch-Ethernet0/0/2] port hybrid pvid vlan 10
[Switch-Ethernet0/0/2] port hybrid untagged vlan 10
[Switch-Ethernet0/0/2] quit
[Switch] interface ethernet 0/0/3
[Switch-Ethernet0/0/3] port hybrid pvid vlan 10
[Switch-Ethernet0/0/3] port hybrid untagged vlan 10
[Switch-Ethernet0/0/3] quit
```

步骤2 使能全局和VLAN10的MLD Snooping功能。

使能全局的MLD Snooping功能。

```
[Switch] mld-snooping enable
```

使能VLAN10的MLD Snooping功能。

```
[Switch] vlan 10
[Switch-vlan10] mld-snooping enable
[Switch-vlan10] quit
```

步骤3 配置静态路由器端口。

```
[Switch] interface ethernet 0/0/3
[Switch-Ethernet0/0/3] mld-snooping static-router-port vlan 10
[Switch-Ethernet0/0/3] quit
```

步骤4 配置静态成员端口。

```
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] mld-snooping static-group ff16::1 vlan 10
[Switch-Ethernet0/0/1] mld-snooping static-group ff16::2 vlan 10
[Switch-Ethernet0/0/1] mld-snooping static-group ff16::3 vlan 10
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/2
[Switch-Ethernet0/0/2] mld-snooping static-group ff16::4 vlan 10
[Switch-Ethernet0/0/2] mld-snooping static-group ff16::5 vlan 10
[Switch-Ethernet0/0/2] quit
```

步骤5 验证配置结果。

查看Switch上的路由器端口信息。

```
<Quidway> display mld-snooping router-port
 Total Number of Router Port on VLAN 10 is 1
   Port Name             UpTime          Expires         Flags
   Eth0/0/3               00:00:06        --              STATIC
```

由显示信息可知，Eth0/0/3已成为静态路由器端口。

查看Switch上的成员端口信息。

```
<Switch> display mld-snooping port-info vlan 10
 ----------------------------------------------------------------------
                     (Source, Group)    Port                          Flag
  Flag: S:Static     D:Dynamic     M: Ssm-mapping
 ----------------------------------------------------------------------
 VLAN 10, 5 Entry(s)
 (              *, ff16:0:0:0:0:0:0:1)  Eth0/0/3                    Router
                                        Eth0/0/1                       S--
                                                2 port(s)
 (              *, ff16:0:0:0:0:0:0:2)  Eth0/0/3                    Router
                                        Eth0/0/1                       S--
                                                2 port(s)
 (              *, ff16:0:0:0:0:0:0:3)  Eth0/0/3                    Router
                                        Eth0/0/1                       S--
                                                2 port(s)
 (              *, ff16:0:0:0:0:0:0:4)  Eth0/0/3                    Router
                                        Eth0/0/2                       S--
                                                2 port(s)
 (              *, ff16:0:0:0:0:0:0:5)  Eth0/0/3                    Router
                                        Eth0/0/2                       S--
                                                2 port(s)
 ----------------------------------------------------------------------
```

由显示信息可知，组FF16::1～FF16::3在Switch上有静态成员端口Eth0/0/1，组FF16::4～FF16::5在Switch上有静态成员端口Eth0/0/2。

----结束

配置文件

- Switch的配置文件

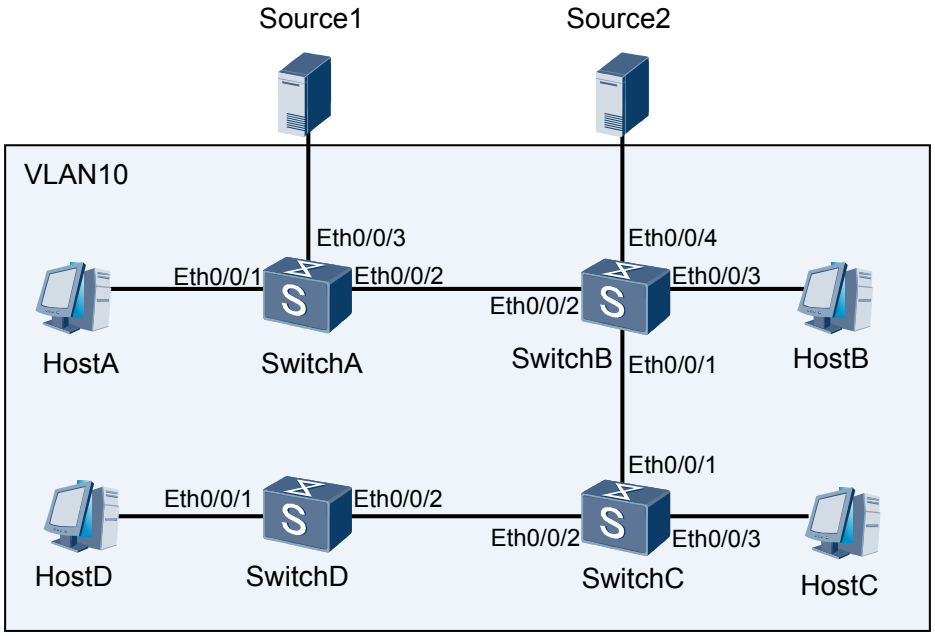
```
#
sysname Switch
#
vlan batch 10
#
mld-snooping enable
#
vlan 10
 mld-snooping enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 mld-snooping static-group ff16:0:0:0:0:0:0:1 vlan 10
 mld-snooping static-group ff16:0:0:0:0:0:0:2 vlan 10
 mld-snooping static-group ff16:0:0:0:0:0:0:3 vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 mld-snooping static-group ff16:0:0:0:0:0:0:4 vlan 10
 mld-snooping static-group ff16:0:0:0:0:0:0:5 vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 mld-snooping static-router-port vlan 10
#
return
```

9.8.3 配置 MLD Snooping 查询器示例

组网需求

如图9-4所示，在一个没有三层设备纯二层网络环境中，组播源Source1和Source2分别向组播组FF16::1和FF16::2发送组播数据，HostA和HostC希望接收组播组FF16::1的数据，HostB和HostD希望接收组播组FF16::2的数据。

图 9-4 配置 MLD Snooping 查询器组网图



配置思路

在网络中各Switch上使能MLD Snooping功能，并配置MLD Snooping查询器，可以实现此需求。同时为防止设备在没有二层组播转发表项时将组播数据在VLAN内广播，在所有Switch上都使能丢弃未知组播数据报文功能。

1. 根据图9-4在所有Switch上创建VLAN并将接口加入VLAN。
2. 在所有Switch上使能全局和VLAN的MLD Snooping功能。
3. 选择距离组播源较近的SwitchA为MLD Snooping查询器。
4. 在所有Switch上使能丢弃未知组播数据报文功能。

操作步骤

步骤1 创建VLAN，配置接口加入VLAN。

配置SwitchA。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface ethernet 0/0/1
[SwitchA-Ethernet0/0/1] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/1] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/1] quit
[SwitchA] interface ethernet 0/0/2
[SwitchA-Ethernet0/0/2] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/2] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/2] quit
[SwitchA] interface ethernet 0/0/3
[SwitchA-Ethernet0/0/3] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/3] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/3] quit
```

SwitchB、SwitchC、SwitchD的配置与此类似，配置过程略。

步骤2 使能MLD Snooping功能。

配置SwitchA。

```
[SwitchA] mld-snooping enable
[SwitchA] vlan 10
[SwitchA-vlan10] mld-snooping enable
[SwitchA-vlan10] quit
```

SwitchB、SwitchC、SwitchD的配置与此类似，配置过程略。

步骤3 配置MLD Snooping查询器。

配置SwitchA为查询器。

```
[SwitchA] vlan 10
[SwitchA-vlan10] mld-snooping querier enable
[SwitchA-vlan10] quit
```

步骤4 配置未知组播数据报文丢弃。

配置SwitchA。

说明

S2700（S2710SI、S2700-52P-EI、S2700-52P-PWR-EI除外）在系统视图下配置此命令。

```
[SwitchA] vlan 10
[SwitchA-vlan10] multicast drop-unknown
[SwitchA-vlan10] quit
```

SwitchB、SwitchC、SwitchD的配置与此类似，配置过程略。

步骤5 验证配置结果。

当MLD Snooping查询器开始工作之后，除查询器以外的所有设备都能收到MLD普遍组查询报文。可以通过命令查看MLD报文的统计信息，例如查看SwitchB上收到的MLD报文统计信息。

```
<SwitchB> display mld-snooping statistics vlan 10
 MLD Snooping Packets Counter
   Statistics for VLAN 10
     Recv V1 Report  316
     Recv V2 Report  0
     Recv V1 Query  305
     Recv V2 Query   0
     Recv Done       2
     Recv Pim Hello  85
     Send Query(S=0) 1
     Send Query(S!=0)0
     Send General Query               0
     Send Group-Specific Query        0
     Send Group-Source-Specific Query 0
```

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10
#
mld-snooping enable
#
vlan 10
 multicast drop-unknown
 mld-snooping enable
 mld-snooping querier enable
```

```
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SwitchB的配置文件

```
#
sysname SwitchB
#
vlan batch 10
#
mld-snooping enable
#
vlan 10
 multicast drop-unknown
 mld-snooping enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/4
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SwitchC的配置文件

```
#
sysname SwitchC
#
vlan batch 10
#
mld-snooping enable
#
vlan 10
 multicast drop-unknown
 mld-snooping enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SwitchD的配置文件

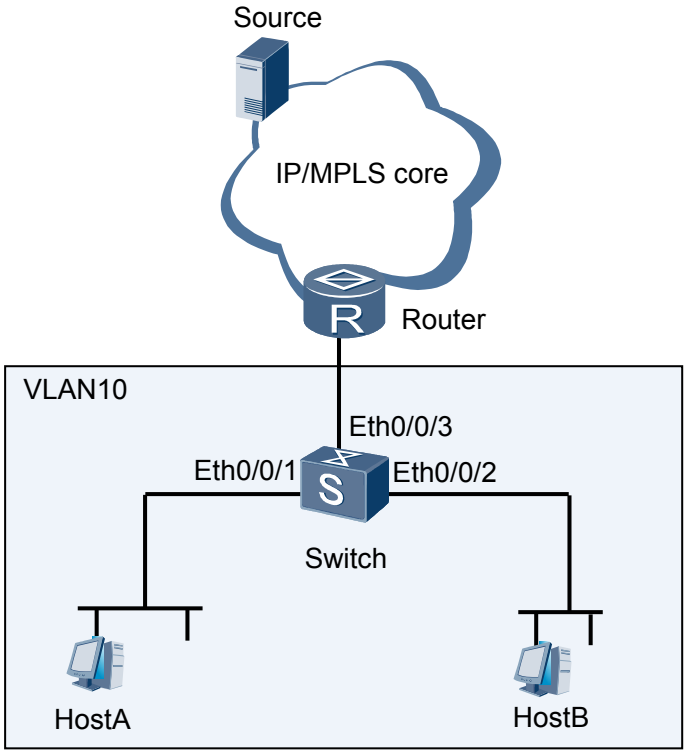
```
#
sysname SwitchD
#
vlan batch 10
#
mld-snooping enable
#
vlan 10
 multicast drop-unknown
 mld-snooping enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

9.8.4 配置成员端口快速离开示例

组网需求

在如图9-5所示的IPv6组播网络中，路由器Router通过二层设备Switch连接用户网络。Switch的接口Eth0/0/1和接口Eth0/0/2分别只连接一台接收者主机。因此，当Switch从这两个接口收到主机发送的MLD Done报文后，不需要等到接口的老化定时器超时，就可以直接将这些接口对应主机要离开的组播组的转发表项删除，以节约带宽和系统资源。

图 9-5 配置成员端口快速离开组网图



配置思路

在Switch上启用MLD Snooping并配置成员端口快速离开，可以满足此需求。

- 创建VLAN并将接口加入VLAN。
- 使能全局和VLAN的MLD Snooping功能。
- 使能VLAN内的成员端口快速离开功能。

操作步骤

步骤1 创建VLAN10，配置接口加入VLAN10。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] port hybrid pvid vlan 10
[Switch-Ethernet0/0/1] port hybrid untagged vlan 10
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/2
[Switch-Ethernet0/0/2] port hybrid pvid vlan 10
[Switch-Ethernet0/0/2] port hybrid untagged vlan 10
[Switch-Ethernet0/0/2] quit
[Switch] interface ethernet 0/0/3
[Switch-Ethernet0/0/3] port hybrid pvid vlan 10
[Switch-Ethernet0/0/3] port hybrid untagged vlan 10
[Switch-Ethernet0/0/3] quit
```

步骤2 使能全局和VLAN10的MLD Snooping功能。

使能全局的MLD Snooping功能。

```
[Switch] mld-snooping enable
```

使能VLAN10的MLD Snooping功能。

```
[Switch] vlan 10
[Switch-vlan10] mld-snooping enable
```

步骤3 配置VLAN10内的成员端口快速离开。

```
[Switch-vlan10] mld-snooping prompt-leave
[Switch-vlan10] quit
```

步骤4 验证配置结果。

在Switch上执行**display mld-snooping**命令，查看VLAN10内的配置信息。

```
<Switch> display mld-snooping vlan 10
MLD Snooping Vlan Information for VLAN 10
     MLD Snooping is Enabled
     MLD Version is Set to default 1
     MLD Query Interval is Set to default 125
     MLD Max Response Interval is Set to default 10
     MLD Robustness is Set to default 2
     MLD Last Member Query Interval is Set to default 1
     MLD Router Port Aging Interval is Set to 180s or holdtime in hello
     MLD Filter Group-Policy is Set to default : Permit All
     MLD Prompt Leave Enable
     MLD Router Alert is Not Required
     MLD Send Router Alert Enable
     MLD Snooping Querier Disable
```

其中“MLD Prompt Leave enable”表示VLAN10内的接口快速离开功能配置成功。

----结束

配置文件

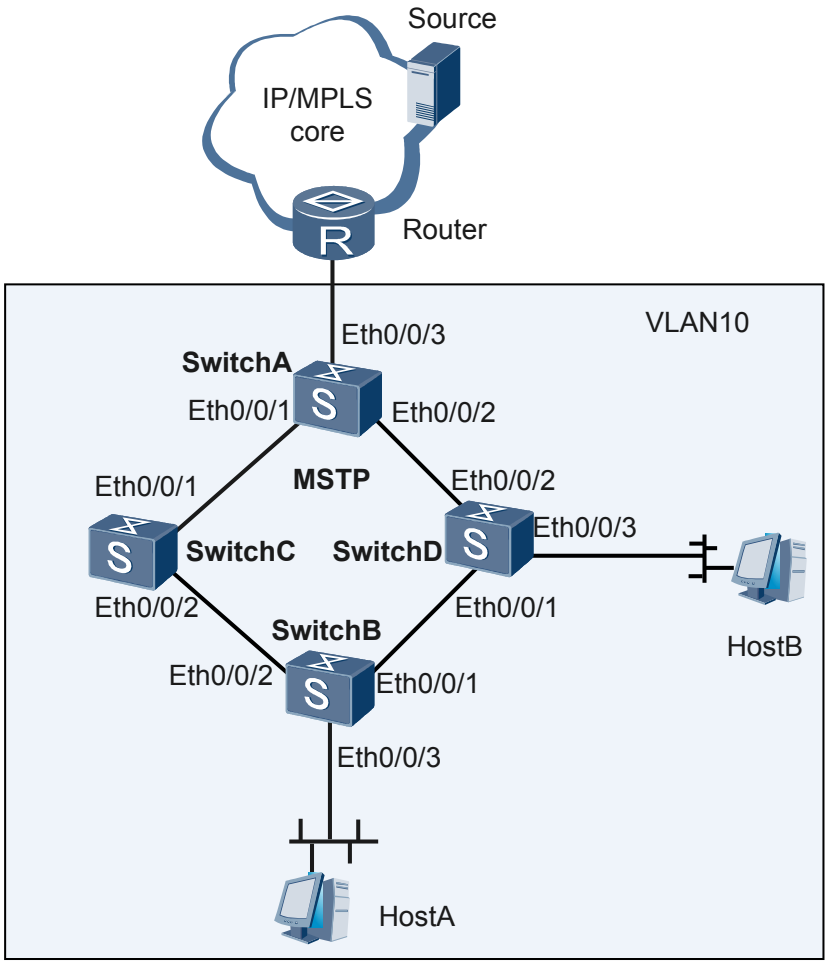
```
#
sysname Switch
#
mld-snooping enable
#
vlan batch 10
#
vlan 10
 mld-snooping enable
 mld-snooping prompt-leave
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

9.8.5 配置 MLD Snooping 响应网络拓扑变化示例

组网需求

在如图9-6所示的IPv6组播网络中，为提高网络可靠性，4台交换机依次连接成环网。为消除环路，在4台交换机上运行STP。HostA和HostB需要接收组播源发出的组播数据。

图 9-6 配置 MLD Snooping 响应二层网络拓扑变化事件示例组网图



配置思路

Switch上启用MLD Snooping，并配置MLD Snooping响应二层网络拓扑变化事件。

1. 在所有Switch上配置STP。
2. 在所有Switch上创建VLAN10，并配置接口加入VLAN10。
3. 使能所有Switch全局和VLAN的MLD Snooping功能。
4. 配置SwitchA的MLD Snooping响应二层网络拓扑变化事件。

操作步骤

步骤1 在所有Switch上配置STP。

配置SwitchA的STP。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] stp enable
```

其他交换机上的配置与SwitchA配置相同，配置过程略。

步骤2 在所有Switch上创建VLAN10，并配置接口加入VLAN10。

配置SwitchA的接口加入VLAN10。

```
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface ethernet 0/0/1
[SwitchA-Ethernet0/0/1] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/1] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/1] quit
[SwitchA] interface ethernet 0/0/2
[SwitchA-Ethernet0/0/2] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/2] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/2] quit
[SwitchA] interface ethernet 0/0/3
[SwitchA-Ethernet0/0/3] port hybrid pvid vlan 10
[SwitchA-Ethernet0/0/3] port hybrid untagged vlan 10
[SwitchA-Ethernet0/0/3] quit
```

其他交换机上的配置与SwitchA配置相同，配置过程略。

步骤3 在所有Switch上使能MLD Snooping功能

使能SwitchA的全局和VLAN10内MLD Snooping功能。

```
[SwitchA] mld-snooping enable
[SwitchA] vlan 10
[SwitchA-vlan10] mld-snooping enable
[SwitchA-vlan10] quit
```

其他交换机上的配置与SwitchA配置相同，配置过程略。

步骤4 配置SwitchA的MLD Snooping响应二层网络拓扑变化事件。

```
[SwitchA] mld-snooping send-query enable
[SwitchA] mld-snooping send-query source-address fe80::1
```

步骤5 验证配置结果。

1. 检查组播数据转发是否正常。

   查看SwitchA上的MLD报文统计信息。

```
<SwitchA> display mld-snooping statistics
 MLD Snooping Events Counter
     Recv VLAN Up Event Times      0
     Recv VLAN Down Event Times    0
     Recv VLAN Del Event Times     0
     Recv Port Up Event Times      0
     Recv Port Down Event Times    0
     Recv Port Del Event Times     0
     Recv Port Inc Event Times     0
     Recv Port Exc Event Times     0
     Recv MSTP Block Event Times   0
     Recv MSTP Forward Event Times 0
     Recv LINK Change Event Times  0
 MLD Snooping Packets Counter
   Statistics for VLAN 10
     Recv V1 Report  12
     Recv V2 Report  0
     Recv V1 Query   15
     Recv V2 Query   0
     Recv Done       0
     Recv Pim Hello  3
     Send Query(S=0) 0
     Send Query(S!=0)0
     Send General Query               0
     Send Group-Specific Query        0
     Send Group-Source-Specific Query 0
```

   可见SwitchA没有发送查询报文。

2. 在所有Switch上使用**display stp brief**命令，查看哪个接口被阻塞，从而判断组播数据的传送路径。

   发现观察结果是SwitchB的Eth0/0/1接口被阻塞。

```
<SwitchB> display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    Ethernet0/0/1               ALTE  DISCARDING    NONE
   0    Ethernet0/0/2               ROOT  FORWARDING      NONE
   0    Ethernet0/0/3               DESI  FORWARDING      NONE
```

   可以判断出，组播数据沿SwitchA→SwitchC→SwitchB到达HostA，沿SwitchA→SwitchD到达HostB。

3. 在SwitchC的接口Eth0/0/1上执行**shutdown**命令关闭该接口，使STP网络拓扑发生变化。

4. 观察网络拓扑发生变化后，HostA和HostB是否仍然能够收到组播数据。

   查看SwitchA的MLD报文统计信息。

```
<SwitchA> display mld-snooping statistics
 MLD Snooping Events Counter
     Recv VLAN Up Event Times      0
     Recv VLAN Down Event Times    0
     Recv VLAN Del Event Times     0
     Recv Port Up Event Times      0
     Recv Port Down Event Times    1
     Recv Port Del Event Times     0
     Recv Port Inc Event Times     1
     Recv Port Exc Event Times     2
     Recv MSTP Block Event Times   0
     Recv MSTP Forward Event Times 1
     Recv LINK Change Event Times  70
 MLD Snooping Packets Counter
   Statistics for VLAN 10
     Recv V1 Report  18
     Recv V2 Report  0
     Recv V1 Query   15
     Recv V2 Query   0
     Recv Done       0
     Recv Pim Hello  38
     Send Query(S=0) 8
     Send Query(S!=0) 0
     Send General Query               0
     Send Group-Specific Query        0
     Send Group-Source-Specific Query 0
```

   可见SwitchA已发送源地址为0的查询报文。

----结束

配置文件

- SwitchA的配置文件。

```
#
 sysname SwitchA
#
 mld-snooping enable
 mld-snooping send-query enable
 mld-snooping send-query source-address fe80:0:0:0:0:0:0:1
#
 vlan batch 10
#
 stp enable
#
vlan 10
 mld-snooping enable
#
interface Ethernet0/0/1
```

```
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SwitchB的配置文件。

```
#
 sysname SwitchB
#
 mld-snooping enable
#
 vlan batch 10
#
 stp enable
#
vlan 10
 mld-snooping enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SwitchC的配置文件。

```
#
 sysname SwitchC
#
 mld-snooping enable
#
 vlan batch 10
#
 stp enable
#
vlan 10
 mld-snooping enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

- SwitchD的配置文件。

```
#
 sysname SwitchD
#
 mld-snooping enable
#
 vlan batch 10
#
```

```
 stp enable
#
vlan 10
 mld-snooping enable
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet0/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

9.9 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。

9.9.1 二层组播不生效

故障现象

未配置MLD Snooping时，组播转发正常，配置了MLD Snooping功能后，发现用户无法收到组播数据。

操作步骤

步骤1 检查是否配置的MLD Snooping Version较低。

如果配置的MLD Snooping Version比用户主机的MLD版本低，设备在收到MLD Report报文后，只会向路由器端口转发，不会生成成员端口和转发表项。

执行**display mld-snooping configuration**命令查看配置信息。如果MLD Snooping Version比用户主机的MLD版本低，执行命令**mld-snooping version** *version*，配置与用户主机的MLD版本保持一致。

步骤2 检查是否配置的普遍组查询间隔不一致。

如果当前MLD Snooping设备的普遍组查询间隔比上游MLD查询器或者MLD Snooping设备的数值小，很容易造成当前MLD Snooping设备的MLD Snooping表项提前老化，无法转发上游发送过来的组播数据。

执行**display mld-snooping**命令查看MLD Snooping运行参数信息。如果普遍组查询间隔比上游MLD查询器或者MLD Snooping设备的数值小，执行命令**mld-snooping query-interval** *query-interval*，重新调整MLD Snooping普遍组查询间隔。建议调整的数值与上下游设备保持一致。

表9-3给出了华为S系列交换机普遍组查询间隔的缺省值。

表 9-3 普遍组查询间隔缺省值

特性	框式交换机缺省值	盒式交换机缺省值
MLD	125s	不涉及
MLD Snooping	60s	125s

步骤3 检查是否配置了成员端口快速离开功能。

当接口下仅有一个成员主机时，才能配置快速离开功能。如果接口下不止一个接收主机，而在VLAN配置了成员端口快速离开功能，则当交换机从成员端口收到MLD Done报文时，不发送特定组查询报文，立即将该接口的转发表项从设备的组播转发表中删除，导致流量不通。

执行**display mld-snooping configuration**命令查看配置信息，如果有“mld-snooping prompt-leave”，在VLAN视图下，执行**undo mld-snooping prompt-leave**命令，取消成员端口快速离开功能。

步骤4 检查是否配置了检查Router-Alert选项功能。

如果配置了对Router-Alert选项进行检查，则交换机会检查MLD报文中的Option字段，对于未携带Router-Alert选项的报文做丢弃处理。

执行**display mld-snooping configuration**命令查看配置信息，如果有“mld-snooping require-router-alert”，在VLAN视图下，执行**undo mld-snooping require-router-alert**命令，取消相关配置。

步骤5 检查是否配置了组播组过滤策略。

如果配置了组播组过滤策略，可能限制了VLAN下的主机加入组播组的范围，可以执行**display mld-snooping configuration**命令，查看组播组策略限制是否正确。如果配置了ACL6规则，再执行**display acl ipv6**命令查看对应的ACL6规则是否正确。

步骤6 检查是否配置了接口下的二层组播数据过滤功能。

如果设备接口下配置了二层组播数据过滤功能，会对来自某VLAN的UDP报文进行过滤，导致二层组播流量不通。

进入物理接口视图，执行**undo multicast-source-deny vlan**命令，取消接口下的二层组播数据过滤功能。

----结束

9.9.2 配置的 IPv6 组播组策略不生效

故障现象

在设备上配置了组播组策略，只允许主机加入某些特定的组播组，但主机仍然可以收到发往其他组播组的组播数据。

操作步骤

步骤1 执行**display acl ipv6**命令查看配置的ACL6规则，检查其是否匹配想要执行的组播组过滤策略。

步骤2 执行**display mld-snooping configuration**命令查看VLAN下是否应用了正确的组播组策略。如果没有，则使用**mld-snooping group-policy**命令应用正确的组播组策略。

步骤3 执行**display current-configuration**命令查看是否已使能丢弃未知组播数据报文的功能。如果没有使能，则使用**multicast drop-unknown**命令使能丢弃未知组播数据报文功能。

----结束