9 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。

说明

本章所涉及的交换机和交换机图标，是指使能了二层组播功能的路由器。

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。

9.11 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。

9.12 IGMP Snooping配置举例
针对如何配置IGMP Snooping基本功能、静态端口、二层组播SSM Mapping，分别提供配置举例。

9.13 IGMP Snooping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。

9.14 IP组播基础FAQ
介绍配置过程中常见的问题，并给出相应的解答。

9.15 IGMP Snooping参考信息
介绍IGMP Snooping的相关RFC清单。

9.1 IGMP Snooping 简介

介绍IGMP Snooping的定义和目的。

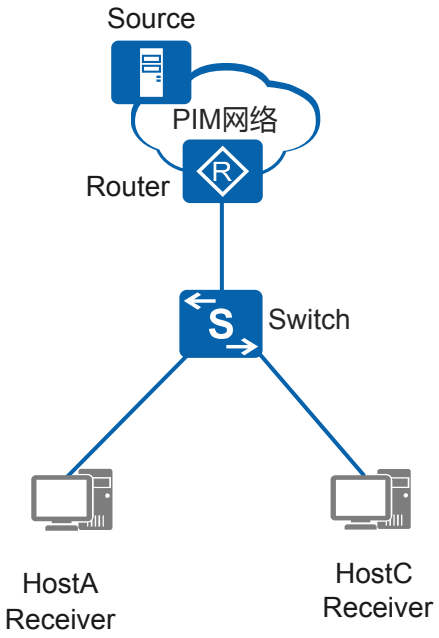
定义

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。

目的

在很多情况下，组播报文要不可避免地经过一些二层交换设备，尤其是在局域网环境里。如**图9-1**所示，在组播用户和三层组播设备Router之间，组播报文要经过二层交换机Switch。

图 9-1 IGMP Snooping 组网图



当Router将组播报文转发至Switch以后，Switch负责将组播报文转发给组播用户。由于组播报文的目的地址为组播组地址，在二层设备上是学习不到这一类MAC表项的，因此组播报文就会在所有接口进行广播，和它在同一广播域内的组播成员和非组播成员都能收到组播报文。这样不但浪费了网络带宽，而且影响了网络信息安全。

IGMP Snooping有效地解决了这个问题。配置IGMP Snooping后，二层组播设备可以侦听和分析组播用户和上游路由器之间的IGMP报文，根据这些信息建立二层组播转发表项，控制组播数据报文转发。这样就防止了组播数据在二层网络中的广播。

9.2 IGMP Snooping 原理描述

介绍IGMP Snooping的实现原理。

9.2.1 IGMP Snooping

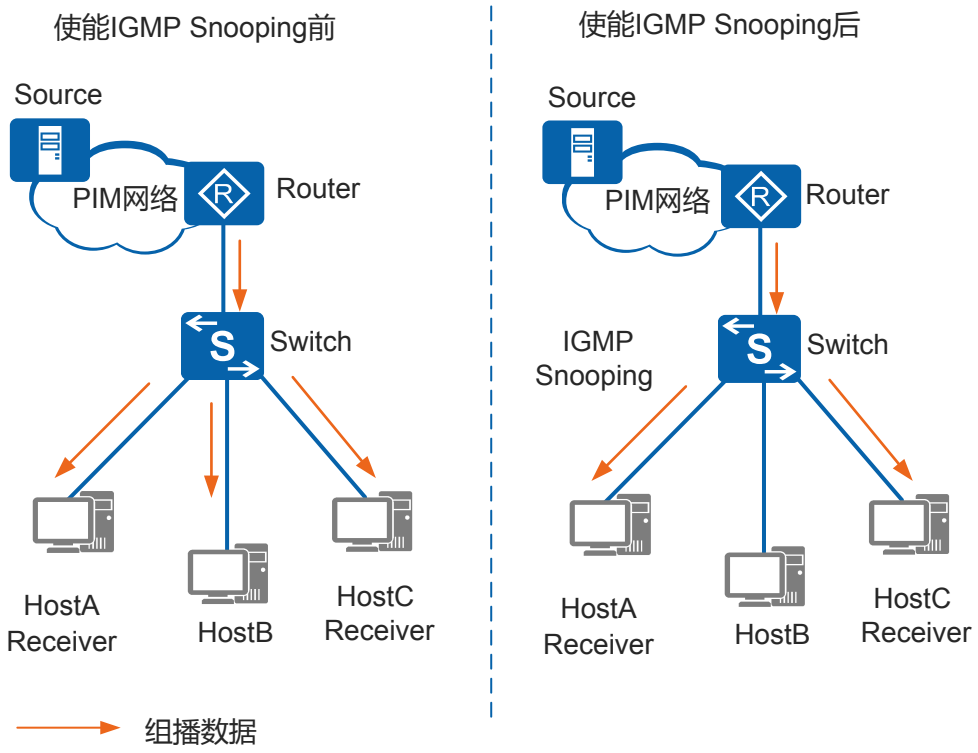
基本原理

IGMP Snooping是二层组播的基本功能，可以实现组播数据在数据链路层的转发和控制。当主机和上游三层设备之间传递的IGMP协议报文通过二层组播设备时，IGMP Snooping分析报文携带的信息，根据这些信息建立和维护二层组播转发表，从而指导组播数据在数据链路层按需转发。

如图9-2所示，当组播数据从三层组播设备Router转发下来以后，处于接入边缘的二层组播设备Switch负责将组播数据转发给用户主机，使用户收看所点播的节目。当Switch没有运行IGMP Snooping时，组播数据在二层被广播；当Switch运行了IGMP Snooping后，组播数据不会在二层广播，而是会被Switch发送给指定的接收者。

使能IGMP Snooping功能后，Switch会侦听主机和上游三层设备之间交互的IGMP报文，通过分析报文中携带的信息（报文类型、组播组地址、接收报文的接口等），建立和维护二层组播转发表，从而指导组播数据在数据链路层按需转发。

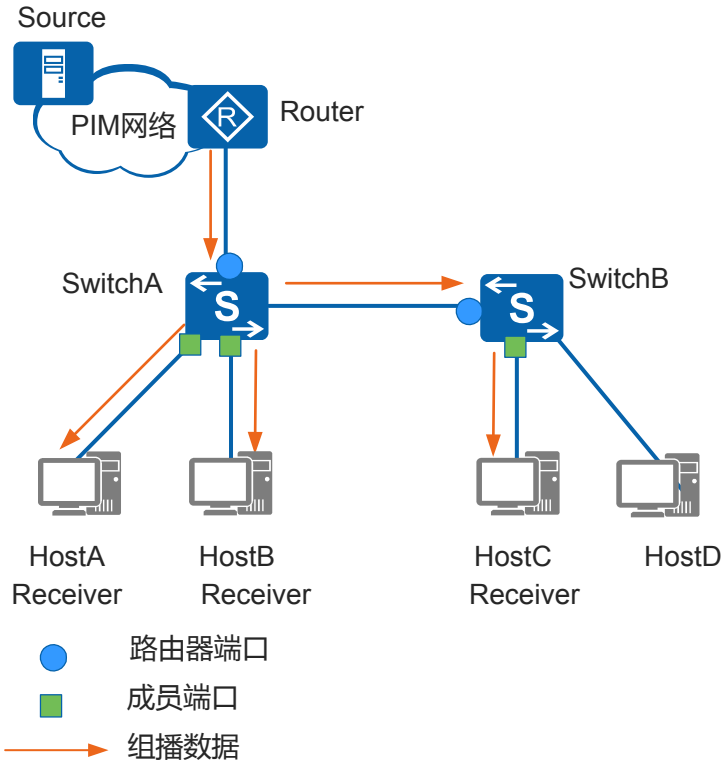
图 9-2 二层组播设备运行 IGMP Snooping 前后对比



基本概念

如图9-3所示，三层设备Router从组播源接收数据并向下游转发，在二层组播设备SwitchA和SwitchB上分别运行IGMP Snooping，HostA、HostB和HostC为接收者主机（即组播组成员）。

图 9-3 IGMP Snooping 相关端口



结合图9-3，介绍IGMP Snooping中相关端口的概念。

表 9-1 IGMP Snooping 中的端口角色

端口角色	作用	如何生成
路由器端口（Router Port） 如SwitchA和SwitchB上蓝色圆圈表示的接口。 **说明** 路由器端口都是指二层组播设备上朝向组播路由器的接口，而不是指路由器上的接口。	二层组播设备上朝向三层组播设备（DR或IGMP查询器）一侧的接口，二层组播设备从此接口接收组播数据报文。	● 由协议生成的路由器端口叫做动态路由器端口。收到源地址不为0.0.0.0的IGMP普遍组查询报文或PIM Hello报文（三层组播设备的PIM接口向外发送的用于发现并维持邻居关系的报文）的接口都将被视为动态路由器端口。 ● 手工配置的路由器端口叫做静态路由器端口。

端口角色	作用	如何生成
成员端口（Member Port） 如SwitchA和SwitchB上绿色方框表示的接口。	又称组播组成员端口，表示二层组播设备上朝向组播组成员一侧的端口，二层组播设备往此接口发送组播数据报文。	● 由协议生成的成员端口叫做动态成员端口。收到IGMP Report报文的接口，二层组播设备会将其标识为动态成员端口。 ● 手工配置的成员端口叫做静态成员端口。

路由器端口和成员端口，是二层组播转发表项中的一个重要信息：出接口。其中路由器端口相当于上游接口，成员端口相当于下游接口。通过协议报文学习到的端口，对应的为动态表项；而手工配置的端口，对应的为静态表项。

除了出接口外，每条表项还包括组播组地址和VLAN编号。

工作机制

二层组播设备运行了IGMP Snooping后，收到不同的IGMP协议报文会进行不同的处理，并在此过程中建立起二层组播转发表项。

表 9-2 IGMP Snooping 对不同报文的处理方式

IGMP工作阶段	二层组播设备收到的报文类型	处理方式
普遍组查询 IGMP查询器定期向本地网段内的所有主机与路由器（目的地址为224.0.0.1）发送IGMP普遍组查询报文，以查询该网段有哪些组播组的成员。	IGMP普遍组查询报文	向VLAN内除接收接口外的其他所有接口转发，并对接收接口做如下处理： ● 如果路由器端口列表中尚未包含该接口，则将其添加进去，并启动老化定时器。 ● 如果路由器端口列表中已包含该动态路由器端口，则重置老化定时器。 **说明** 收到IGMP普遍组查询报文时，动态路由器端口的老化定时器缺省为180秒，可以通过命令行配置。

IGMP工作阶段	二层组播设备收到的报文类型	处理方式
成员报告 有两种情况： ● 成员收到IGMP普遍组查询报文后，回应IGMP报告报文。 ● 成员主动向IGMP查询器发送IGMP报告报文以声明加入该组播组。	IGMP报告报文	向VLAN内所有路由器端口转发。从报文中解析出主机要加入的组播组地址，并对接收接口做如下处理： ● 如果不存在该组对应的转发表项，则创建转发表项，将该接口作为动态成员端口添加到出接口列表中，并启动老化定时器。 ● 如果已存在该组对应的转发表项，但出接口列表中未包含该接口，则将该接口作为动态成员端口添加到出接口列表，并启动老化定时器。 ● 如果已存在该组所对应的转发表项，且出接口列表中已包含该动态成员端口，则重置其老化定时器。 **说明** 收到IGMP报告报文后，动态成员端口的老化定时器 = 健壮系数 x 普遍组查询间隔 + 最大响应时间。

IGMP工作阶段	二层组播设备收到的报文类型	处理方式
成员离开组播组 有两个阶段： 1. 运行IGMPv2或IGMPv3的成员发送IGMP离开报文，以通知IGMP查询器自己离开了某个组播组。 2. IGMP查询器收到IGMP离开报文后，从中解析出组播组地址，并通过接收接口向该组播组发送IGMP特定组查询报文/IGMP特定源组查询报文。	IGMP离开报文	判断离开的组是否存在对应的转发表项，以及转发表项出接口列表是否包含报文的接收接口： ● 如果不存在该组对应的转发表项，或者该组对应转发表项的出接口列表中不包含接收接口，二层组播设备不转发该报文，将其直接丢弃。 ● 如果存在该组对应的转发表项，且转发表项的出接口列表中包含该接口，二层组播设备会将报文向VLAN内所有路由器端口转发。 对于IGMP离开报文的接收接口（假定为动态成员端口），二层组播设备在其老化时间内： ● 如果从该接口收到了主机响应IGMP特定组/源组查询的报告报文，表示接口下还有该组的成员，于是重置其老化定时器。 ● 如果没有从该接口收到主机响应IGMP特定组/源组查询的报告报文，则表示接口下已没有该组成员，则在老化时间超时后，将接口从该组的转发表项出接口列表中删除。 **说明** 收到IGMP离开报文后，动态成员端口的老化定时器＝健壮系数 x 特定组查询间隔。
	IGMP特定组查询报文/IGMP特定源组查询报文	向有特定组成员的接口转发。

此外，当二层组播设备收到PIM Hello报文时，向VLAN内除接收接口外的其他所有接口转发，并对接收接口做如下处理：

- 如果路由器端口列表中已包含该动态路由器端口，则重置老化定时器。
- 如果路由器端口列表中尚未包含该接口，则将其添加进去，并启动老化定时器。

说明

收到PIM Hello报文时，动态路由器端口的老化时间为Hello报文中Holdtime字段的值。

如果配置了静态路由器端口，二层组播设备收到IGMP报告和离开报文也会向静态路由器端口转发。如果配置了静态成员端口，则转发表项中会添加该接口为出接口。

当二层组播设备上建立了二层组播转发表项以后，二层组播设备接收到组播数据报文时，依据报文所属VLAN和报文的目的地址（即组播组地址）查找转发表项是否存在对应的“出接口信息”。如果存在，则将报文发送到相应的组播组成员端口和路由器端口；如果不存在，则丢弃该报文或将报文在VLAN内广播。

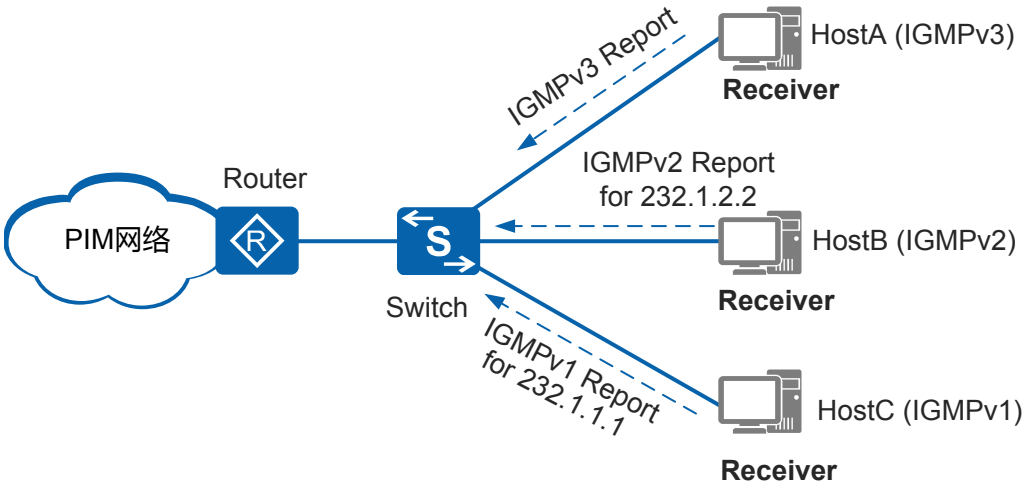
9.2.2 IGMP Snooping SSM Mapping

SSM（Source-Specific Multicast）称为指定源组播，SSM相比ASM（Any-Source Multicast）组播技术，可节省组播地址并有更好的安全性，但只有IGMPv3支持SSM。如果成员主机上运行IGMPv3，可以在成员报告报文中直接指定组播源地址。但是某些情况下，用户主机只能运行IGMPv1或IGMPv2，为了使其也能够使用SSM服务，组播设备需要提供IGMP Snooping SSM Mapping功能。

IGMP Snooping SSM Mapping就是IPv4组播网络中的二层SSM Mapping。IGMP Snooping SSM Mapping通过在二层设备上静态配置SSM地址的映射规则，将IGMPv1和IGMPv2报告报文中的（*，G）信息转化为对应的（S，G）信息，以提供SSM组播服务。S表示组播源，G表示组播组，*表示任意组播源。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SSM组策略，改变SSM组地址范围。

如图9-4所示，三个接收者运行不同版本的IGMP，HostB和HostC无法升级到IGMPv3，如果要为该网段中的所有主机提供SSM服务，可以在二层设备Switch上使用IGMP Snooping SSM Mapping功能。

图 9-4 IGMP Snooping SSM Mapping 组网图



假如在Switch上配置如下映射关系。

组播组地址	映射的组播源地址
232.1.1.0/24	10.10.1.1
232.1.2.0/24	10.10.2.2
232.1.3.0/24	10.10.3.3

则经过映射后，Switch收到HostB和HostC的成员报告报文时，首先判断报文携带的组地址是否在SSM范围内，发现在SSM范围内，则根据配置的映射规则生成如下所示的组播表项。

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

如果报告报文携带的组地址在SSM范围内，但是Switch上没有对应的SSM Mapping规则，则无法提供SSM服务，丢弃该报文。

如果报告报文携带的组地址不在SSM范围内，则只提供ASM服务。

说明

实际组网中如果存在上游IGMP查询器，则二层SSM Mapping功能需要与IGMP查询器的三层SSM Mapping功能配合使用（配置相应的映射规则），才能实现组播数据的正常转发。

9.3 IGMP Snooping 应用场景

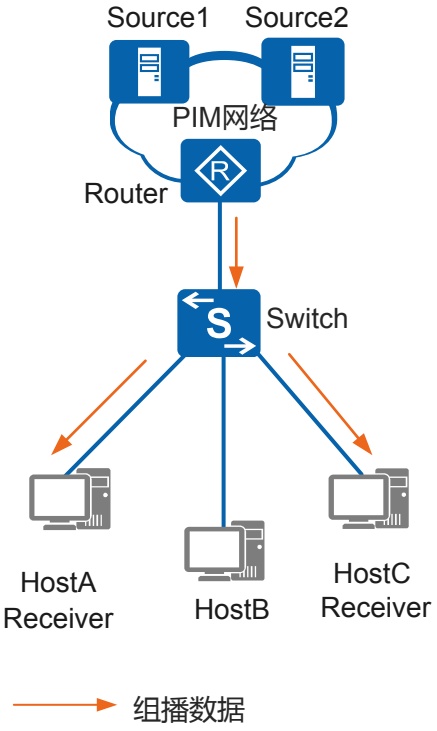
介绍IGMP Snooping的应用场景。

9.3.1 IGMP Snooping 的应用

组网描述

如图9-5所示，PIM网络中有多个组播源（如Source1和Source2）向局域网提供组播视频服务，局域网中部分用户（如HostA和HostC）希望通过组播方式接收视频数据。为了避免组播数据在局域网中广播而引起的网络带宽浪费和无法预知的网络信息安全问题，可以在二层组播设备上部署IGMP Snooping，实现组播数据在二层网络中的精确转发。

图 9-5 IGMP Snooping 应用组网图



部署特性

可以在图9-5所示组网中部署以下特性来实现组播数据在网络中的精确转发。

- 在三层组播设备Router上部署PIM和IGMP，将组播数据引流到用户网段。
- 在二层组播设备Switch上部署IGMP Snooping，使得Switch可以建立和维护二层组播转发表，指导组播数据只转发给有组播数据需求的用户。
- 当成员主机只能运行IGMPv1/IGMPv2又想使用SSM服务时（即想指定接收哪些组播源的组播数据），可以在Switch上部署IGMP Snooping SSM Mapping，为这部分用户提供SSM服务。

  说明

  二层SSM Mapping功能需要与IGMP查询器的三层SSM Mapping功能配合使用（配置相应的映射规则），才能实现组播数据的正常转发。

9.4 配置 IGMP Snooping 任务概览

介绍IGMP Snooping的配置任务概览。

IGMP Snooping的配置任务如表9-3所示。

表 9-3 IGMP Snooping 的配置任务概览

场景	描述	对应任务
配置IGMP Snooping基本功能	当组播数据转发至用户网段的二层组播设备时，为了避免组播数据在广播域中的泛滥，实现组播数据在数据链路层的精确转发，可以在二层组播设备上配置IGMP Snooping基本功能。配置IGMP Snooping后，二层组播设备可以侦听和分析组播用户和上游路由器之间的IGMP报文，从而建立二层组播转发表项，控制组播数据报文转发。这样就防止了组播数据在二层网络中的广播。	**9.7 配置IGMP Snooping基本功能**
配置IGMP Snooping策略	如果需要在二层组播设备上对组播报文进行过滤，或者需要限制成员主机加入的组播组范围，可以在二层组播设备上配置相应的IGMP Snooping策略。	**9.8 配置IGMP Snooping策略**
配置成员关系快速刷新	为了提高组播业务运行效率、提升用户体验，使得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，可以在二层组播设备上配置成员关系快速刷新。	**9.9 配置成员关系快速刷新**
配置IGMP Snooping SSM Mapping	在二层网络中，如果某些成员主机只能运行IGMPv1或IGMPv2，但是这些用户希望享受SSM服务，就需要在二层组播设备上配置IGMP Snooping SSM Mapping功能。	**9.10 配置IGMP Snooping SSM Mapping**

9.5 IGMP Snooping 配置注意事项

介绍配置IGMP Snooping的配置注意事项。

涉及网元

一个完整的IPv4组播网络涉及以下网元：

- 组播源：发送组播数据给组播用户主机，比如视频服务器。
- 运行PIM（IPv4）协议的设备：通过PIM（IPv4）协议生成组播路由表项，转发组播数据。在组播网络里，所有三层设备上都需要运行PIM（IPv4）协议，否则组播转发路径无法正常建立。
- 运行MSDP协议的设备：实现跨PIM网络的组播数据转发，所以主要应用在网络规模大的场合。比如两个AS系统需要实现组播通信，就在AS间的边缘设备上运行MSDP协议。
- IGMP查询器：与组播用户主机之间交互IGMP报文，建立和维护组播组成员关系。在组播网络里，连接用户侧的三层设备都需要运行IGMP协议或者静态配置IGMP组播组，否则上游运行PIM协议的设备无法了解到用户需求，组播转发路径无法正常建立。
- 运行IGMP Snooping的设备：通过侦听上游三层组播设备与组播用户主机之间交互的IGMP报文，生成二层组播转发表项，指导组播数据在二层网络的精确转发。为了避免组播报文二层网络广播，减少带宽浪费，建议在二层设备上配置IGMP Snooping功能。
- 接收者：接收组播数据的组播用户。接收者可以为PC、机顶盒等，但是需要具备相应的组播客户端软件。

License 支持

IGMP Snooping是路由器的基本特性，无需获得License许可应用此功能。

特性依赖和限制

在路由器上部署IGMP Snooping功能时需注意：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。

说明

仅AR2200&AR3200&AR3600系列支持IGMP Snooping。

仅8FE1GE、24GE和24ES2GP单板支持IGMP Snooping。

9.6 IGMP Snooping 缺省配置

介绍缺省情况下，IGMP Snooping的配置信息。

表 9-4 IGMP Snooping 缺省配置

参数	缺省值
IGMP Snooping功能	未使能
IGMP Snooping版本	缺省情况下，IGMP Snooping可以处理IGMPv1、IGMPv2版本的报文。
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	60s

参数	缺省值
IGMP Snooping报文抑制	未使能
IGMP Snooping SSM Mapping	未使能

9.7 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

9.7.1 使能IGMP Snooping功能和**9.7.2 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。

9.7.1 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，路由器的全局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 执行命令**igmp-snooping enable**，使能VLAN的IGMP Snooping功能。

----结束

9.7.2 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。

----结束

9.7.3 （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

9.7.4 （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

9.7.5 （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接口使能了三层组播功能（例如IGMP、PIM），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，路由器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，请确保路由器发送的普遍组查询报文的源IP地址比上游IGMP查询器的IP地址大。

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。	60秒	IGMPv1、IGMPv2、IGMPv3
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

查询器参数	配置命令	参数说明	缺省值	支持的版本
IGMP查询报文的最大响应时间	**igmp-snooping max-response-time** *max-response-time*	当路由器收到主机的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
特定组查询报文的发送间隔	**igmp-snooping lastmember-queryinterval** *lastmember-queryinterval*	当路由器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

9.7.6 （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，路由器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接口使能三层组播功能（例如IGMP、PIM）。
- 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

9.7.7 （可选）配置 Router-Alert 选项

背景信息

出于兼容性考虑，缺省情况下路由器不对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，路由器在发送的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

9.7.8 检查配置 IGMP Snooping 基本功能的结果

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。
- 使用命令**display igmp-snooping querier vlan** [*vlan-id*]，查看IGMP Snooping查询器使能信息。

----结束

9.8 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

9.7 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。

9.8.1 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《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列企业路由器 配置指南-安全》中的“ACL配置”。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 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，则路由器对接收到的所有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。

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。

----结束

9.8.2 配置丢弃未知组播流

背景信息

未知组播流，即组播转发表中不存在对应表项的组播报文。缺省情况下，路由器对未知组播流的处理方式为在VLAN内广播。通过配置丢弃未知组播流，可以节省瞬时带宽占用率。

说明

AR2204-24GE、AR2204-27GE、AR2204-27GE-P、AR2204-48GE-P、AR2204-51GE、AR2204-51GE-P、AR2204-51GE-R、AR2204E、AR2204E-D、AR2204XE、AR2204XE-DC、AR2220L、AR2220E和AR2240C不支持此功能。

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**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

配置本命令后，丢弃一切未知组播报文，包括在VLAN内透传的使用保留组播地址的协议报文。

----结束

9.8.3 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。

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。

----结束

9.8.4 检查配置 IGMP Snooping 策略的结果

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

9.9 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

9.7 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。

9.9.1 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60秒。

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

9.9.2 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

9.9.3 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路由器从成员端口接收到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。
- 只有当路由器在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《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列企业路由器 配置指南-安全》中“ACL配置”。

----结束

9.9.4 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。配置路由器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，将组播数据流及时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），保证设备能够及时更新端口信息，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

9.9.5 检查配置成员关系快速刷新的结果

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

9.10 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**9.7.1 使能IGMP Snooping功能**。

配置流程

一般情况下**9.10.2 配置IGMP Snooping SSM Mapping功能**即可，如果需要改变SSM组地址范围，可以选配**9.10.1 （可选）配置SSM组策略**。

9.10.1 （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《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列企业路由器 配置指南-安全》中的“ACL配置”。

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

9.10.2 配置 IGMP Snooping SSM Mapping 功能

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。

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**9.10.1 （可选）配置SSM组策略**。

----结束

9.10.3 检查配置 IGMP Snooping SSM Mapping 的结果

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

9.11 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。

9.11.1 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

9.11.2 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

9.11.3 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-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

9.12 IGMP Snooping 配置举例

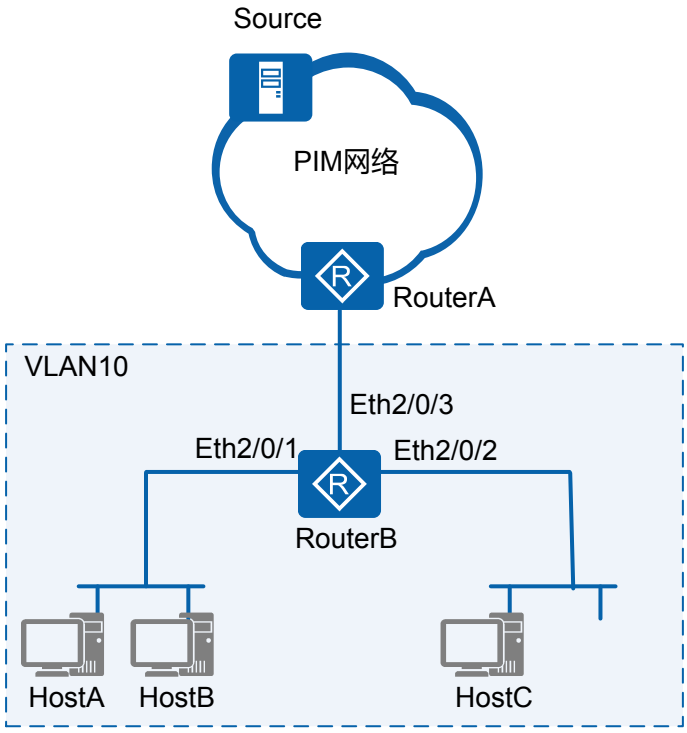
针对如何配置IGMP Snooping基本功能、静态端口、二层组播SSM Mapping，分别提供配置举例。

9.12.1 配置 IGMP Snooping 示例

组网需求

如图9-6所示组播网络中，路由器RouterA通过二层设备RouterB连接用户网络，RouterB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 9-6 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RouterB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。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] vlan 10
[RouterB-vlan10] quit
[RouterB] interface ethernet 2/0/1
[RouterB-Ethernet2/0/1] port hybrid pvid vlan 10
[RouterB-Ethernet2/0/1] port hybrid untagged vlan 10
[RouterB-Ethernet2/0/1] quit
[RouterB] interface ethernet 2/0/2
```

```
[RouterB-Ethernet2/0/2] port hybrid pvid vlan 10
[RouterB-Ethernet2/0/2] port hybrid untagged vlan 10
[RouterB-Ethernet2/0/2] quit
[RouterB] interface ethernet 2/0/3
[RouterB-Ethernet2/0/3] port hybrid pvid vlan 10
[RouterB-Ethernet2/0/3] port hybrid untagged vlan 10
[RouterB-Ethernet2/0/3] quit
```

步骤2 使能IGMP Snooping功能。

使能全局的IGMP Snooping功能。

```
[RouterB] igmp-snooping enable
```

使能VLAN10的IGMP Snooping功能。

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

步骤3 配置并应用组播组过滤策略。

配置组播组过滤策略。

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

在VLAN10内应用组播组过滤策略。

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

步骤4 验证配置结果。

查看RouterB上的端口信息。

```
<RouterB> display igmp-snooping port-info vlan 10
 ----------------------------------------------------------------------
                    (Source, Group)  Port                          Flag
 ----------------------------------------------------------------------
 VLAN 10, 3 Entry(s)
                     (*, 225.1.1.1)  Ethernet2/0/1                 -D-
                                     Ethernet2/0/2                 -D-
                                               2 port(s)
                     (*, 225.1.1.2)  Ethernet2/0/1                 -D-
                                     Ethernet2/0/2                 -D-
                                               2 port(s)
                     (*, 225.1.1.3)  Ethernet2/0/1                 -D-
                                     Ethernet2/0/2                 -D-
                                               2 port(s)
 ----------------------------------------------------------------------
```

由显示信息可知，组225.1.1.1～225.1.1.3已在RouterB上动态生成的成员端口为Eth2/0/1和Eth2/0/2。

查看RouterB上二层组播转发表。

```
<RouterB> display l2-multicast forwarding-table vlan 10
VLAN ID : 10, Forwarding Mode : IP
--------------------------------------------------------------------------
                    (Source, Group)    Interface               Out-Vlan
--------------------------------------------------------------------------
                       Router-port     Ethernet2/0/3             10
                     (*, 225.1.1.1)    Ethernet2/0/3             10
                                       Ethernet2/0/1             10
                                       Ethernet2/0/2             10
```



```
                      (*, 225.1.1.2)    Ethernet2/0/3             10
                                        Ethernet2/0/1             10
                                        Ethernet2/0/2             10
                      (*, 225.1.1.3)    Ethernet2/0/3             10
                                        Ethernet2/0/1             10
                                        Ethernet2/0/2             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

- RouterB的配置文件

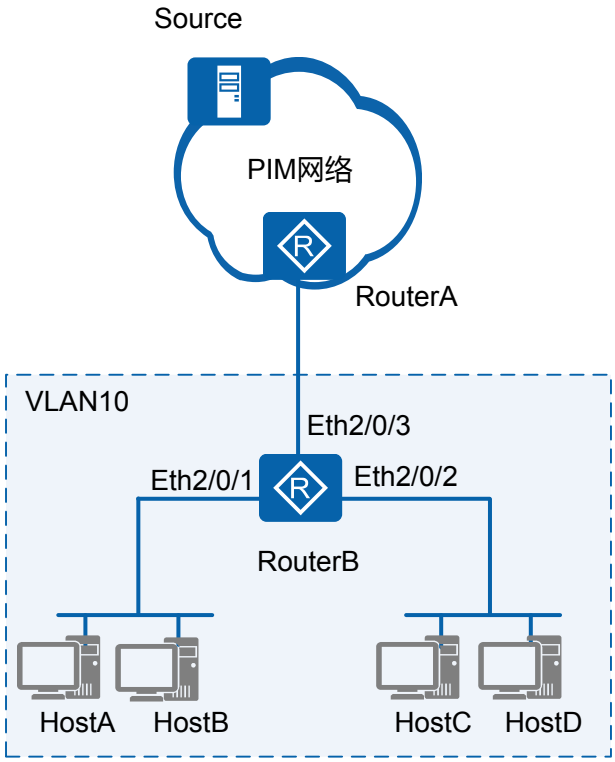
```
#
 sysname RouterB
#
vlan batch 10
#
igmp-snooping enable
#
acl number 2000
 rule 5 deny source 225.1.1.4 0
 rule 10 deny source 225.1.1.5 0
#
vlan 10
 igmp-snooping enable
 igmp-snooping group-policy 2000
#
interface Ethernet2/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet2/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet2/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

9.12.2 配置使用静态端口实现二层组播示例

组网需求

如图9-7所示组播网络中，路由器RouterA通过二层设备RouterB连接用户网络，RouterA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 9-7 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RouterB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。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] vlan 10
[RouterB-vlan10] quit
[RouterB] interface ethernet 2/0/1
[RouterB-Ethernet2/0/1] port hybrid pvid vlan 10
[RouterB-Ethernet2/0/1] port hybrid untagged vlan 10
[RouterB-Ethernet2/0/1] quit
[RouterB] interface ethernet 2/0/2
[RouterB-Ethernet2/0/2] port hybrid pvid vlan 10
[RouterB-Ethernet2/0/2] port hybrid untagged vlan 10
[RouterB-Ethernet2/0/2] quit
[RouterB] interface ethernet 2/0/3
[RouterB-Ethernet2/0/3] port hybrid pvid vlan 10
[RouterB-Ethernet2/0/3] port hybrid untagged vlan 10
[RouterB-Ethernet2/0/3] quit
```

步骤2 使能IGMP Snooping功能。

使能全局的IGMP Snooping功能。

```
[RouterB] igmp-snooping enable
```

使能VLAN10的IGMP Snooping功能。

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

步骤3 配置静态路由器端口。

```
[RouterB] interface ethernet 2/0/3
[RouterB-Ethernet2/0/3] igmp-snooping static-router-port vlan 10
[RouterB-Ethernet2/0/3] quit
```

步骤4 配置静态成员端口。

```
[RouterB] interface ethernet 2/0/1
[RouterB-Ethernet2/0/1] l2-multicast static-group group-address 225.1.1.1 to 225.1.1.3 vlan 10
[RouterB-Ethernet2/0/1] quit
[RouterB] interface ethernet 2/0/2
[RouterB-Ethernet2/0/2] l2-multicast static-group group-address 225.1.1.4 to 225.1.1.5 vlan 10
[RouterB-Ethernet2/0/2] quit
```

步骤5 验证配置结果。

查看RouterB上的路由器端口信息。

```
<RouterB> display igmp-snooping router-port vlan 10
 Port Name                       UpTime        Expires       Flags
 ----------------------------------------------------------------------
 VLAN 10, 1 router-port(s)
 Ethernet2/0/3                   00:20:09      --            STATIC
```

由显示信息可知，Eth2/0/3已成为静态路由器端口。

查看RouterB上的成员端口信息。

```
<RouterB> display igmp-snooping port-info vlan 10
 ----------------------------------------------------------------------
                     (Source, Group)  Port                          Flag
 ----------------------------------------------------------------------
 VLAN 10, 5 Entry(s)
                      (*, 225.1.1.1)  Ethernet2/0/1                 S--
                                                1 port(s)
                      (*, 225.1.1.2)  Ethernet2/0/1                 S--
                                                1 port(s)
                      (*, 225.1.1.3)  Ethernet2/0/1                 S--
                                                1 port(s)
                      (*, 225.1.1.4)  Ethernet2/0/2                 S--
                                                1 port(s)
                      (*, 225.1.1.5)  Ethernet2/0/2                 S--
                                                1 port(s)
 ----------------------------------------------------------------------
```

由显示信息可知，组225.1.1.1～225.1.1.3在RouterB上有静态成员端口Eth2/0/1，组225.1.1.4～225.1.1.5在RouterB上有静态成员端口Eth2/0/2。

查看RouterB上二层组播转发表。

```
<RouterB> display l2-multicast forwarding-table vlan 10
VLAN ID : 10, Forwarding Mode : IP
------------------------------------------------------------------------------
                     (Source, Group)    Interface                 Out-Vlan
------------------------------------------------------------------------------
                        Router-port     Ethernet2/0/3             10
                      (*, 225.1.1.1)    Ethernet2/0/1             10
```



```
                                    Ethernet2/0/3              10
                    (*, 225.1.1.2)  Ethernet2/0/1              10
                                    Ethernet2/0/3              10
                    (*, 225.1.1.3)  Ethernet2/0/1              10
                                    Ethernet2/0/3              10
                    (*, 225.1.1.4)  Ethernet2/0/2              10
                                    Ethernet2/0/3              10
                    (*, 225.1.1.5)  Ethernet2/0/2              10
                                    Ethernet2/0/3              10
Total Group(s) : 5
------------------------------------------------------------------------------
```

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

----结束

配置文件

- RouterB的配置文件

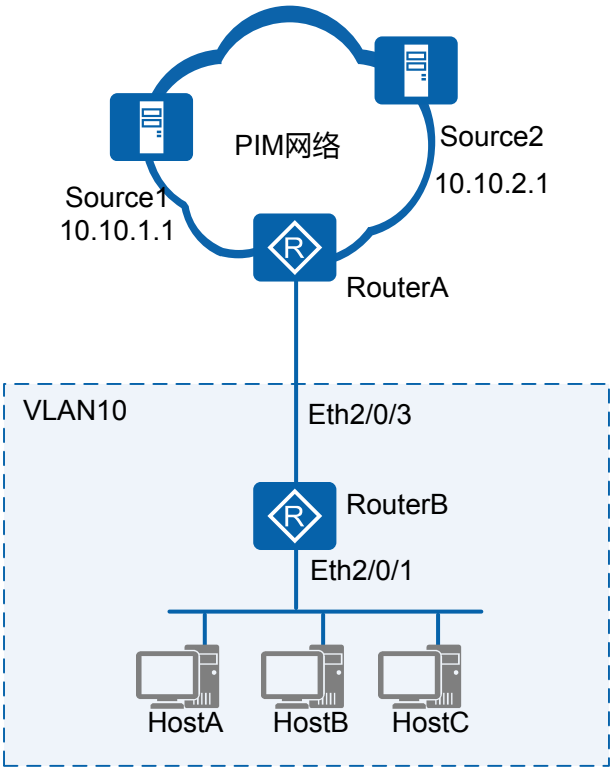
```
#
 sysname RouterB
#
vlan batch 10
#
igmp-snooping enable
#
vlan 10
 igmp-snooping enable
#
interface Ethernet2/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 l2-multicast static-group group-address 225.1.1.1 to 225.1.1.3 vlan 10
#
interface Ethernet2/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 l2-multicast static-group group-address 225.1.1.4 to 225.1.1.5 vlan 10
#
interface Ethernet2/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 igmp-snooping static-router-port vlan 10
#
return
```

9.12.3 配置二层组播 SSM Mapping 功能示例

组网需求

如图9-8所示组播网络中，路由器RouterA通过二层设备RouterB连接用户网络。RouterA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 9-8 配置二层组播 SSM Mapping 功能组网图



配置思路

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

1. 在RouterB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的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。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] vlan 10
[RouterB-vlan10] quit
[RouterB] interface ethernet 2/0/1
[RouterB-Ethernet2/0/1] port hybrid pvid vlan 10
[RouterB-Ethernet2/0/1] port hybrid untagged vlan 10
[RouterB-Ethernet2/0/1] quit
[RouterB] interface ethernet 2/0/3
[RouterB-Ethernet2/0/3] port hybrid pvid vlan 10
[RouterB-Ethernet2/0/3] port hybrid untagged vlan 10
[RouterB-Ethernet2/0/3] quit
```

步骤2 使能IGMP Snooping功能。

使能全局的IGMP Snooping功能。

```
[RouterB] igmp-snooping enable
```

使能VLAN10的IGMP Snooping功能。

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

```
[RouterB] acl number 2008
[RouterB-acl-basic-2008] rule 5 permit source 225.1.1.1 0
[RouterB-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。

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

步骤4 配置SSM Mapping功能。

配置RouterB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。

```
[RouterB-vlan10] igmp-snooping version 3
[RouterB-vlan10] igmp-snooping ssm-mapping enable
[RouterB-vlan10] igmp-snooping ssm-mapping 225.1.1.1 32 10.10.1.1
[RouterB-vlan10] quit
```

步骤5 验证配置结果。

查看VLAN内IGMP Snooping的配置情况。

```
<RouterB> display igmp-snooping vlan configuration
 IGMP Snooping Configuration for VLAN 10
     igmp-snooping enable
     igmp-snooping version 3
     igmp-snooping ssm-mapping enable
     igmp-snooping ssm-policy 2008
     igmp-snooping ssm-mapping 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。

```
<RouterB> display l2-multicast forwarding-table vlan 10
VLAN ID : 10, Forwarding Mode : IP
--------------------------------------------------------------------------------
                    (Source, Group)    Interface                   Out-Vlan
--------------------------------------------------------------------------------
                        Router-port    Ethernet2/0/3               10
             (10.10.1.1, 225.1.1.1)    Ethernet2/0/1               10
                                       Ethernet2/0/3               10
Total Group(s) : 1
--------------------------------------------------------------------------------
```

由显示信息可知，RouterB上生成(10.10.1.1, 225.1.1.1)表项，是Source1发送的数据。

----结束

配置文件

- RouterB的配置文件

```
#
 sysname RouterB
```

```
#
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 Ethernet2/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet2/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

9.13 IGMP Snooping 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。

9.13.1 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。

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，则当路由器从成员端口收到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，则路由器会检查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。

----结束

9.13.2 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

9.14 IP 组播基础 FAQ

介绍配置过程中常见的问题，并给出相应的解答。

9.14.1 AR 路由器是否支持报文按组播 MAC 地址转发

不支持。

9.15 IGMP Snooping 参考信息

介绍IGMP Snooping的相关RFC清单。

本特性的参考资料清单如下：

文档	描述	备注
RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches	-
RFC 1112	Host Extensions for IP Multicasting	-
RFC 2236	Internet Group Management Protocol, Version 2	-
RFC 3376	Internet Group Management Protocol, Version 3	-
RFC 4604	Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast	-

