H3C Comware V7 平台交换机 IGMP-Snooping 转发表项 生成部署经验分享

IGMP IGMP Snooping 二层转发 丁犁 2021-02-27 发表

组网及说明

背景介绍

IGMP Snooping（Internet Group Management Protocol Snooping，互联网组管理协议窥探）官方的解释为：运行在二层设备上，通过侦听三层设备与主机之间的IGMP报文来生成二层组播转发表，从而管理和控制组播数据报文的转发，实现组播数据报文在二层的按需分发。

翻译一下 IGMP Snooping 的作用，即：在（注意）二层 设备，广播域（VLAN）中，组播流量不再采用“泛洪”转发，而是采用“按需分发”（谁请求就发给谁）的方式转发。避免了二层网络带宽的浪费，有效控制组播转发范围提高安全性。

IGMP Snooping转发表项介绍

IGMP-Snooping 想要实现上述背景介绍中的功能，其中依靠的核心技术（表项）之一，即是——“IGMP Snooping转发表项”（display igmp-snooping group）。该表项包含如下三个重要参数：

VLAN	组播IP	Host Ports

可理解为：某个VLAN中的组播IP流量，通过匹配上述表项，获悉需要转发的“Host Ports”的组播接收端成员接口，其他非“Host Ports”下的组播接收端将不会收到相应组播流量。

IGMP Snooping转发表项可通过静态/动态方式，进行“VLAN、组播IP、Host Ports（成员端口）”对应关系的建立：

- 动态方式：通过自动监听组播接收端发出的 IGMP成员关系报告报文（该报文可简单理解为：组播接收端发声说“我想获取某组播IP流量，快将相关流量发给我吧“），动态建立；
- 静态方式：通过手动接口视图下配置igmp-snooping static-group命令，静态建立。

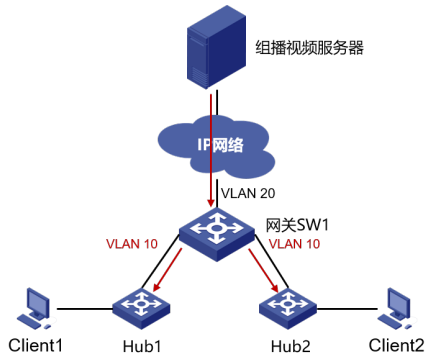
实际网络中，由于组播IP的多样性，以及组播接收端的移动性（Host Ports 成员端口不固定），通常采用动态方式生成相关IGMP Snooping转发表项。

问题描述

实际场景

用如下简图进行说明，网络中 Client1、Client2 作为组播接收端，属于相同的广播域（VLAN 10）中，其网关均在 SW1 三层交换机上。

通过在 SW1 交换机上使能 IGMP + PIM 功能，实现组播视频服务器的组播流量可转发给 Client1、Client2 。



在这样的场景中，实际存在二层网络带宽资源浪费和安全的问题。

即，当 Client 1 请求并接收相关组播视频流量后，即便 Client 2 没有请求，也将被动的收到自身不需要的组播视频流量（与 Client 1 接收到的流量相同）。

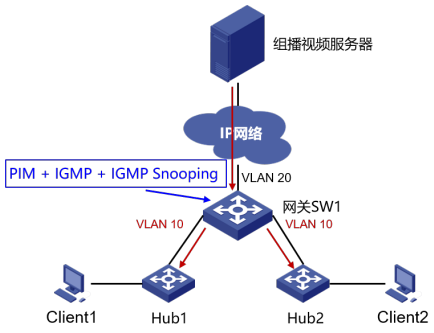
因为，SW1 没有部署 IGMP Snooping ，只要 VLAN 10 中有任意一个组播接收者，请求了组播流量，当组播流量送达 SW1 后，SW1 天然就会在 VLAN 10 中“泛洪”转发。导致 SW1 至 Client2 中间的网络带宽被占用，同时 Client 2 可嗅探到 Client 1访问的视频流量，造成Client 1 访问流量泄密。

新增 IGMP-Snooping 功能后业务断开后自动恢复

通过上述实际场景介绍，我们得知若需要避免资源浪费和安全的问题，就得部署 IGMP-Snooping 功能。

目前我司Comware V7平台大部分交换机（具体可来电400，咨询产品人员），新软件版本均支持在部署 IGMP 的情况下，同时部署开启 IGMP-Snooping 功能。

但是，当在如下图所示的环境中（SW1 已经使能 PIM + IGMP ，并且组播业务已在正常转发的网络中），再在 SW1 上使能 IGMP-Snooping 功能后，组播接收者将立刻出现组播流量异常中断的故障，但过几秒或几分钟后就自动恢复的情况。



过程分析

开始分析

为何在上述情况新增使能 IGMP-Snooping 功能后，就出现组播接收者流量立刻中断，过一会儿又自动恢复呢？要想理解该问题，我们需要了解使能 IGMP-Snooping 功能后，设备所产生了哪些动作。

回顾前面“IGMP Snooping转发表项介绍”内容，我们可得知，当使能 IGMP-Snooping 功能后，设备将生成“IGMP Snooping转发表项”，但是刚生成时，表项如下图所示，数据为空。即此时 display igmp-snooping group 为空。

VLAN	组播IP	Host Ports

当“IGMP Snooping转发表项”为空时，组播流量将无法在设备上进行转发。这就是为何使能 IGMP-Snooping功能后组播接收者立刻出现组播流量异常中断的故障原因。

后续随着时间推移，当 SW1 监听到（收到）组播接收端（Client 1 或 Client 2），发出的IGMP成员关系报告报文，自动填充 IGMP Snooping转发表项相关内容后，组播业务流量就将根据表项指定的 Host Ports 进行后续的处理，最终完成组播业务流量“定向”的转发。即，故障出现时，等待几秒或几分钟后就自动恢复的原因。

VLAN	组播IP	Host Ports
10	224.1.1.1	Client1 Port

决定组播业务自动恢复的时间，到底是几秒钟还是几分钟，其关键点就是 SW1 何时能够收到组播接收端（Client 1 或 Client 2）发出的 IGMP成员关系报告报文。对于组播接收端 Client 何时发送IGMP成员关系报告报文的因素，通常有以下两种：

1. 如果主机要加入某个组播组，它会主动向IGMP查询器发送 IGMP 成员关系报告报文以声明加入该组播组。

2. 当组播组接收端 Client 收到 网关设备发送的 IGMP 普遍组查询报文后，会回复 IGMP 成员关系报告报文。

对于第1点，决定权在主机 Client 侧，网络设备无法进行控制；

对于第2点，网络设备网（关 SW1）只要 能够“即时快速”的发送IGMP 普遍组查询报文，理论上就可快速收到 Client 回复的 IGMP 成员关系报告报文，进而缩短 IGMP Snooping转发表项为空的时间，保证组播业务快速恢复。

当前 Comware V7 平台交换机缺省 IGMP 普遍组查询报文的发送间隔为125秒；缺省 IGMP 普遍组查询报文的最大响应时间10秒。

因此缺省情况下，在已经存在组播业务转发的网络设备中，使能 IGMP-Snooping功能后，若组播接收者 Client 不即时主动的发送 IGMP 成员关系报告报文，则理论上组播转发恢复需要最大 135秒（125秒 + 10秒）的时间。

即对于网关 SW1 设备，等待 IGMP 普遍组查询报文计时器 125 秒到期结束后，才发送查询报文。当 Client收到查询报文后，最大等待最大响应时间10秒的时间，才回应IGMP 成员关系报告报文（Client 在收到 IGMP 查询报文后，主机会为其所加入的每个组播组都启动一个延迟定时器，其值在0到最大响应时间（缺省10秒）中随机选定，当定时器的值减为0时，主机就会向该定时器对应的组播组发送IGMP成员关系报告报文。这样可避免量主机同时发送报告报文而引起的网络拥塞）。因此理论上，最大需要等待 135 秒后，SW1 才能将 IGMP Snooping转发表项变为非空，进而组播业务转发才可恢复。

解决方法

优化方法

通过前面的分析，对于网络设备而言，其优化缩短 IGMP-Snooping 导致的业务中断时间，关键即缩短 IGMP 普遍组查询报文的发送间隔 和 IGMP普遍组查询报文的最大响应时间。

IGMP 普遍组查询报文的发送间隔可调整为2秒，igmp query-interval 2；

IGMP普遍组查询报文的最大响应时间可调整为1秒，igmp max-response-time 1；

总结

1. 建议组播网络开局就使能 IGMP Snooping 功能，从根本上杜绝组播断流情况；
2. 在已正常承担业务组播转发的网络中，部署 IGMP Snooping 功能之前，请先修改 IGMP 普遍组查询报文的发送间隔 和 IGMP普遍组查询报文的最大响应时间，对于目前 Comware V7 平台交换机，从理论上可以减少组播断流时间到 3秒。当IGMP Snooping 功能开启组播流量恢复转发后。再将 IGMP 普遍组查询报文的发送间隔 和 IGMP普遍组查询报文的最大响应时间恢复到缺省数值，以减轻网络设备处理报文压力。

PS

- 有思路灵活的同学，可能会想到，既然 IGMP Snooping转发表项可通过动态/静态方式建立，那么为何我们不提前先人工静态建立 IGMP Snooping转发表项后，再使能 IGMP Snooping 功能，这样不就解决动态建立的等待时间导致的组播断流问题么？Sorry，当前 Comware V7平台交换机必须先开启IGMP Snooping功能后，相关静态建立 IGMP Snooping转发表项的配置才能部署。因此，此路不通。
- 对于网络设备而言，当使能 IGMP Snooping 功能后，除了 IGMP Snooping转发表项 中 “VLAN、组播IP、Host Ports（成员端口）”参数指导流量的转发外，还有“路由器端口”等其他参数，也同样会影响组播流量的转发。同时组播 MAC地址表也将参与到组播流量的转发控制。想要了解的同学，欢迎对此案例多评论，多收藏，以便作者后续再与大家分享。