

修复Catalyst交换机上同一VLAN中的组播流量问题

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[问题](#)

[重新访问关键组播概念](#)

[IGMP](#)

[IGMP 侦听](#)

[Mrouter 端口](#)

[L2 上的多播](#)

[了解问题及其解决方案](#)

[解决方案](#)

[解决方案1：在第3层路由器/VLAN接口上启用PIM](#)

[解决方案2：在第2层Catalyst交换机上启用IGMP查询器功能](#)

[解决方案3：在交换机上配置静态Mrouter端口](#)

[解决方案4：在所有交换机上配置静态组播MAC条目](#)

[解决方案5：在所有交换机上禁用IGMP监听](#)

[相关信息](#)

简介

本文档介绍当组播应用部署在Catalyst交换机之间的同一个VLAN中时，如何修复该故障。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行 Cisco IOS® 软件版本 12.2(18)SXD5 的 Catalyst 6500 (带有 Supervisor 引擎 720)
- 运行Cisco IOS软件版本12.2(25)SEB2映像的Catalyst 3750
- 运行Cisco IOS软件版本并且也支持互联网组管理协议(IGMP)监听的任何Catalyst交换机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

背景信息

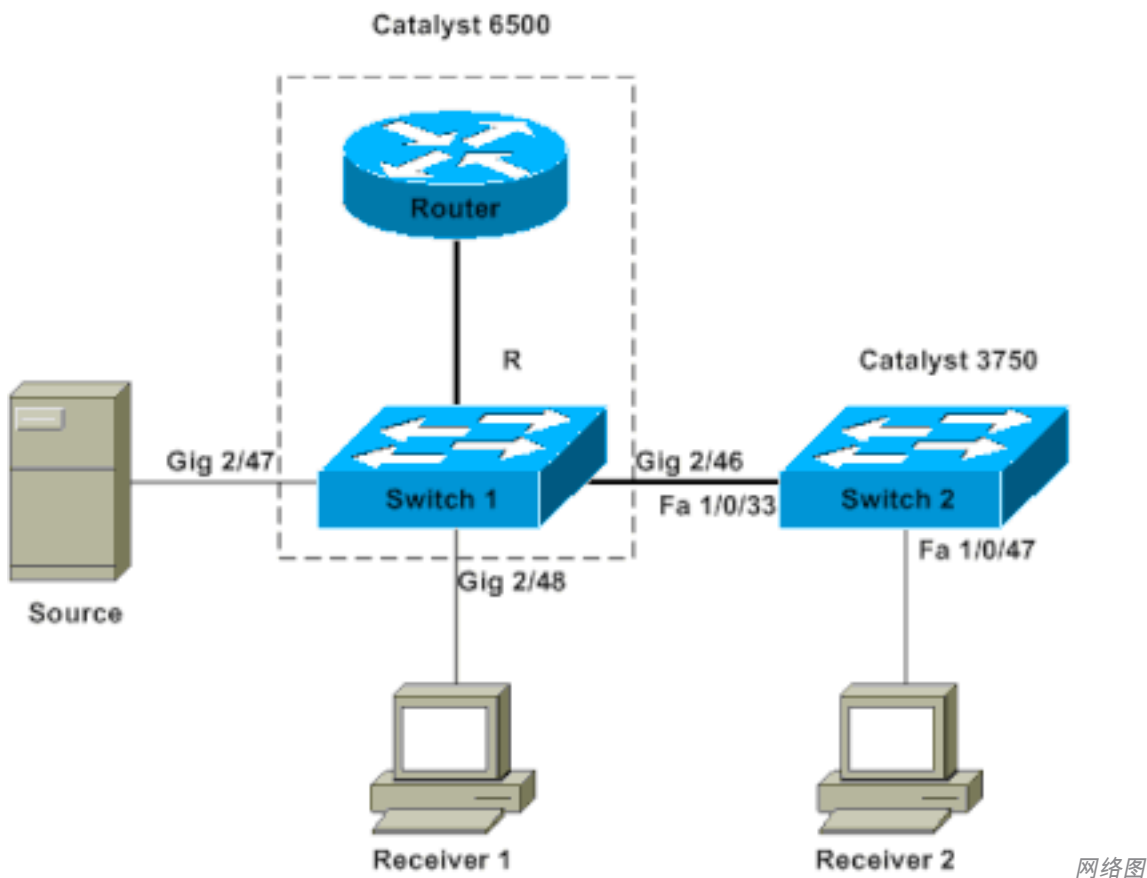
此外，如果您未正确配置交换机，一些使用组播数据包进行集群/高可用性操作的服务器/应用程序可能无法工作。本文也对此进行了介绍。

注意：请参阅文档[组播Catalyst交换机支持表](#)中的[IGMP监听功能Catalyst交换机支持表](#)部分，以帮助识别这些交换机。

问题

组播流量不会通过Catalyst交换机传输，即使在同一个VLAN中也是如此。图1描述了此场景。

图 1 - 多播源和接收方的网络设置



多播源连接到交换机 1，这是一台运行 Cisco IOS 软件的带有 Supervisor 引擎 720 的 Catalyst 6500 交换机。接收器 1 连接到交换机 1，接收器 2 连接到交换机 2。交换机 2 是 Catalyst 3750。交换机 1 和交换机 2 之间有一个第 2 层链路（接入或中继）。

在此设置中，您发现接收方 1（与源在同一台交换机上）可以顺利地获得多播流。但是，接收器 2 不

获得任何组播流量。本文档旨在解决此问题。

重新访问关键组播概念

在研究所拥有的解决方案和不同选项之前，您必须清楚地了解第 2 层多播的一些关键概念。此部分定义了这些概念。

注意：本部分提供非常简单和直接的解释，仅重点介绍此特定问题。有关这些术语的详细说明，请参阅本文档末尾的**相关信息**部分。

IGMP

IGMP 是一种协议，它使终端主机（接收方）能够向多播路由器（IGMP 查询者）通知终端主机接收特定多播数据流的意图。因此，这是一种在路由器和终端主机之间运行的协议，它允许：

- 路由器询问终端主机是否需要特定的多播流（IGMP 查询）
- 终端主机通知或回应路由器它们是否查找特定的多播流（IGMP 报告）

IGMP 侦听

IGMP 侦听是一种机制，用来将多播数据流限定为只能从附加了接收方的端口上发出。该机制可提高效率，这是因为它使第 2 层交换机能够有选择地仅在需要多播数据包的端口上发出多播数据包。如果没有 IGMP 侦听，交换机会使每个端口上的数据包泛洪。交换机“侦听”路由器和终端主机的 IGMP 消息交换。通过这种方式，交换机可生成一个 IGMP 侦听表，其中列出了已请求特定多播组的所有端口。

Mrouter 端口

Mrouter 端口仅仅是连接到多播路由器的端口（从交换机的角度来说）。为使 IGMP 侦听操作能够跨交换机进行，至少存在一个 mrouter 端口是绝对必要的。有关详细信息，请参阅本文档的[了解问题及其解决方案](#)部分。

L2 上的多播

目标 IP 在 224.0.0.0 到 239.255.255.255 范围中的任何 IP 版本 4 (IPv4) 数据流都是多播流。所有 IPv4 组播数据包都映射到格式为 01.00.5e. xx . xx.xx 的预定义 IEEE MAC 地址。

注意：仅当组播 MAC 地址映射到此符合 IEEE 的 MAC 范围时，IGMP 侦听才起作用。某些保留的组播范围会从设计侦听的组播范围中排除。如果在交换网络上发出了一个不符合规定的多播数据包，则此数据包将在该 VLAN 中泛洪，这意味着它被视为广播数据流。

了解问题及其解决方案

默认情况下，Catalyst 交换机启用了 IGMP 侦听。使用 IGMP 侦听，交换机会侦听（或侦听）所有端口上的 IGMP 消息。交换机会生成一个 IGMP 侦听表，该表主要将多播组映射到已请求它的所有交换机端口。

假设在事先未进行任何配置的情况下，接收方 1 和接收方 2 发出了表示它们要接收 239.239.239.239 (映射到 L2 多播 MAC 地址 01.00.5e.6f.ef.ef) 的多播流的信号。交换机 1 和交换机 2 在其监听表中为这些接收方创建一个条目以响应这些接收方生成的 IGMP 报告。交换机 1 在其表中输入端口千兆以太网 2/48，交换机 2 在其表中输入端口快速以太网 1/0/47。

注：此时，组播源尚未启动其流量，并且所有交换机均不知道交换机的 mrouter 端口。

当交换机 1 上的源开始传输组播流量时，交换机 1 已“看到”来自接收器 1 的 IGMP 报告。因此，交换机 1 将组播从端口 Gigabit Ethernet 2/48 发出。但是，因为交换机 2 在 IGMP 监听过程中从接收方 2“吸收”了 IGMP 报告，因此交换机 1 在端口千兆以太网 2/46 上看不到 IGMP 报告（多播请求）。因此，交换机 1 不会向交换机 2 发出任何多播数据流。所以，接收方 2 永远不会获得任何多播数据流，即使接收方 2 在同一 VLAN 中但只是位于与多播源不同的交换机上也是如此。

此问题的原因是任何没有 mrouter 的 Catalyst 平台实际上并不支持 IGMP 监听。该机制在缺少 mrouter 端口时将“崩溃”。如果要修正此解决方案，必须让交换机识别或知道 mrouter 端口。有关此过程的附加说明，请参阅本文档的[解决方案](#)部分。您仍然需要了解交换机上存在 mrouter 端口如何解决此问题。

基本上，当交换机识别或以静态方式知道 mrouter 端口时，会发生两件重要的事情：

- 交换机将 IGMP 报告从接收方“中继”到 mrouter 端口，这意味着 IGMP 报告将转发到多播路由器。交换机不中继所有 IGMP 报告，而是仅将其中的少数报告发送到 mrouter。对于此讨论的目的而言，报告的数量并不重要。多播路由器只需要知道是否至少有一个接收方仍在关注多播下游。为了做出决定，多播路由器接收定期 IGMP 报告以响应其 IGMP 查询。
- 在还没有任何接收方“加入”的仅源多播方案中，交换机只从其 mrouter 端口发出多播流。

当交换机知道其 mrouter 端口时，交换机 2 会将该交换机从接收方 2 收到的 IGMP 报告中继到其 mrouter 端口。此端口是快速以太网 1/0/33。交换机 1 在交换机端口千兆以太网 2/46 上获得此 IGMP 报告。从交换机 1 的角度来说，该交换机只是收到了另一个 IGMP 报告。该交换机将该端口添加到其 IGMP 监听表中，并也开始在该端口上发出多播数据流。这时，两个接收方都收到请求的多播数据流，并且应用程序按照预期正常工作。

要了解交换机如何标识其 mrouter 端口，以使 IGMP 监听按预期在简单环境中正常工作，请参阅解决方案部分了解答案。

解决方案

可以使用这些解决方案来解决问题。

解决方案 1：在第 3 层路由器/VLAN 接口上启用 PIM

所有 Catalyst 平台都能够动态地识别 mrouter 端口。交换机被动侦听多播路由器定期发出的独立于协议的多播 (PIM) hello 或 IGMP 查询消息。

本示例使用 CLI 在 Catalyst 6500 上配置 VLAN 1 交换虚拟接口 (SVI) ip pim sparse-dense-mode。

```
Switch1#show run interface vlan 1
!
interface Vlan1
 ip address 10.1.1.1 255.255.255.0
```

```
ip pim sparse-dense-mode
end
```

Switch 1 now reflects itself (Actually the internal router port) as an Mrouter port.

```
Switch1#show ip igmp snooping mrouter
vlan          ports
```

```
-----+-----
1 Router
```

Switch 2 receives the same PIM hellos on its Fa 1/0/33 interface. So it assigns that port as its Mrouter port.

```
Switch2#show ip igmp snooping mrouter
```

```
Vlan          ports
```

```
----         -----
1 Fa1/0/33(dynamic)
```

解决方案2：在第2层Catalyst交换机上启用IGMP查询器功能

IGMP 查询者是第 2 层交换机上的一个相对较新的功能。当网络/VLAN 没有可在交换机上承担多播路由器角色并在交换机上提供 mrouter 发现的的路由器时，您可以打开 IGMP 查询者功能。此功能允许第 2 层交换机在该网络中为多播路由器提供代理并发出定期 IGMP 查询。此操作会使交换机将其自身视为 mrouter 端口。网络中的其余交换机只是将各自的路由器端口定义为接收此IGMP查询的接口。

```
Switch2(config)#ip igmp snooping querier
```

```
Switch2#show ip igmp snooping querier
```

```
Vlan          IP Address      IGMP Version  Port
```

```
-----+-----
1          10.1.1.2          v2           Switch
```

交换机1现在将到交换机2的端口Gig 2/46链路视为路由器端口。

```
Switch1#show ip igmp snooping mrouter
```

```
vlan          ports
```

```
-----+-----
1 Gi2/46
```

当交换机1上的源开始传输组播流量时，交换机1将组播流量转发到通过IGMP监听发现的接收器1（即输出端口Gig 2/48）和路由器端口（即输出端口Gig 2/46）。

解决方案3：在交换机上配置静态Mrouter端口

由于交换机上缺少mrouter端口，同一第2层VLAN中的组播流量会失败，[了解问题及其解决方案](#)部分将介绍此主题。如果以静态方式在所有交换机上配置 mrouter 端口，则可以在该 VLAN 中将 IGMP 报告中继到所有交换机。因此，无法进行多播。因此，在该示例中，您必须以静态方式将 Catalyst 3750 交换机配置为将快速以太网 1/0/33 作为 mrouter 端口。

在该示例中，只需在交换机 2 上具有静态 mrouter 端口：

```
Switch2(config)#ip igmp snooping vlan 1 mrouter interface fastethernet 1/0/33
```

```
Switch2#show ip igmp snooping mrouter
```

```
Vlan    ports
----    -
1      Fa1/0/33(static)
```

解决方案4：在所有交换机上配置静态组播MAC条目

您可以为所有接收端口和下游交换机端口的所有交换机上的组播MAC地址创建静态内容可寻址存储器(CAM)条目。所有交换机都遵守静态 CAM 条目规则并从在 CAM 表中指定的所有接口发送数据包。对于拥有大量多播应用程序的环境，这是可扩展性最差的解决方案。

```
Switch1(config)#mac-address-table static 0100.5e6f.efef vlan 1 interface
gigabitethernet 2/46 gigabitethernet 2/48
```

!--- Note: This command should be on one line. Switch1#show mac-address-table multicast vlan 1

```
vlan    mac address      type   learn qos          ports
-----+-----+-----+-----+-----+-----
1      0100.5e6f.efef    static Yes           -    Gi2/46,Gi2/48
```

```
Switch2(config)#mac-address-table static 0100.5e6f.efef vlan 1 interface
fastethernet 1/0/47
```

!--- Note: This command should be on one line. Switch2#show mac-address-table multicast vlan 1

```
Vlan    Mac Address      Type      Ports
----    -
1      0100.5e6f.efef    USER     Fa1/0/47
```

解决方案5：在所有交换机上禁用IGMP监听

如果禁用 IGMP 监听，所有交换机会将多播数据流视为广播数据流。这会使该数据流泛洪到该 VLAN 中的所有端口，而不管端口是否具有与该多播流相关的接收方。

```
Switch1(config)#no ip igmp snooping
```

```
Switch2(config)#no ip igmp snooping
```

相关信息

- [园区网络中的组播：CGMP和IGMP监听](#)
- [组播 Catalyst 交换机支持表](#)
- [IP组播支持](#)
- [排除IP组播问题的技术说明](#)
- [IP组播故障排除指南](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。