Fix Multicast Traffic Issues in Same VLAN on Catalyst Switches

Contents

Introduction

This document describes how to fix a multicast application failure when it is deployed in the same VLAN between Catalyst switches.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 6500 with Supervisor Engine 720 that runs Cisco IOS® Software
- Catalyst 3750 that runs a Cisco IOS Software

- Any Catalyst switch that runs a Cisco IOS Software release and also supports Internet Group Management Protocol (IGMP) snooping

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

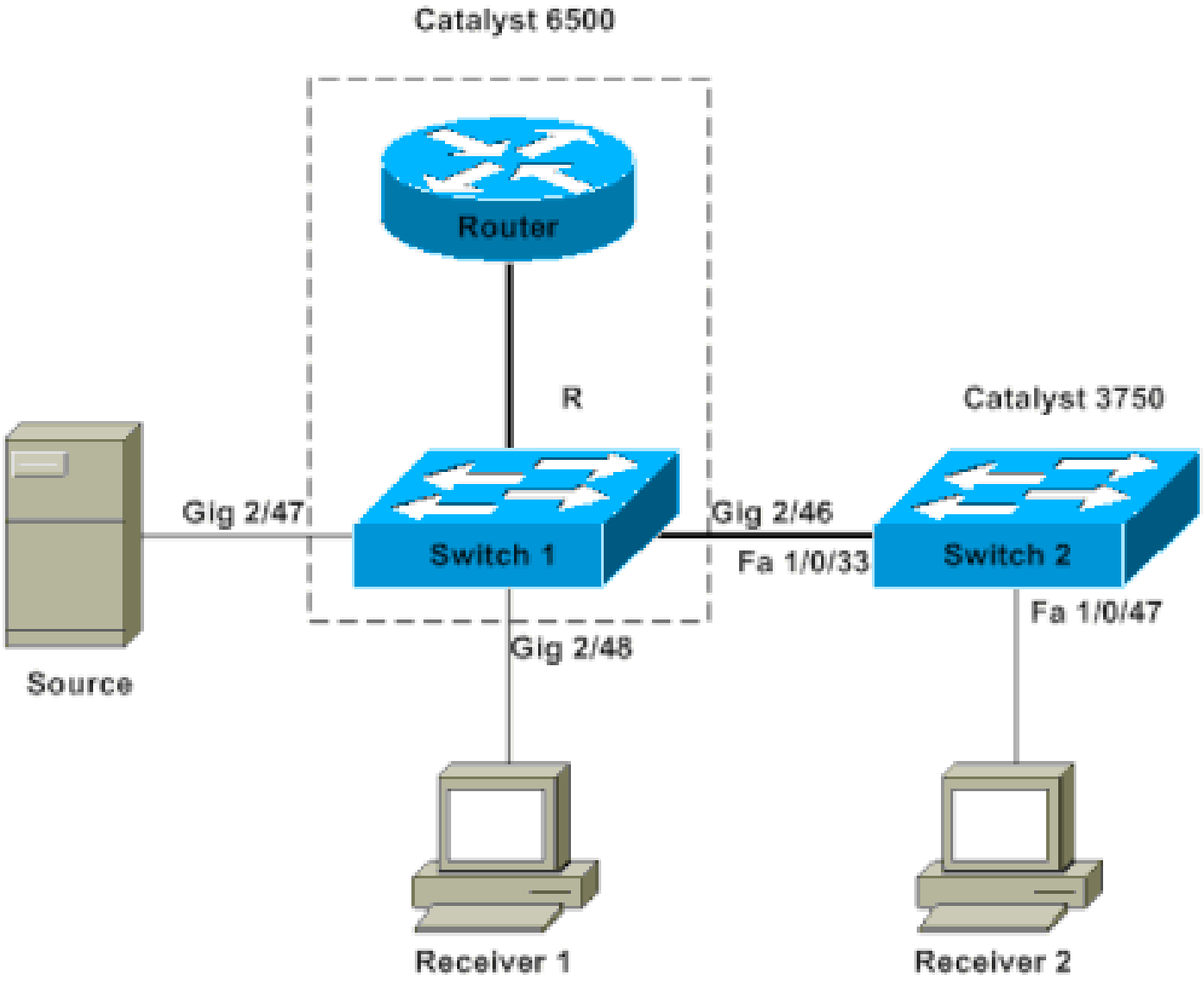
Additionally, some servers/applications that use multicast packets for the cluster/high-availability operation can fail to work if you do not configure the switches appropriately. This is also covered in this article.

Note: Refer to the IGMP Snooping Feature Catalyst Switch Support Matrix section of the document Multicast Catalyst Switches Support Matrix to help identify these switches.

Problem

Multicast traffic does not pass across Catalyst switches, even in the same VLAN.Figure 1 depicts this scenario.

Figure 1 – Network Setup with Multicast Source and Receivers



Network Diagram

The multicast source is connected to Switch 1, which is a Catalyst 6500 Switch with Supervisor Engine 720 that runs Cisco IOS Software. Receiver 1 is connected to Switch 1, and Receiver 2 is connected to Switch 2. Switch 2 is a Catalyst 3750. There is a Layer 2 link, either access or trunk, between Switch 1 and Switch 2.

In this setup, you find that Receiver 1, which is on the same switch as the source, gets the multicast stream with no problems. However, Receiver 2*does not*get any multicast traffic. This document aims to resolve this issue.

Revisit Key Multicast Concepts

Before you explore the solution and the different options you have, you must be clear on certain key concepts of Layer 2 multicast. This section defines these concepts.

Note: This section provides a very simple and direct explanation that focuses only on this particular issue. See the **Related Information** section at the end of this document for detailed explanation of these terms.

IGMP

IGMP is a protocol that enables end hosts (receivers) to inform a multicast router (IGMP querier) of the end host intention to receive particular multicast traffic. So this is a protocol that runs between a router and end hosts and allows:

- Routers to ask end hosts if they need a particular multicast stream (IGMP query)
- End hosts to tell or respond to the router if they seek a particular multicast stream (IGMP reports)

IGMP Snooping

IGMP snooping is a mechanism to constrain multicast traffic to only the ports that have receivers attached. The mechanism adds efficiency because it enables a Layer 2 switch to selectively send out multicast packets on only the ports that need them. Without IGMP snooping, the switch floods the packets on every port. The switch "listens" for the exchange of IGMP messages by the router and the end hosts. In this way, the switch builds an IGMP snooping table that has a list of all the ports that have requested a particular multicast group.

Mrouter Port

The mrouter port is simply the port from the switch point of view that connects to a multicast router. The presence of at least one mrouter port is absolutely essential for the IGMP snooping operation to work across switches.

Multicast at L2

Any IP version 4 (IPv4) traffic with a destination IP in the range of 224.0.0.0 to 239.255.255.255 is a multicast stream. All IPv4 multicast packets map to a predefined IEEE MAC address that has the format 01.00.5e. xx . xx . xx .

Note: IGMP snooping works only if the multicast MAC address maps to this IEEE-compliant MAC range. Some reserved multicast ranges are excluded from those snooped by design. If a nonconforming multicast packet is sourced on a switched network, the packet is flooded throughout that VLAN, which means that it is treated like broadcast traffic.

Understand the Problem and Possible Solutions

By default, the Catalyst switches have IGMP snooping enabled. With IGMP snooping, the switch snoops (or listens) for IGMP messages on all the ports. The switch builds an IGMP snooping table that basically maps a multicast group to all the switch ports that have requested it.

Assume that, without any prior configuration, Receiver 1 and Receiver 2 have signaled their intentions to receive a multicast stream for 239.239.239.239 that maps to the L2 multicast MAC address of 01.00.5e.6f.ef.ef. Both Switch 1 and Switch 2 create an entry in their snooping tables for these receivers in response to the IGMP reports that the receivers generate. Switch 1 enters port Gigabit Ethernet 2/48 in its table, and Switch 2 enters port Fast Ethernet 1/0/47 in its table.

Note: At this point, the multicast source has not started its traffic, and none of the switches knows about the switch mrouter port.

When the source on Switch 1 starts to stream multicast traffic, Switch 1 has "seen" the IGMP report from Receiver 1. As a result, Switch 1 delivers the multicast out port Gigabit Ethernet 2/48. But, since Switch 2 "absorbed" the IGMP report from Receiver 2 as part of the IGMP snooping process, Switch 1 does not see

an IGMP report (multicast request) on port Gigabit Ethernet 2/46. As a result, Switch 1 does not send any multicast traffic out to Switch 2. Therefore, Receiver 2 never gets any multicast traffic, even though Receiver 2 is in the same VLAN but merely on a different switch than the multicast source.

The reason for this issue is that IGMP snooping is not really supported on any Catalyst platform without an mrouter. The mechanism "breaks down" in the absence of an mrouter port. If you want a fix for this solution, you must have the switches somehow learn or know of an mrouter port. See the Solutions section of this document for additional explanation of the procedure. You still need to discover how the presence of an mrouter port on the switches remedy the issue.

Basically, when the switches learn or statically know about an mrouter port, two critical things occur:

- The switch "relays" the IGMP reports from the receivers to the mrouter port, which means that the IGMP reports go toward the multicast router. The switch does not relay all the IGMP reports. Instead, the switch sends only a few of the reports to the mrouter. For the purpose of this discussion, the number of reports is not important. The multicast router only needs to know if there is at least one receiver that is still interested in the multicast downstream. In order to make the determination, the multicast router receives the periodic IGMP reports in response to its IGMP queries.

- In a source-only multicast scenario, in which no receivers have yet "joined" in, the switch only sends the multicast stream out its mrouter port.

When the switches know their mrouter port, Switch 2 relays out the IGMP report that the switch received from Receiver 2 to its mrouter port. This port is Fast Ethernet 1/0/33. Switch 1 gets this IGMP report on the switch port Gigabit Ethernet 2/46. From the perspective of Switch 1, the switch has received merely another IGMP report. The switch adds that port into its IGMP snooping table and begins to send out the multicast traffic on that port as well. At this point, both the receivers receive the requested multicast traffic, and the application works as expected.

To find out how the switches identify their mrouter port so that IGMP snooping works as it is expected to work in a simple environment see the Solutions section for answers.

Solutions

Option 1: Enable PIM on the Layer 3 Router/VLAN Interface

All Catalyst platforms have the ability to dynamically learn about the mrouter port. The switches passively listen to either the Protocol Independent Multicast (PIM) hellos or the IGMP query messages that a multicast router sends out periodically.

This example configures the VLAN 1 switched virtual interface (SVI) on the Catalyst 6500 with ip pim sparse-mode .

```
<#root>

Switch1#

show run interface vlan 1

!
interface Vlan1
 ip address 10.1.1.1 255.255.255.0
 ip pim sparse-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

Switch2#
show ip igmp snooping mrouter

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

Option 2: Enable IGMP Querier Feature on a Layer 2 Catalyst Switch

When a network/VLAN does not have a router that can take on the multicast router role and provide the mrouter discovery on the switches, you can turn on the IGMP querier feature. The feature allows the Layer 2 switch to proxy for a multicast router and send out periodic IGMP queries in that network. This action causes the switch to consider itself an mrouter port. The rest of the switches in the network simply define their respective mrouter ports as the interface on which they received this IGMP query.

```
<#root>

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
```

Switch 1 now sees that port Gig 2/46 links to Switch 2 as an mrouter port.

```
<#root>

Switch1#
show ip igmp snooping mrouter

vlan            ports
```

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

When the source on Switch 1 starts to stream multicast traffic, Switch 1 forwards the multicast traffic to the Receiver 1 found via IGMP snooping (that is, out port Gig 2/48) and to the mrouter port (that is, out port Gig 2/46).

Option 3: Configure Static Mrouter Port on the Switch

The multicast traffic fails within the same Layer 2 VLAN because of the lack of an mrouter port on the switches, the section Understand the Problem and Its Solutions covers this topic. If you statically configure an mrouter port on all the switches, IGMP reports can be relayed in that VLAN to all switches. As a result, multicasting is possible. So, in the example, you must statically configure the Catalyst 3750 Switch to have Fast Ethernet 1/0/33 as an mrouter port.

In this example, you need a static mrouter port on Switch 2 only:

```
<#root>

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)
```

Option 4: Configure Static Multicast MAC Entries on All the Switches

You can make a static content-addressable memory (CAM) entry for the multicast MAC address on all the switches for all the receiver ports*and*the downstream switch ports. Any switch obeys the static CAM entry rules and sends the packet out all the interfaces that are specified in the CAM table. This is the least-scalable solution for an environment that has a lot of multicast applications.

```
<#root>

Switch1(config)#

mac-address-table static 0100.5e6f.efef vlan 1 interface gigabitethernet 2/46 gigabitethernet 2/48


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


Switch2#

show mac-address-table multicast vlan 1

Vlan    Mac Address       Type       Ports
----    -----------       ----       -----
   1    0100.5e6f.efef

USER

        Fa1/0/47
```

Option 5: Disable IGMP Snooping on All the Switches

If you disable IGMP snooping, all switches treat multicast traffic as a broadcast traffic. This floods the traffic to *all* the ports in that VLAN, regardless of whether the ports have interested receivers for that multicast stream.

```
<#root>

Switch1(config)#

no ip igmp snooping


Switch2(config)#

no ip igmp snooping
```

Related Information

- **Multicast in a Campus Network: CGMP and IGMP Snooping**
- **Multicast Catalyst Switches Support Matrix**
- **IP Multicast Support**
- **TechNotes to Troubleshoot Issues with IP Multicast**
- **IP Multicast Troubleshoot Guide**
- **Cisco Technical Support & Downloads**