El Multicast no trabaja en el mismo VLA N en los switches de Catalyst

Contenido

Introducción

Este documento trata un problema común que ocurre cuando se instala la aplicación de multidifusión por primera vez en una red de switch Cisco Catalyst y no funciona el multidifusión. Además, algunos servidores/aplicaciones que utilizan paquetes de multidifusión para el funcionamiento de gran disponibilidad/clúster pueden no trabajar si no configura los switches apropiadamente. El documento abarca este problema también.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 6500 con el Supervisor Engine 720 que funciona con el Software Release 12.2(18)SXD5 de Cisco IOS®
- Catalyst 3750 que funciona con una imagen del Cisco IOS Software Release 12.2(25)SEB2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Este documento se puede también utilizar con estas versiones de software y hardware:

- Cualquier switch de Catalyst que funcione con una versión de Cisco IOS Software que soporte el snooping del Internet Group Management Protocol (IGMP)**Nota:** Refiera a la sección de la *matriz de soporte de switch Catalyst para la función de indagación de IGMP de la* matriz de soporte de los switches de Catalyst del Multicast del documento para identificar este Switches.

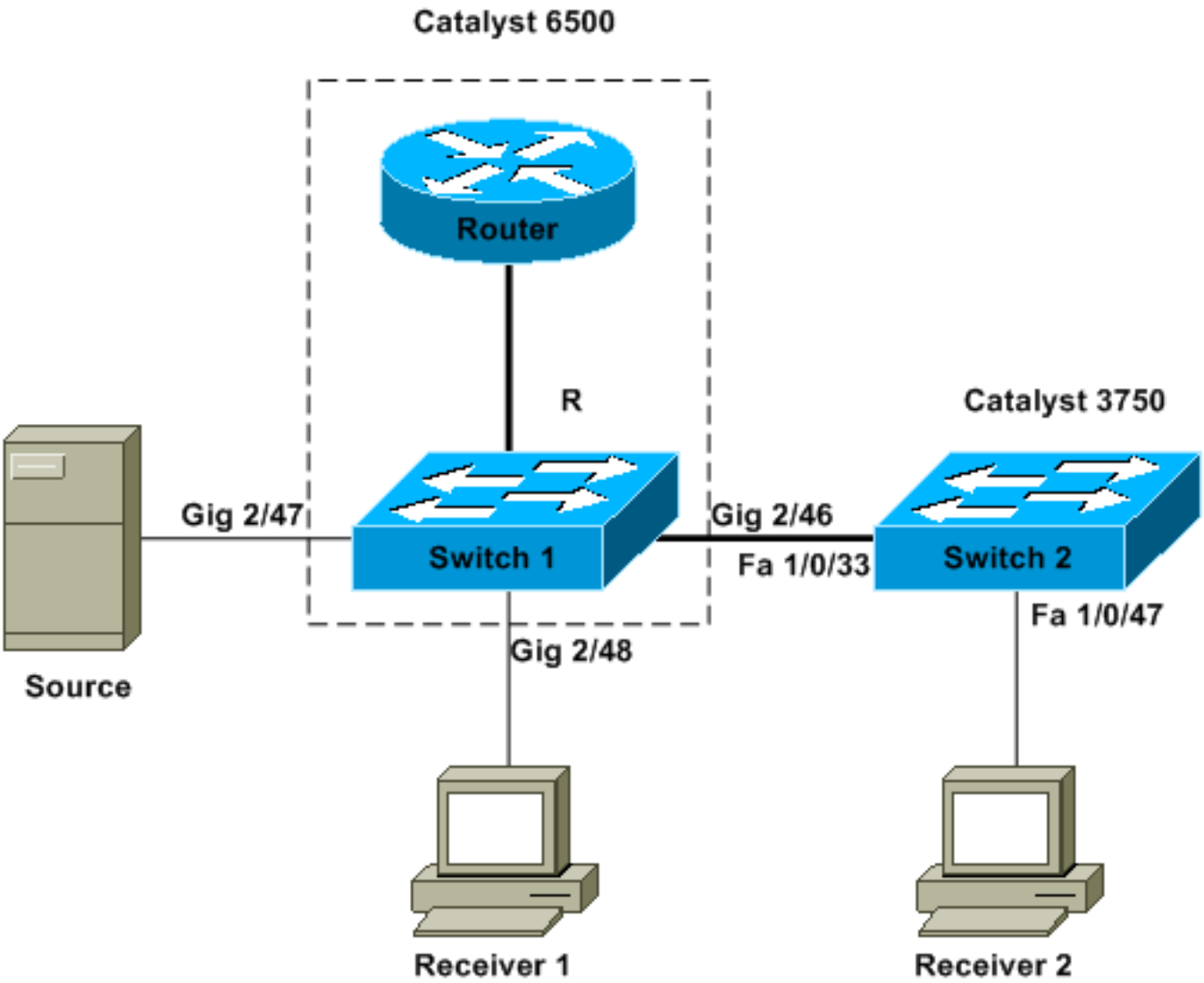
Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Problema

El tráfico Multicast no parece pasar a través de los switches de Catalyst, incluso en el mismo VLA N. El cuadro 1 representa un escenario típico:

Cuadro 1 – Configuración de la red con el origen de multidifusión y los receptores



El origen de multidifusión está conectado con el Switch1, que es un Catalyst 6500 Switch con el Supervisor Engine 720 que funciona con el Cisco IOS Software. El receptor 1 está conectado con el Switch1, y el receptor 2 está conectado para conmutar 2. Switch2 es un Catalyst 3750. Hay un link de la capa 2, acceso o trunk, entre el Switch1 y el Switch2.

En esta configuración, usted encuentra ese receptor 1, que está en el mismo Switch que la fuente, consigue la secuencia de multidifusión sin los problemas. Sin embargo, el receptor 2 no consigue ningún tráfico Multicast. Este documento apunta resolver este problema.

Revisite algunos conceptos dominantes del Multicast

Antes de que usted explore la solución y las diversas opciones que usted tiene, usted debe estar claro en ciertos conceptos fundamentales de Multicast de la capa 2. Esta sección define estos conceptos.

Nota: Esta sección proporciona una explicación muy simple y directa esa los focos solamente en este problema determinado. Vea la sección de información relacionada de este documento para una más explicación detallada de estos términos.

IGMP

El IGMP es un protocolo que permite a los host extremos (receptores) para informar a un router

de multidifusión (interrogador IGMP) la intención del host extremo de recibir el tráfico Multicast determinado. Éste es tan un protocolo que los funcionamientos entre un router y los host extremos y permiten:

- Routers para preguntar a host extremos si necesitan una secuencia de multidifusión determinada (interrogación IGMP)
- Host extremos a decir o a responder al router si buscan una secuencia de multidifusión determinada (informes IGMP)

IGMP Snooping

El IGMP Snooping es un mecanismo para obligar el tráfico Multicast solamente a los puertos que tienen receptores asociados. El mecanismo agrega la eficacia porque permite a un 2 Switch de la capa para enviar selectivamente los paquetes de multidifusión en solamente los puertos que los necesitan. Sin el IGMP Snooping, el Switch inunda los paquetes en cada puerto. El Switch "escucha" el intercambio de los mensajes IGMP del router y de los host extremos. De esta manera, el Switch construye una tabla del IGMP Snooping que tenga una lista de todos los puertos que han pedido a un grupo de multidifusión determinado.

Puerto del mrouter

El puerto del mrouter es simplemente el puerto desde el punto de vista del Switch que conecta con un router de multidifusión. La presencia por lo menos de un puerto del mrouter es absolutamente esencial para que la operación del IGMP Snooping trabaje a través del Switches. La comprensión el problema y sus soluciones secciona de este documento discute este requisito más detalladamente.

Multicast en el L2

Versión IP el tráfico 4 (del IPv4) con un IP de destino en el rango de 224.0.0.0 a 239.255.255.255 es una secuencia de multidifusión. Todos los paquetes de multidifusión del IPv4 asocian a una dirección MAC predefinida de IEEE que tenga el formato 01.00.5e.xx.xx.xx.

Nota: El IGMP Snooping trabaja solamente si el Multicast MAC Address asocia a este rango IEEE-obediente MAC. Algunos rangos reservados del Multicast son excluidos de snooped por el diseño. Si un paquete de multidifusión no conforme es originado en una red de switch, el paquete se inunda en ese VLA N, así que significa que está tratado como el tráfico de broadcast.

Entienda el problema y sus soluciones

Por abandono, los switches de Catalyst tienen IGMP Snooping habilitado. Con el IGMP Snooping, el Switch snoops (o escucha) para los mensajes IGMP en todos los puertos. El Switch construye una tabla del IGMP Snooping que asocie básicamente a un grupo de multidifusión a todos los puertos del switch que lo han pedido.

Asuma que, sin ninguna configuración anterior, el receptor 1 y el receptor 2 han señalado sus intenciones de recibir una secuencia de multidifusión para 239.239.239.239 ese las correspondencias al Multicast MAC Address L2 de 01.00.5e.6f.ef.ef. El Switch1 y el Switch2 crean una entrada en sus tablas del snooping para estos receptores en respuesta al IGMP señala que los receptores generan. El Switch1 ingresa los Ethernetes de Gigabit de un puerto 2/48 en su

tabla, y el Switch2 ingresa los fast ethernet 1/0/47 del puerto en su tabla.

Nota: En este momento, el origen de multidifusión no ha comenzado su tráfico, y ninguno del Switches sabe sobre el puerto del mrouter del Switch.

Cuando la fuente en el Switch1 comienza a fluir el tráfico Multicast, el Switch1 “ha visto” el informe IGMP del receptor 1. como consecuencia, Switch1 entrega los Ethernetes de Gigabit de un puerto 2/48 del Multicast hacia fuera. Pero, puesto que el Switch2 “absorbió” el informe IGMP del receptor 2 como parte del proceso del IGMP Snooping, el Switch1 no ve un informe IGMP (pedido de multidifusión) sobre los Ethernetes de Gigabit de un puerto 2/46. Como consecuencia, el Switch1 no manda ningún tráfico Multicast al Switch2. Por lo tanto, el receptor 2 nunca consigue cualquier tráfico Multicast, aunque el receptor 2 está en el mismo VLA N pero simplemente en un diverso Switch que el origen de multidifusión.

La razón de este problema es que el IGMP Snooping no está soportado realmente en ninguna plataforma Catalyst sin un mrouter. El mecanismo “analiza” en ausencia de un puerto del mrouter. Si usted quiere un arreglo para esta solución, usted debe hacer que el Switches de alguna manera aprenda o sepa de un puerto del mrouter. La sección de las soluciones de este documento explica el procedimiento. ¿Pero cómo la presencia de un puerto del mrouter en el Switches remedia la situación?

, Cuando el Switches aprende o sabe estáticamente sobre un puerto del mrouter, dos cosas críticas ocurren básicamente:

- El Switch “retransmite” los informes IGMP de los receptores al puerto del mrouter, así que significa que los informes IGMP van hacia el router de multidifusión. El Switch no retransmite todos los informes IGMP. En lugar, el Switch envía solamente algunos de los informes al mrouter. Con el fin de esta discusión, el número de informes no es importante. Las necesidades del router de multidifusión solamente de saber si hay por lo menos un receptor que todavía está interesado en el Multicast rio abajo. Para hacer la determinación, el router de multidifusión recibe los informes periódicos IGMP en respuesta a sus interrogaciones IGMP.
- En un escenario del Multicast de la fuente-solamente, en el cual ningunos receptores tienen todavía “se unió a” adentro, el Switch solamente manda la secuencia de multidifusión su puerto del mrouter.

Cuando el Switches conoce su puerto del mrouter, el Switch2 retransmite hacia fuera el informe IGMP que el Switch recibió del receptor 2 a su puerto del mrouter. Este puerto es el fast ethernet 1/0/33. El Switch1 consigue este informe IGMP sobre el puerto del switch Gigabit Ethernet 2/46. Desde la perspectiva del Switch1, el Switch ha recibido simplemente otro informe IGMP. El Switch agrega ese puerto en su tabla del IGMP Snooping y comienza a enviar el tráfico Multicast en ese puerto también. En este momento, ambos los receptores reciben el tráfico Multicast pedido, y la aplicación trabaja como se esperaba.

¿Pero cómo el Switches identifica su puerto del mrouter de modo que el IGMP Snooping trabaje mientras que se espera que trabaje en un entorno simple como esto? La sección de las soluciones proporciona algunas respuestas.

Soluciones

Utilice estas soluciones para solucionar el problema.

Solución 1: Permiso PIM en la interfaz de la capa 3 Router/VLAN

Todas las plataformas Catalyst tienen la capacidad de aprender dinámicamente sobre el puerto del mrouter. El Switches escucha pasivo el hellos de la multidifusión independiente de protocolo (PIM) o los Mensajes de consulta de IGMP que un router de multidifusión envía periódicamente.

Este ejemplo configura el Switched Virtual Interface del VLAN1 (SVI) en el Catalyst 6500 con el `sparse-dense-mode del pim del IP.`

```
Switch1#show run interface vlan 1 ! interface Vlan1  ip address 1.1.1.1 255.255.255.0  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)
```

Solución 2: Característica del interrogador IGMP del permiso en un switch de Catalyst de la capa 2

El interrogador IGMP es relativamente una nueva función en los 2 Switch de la capa. Cuando un network/VLAN no tiene un router que pueda adquirir el papel del router de multidifusión y proporcionar la detección de mrouter en el Switches, usted puede girar la característica del interrogador IGMP. La característica permite el 2 Switch de la capa al proxy para un router de multidifusión y envía las interrogaciones periódicas IGMP en esa red. Esta acción hace el Switch considerarse un puerto del mrouter. Los switches restantes en la red definen simplemente sus puertos respectivos del mrouter como la interfaz en la cual recibieron esta interrogación IGMP.

```
Switch2(config)#ip igmp snooping querier Switch2#show ip igmp snooping querier Vlan      IP
Address     IGMP Version   Port               ------------------------------------------------
---------- 1         1.1.1.2        v2             Switch
```

El Switch1 ahora ve el carruaje 2/46 del puerto el conectar al Switch2 como puerto del mrouter.

```
Switch1#show ip igmp snooping mrouter vlan            ports -----+------------------------------
----------    1  Gi2/46
```

Cuando la fuente en el Switch1 comienza a fluir el tráfico Multicast, Switch1 adelante el tráfico Multicast al receptor 1 encontrado vía el IGMP Snooping (es decir, hacia fuera vire el carruaje hacia el lado de babor 2/48) y al puerto del mrouter (es decir, hacia fuera vire el carruaje hacia el lado de babor 2/46).

Solución 3: Puerto estático del mrouter de la configuración en el Switch

El tráfico Multicast falla dentro del mismo VLA N de la capa 2 debido a la falta de un puerto del mrouter en el Switches, pues la comprensión el problema y su sección de las soluciones discute. Si usted configura estáticamente un puerto del mrouter en todo el Switches, los informes IGMP se pueden retransmitir en ese VLA N a todo el Switches. Como consecuencia, el multicasting es posible. Así pues, en el ejemplo, usted debe configurar estáticamente el Catalyst 3750 Switch para tener fast ethernet 1/0/33 como puerto del mrouter.

En este ejemplo, usted necesita un puerto estático del mrouter en el Switch2 solamente:

```
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)
```

Solución 4: Entradas MAC estáticas del Multicast de la configuración en todo el Switches

Usted puede hacer una entrada estática de memoria direccionable por contenido (CAM) para el Multicast MAC Address en todo el Switches para todos los puertos del receptor *y los* puertos del switch rio abajo. Cualquier Switch obedece las reglas de la entrada de CAM estática y manda el paquete todas las interfaces que se especifican en la tabla CAM. Ésta es la solución menos-scalable para un entorno que tenga muchas aplicaciones de multidifusión.

```
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
```

Solución 5: IGMP Snooping de la neutralización en todo el Switches

Si usted inhabilita el IGMP Snooping, todo el Switches trata el tráfico Multicast como tráfico de broadcast. Esto inunda el tráfico a *todos los* puertos en ese VLA N, sin importar si los puertos han interesado a los receptores para esa secuencia de multidifusión.

```
Switch1(config)#no ip igmp snooping Switch2(config)#no ip igmp snooping
```

Información Relacionada

- Multicast en una red de oficinas centrales: Indagación CGMP y IGMP
- Matriz de Soporte de Switches de Catalyst Multicast
- Página de soporte de multidifunsión IP
- Notas técnicas de Troubleshooting del Multicast IP
- Guía de resolución de problemas de multidifunción IP
- Páginas de Soporte de Productos de LAN
- Página de Soporte de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems