Contenido

Introducción

Este documento describe los problemas comunes y soluciones del IP multicast.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

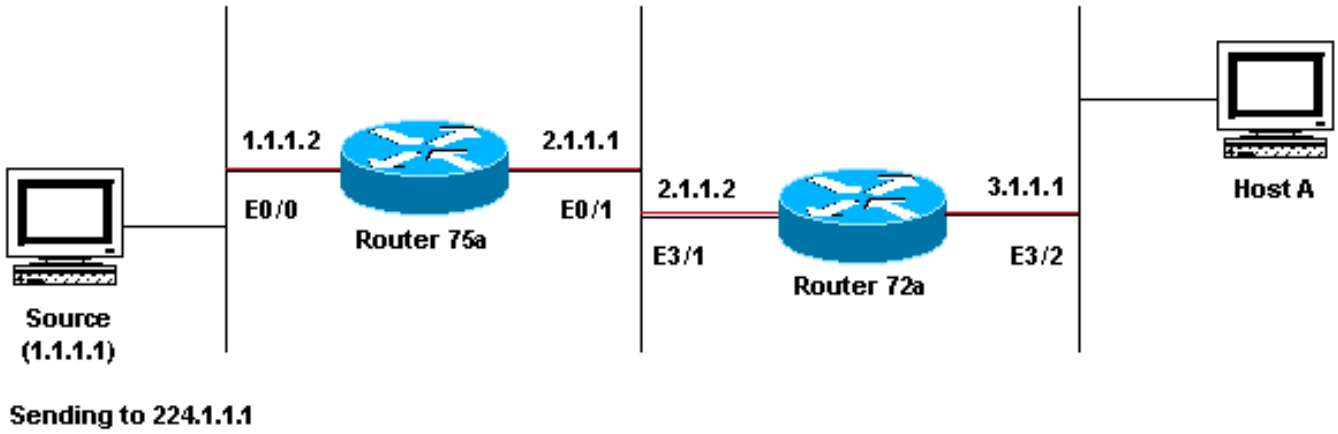
Antecedentes

Cuando usted resuelve problemas el ruteo multicast, el problema principal es la dirección de origen. El Multicast tiene un concepto de control del reenvío de trayecto inverso (RPF). Cuando un paquete de multidifusión llega en una interfaz, las pruebas del proceso RPF para asegurarse de que esta interfaz entrante sea la interfaz saliente utilizaron por el Unicast Routing para alcanzar la fuente del paquete de multidifusión. Este proceso de verificación del RPF evita los loops. El ruteo multicast no remite un paquete a menos que la fuente del paquete pase a revisión de "RPF". Una vez que un paquete pasa el control RPF, el ruteo multidifusión reenvía el paquete basándose sólo en la dirección de destino.

Como el Unicast Routing, el ruteo multicast tiene varios protocolos disponibles, tales como modo denso de la multidifusión independiente de protocolo (PIM-DM), modo disperso de PIM (PIM-S), Distance Vector Multicast Routing Protocol (DVMRP), protocolo multicast border gateway (MBGP), y Multicast Source Discovery Protocol (MSDP). Los casos prácticos en este documento recorren usted con el proceso para resolver problemas los diversos problemas. Usted verá se utilizan qué comandos para establecer claramente rápidamente el problema y aprender cómo resolverlo. Están genéricos los casos prácticos enumerados aquí a través de los protocolos, a menos que donde observados.

El router no remite los paquetes de multidifusión al host debido a la falla de RPF

Esta sección proporciona una solución al problema común de una falla de RPF del Multicast IP. Este diagrama de la red se utiliza como un ejemplo.



En esta figura, los paquetes de multidifusión entran en el E0/0 del router 75a de un servidor cuya dirección IP sea 1.1.1.1 y envíe para agrupar 224.1.1.1. Esto es conocido como un (S,G) o (1.1.1.1, 224.1.1.1).

Diagnostique el problema

Los host conectados directamente con el router 75a reciben el suministro de multidifusión, pero los host conectados directamente con el router 72a no hacen. Primero, ingrese el comando de **224.1.1.1 de la ruta multicast del IP de la demostración** para ver qué está continuando con el router 75a. Este comando examina la ruta de Multicast (ruta multicast) para el grupo de dirección 224.1.1.1:

Puesto que el router funciona con al modo denso de PIM (usted sabe que es modo denso debido al indicador D), ignore *, entrada G y foco en el S, entrada G. Esta entrada le dice que los paquetes de multidifusión son originados de un servidor cuyo direccionamiento sea 1.1.1.1, que envía a un grupo de multidifusión de 224.1.1.1. Los paquetes entran en la interfaz del Ethernet0/0 y se remiten hacia fuera la interfaz Ethernet0/1. Esto es un escenario perfecto.

Ingrese el **comando show ip pim neighbor** para ver si el router 72a muestra al router ascendente (75a) como vecino del PIM:

De la salida del **comando show ip pim neighbor**, la vecindad PIM parece buena.

Ingrese el **comando show ip mroute** para ver si el router 72a tiene buena ruta multicast:

Usted puede ver del comando de **224.1.1.1 de la ruta multicast del IP de la demostración** que la interfaz entrante es Ethernet2/0, mientras que se espera Etheret3/1.

Ingrese el **comando count de 224.1.1.1 de la ruta multicast del IP de la demostración** para ver si algún tráfico Multicast para este grupo llega al router 72a y qué sucede después:

Usted puede ver de las `otras` cuentas que el tráfico consigue caída debido a la falla de RPF:
`¿descensos del total 471, debido a la falla de RPF? ¿471?`

Ingrese el **comando show ip rpf <source>** para ver si hay un error RPF:

El Cisco IOS$^{Â®}$ calcula la interfaz RPF de esta manera. Las fuentes posibles de información RPF

son tabla de Unicast Routing, tabla de ruteo MBGP, tabla de ruteo DVMRP, y tabla del mRoute estático. Cuando usted calcula la interfaz RPF, sobre todo la distancia administrativa se utiliza para determinar exactamente que la fuente de información el cálculo del RPF se basa encendido. Las reglas específicas son:

- Todas las fuentes precedentes de datos RPF se buscan para una coincidencia en la dirección IP de origen. Cuando usted utiliza los árboles compartidos, el direccionamiento RP se utiliza en vez de la dirección de origen.
- Si se encuentra más de una ruta que corresponde con, la ruta con la mínima distancia administrativa se utiliza.
- Si las distancias administrativas son iguales, después se utiliza este orden de preferencia:MRoutes estáticosRutas DVMRPRutas MBGPRutas Unicast
- Si las entradas múltiples para una ruta ocurren dentro de la misma tabla de ruta, se utiliza la ruta más larga de la coincidencia.

La salida de comando **rpf 1.1.1.1 del IP de la demostración** muestra la interfaz RPF que es E2/0, pero la interfaz entrante debe ser E3/1.

Ingrese el comando de **1.1.1.1 de la ruta de IP de la demostración** para ver porqué la interfaz RPF es diferente de lo que fue esperado.

Usted puede ver de esta salida de comando de **1.1.1.1 de la ruta de IP de la demostración** que hay una ruta estática de `/32`, que hace la interfaz incorrecta que se elegirá como interfaz RPF.

Ingrese algunos otros **comandos debug**:

Los paquetes vienen adentro en el E3/1, que está correcto. Sin embargo, se caen porque ésa no es la interfaz que la tabla de Unicast Routing utiliza para revisión de "RPF".

> Nota: Hacer el debug de los paquetes es peligroso. El debugging del paquete acciona el process switching de los paquetes de multidifusión, que es uso intensivo de la CPU. También, el debugging del paquete puede producir la salida enorme que puede colgar el router totalmente debido reducir la salida al puerto de la consola. Antes de que usted haga el debug de los paquetes, el particular cuidado debe ser orden admitida para inhabilitar la salida de registro a la consola, y habilita el registro a memoria intermedia. Para alcanzar esto, no configure **ninguna consola de registro** y **debugging guardada en la memoria intermedia del registro**. Los resultados del debug se pueden considerar con el **comando show logging**.

Correcciones posibles

Usted puede o cambiar la tabla de Unicast Routing para satisfacer este requisito o usted puede agregar un mRoute estático para forzar el Multicast al RPF hacia fuera una interfaz particular, sin importar lo que estado la tabla de Unicast Routing. Agregue un mRoute estático:

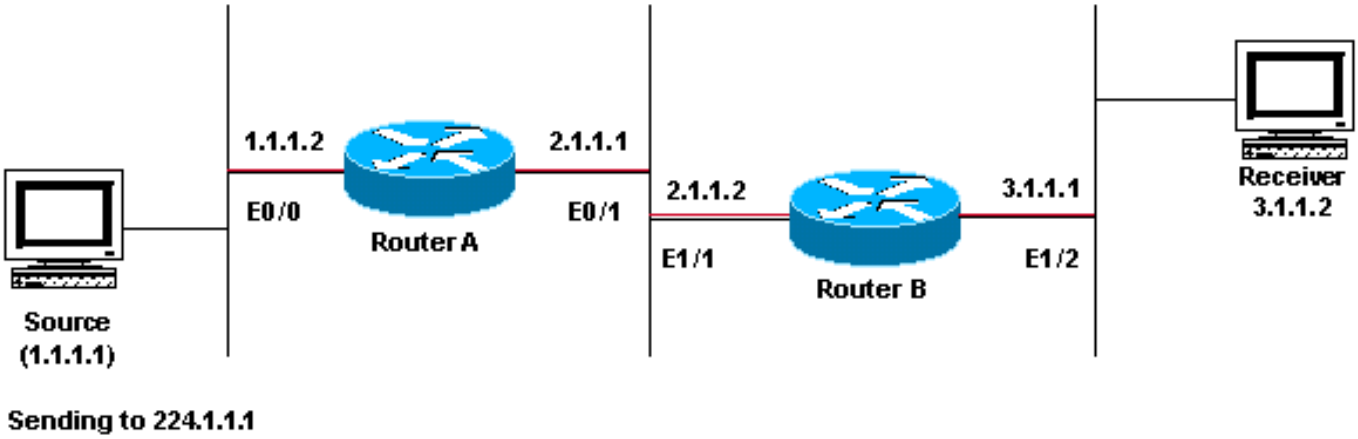
Estados de este mRoute estático que a conseguir al direccionamiento 1.1.1.1 para el RPF, uso 2.1.1.1 como el salto siguiente que está hacia fuera la interfaz E3/1.

La salida de las miradas del **mpacket del IP de la ruta multicast** y del **debug del IP de la**

demostración buenas, el número de paquetes enviados en los aumentos de la **cuenta de la ruta multicast del IP de la demostración**, y el HostA recibe los paquetes.

El router no remite los paquetes de multidifusión al host debido al TTL establece el valor del origen

Esta sección proporciona una solución al problema común de los paquetes del Multicast IP que no se remiten porque el valor del Time to Live (TTL) decremented a cero. Esto es un problema común, pues hay muchas aplicaciones de multidifusión. Estas aplicaciones de multidifusión se diseñan sobre todo para el uso de LAN, y fijan así TTL a un valor bajo o aún a un 1. Utilice este diagrama de la red como un ejemplo.



Diagnostique el problema

En la figura anterior, el router A no remite los paquetes de las fuentes al receptor conectado de forma directa del router B. Mire la salida del **comando show ip mroute** en el router A para ver el estado del ruteo multicast:

Usted puede ignorar 224.0.1.40 en la salida puesto que todo el Routers se une a este auto-RP grupo de la detección. Pero no hay fuente enumerada para 224.1.1.1. Además de “*, 224.1.1.1” usted debe ver "1.1.1.1, el 224.1.1.1".

Ingrese el **comando show ip rpf** para ver si es un problema RPF:

De la salida, usted ve que no es un problema RPF. Revisión de "RPF" señala correctamente el E0/0 para conseguir a la dirección IP de la fuente.

Marque si el PIM está configurado en las interfaces con el **comando show ip pim interface**:

La salida parece buena, así que éste no es el problema. Marque si el router reconoce algún tráfico activo con el **comando show ip mroute active**:

De acuerdo con la salida, el router no reconoce ningún tráfico activo.

Quizás el receptor no está enviando ninguna informes del Internet Group Management Protocol (IGMP) (se une a) para el grupo 224.1.1.1. Usted puede marcarlo con el **comando show ip igmp group**:

224.1.1.1 se ha unido a en el E1/2, que está muy bien.

El modo PIM denso es un protocolo de saturación y separación, por lo que no hay incorporaciones pero sí injertos. Puesto que el router B no ha recibido una inundación del router A, no sabe dónde enviar un injerto.

Usted puede marcar para ver si es un problema de TTL con la captura del sniffer y también visto con el **comando show ip traffic**:

La salida muestra 63744 malos conteos saltos. Cada vez que usted teclea este comando, el mún conteo saltos aumenta. Éste es un indicio sólido que el remitente envía los paquetes con un TTL=1, que el router A decrements a cero. Esto da lugar a un aumento del mún campo de conteo de saltos.

Correcciones posibles

Para solucionar el problema, usted necesita aumentar TTL. Esto se realiza en el nivel de aplicación del Remitente. Si desea obtener más información, consulte el manual de instrucciones de su aplicación de multidifusión.

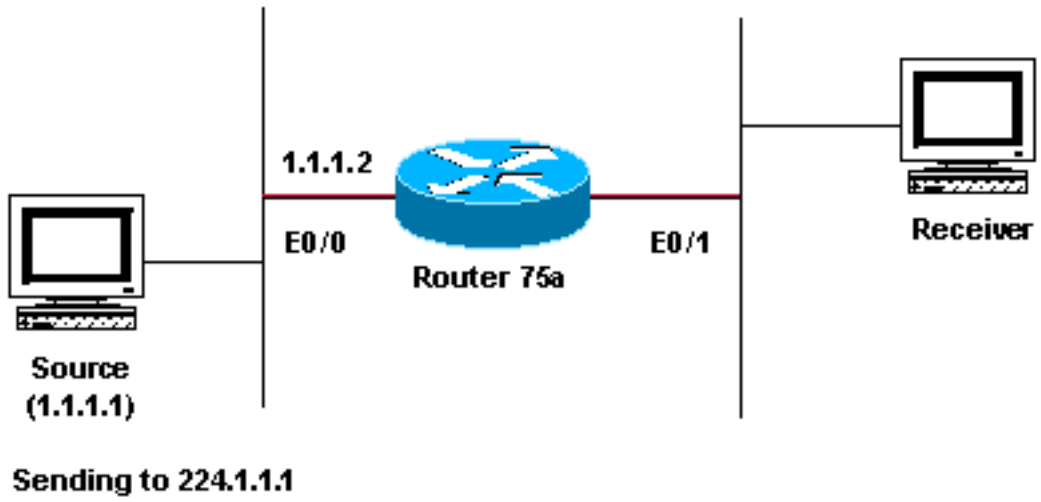
Una vez que se hace esto, el router A parece esto:

Ésta es la clase de salida que usted quiere ver.

En el router B usted ve:

El router no remite los paquetes de multidifusión debido al umbral TTL del router

Esta sección proporciona una solución al problema común donde el umbral TTL se fija demasiado bajo, de modo que el tráfico del Multicast IP no alcance el receptor. Este diagrama de la red se utiliza como un ejemplo.



Diagnostique el problema

En la figura anterior, el receptor no recibe los paquetes de multidifusión de la fuente. Pudo haber vario Routers entre la fuente y el router 75a. Primera mirada en el router 75a, puesto que está conectada directamente con el receptor.

La salida muestra los paquetes hacia fuera Ethernet0/1 del router 75a adelante. Para ser el router absolutamente seguro 75a adelante los paquetes, gire el **debug** apenas para esta fuente y grupo de multidifusión:

Los mensajes del **debug** indican que el router 75a no remite los paquetes de multidifusión porque se ha alcanzado el umbral TTL. Mire la configuración del router para ver si usted puede encontrar la razón. Esta salida muestra al culpable:

El router tiene un umbral TTL de 15, pero éste no significa que cualquier cosa mayor que TTL de 15 no está enviada. De hecho, se aplica lo contrario. La aplicación se envía con TTL de 15. Para el momento en que consiga al router 75a, los paquetes de multidifusión tienen TTL menos de 15.

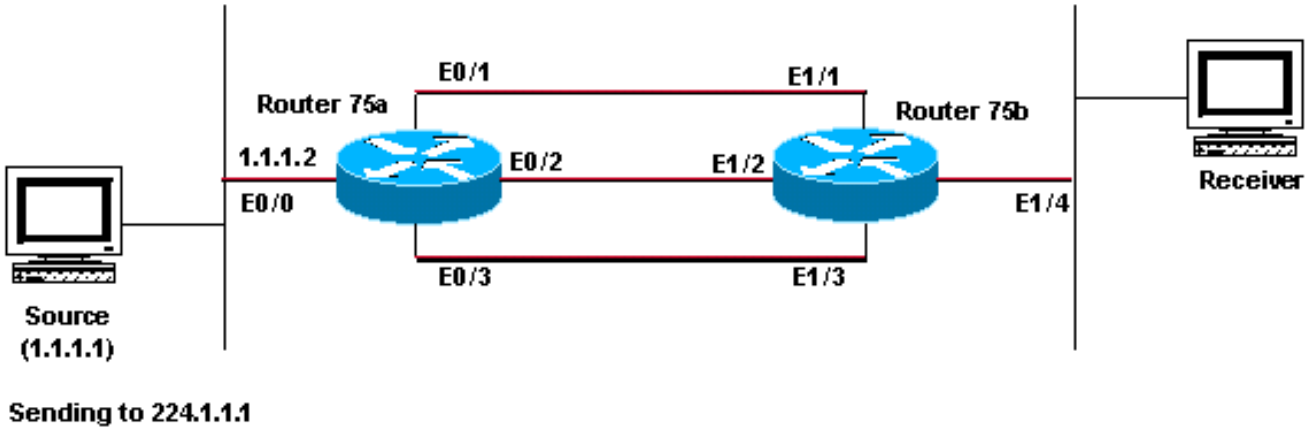
El comando ip multicast ttl-threshold <value> significa que cualquier paquete con TTL baja que el umbral especificado, en este caso, 15, no se remite. Este comando se utiliza generalmente para proporcionar una frontera para guardar el tráfico Multicast interno del intranet de deriva de los.

Correcciones posibles

Cualquiera quita el **comando ip multicast ttl-threshold <value>** con la **ninguna** forma de este comando, que invierte al valor de umbral TTL predeterminado de 0, o baja el umbral TTL de modo que el tráfico pueda pasar.

Los Trayectos múltiples de igual costo dan lugar al comportamiento indeseado RPF

Esta sección muestra cómo los trayectos de igual costo a un origen de multidifusión pueden causar el comportamiento indeseado RPF. También describe cómo configurar el Multicast IP para evitar este comportamiento. Este diagrama de la red se utiliza como un ejemplo.



Diagnostique el problema

En la figura, el router 75b tiene tres trayectos de igual costo de nuevo a la fuente (1.1.1.1), y elige un link que usted no quisiera que fuera su primera opción como el link RPF.

Cuando está hecho frente con los Trayectos múltiples de igual costo a una fuente, el Multicast IP elige la interfaz que tiene un vecino de la multidifusión independiente de protocolo (PIM) con la dirección IP más alta pues la interfaz entrante y después envía las pasas a los vecinos del PIM en los otros links.

Correcciones posibles

Para cambiar el Multicast IP de la interfaz elige como su interfaz entrante, usted puede hacer uno de éstos:

- Sólo configure la PIM en las interfaces que quiere que atraviese la multidifusión. Esto significa que se pierde redundancia de multidifusión.
- Cambie las subredes así que la dirección IP más alta está en el link que usted quiere ser el link primario del Multicast.
- Cree una ruta de Multicast estática (ruta multicast) que señale la interfaz preferida del Multicast, que significa que usted pierde la redundancia de multidifusión.

Como un ejemplo, se crea un mRoute estático.

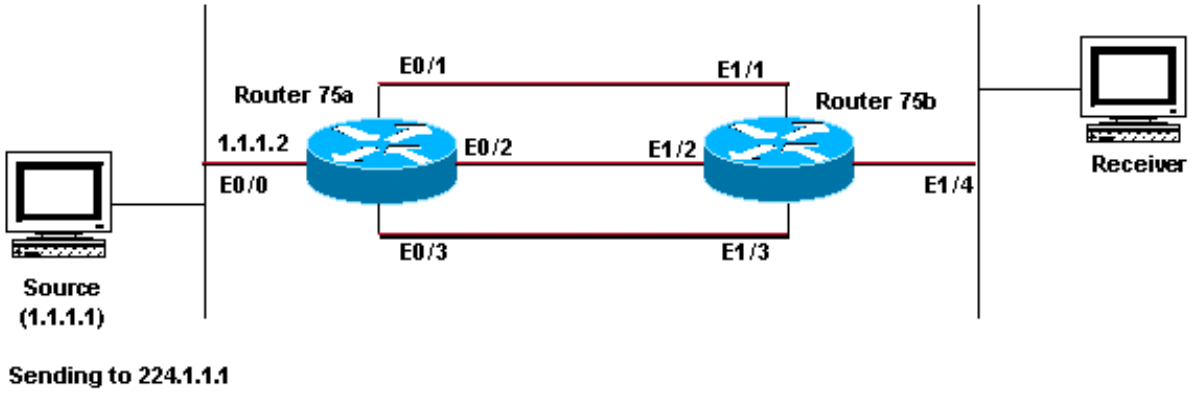
Antes de que usted instale un mRoute estático, usted ve en esta salida que la tabla de ruteo tiene tres rutas de costo equivalente para la dirección de origen 1.1.1.1. La información RPF indica que la interfaz RPF es E1/3:

Después de que usted configure el mRoute estático, usted ve en este hecho salir la interfaz RPF ha cambiado al E1/1:

¿Por qué la carga del Multicast IP no equilibra a través de todos los trayectos de igual costo disponibles?

Esta sección proporciona una solución al problema común de cómo configurar el Multicast IP para cargar la balanza a través de todos los links de costo equivalente disponibles. Este diagrama de la red se utiliza como un ejemplo.

> Nota: Antes de que usted cargue el tráfico partido del Multicast IP a través de los links de costo equivalente sobre un túnel, el Equilibrio de carga por paquete de la configuración CEF o bien los Paquetes GRE no será carga equilibrada por el paquete. Para que otros métodos carguen la parte en los entornos del Multicast, vea el tráfico del Multicast IP de la carga que parte sobre el ECMP.



En la figura, el router 75b tiene tres links de costo equivalente de nuevo a la fuente (1.1.1.1). Usted quiere al balance de la carga el tráfico Multicast a través de los tres links.

Correcciones posibles

Como usted vio en los Trayectos múltiples de igual costo para dar lugar a la sección indeseada del comportamiento RPF, la multidifusión independiente de protocolo (PIM) elige solamente una interfaz para revisión de "RPF" y poda las otras. Esto significa que no ocurre el Equilibrio de carga. Para lograr un equilibrio de carga, debe quitar el PIM de los links redundantes y crear un túnel entre el Router 75a y el Router 75b. Luego puede equilibrar la carga en el nivel de link y las ejecuciones de IP sobre el túnel.

Éstas son las configuraciones para el túnel.

Router 75a
Router 75b

Después de que usted configure el túnel, ingrese el **comando show ip mroute** para ver la ruta de Multicast (ruta multicast) para el grupo:

Para marcar que son los datos de multidifusión la carga equilibró igualmente a través de los tres links, mira los datos de la interfaz del router 75a.

La interfaz entrante es los dígitos por segundo 9000:

Las tres interfaces salientes cada dígitos por segundo de la demostración 3000:

¿Por qué recibimos en el router mensajes de error de multidifusión IP del tipo "INVALID_RP_JOIN"?

Esta sección proporciona las soluciones al problema común del Multicast IP “INVALID_RP_JOIN” mensaje de error.

Diagnostique el problema - Parte 1

Este los mensajes de error se reciben en el (RP) del punto de encuentro:

En Mensajes de error del sistema de software de Cisco IOS, se proporciona una explicación de las causas de este error: un router PIM de descarga envió un mensaje de incorporación para el árbol compartido, que este router no quiere validar. Este comportamiento indica que este router permite solamente a los routeres en sentido descendente se une a un RP específico.

Se sospecha que está continuando una cierta clase de filtración. Usted necesita hechar una ojeada la configuración del router:

¿Cuál es el **sentencia accept-rp** en la configuración supuesta para lograr? En los comandos ip multicast routing, los estados de este documento que “configurar a un router para validar se une a o las pasas destinadas para un RP especificado y para una lista específica de grupos, utilizan el **comando ip pim accept-rp global configuration**. Para quitar ese control, no utilice la **ninguna** forma de este comando.”

Cuando usted quita el **comando ip pim accept-rp**, los mensajes desaparecen. ¿El comando que causa el problema fue encontrado, solamente qué si usted quiere mantener ese comando la configuración? Usted puede ser que permita el direccionamiento incorrecto RP. Ingrese el **comando show ip pim rp mapping** para ver el direccionamiento correcto RP:

Según la salida, 1.1.5.4 es el único RP aprendido vía auto-RP o de otra manera. Sin embargo, este router es solamente el RP para los grupos 224.0.0.0/4. Así pues, la declaración del **pim accept-rp** en la configuración es incorrecta.

Correcciones posibles

La solución es corregir la dirección IP en la instrucción ip pim accept-rp como sigue:

Cambie esta declaración:

A esto:

Usted puede también cambiar la declaración para validar cuál está en el caché auto-RP, y para asegurarse que la lista de acceso (8 en este ejemplo) permita el rango de grupos de multidifusión necesario. Aquí tiene un ejemplo:

Diagnostique el problema - Parte 2

Este mensaje de error se considera en el router2.

Marque para ver si el router2 es el RP para el grupo 224.1.1.1:

El RP para 224.1.1.1 es 1.1.1.1.

Marque si éste es una de las interfaces del router2:

Puesto que el router2 no es un RP, debe no haber recibido esto RP-se une al paquete. Marque porqué el router en sentido descendente envió el unir a al router2, mientras que no debe:

Como usted ve, el router3 ha configurado estáticamente la información y las puntas RP al router2, que es incorrecta. Esto explica porqué el router3 envía RP-se une a al router2.

Correcciones posibles

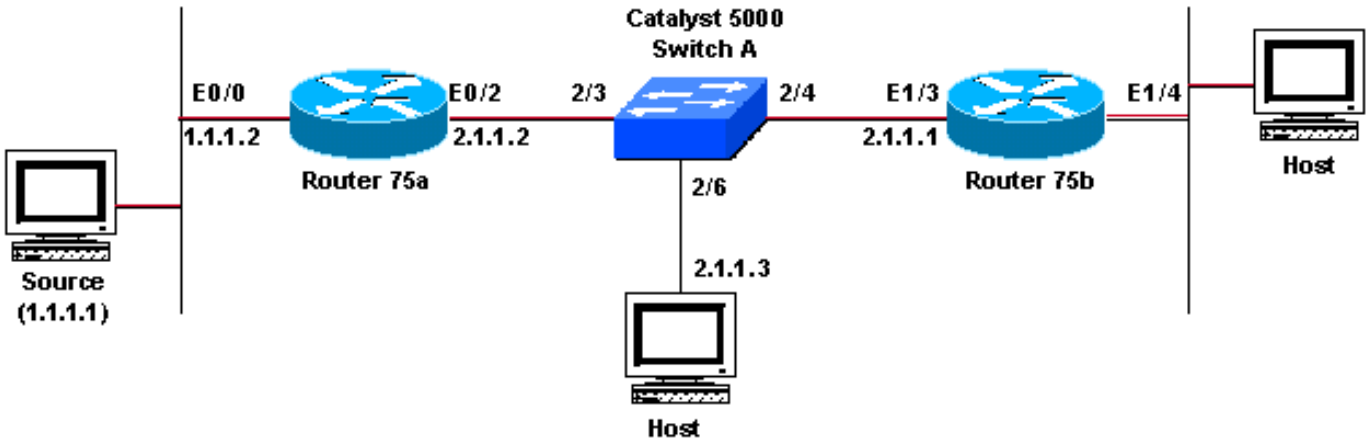
Haga router2 el RP para el grupo 224.1.1.1 o cambie la configuración en el router3 así que refiere al direccionamiento correcto RP.

Después de que la configuración en el router3 se corrija, el router3 refiere al direccionamiento correcto RP y el mensaje de error para el aparecer.

El CGMP no previene la inundación de los paquetes de multidifusión

Esta sección explica cómo la saturación no deseada de los paquetes de multidifusión puede ocurrir cuando el Cisco Group Management Protocol (CGMP) no se habilita en todo el Routers en

una subred determinada, y cómo este problema puede ser evitado. Este diagrama de la red se utiliza como un ejemplo.



Diagnostique el problema

En la figura, la tabla de CAM estática en el Catalyst 5000 Switch A no muestra los puertos correctos uces de los se pueblan que. El router con CGMP configurado no envía los paquetes CGMP.

El CGMP se configura correctamente con el **comando set cgmp enable** en el Switch A y el **comando ip cgmp** en la interfaz E0/2 del router 75a. Sin embargo consideran a los grupos del no multicast en el Switch A cuando publican el **comando show multicast group**:

La salida de este comando debe mostrar cada puerto que tenga un router con CGMP configurado en ella (puerto 2/3) y cada puerto que tenga un receptor interesado en él (puerto 2/6). Puesto que 0 es mencionado, usted puede asumir que todos los puertos se están inundando innecesario con el tráfico Multicast si lo quieren o no.

'Observaciones'

Marque para ver si hay algunos vecinos de la multidifusión independiente de protocolo (PIM) en el router 75a:

La salida muestra que el router 75a puede ver al router 75b como vecino PIM válido con el Switch A.

Ahora marque si usted recibe la información correcta de la ruta de Multicast (ruta multicast) sobre el Routers:

La salida muestra a router 75a adelante los paquetes de multidifusión hacia fuera E0/2 hacia el Switch A. Esta salida muestra que el router 75b consigue los paquetes de multidifusión y adelante los correctamente:

Desde el punto de vista del Switch a, usted ve que considera al router 75a apagado del puerto 2/3.

Todo vista hasta ahora parece muy bien. Ingrese algunos **comandos debug** en el router 75a para ver lo que usted puede descubrir:

En la salida, 0000.0000.0000 es los todo-grupos direccionamiento y se utiliza cuando el Routers envía el CGMP se une a/los mensajes de ausencia así que el Switches puede poblar los puertos de router. Dirección destino del grupo de la significa GDA en la dirección de origen de Unicast llana del formato del Media Access Control (MAC) y de la significa USA. Éste es el direccionamiento del host que originó el informe IGMP para el cual se genera este mensaje CGMP. En este caso, es la dirección MAC para la interfaz E0/2 del router 75a. La dirección MAC para el E0/2 del router 75a se puede considerar con el **comando show interface** según lo considerado aquí:

Además, usted puede ser que vea periódicamente esto cuando giran al **comando debug ip igmp**:

Sin embargo, usted no ve posteriormente un paquete CGMP correspondiente del router 75a. Esto significa que el router 75a recibe los informes IGMP, pero que no genera los paquetes CGMP necesarios para ayudar al Switch A para saber qué puertos a bloquear. Éste es algo que se espera del router 75a si es el interrogador IGMP. Esta salida del router 75a nos dice porqué no ocurre la conducta esperada:

Si usted tiene dos Routers en la misma subred, y usted configura ambos para el CGMP, sólo uno enviará los paquetes CGMP. El router que envía los paquetes CGMP es el router de interrogación IGMP. Esto significa al router con el Unicast IP Address más bajo del Routers IGMP-habilitado.

En este caso, el Routers 75a y el router 75b hacen el IGMP habilitar (el router 75b hizo el router de interrogación IGMP), pero solamente el router 75a hace el CGMP habilitar. Puesto que el router 75a no es el router de interrogación IGMP, no se envía ningunos paquetes CGMP.

Correcciones posibles

Para solucionar el problema, usted necesita configurar el CGMP en el router de interrogación IGMP. En este caso, router 75b. Primero, gire los comandos debug en el router 75b:

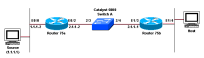
El router 75b recibe un informe IGMP desde 2.1.1.3 para el grupo 224.1.1.1. Posteriormente envía una incorporación CGMP al Switch A para el 224.1.1.1 equivalente de MAC con la dirección MAC (USA) del host interesado 2.1.1.3. El switch A conoce el puerto en el que se encuentra el host, de manera que lo marca como abierto y bloquea a los demás.

Las cosas deben ahora trabajar en el Switch A:

Esto es mucho mejor. Los paquetes de 224.1.1.1 (01-00-5e-01-01-01) son solamente los puertos enviados 2/3, 2/4, y 2/6 en el Switch A, como deben. El inundar al resto de los puertos ha parado. El número total de entradas ahora se enumera correctamente como 2. La dirección MAC 01-00-5e-00-01-28 se asocia de la dirección Multicast 224.0.1.40, que se utiliza para el CGMP propio se une a.

El CGMP no previene las inundaciones de paquetes de multidifusión, debido a la colocación del receptor/fuente

Esta sección proporciona una solución al problema común de un switch de Catalyst que inunde el tráfico a cada puerto, en vez de apenas al host correcto. Este diagrama de la red se utiliza como un ejemplo.



Diagnostique el problema

En la figura, Routers 75a y 75b y el Catalyst 5000 (el Switch A) se configura correctamente para el Multicast y el Cisco Group Management Protocol (CGMP). El host consigue el tráfico Multicast. Sin embargo, está tan cada otro host apagado del Switch A del Switch A. inunda el tráfico hacia fuera cada puerto, así que significa que el CGMP no trabaja.

El resultado del comando show multicast group en el Switch A tiene el siguiente aspecto:

Usted puede ver de la salida que el único grupo es 224.0.1.40, que es utilizado por el router cuando envía las autoincorporaciones de CGMP para grupo RP automático. ¿Como se hace no hay otros grupos?

Correcciones posibles

Para entender la solución, usted necesita entender cómo el CGMP se comporta bajo ciertas condiciones. Un router habilitado para CGMP envía el CGMP se une a un Switch para informar al Switch los host interesados en un grupo de multidifusión determinado. El switch busca las direcciones MAC para estos hosts en su tabla CAM, luego reenvía los paquetes de multidifusión a los puertos con hosts interesados y evita que el resto de los puertos reenvíe paquetes de multidifusión.

Un router manda las autoincorporaciones de CGMP una interfaz habilitada para CGMP si recibe los paquetes de multidifusión de una fuente que esté en la misma interfaz en la cual (el router) hace el CGMP habilitar.

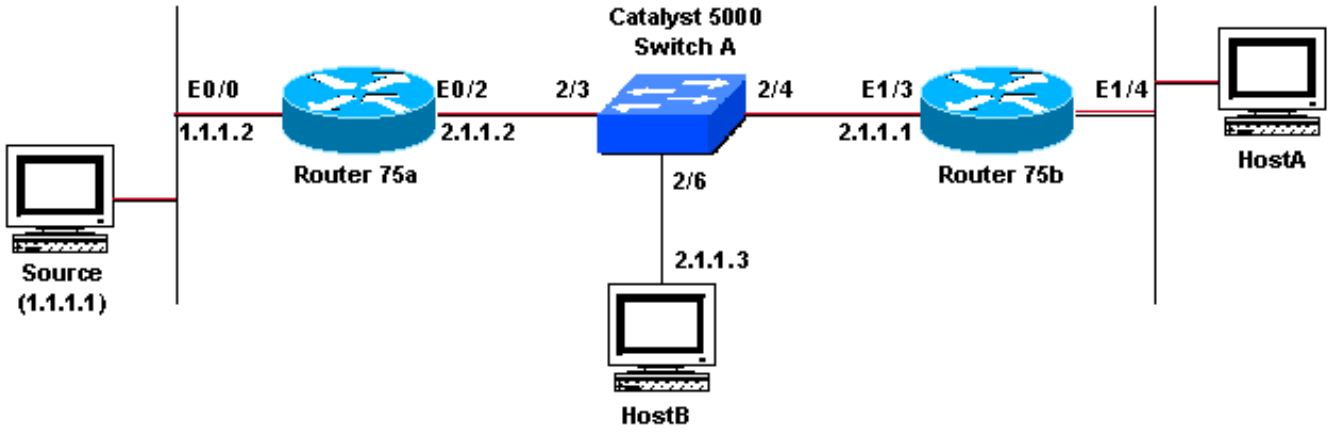
Por ejemplo, si la fuente estuviera en la misma subred (VLAN), 2.1.1.0/24, como los routers 75a y 75b, CGMP funcionaría perfectamente. Al ver los paquetes provenientes de la fuente, el router enviaría un mensaje de autoincorporación de CGMP al switch, que luego aprendería en forma dinámica en qué puertos está el router e impediría al resto de los puertos el envío de paquetes de multidifusión.

Un router envía el CGMP se une a hacia fuera una interfaz habilitada para CGMP si recibe los informes IGMP de un host en la misma interfaz que (el router) hace el CGMP habilitar.

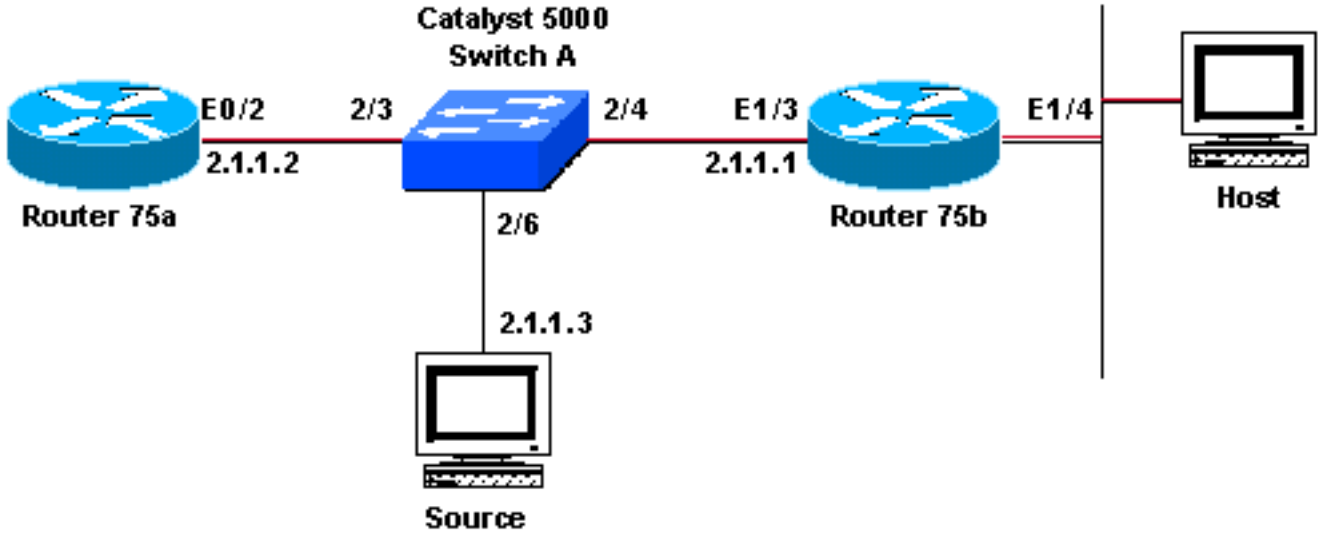
Otro ejemplo es si usted tenía un host interesado en este mismo VLA N. En ese caso, cuando un router habilitado para CGMP recibió un informe del Internet Group Management Protocol (IGMP) de un host que está interesado en un grupo de multidifusión determinado, el router enviaría un CGMP se une a. El unir a indicaría el Media Access Control (MAC) Address del host que quiso unirse a y del grupo que quiso unirse a. El Catalyst 5000 verificaría luego su tabla CAM para la dirección MAC del host, pondría al puerto asociado en la lista del grupo de multidifusión y bloquearía todos los otros puertos no interesantes.

Lo mismo no es verdad cuando la fuente y el host interesado están en una subred con excepción de la subred habilitada para CGMP (VLA N). Los paquetes de multidifusión, eso vienen de la fuente, no accionan al router para enviar las autoincorporaciones de CGMP al Switch. Por lo tanto los paquetes golpean el Switch y consiguen inundados por todas partes dentro del VLA N. Este escenario continúa hasta un host en el VLA N, eso sale un puerto en el Switch, envía un IGMP se une a. Sólo con la recepción de un informe IGMP el router envía un paquete CGMP que provoca que el switch agregue el puerto de host apropiado como puerto de reenvío y se bloqueen los demás puertos (además de los puertos del router).

Por lo tanto, para que el CGMP funcione en esta topología de tipo de tránsito, puede agregar un host al mismo VLAN que los routers 75a y 75b, como en este diagrama de red.



O mueva la fuente en la misma subred como routers 75a y 75b, como en este ejemplo.



Mueva la fuente a la misma subred y después marque la salida del Switch A:

Ahora 224.1.1.1 (01-00-5e-01-01-01) se inunda solamente a los puertos de router 2/3 y 2/4, y no a cada puerto del Switch A.

El CGMP no previene los grupos de dirección de las inundaciones de paquetes de multidifusión con certeza

Esta sección describe los motivos por los cuales algunas direcciones IP hacen que el protocolo de administración de grupo de Cisco (CGMP) se inunde con tráfico multidifusión afuera de todos los puertos de una red de área local (LAN). Cuando usted utiliza a la dirección de grupo de multidifusión 225.0.0.1, el CGMP no trabaja. Inunda el flujo de secuencia de multidifusión fuera de todos los puertos del switch y desperdicia ancho de banda. Sin embargo, si usted cambia el direccionamiento a los trabajos de 225.1.1.1 CGMP muy bien. ¿Cuál es incorrecto con usar 225.0.0.1, puesto que no es una dirección registrada para un Routing Protocol?

Correcciones posibles

Primero, es importante entender cómo asocian a las direcciones Multicast de la capa 3 para acodar a 2 direcciones Multicast. Todas las tramas del Multicast IP utilizan los MAC Layer Address de IEEE que comienzan con el prefijo 24-bit de 0x0100.5e. Cuando usted asocia la capa 3 para acodar 2 direccionamientos, los 23 bits de orden inferior de la dirección Multicast de la capa 3 se asocian en los 23 bits de orden inferior de la dirección MAC de IEEE.

Otro hecho importante a entender es allí es 28 bits de espacio único de direcciones para un IP Multicast Address (32 bits menos los primeros 4 bits que contienen el prefijo de 1110 clases D). Como sólo hay 23 bits conectados a la dirección MAC de IEEE, quedan 5 bits de superposición. Esto significa que las múltiples direcciones multidifusión de capa 3 pueden mapear hacia la misma dirección multidifusión de capa 2.

Por ejemplo:

Note en el ejemplo 224.0.0.1 y correspondencia de 224.128.0.1 lo mismo dirección Multicast de la capa 2.

Ahora que usted sabe la capa 3 acodar a 2 direcciones Multicast se asocia, proceda a la solución específica al este problema.

El Switch A inunda los paquetes de multidifusión a 224.0.0.x porque esos direccionamientos son local de la conexión y usted quiere aseegurarse a las direcciones locales del link conseguir a todos los dispositivos en el red de área local (LAN). Los switches de Catalyst también inundan los paquetes de multidifusión a otras direcciones Multicast que sean nivel MAC ambiguo con 224.0.0.x (por ejemplo, 224.0.0.1 y 225.0.0.1 ambo correspondencia a 0100.5e00.0001). El switch inunda los paquetes de multidifusión destinados a estas direcciones locales del link sin tener en cuenta si CGMP está activado o no.

Por lo tanto, la aplicación de multidifusión debe evitar el uso de direcciones clase D que corresponden a una dirección de multidifusión de Capa 2 de 0100.5e00.00xx, donde xx puede ser 00 a FF en formato hexadecimal. Esto consiste en éstos los direccionamientos de la clase D:

Se reciben las secuencias duplicados del paquete de multidifusión

Causa 1

Se reciben los paquetes de multidifusión duplicados cuando configuran a dos Routers en el modo denso. En el modo denso, el dispositivo inunda periódicamente la secuencia. Después de inundar, poda de las interfaces donde el vapor no se quiere. El dos Routers también pasa con el proceso de la aserción y decide quién es el promotor. Cada vez que suceden los temporizadores salen esto, y hasta este proceso es completo, ambo Routers remite la secuencia. Esto hace la aplicación recibir las secuencias de multidifusión duplicados.

Arreglo posible 1

Este problema puede ser resuelto si usted tiene uno del Routers configurado para el ruteo multicast y configurar al otro router para ser el RP en la conexión en sentido ascendente. Configurelo para convertir la secuencia en el modo disperso antes de que la secuencia entre en al router. Esto puede evitar que los paquetes duplicados alcancen la aplicación. No es una parte de la responsabilidad de las redes de asegurarse de que ningunos paquetes duplicados alcanzan

nunca un host extremo. Es una parte de la responsabilidad de la aplicación de manejar los paquetes duplicados y de ignorar los datos innecesarios.

Causa 2

Este problema puede ocurrir en los Cisco Catalyst 6500 Switch, que se configuran para el modo de la replicación de multidifusión de la salida y se pueden accionar por el retiro y la reinserción de cualquier [OIR] del linecards. Después del OIR, el puerto de la tela de [FPOE] de la salida puede misprogrammed, que puede hacer los paquetes ser dirigido al canal incorrecto de la salida de la tela y ser enviado al linecards incorrecto. El resultado es que son circuito hecho atrás a la tela y las épocas múltiples replicadas en que salen en el linecard correcto.

Arreglo posible 2

Como solución alternativa, cambie al modo de la replicación del ingreso. Durante un cambio de la salida al modo de la ingreso-replicación, las interrupciones del tráfico pueden ocurrir porque se purgan y están reinstalados los accesos directos.

Actualice el Cisco IOS Software a una versión no afectada por el Id. de bug Cisco CSCeg28814 (clientes registrados solamente) para permanantly resolver el problema.

Causa 3

Este problema puede también ocurrir si la configuración del escalamiento del lado de recepción (RSS), en los host extremos o los servidores, se inhabilita.

Arreglo posible 3

La configuración RSS facilita una transición transmisión de datos más rápida a través de los CPU múltiples. Habilite la configuración RSS en el host extremo o el servidor. Refiera al establecimiento de una red scalable del artículo de Microsoft con el RSS para más información.

¿Por qué se caen los paquetes de multidifusión?

Causa 1

Es posible que usted ve los rubores y los descensos excesivos del paquete de entrada en las interfaces cuando fluye el tráfico Multicast. Usted puede marcar los rubores con el **comando show interface**.

Arreglo posible 1

Usted puede fijar el valor SPT como infinito para la interfaz donde se consideran los rubores excesivos.

Configure esto:

Causa 2

Cuando usted utiliza el comando del unir a-**grupo del igmp del IP <group-name>** en cualquier interfaz, hace el process switching. Si los paquetes de multidifusión son proceso conmutado en cualesquiera interfaces, consume más CPU como él asigna el process switching por mandato de todos los paquetes a ese grupo. Usted puede funcionar con el **comando show buffers input-interface** y marcar el tamaño anormal.

Arreglo posible 2

Usted puede utilizar el comando del estático-**grupo del igmp del IP <group-name>** en vez del comando del unir a-**grupo del igmp del IP <group-name>**.

> Nota: Debido a los problemas anteriores, es posible que usted ve CPU elevada el uso el alrededor 90 por ciento. El CPU baja a normal cuando usted lo resuelve con estos arreglos posibles.

Información Relacionada

- Herramientas de resolución de problemas de la multidifusión básica
- Guía rápida de configuración para Multicast (Multidifusión)
- Soporte de tecnología del Multicast IP
- Soporte de los IP Routing Protocol
- Soporte técnico y documentación Cisco Systems