Comprender los mensajes de redirección ICMP

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Mensajes de Redireccionamiento de ICMP](#)
[Rutas subóptimas a través de redes Ethernet](#)
[Routing estático](#)
[Policy-Based Routing](#)
[Redirecciones ICMP en links punto a punto](#)
[Consideraciones sobre la plataforma Nexus](#)
[Herramientas para supervisar y diagnosticar el tráfico](#)
[show ip traffic](#)
[Etanizador](#)
[Inhabilitación de Mensajes de Redirección ICMP](#)
[Summary](#)

Introducción

Este documento describe la funcionalidad de redirección de paquetes del Protocolo de mensajes de control de Internet (ICMP).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Arquitectura de la plataforma Nexus 7000
- Configuración del software Cisco NX-OS
- Protocolo de mensajes de control de Internet como se describe en la solicitud de comentarios (RFC) 792

Componentes Utilizados

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

- Nexus 7000
- Software Cisco NX-OS

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento describe la funcionalidad de redirección de paquetes proporcionada por el Protocolo de mensajes de control de Internet (ICMP). El documento explica qué indica generalmente la presencia de mensajes de redirección ICMP en la red y qué se puede hacer para minimizar los efectos secundarios negativos asociados con las condiciones de la red que causan la generación de mensajes de redirección ICMP.

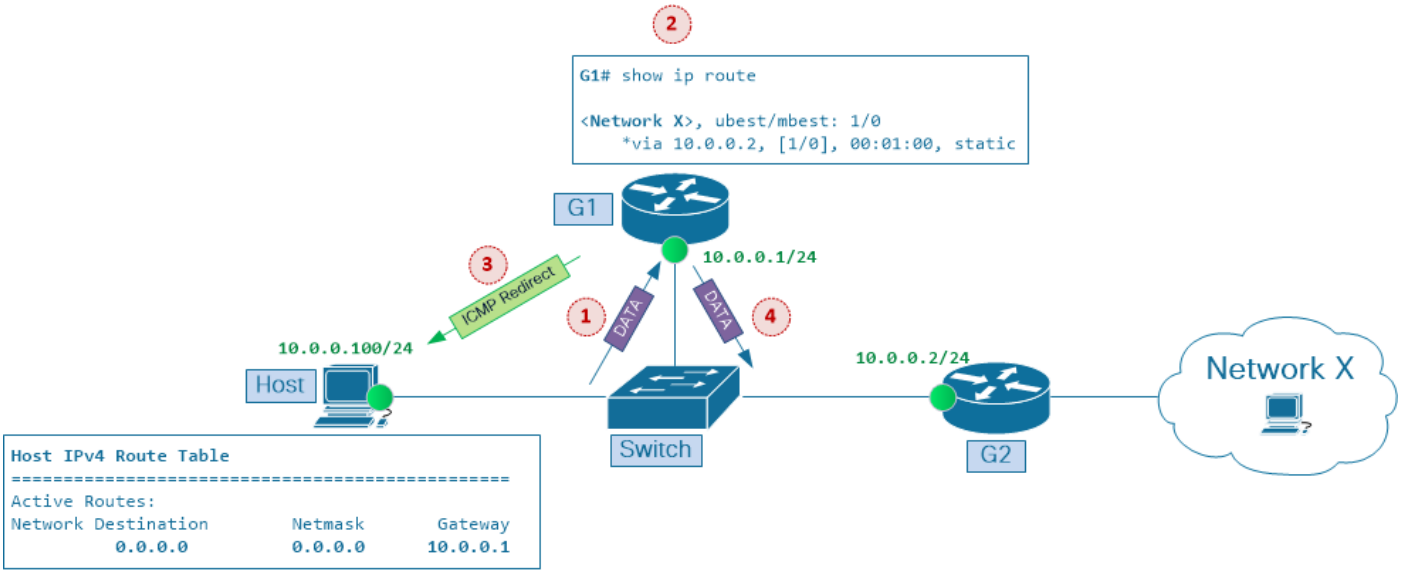
Mensajes de Redireccionamiento de ICMP

La funcionalidad de redirección ICMP se explica en RFC 792 Internet Control Message Protocol con este ejemplo:

> El gateway envía un mensaje de redirección a un host en esta situación.
>
> Una puerta de enlace, G1, recibe un datagrama de Internet de un host de una red a la que está conectada la puerta de enlace. La puerta de enlace, G1, comprueba su tabla de routing y obtiene la dirección de la siguiente puerta de enlace, G2, en la ruta a la red de destino de Internet de datagrama, X
>
> Si G2 y el host identificado por la dirección de origen de Internet del datagrama están en la misma red, se envía un mensaje de redirección al host. El mensaje de redirección aconseja al host enviar su tráfico para la red X directamente al gateway G2, ya que es un trayecto más corto al destino.
>
> El gateway reenvía los datos del datagrama original a su destino de Internet.

Este escenario se muestra en la figura 1. El host y dos routers, G1 y G2, están conectados al segmento Ethernet compartido y tienen direcciones IP en la misma red 10.0.0.0/24

Figura 1 Redirecciones ICMP en Redes Ethernet Multipunto



El host tiene la dirección IP 10.0.0.100. La tabla de routing de host tiene una entrada de ruta predeterminada que señala a la dirección IP 10.0.0.1 del router G1 como gateway predeterminada. El router G1 utiliza la dirección IP 10.0.0.2 del router G2 como salto siguiente al reenviar tráfico a la red de destino X.

Esto es lo que sucede cuando el host envía un paquete a la red de destino X:

1. La puerta de enlace G1 con dirección IP 10.0.0.1 recibe el paquete de datos del host 10.0.0.100 en una red a la que está conectada.

2. La gateway, G1, verifica su tabla de ruteo y obtiene la dirección IP 10.0.0.2 de la siguiente gateway, G2, en la ruta a la red de destino del paquete de datos, X.

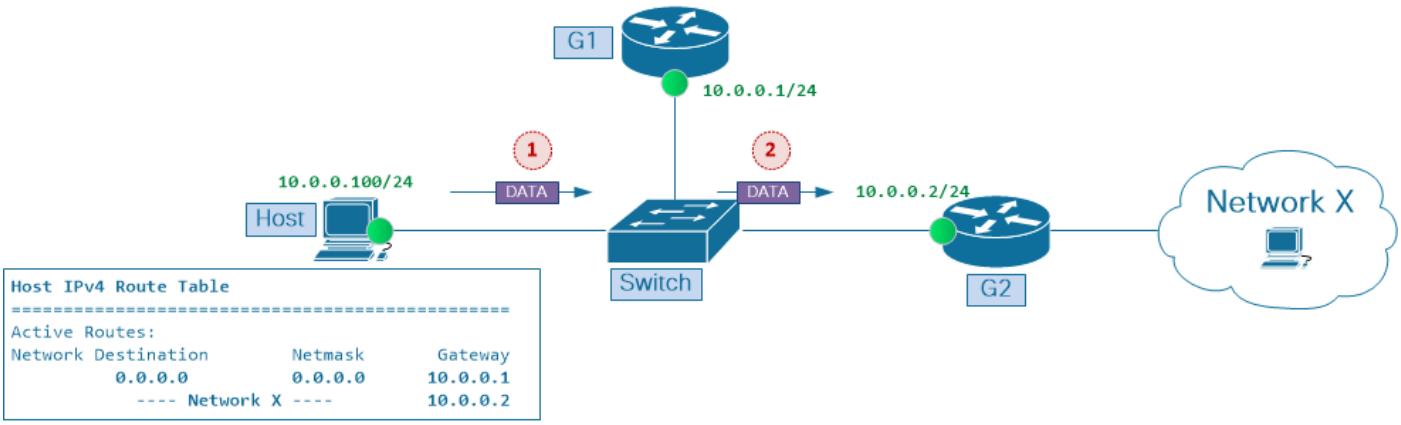
3. Si G2 y el host identificado por la dirección de origen del paquete IP están en la misma red, el mensaje de redirección ICMP se envía al host. El mensaje de redirección ICMP aconseja al host enviar su tráfico para la red X directamente al gateway G2, ya que es una ruta más corta al destino.

4. El gateway G1 reenvía el paquete de datos original a su destino.

Dependiendo de la configuración del host, puede optar por ignorar los mensajes de redirección ICMP que G1 le envía. Sin embargo, si el Host utiliza mensajes de Redirección ICMP para ajustar su caché de ruteo y comienza a enviar los paquetes de datos subsiguientes directamente a G2, estas ventajas se logran en esta situación

- Optimización de la ruta de reenvío de datos a través de la red; el tráfico llega a su destino más rápido
- Reducción de la utilización de recursos de red, como ancho de banda y carga de CPU del router

Figura 2 Siguiente Salto G2 Instalado en la Caché de Ruteo de Host



Próximo salto G2 instalado en caché de routing de host

Como se muestra en la figura 2, después de que el host creara la entrada de caché de ruta para la red X con G2 como salto siguiente, se observan estas ventajas en la red:

- La utilización del ancho de banda en el enlace entre el switch y el router G1 disminuye en ambas direcciones.

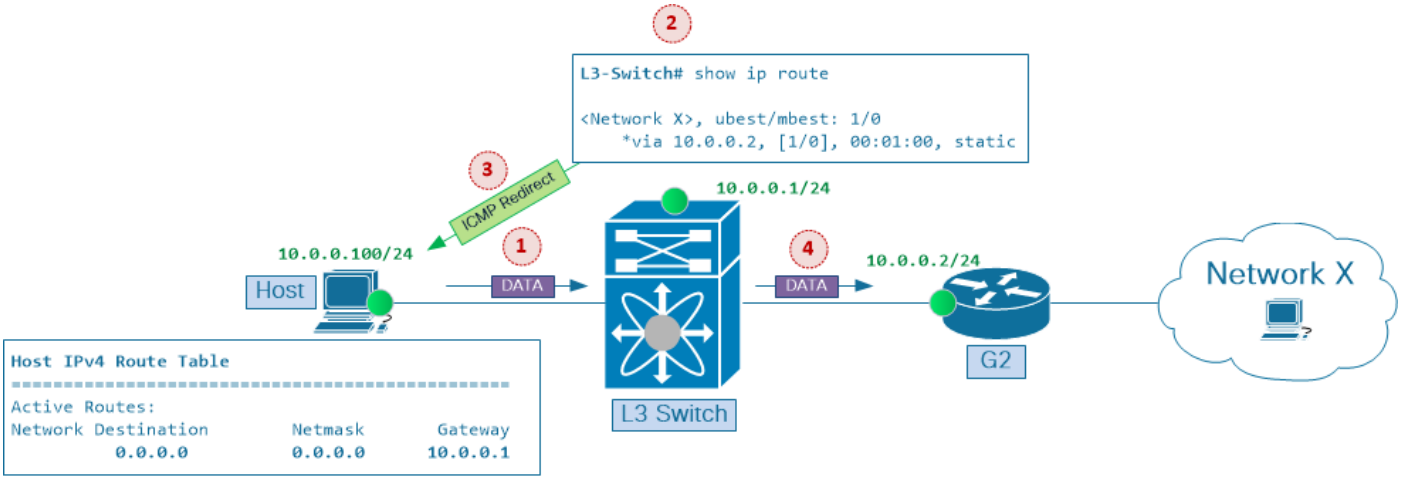
- La utilización de la CPU en el router G1 se reduce, ya que el flujo de tráfico del host a la red X ya no atraviesa este nodo.
- Mejora el retraso de la red de extremo a extremo entre el host y la red X.

Para comprender la importancia del mecanismo de redirección ICMP, recuerde que las primeras implementaciones del router de Internet dependían principalmente de los recursos de la CPU para procesar el tráfico de datos. Por lo tanto, era deseable reducir el volumen de tráfico que debía gestionar cualquier router individual y también minimizar el número de saltos de router que un flujo de tráfico concreto debía atravesar en su camino al destino. Al mismo tiempo, el reenvío de la capa 2 (también conocido como switching) se implementó principalmente en circuitos integrados específicos de las aplicaciones (ASIC) personalizados y, desde la perspectiva del rendimiento de reenvío, fue relativamente "barato" en comparación con el reenvío de la capa 3 (también llamado routing), que, de nuevo, se llevó a cabo en procesadores de uso general.

Las generaciones ASIC más recientes pueden realizar el reenvío de paquetes de Capa 2 y Capa 3. La búsqueda de la tabla de capa 3 realizada en hardware ayuda a reducir el coste de rendimiento asociado con la gestión de paquetes por parte de los routers. Además, cuando se integró la funcionalidad de reenvío de la capa 3 en los switches de la capa 2 (que ahora se denominan switches de la capa 3), el funcionamiento del reenvío de paquetes fue más eficiente, se eliminó la necesidad de opciones de diseño de **router con un brazo** (también conocido como **router en un solo sentido**) y se evitaron las limitaciones asociadas a dichas configuraciones de red.

La figura 3 se basa en el escenario de la figura 1. Ahora, las funciones de capa 2 y capa 3, proporcionadas originalmente por dos nodos independientes, el switch y el router G1, se consolidan en un único switch de capa 3, como la plataforma Nexus serie 7000.

Figura 3 El switch de capa 3 reemplaza la configuración de "router con un solo brazo"



El switch de capa 3 sustituye la configuración de "router con un solo brazo"

Esto es lo que sucede cuando el Host envía un paquete a la Red X de destino:

1. El switch de gateway L3 con dirección IP 10.0.0.1 recibe el paquete de datos de un host 10.0.0.100 en una red a la que está conectado.

2. El gateway, switch L3, verifica su tabla de ruteo y obtiene la dirección 10.0.0.2 del siguiente gateway, G2, en la ruta a la red de destino de paquete de datos, X.

3. Si G2 y el host identificado por la dirección de origen del paquete IP están en la misma red, el

mensaje de redirección ICMP se envía al host. El mensaje de redirección ICMP aconseja al host enviar su tráfico para la red X directamente al gateway G2, ya que es una ruta más corta al destino.

4. El gateway reenvía el paquete de datos original a su destino.

Con los switches de la capa 3 que ahora pueden realizar el reenvío de paquetes tanto de la capa 2 como de la capa 3 en el nivel ASIC, se puede concluir que se consiguen las dos ventajas de la funcionalidad de redirección ICMP, (a) la mejora del retraso a través de la red y (b) la reducción de la utilización de los recursos de red, y que ya no es necesario prestar mucha atención a las técnicas de optimización de rutas en segmentos Ethernet multipunto.

Sin embargo, con la funcionalidad de redirección ICMP habilitada en las interfaces de capa 3, el reenvío por debajo del nivel óptimo a través de segmentos Ethernet multipunto sigue presentando cuellos de botella de rendimiento potenciales, aunque por una razón diferente, como se explica en la sección Consideraciones sobre la plataforma Nexus más adelante en este documento.

> **Nota:** Las redirecciones ICMP están habilitadas de forma predeterminada en las interfaces de capa 3 en el software Cisco IOS y Cisco NX-OS.

> **Nota:** Resumen de las condiciones cuando se generan mensajes de redirección ICMP: El switch de Capa 3 genera un mensaje de redirección ICMP de vuelta al origen del paquete de datos, si el paquete de datos se reenvía fuera de la interfaz de Capa 3 en la que se recibe este paquete.

Rutas subóptimas a través de redes Ethernet

Los protocolos de gateway interior (IGP), como Open Shortest Path First (OSFP) y Cisco Enhanced Interior Gateway Routing Protocol (EIGRP), están diseñados para sincronizar la información de routing entre routers y para proporcionar un comportamiento de reenvío de paquetes coherente y predecible en todos los nodos de red que cumplen con dicha información. Por ejemplo, con las redes Ethernet multipunto, si todos los nodos de Capa 3 en un segmento utilizan la misma información de ruteo y coinciden en el mismo punto de salida al destino, rara vez ocurre un reenvío subóptimo a través de dichas redes.

Para comprender las causas de los trayectos de reenvío subóptimos, recuerde que los nodos de la Capa 3 toman decisiones de reenvío de paquetes independientes entre sí. Es decir, la decisión de reenvío de paquetes tomada por el Router B no depende de la decisión de reenvío de paquetes tomada por el Router A. Este es uno de los principios clave que debe recordar al resolver problemas de reenvío de paquetes a través de redes IP, y es importante tenerlo en cuenta al investigar la trayectoria de reenvío subóptima en redes Ethernet multipunto.

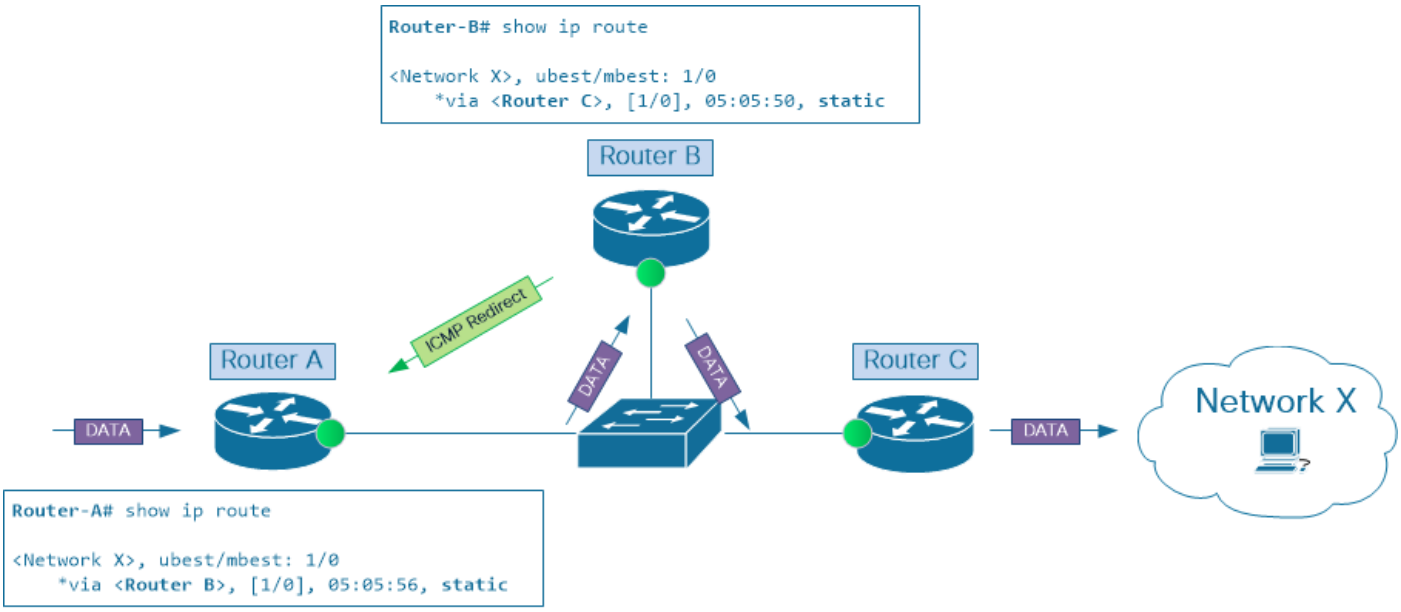
Como se ha mencionado anteriormente, en las redes en las que todos los routers dependen de un único protocolo de routing dinámico para distribuir el tráfico entre los terminales, no debe producirse un reenvío por debajo del nivel óptimo a través de segmentos Ethernet multipunto. Sin embargo, en las redes del mundo real es muy común encontrar una combinación de varios mecanismos de reenvío y ruteo de paquetes. Ejemplos de tales mecanismos son varios IGP, ruteo estático y ruteo basado en políticas. Estas funciones se suelen utilizar conjuntamente para conseguir el reenvío de tráfico deseado a través de la red.

Si bien el uso combinado de estos mecanismos puede ayudar a ajustar el flujo de tráfico y cumplir los requisitos de un diseño de red en particular, pasan por alto los efectos secundarios que estas herramientas juntas pueden causar en las redes Ethernet multipunto, que pueden dar lugar a un rendimiento de red general deficiente.

Routing estático

Para ilustrar esto, considere el escenario de la Figura 4. El Router A tiene una ruta estática a la Red X con el Router B como su salto siguiente. Al mismo tiempo, el Router B utiliza el Router C como su salto siguiente en la ruta estática a la Red X.

Figura 4 Ruta subóptima con routing estático



Ruta subóptima con enrutamiento estático

Mientras el tráfico ingresa a esta red en el Router A, la deja a través del Router C y finalmente llega a la Red X de destino, los paquetes tienen que cruzar esta red IP dos veces en su camino al destino. Esto no es un uso eficiente de los recursos de red. En su lugar, enviar paquetes desde el router A directamente al router C lograría los mismos resultados, mientras que y consumiría menos recursos de red.

> **Nota:** Aunque en este escenario el Router A y el Router C se utilizan como nodos de ingreso y egreso de Capa 3 para este segmento de red IP, ambos nodos pueden ser reemplazados por dispositivos de red (como balanceadores de carga o firewalls) si estos últimos tienen una configuración de ruteo que resulta en el mismo comportamiento de reenvío de paquetes.

Policy-Based Routing

El routing basado en políticas (PBR) es otro mecanismo que puede provocar que la ruta a través de las redes Ethernet no sea óptima. Sin embargo, a diferencia del enrutamiento estático o dinámico, PBR no funciona en el nivel de la tabla de enrutamiento. En su lugar, programa la lista de control de acceso (ACL) de redirección del tráfico directamente en el hardware del switch. Como resultado, para los flujos de tráfico seleccionados, la búsqueda de reenvío de paquetes en la tarjeta de línea de entrada omite la información de enrutamiento que se obtiene mediante el

enrutamiento estático o dinámico.

En la Figura 4, los Routers A y B intercambian información de ruteo sobre la Red X de destino con uno de los protocolos de ruteo dinámico. Ambos coinciden en que el Router B es el mejor salto siguiente a esta red.

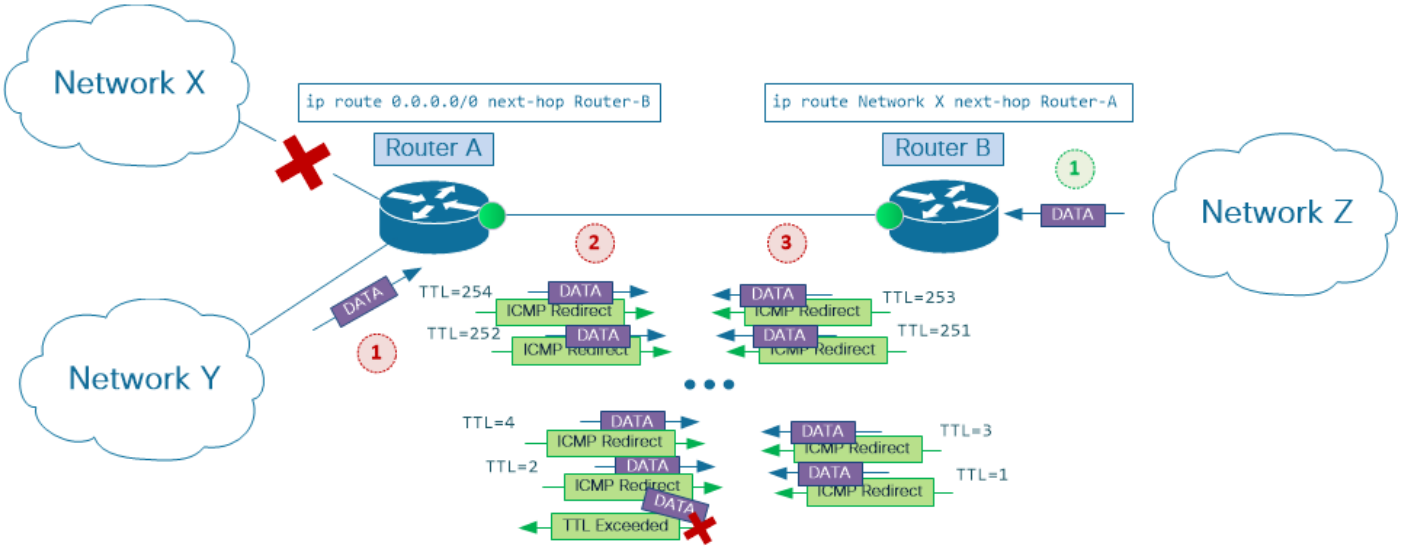
Sin embargo, con una configuración PBR en el Router B que invalida la información de ruteo recibida del protocolo de ruteo y establece el Router C como salto siguiente a la red X, se cumple la condición para activar la función Redireccionamiento ICMP y el paquete se envía a la CPU del Router B para procesarlo más.

Redirecciones ICMP en links punto a punto

Hasta ahora, este documento se refería a las redes Ethernet que tienen tres (o más) nodos de Capa 3 conectados, de ahí el nombre de redes Ethernet multipunto. Sin embargo, tenga en cuenta que los mensajes de redirección ICMP también se pueden generar en links Ethernet punto a punto.

Considere el escenario de la Figura 5. El router A utiliza una ruta estática predeterminada para enviar tráfico al router B, mientras que el router B tiene una ruta estática a la red X que apunta al router A.

Figura 5 Redirecciones ICMP en Links Punto a Punto



Ruta subóptima con enrutamiento estático

Esta opción de diseño, también conocida como conexión de enlace único, es una opción popular cuando conecta entornos de usuarios pequeños a redes de proveedores de servicios. En este caso, el router B es un dispositivo periférico del proveedor (PE) y el router A es un dispositivo periférico del usuario (CE).

Observe que la configuración CE típica incluye rutas estáticas agregadas a bloques de direcciones IP de usuario que apuntan a la interfaz Null0. Esta configuración es una práctica recomendada para la opción de conectividad CE-PE de enlace único con routing estático. Sin embargo, para los fines de este ejemplo, supongamos que no existe tal configuración.

Suponga que el Router A pierde conectividad con la Red X como se muestra en la Figura.

Cuando los paquetes de la red Y del usuario o de la red Z remota intentan llegar a la red X, los routers A y B pueden rebotar el tráfico entre sí y disminuir el campo Tiempo de vida de IP en cada paquete hasta que su valor alcance 1, momento en el cual no es posible un mayor ruteo del paquete.

Mientras que el tráfico a la Red X rebota entre los routers PE y CE, aumenta dramáticamente (e innecesariamente) la utilización del ancho de banda del link CE-PE, el problema se agrava si las Redirecciones ICMP están habilitadas en uno o ambos lados de la conexión PE-CE punto a punto. En este caso, cada paquete en el flujo dirigido a la Red X se procesa en la CPU en cada router varias veces para ayudar a generar los mensajes de redirección ICMP.

Consideraciones sobre la plataforma Nexus

Cuando se habilitan las redirecciones ICMP en la interfaz de Capa 3 y un paquete de datos entrante utiliza esta interfaz tanto para ingresar como para egresar un switch de Capa 3, se genera un mensaje de redirección ICMP. Mientras que el reenvío de paquetes de Capa 3 se realiza en hardware en la plataforma Cisco Nexus 7000, sigue siendo responsabilidad de la CPU del switch construir los mensajes de redirección ICMP. Para ello, la CPU en el módulo Supervisor Nexus 7000 necesita obtener información de dirección IP del flujo cuya trayectoria a través del segmento de red se puede optimizar. Esta es la razón detrás del paquete de datos enviado por la tarjeta de línea de ingreso al módulo Supervisor.

Si los destinatarios del mensaje de redirección ICMP lo ignoran y continúan reenviando tráfico de datos a la interfaz de Capa 3 del switch Nexus en el que están habilitados los redireccionamientos ICMP, se activa el proceso de generación de redirección ICMP para cada paquete de datos.

En el nivel de tarjeta de línea, el proceso comienza en forma de excepción de reenvío de hardware. Se producen excepciones en los ASIC cuando el módulo de tarjeta de línea no puede completar correctamente la operación de reenvío de paquetes. En este caso, el paquete de datos debe ser enviado al módulo Supervisor para el manejo correcto del paquete.

> **Nota:** La CPU en el módulo Supervisor no sólo genera mensajes de redirección ICMP, sino que también gestiona muchas otras excepciones de reenvío de paquetes, como paquetes IP con un valor de tiempo de vida (TTL) establecido en 1 o paquetes IP que deben fragmentarse antes de enviarse al siguiente salto.

Después de que la CPU en el módulo Supervisor envió el mensaje de redirección ICMP al origen, completa el manejo de excepciones reenviando el paquete de datos al siguiente salto a través del módulo de tarjeta de línea de salida.

Aunque los módulos de supervisor de Nexus 7000 utilizan potentes procesadores de CPU que pueden procesar grandes volúmenes de tráfico, la plataforma está diseñada para gestionar la mayor parte del tráfico de datos en el nivel de tarjeta de línea sin necesidad de involucrar al procesador de CPU del supervisor en el proceso de reenvío de paquetes. Esto permite que la CPU se centre en sus tareas principales y deja la operación de reenvío de paquetes a motores de hardware dedicados en tarjetas de línea.

En redes estables, se espera que las excepciones de reenvío de paquetes, si ocurren, ocurran a una velocidad razonablemente baja. Con esta suposición, pueden ser manejadas por la CPU del Supervisor sin un impacto significativo en su rendimiento. Por otro lado, con una CPU que se ocupa de las excepciones de reenvío de paquetes que se producen a una velocidad muy alta

puede tener un efecto negativo en la estabilidad y la capacidad de respuesta globales del sistema.

El diseño de la plataforma Nexus 7000 proporciona una serie de mecanismos para proteger la CPU del switch de cantidades significativas de tráfico. Estos mecanismos se implementan en diferentes puntos del sistema. En el nivel de tarjeta de línea, hay limitadores de velocidad de hardware y plano de control Policing (CoPP). Ambos establecen umbrales de velocidad de tráfico, que controlan de manera efectiva la cantidad de tráfico que se reenvía al Supervisor desde cada módulo de tarjeta de línea.

Estos mecanismos de protección dan preferencia al tráfico de varios protocolos de control que son críticos para la estabilidad de la red y la capacidad de administración del switch, como OSPF, BGP o SSH, y al mismo tiempo filtran agresivamente tipos de tráfico que no son críticos para la funcionalidad del plano de control del switch. La mayor parte del tráfico de datos, si se reenvía a la CPU como resultado de las excepciones de reenvío de paquetes, está fuertemente controlado por estos mecanismos.

Mientras que los limitadores de velocidad de hardware y CoPP policing los mecanismos proporcionan estabilidad en el plano de control del switch y se recomienda encarecidamente que estén siempre activados; pueden ser una de las principales razones de las caídas de paquetes de datos, los retrasos en las transferencias y el bajo rendimiento general de las aplicaciones en la red. Es por esto que es importante entender las rutas que los flujos de tráfico toman a través de la red y el uso de herramientas para monitorear el equipo de red que puede y/o se espera que utilice la funcionalidad de Redirección ICMP.

Herramientas para supervisar y diagnosticar el tráfico

show ip traffic

Tanto el software Cisco IOS como el Cisco NX-OS proporcionan una forma de comprobar las estadísticas del tráfico gestionado por la CPU. Esto se hace con **show ip traffic** comando. Este comando se puede utilizar para verificar la recepción y/o generación de mensajes de redirección ICMP por el switch o router de Capa 3.

```
Nexus7000#show ip traffic | begin ICMP

ICMP Software Processed Traffic Statistics
-----------------------------------------
Transmission:
Redirect: 1000, unreachable: 0, echo request: 0, echo reply: 0,

<output omitted for brevity>

ICMP originate Req: 0, Redirects Originate Req: 1000
Originate deny - Resource fail: 0, short ip: 0, icmp: 0, others: 0
Reception:
Redirect: 0, unreachable: 0, echo request: 0, echo reply: 0,
```

```
<output omitted for brevity>

Nexus7000#
```

Ejecute show ip traffic varias veces y compruebe si los contadores de redirección ICMP aumentan.

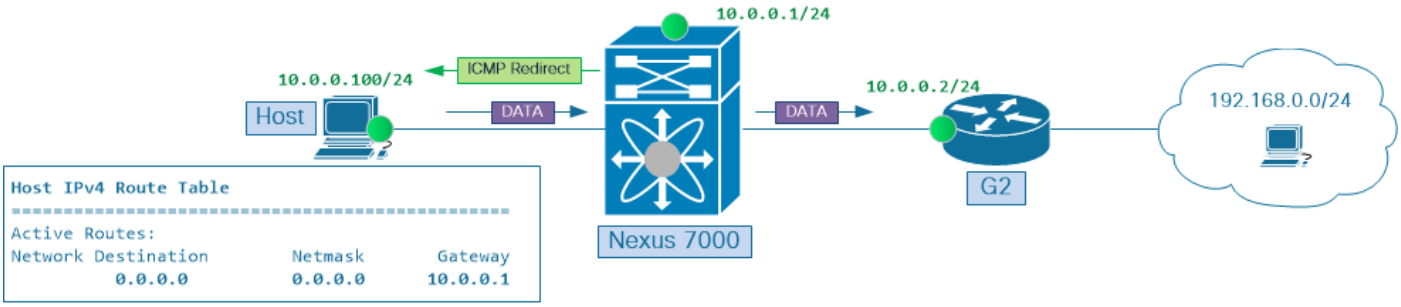
Etanizador

El software Cisco NX-OS cuenta con una herramienta integrada para capturar el tráfico flowing hacia y desde la CPU del switch, conocida como Ethanalyzer.

> **Nota:** Para obtener más información sobre Ethanalyzer, consulte la Guía de Troubleshooting de Ethanalyzer en Nexus 7000.

La figura 6 muestra un escenario similar al de la figura 3. En este caso, la red X se sustituye por la red 192.168.0.0/24.

Figura 6 Ejecución de la captura de Ethanalyzer



Ejecutar captura de Ethanalyzer

El host 10.0.0.100 envía un flujo continuo de solicitudes de eco ICMP a la dirección IP de destino 192.168.0.1. El host utiliza la interfaz virtual de switch (SVI) 10 del switch Nexus 7000 como su próximo salto a la red remota 192.168.0.0/24. A modo de demostración, el host está configurado para ignorar los mensajes de redirección ICMP.

Utilice este siguiente comando para capturar el tráfico ICMP recibido y enviado por la CPU Nexus 7000:

```
Nexus7000#ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000

Capturing on inband
2018-09-15 23:45:40.124077   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.124477     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.124533   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126344   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.126655   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
    2018-09-15 23:45:40.128348   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
    2018-09-15 23:45:40.128611     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
    2018-09-15 23:45:40.128659   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.130362   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.130621     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.130669   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
```

```
2018-09-15 23:45:40.132392   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.132652     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.132700   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134612     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.134660   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136598     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.136645   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138351   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.138656   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request

...
```

Las marcas de tiempo en la salida anterior sugieren que tres paquetes destacados en este ejemplo fueron capturados al mismo tiempo, 2018-09-15 23:45:40.128. El siguiente es un desglose por paquete de este grupo de paquetes

- El primer paquete es el paquete de datos de ingreso, que en este ejemplo es una solicitud de eco ICMP.

  2018-09-15 23:45:40.128348 10.0.0.100 -> 192.168.0.1 Solicitud de eco ICMP (ping)

- El segundo paquete es un paquete de redirección ICMP, generado por el gateway. Este paquete se devuelve al host.

  2018-09-15 23:45:40.128611 10.0.0.1 -> 10.0.0.100 Redirección ICMP (Redirección para host)

- El tercer paquete es el paquete de datos capturado en la dirección de salida, después de haber sido enrutado por la CPU. Aunque no se ha mostrado anteriormente, este paquete tiene su TTL IP disminuido y se vuelve a calcular la suma de comprobación.

  2018-09-15 23:45:40.128659 10.0.0.100 -> 192.168.0.1 Solicitud de eco ICMP (ping)

Mientras navega a través de grandes capturas de Ethanalyzer que tienen muchos paquetes de diferentes tipos y flujos, puede ser difícil correlacionar los mensajes de Redirección ICMP con el tráfico de datos que corresponde a ellos.

En estas situaciones, céntrese en los mensajes de redirección ICMP para recuperar información sobre los flujos de tráfico reenviados por debajo del nivel óptimo. Los mensajes de redirección ICMP incluyen el encabezado de Internet más los primeros 64 bits de los datos del datagrama original. El origen del datagrama utiliza estos datos para hacer coincidir el mensaje con el proceso adecuado.

Utilice la herramienta de captura de paquetes Ethanalyzer con la palabra clave **detail** para mostrar el contenido de los mensajes de redirección ICMP y encontrar la información de dirección IP del flujo de datos que se reenvía subóptimamente

```
Nexus7000#ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000
detail

...
Frame 2 (70 bytes on wire, 70 bytes captured)
Arrival Time: Sep 15, 2018 23:54:04.388577000
[Time delta from previous captured frame: 0.000426000 seconds]
[Time delta from previous displayed frame: 0.000426000 seconds]
```

[Time since reference or first frame: 0.000426000 seconds]
Frame Number: 2
Frame Length: 70 bytes
Capture Length: 70 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:icmp:ip:icmp:data]
Ethernet II, Src: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf), Dst: 00:0a:00:0a:00:0a
(00:0a:00:0a:00:0a)
Destination: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
Address: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
Source: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
Address: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.100 (10.0.0.100)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 56
Identification: 0xf986 (63878)
Flags: 0x00
0.. = Reserved bit: Not Set
.0. = Don't fragment: Not Set
..0 = More fragments: Not Set
Fragment offset: 0
Time to live: 255
Protocol: ICMP (0x01)
Header checksum: 0xadd9 [correct]
[Good: True]
[Bad : False]
Source: 10.0.0.1 (10.0.0.1)
Destination: 10.0.0.100 (10.0.0.100)
Internet Control Message Protocol
Type: 5 (Redirect)
Code: 1 (Redirect for host)
Checksum: 0xb8e5 [correct]
Gateway address: 10.0.0.2 (10.0.0.2)
Internet Protocol, Src: 10.0.0.100 (10.0.0.100), Dst: 192.168.0.1 (192.168.0.1)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 84
Identification: 0xf986 (63878)
Flags: 0x00
0.. = Reserved bit: Not Set
.0. = Don't fragment: Not Set
..0 = More fragments: Not Set
Fragment offset: 0
Time to live: 254
Protocol: ICMP (0x01)
Header checksum: 0xa8ae [correct]
[Good: True]
[Bad : False]
Source: 10.0.0.100 (10.0.0.100)
Destination: 192.168.0.1 (192.168.0.1)

```
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0 ()
Checksum: 0x02f9 [incorrect, should be 0xcae1]
Identifier: 0xa01d
Sequence number: 36096 (0x8d00)

...
```

Inhabilitación de Mensajes de Redirección ICMP

Si el diseño de red requiere que el flujo de tráfico se enrute desde la misma interfaz de Capa 3 en la que ingresó al switch o router, es posible evitar que el flujo se enrute a través de la CPU si inhabilita la funcionalidad de Redirección ICMP en la interfaz de Capa 3 que le corresponde.

De hecho, para la mayoría de las redes es una buena práctica desactivar proactivamente las redirecciones ICMP en todas las interfaces de Capa 3, tanto físicas, como interfaces Ethernet, como virtuales, como interfaces Port-Channel y SVI. Use el comando no ip redirects Comando de nivel de interfaz de Cisco NX-OS para desactivar las redirecciones ICMP en una interfaz de capa 3. Para verificar que la funcionalidad de Redirección ICMP está inhabilitada:

- Garantía**no ip** se agrega el comando **redirects** a la configuración de la interfaz.

```
Nexus7000#show run interface vlan 10

interface Vlan10
no shutdown no ip redirects
  ip address 10.0.0.1/24
```

- Asegúrese de que el estado de Redirecciones ICMP en la interfaz muestre "desactivado".

```
Nexus7000#show ip interface vlan 10 | include redirects
  IP icmp redirects: disabled
```

- Asegúrese de que el indicador de activación/desactivación de redirección ICMP esté configurado en **0** por el componente de software Cisco NX-OS que envía la configuración de interfaz desde el Supervisor del switch a una de más tarjetas de línea.

```
Nexus7000#show system internal eltm info interface vlan 10 | i icmp_redirect
  per_pkt_ls_en = 0, icmp_redirect = 0, v4_same_if_check = 0
```

- Asegúrese de que el indicador de habilitación/inhabilitación de redirección ICMP para una interfaz de Capa 3 determinada esté configurado en **0** en una o más tarjetas de línea.

```
Nexus7000#attach module 7
Attaching to module 7 ...
To exit type 'exit', to abort type '$.'
Last login: Wed Sep 15 23:56:25 UTC 2018 from 127.1.1.1 on pts/0
module-7#

!--- Optionally, jump to non-admin Virtual Device Context (VDC) if verification needs to be done
in one of the custom VDCs
module-7#vdc 6

module-7#show system internal iftmc info interface vlan 10 | include icmp_redirect
```

icmp_redirect : 0x0 ipv6_redirect : 0x1

Summary

El mecanismo de redirección ICMP, tal y como se describe en RFC 792, se diseñó para optimizar la ruta de reenvío a través de segmentos de red multipunto. Al inicio de Internet, dicha optimización ayudó a proteger recursos de red caros, como el ancho de banda de los enlaces y los ciclos de CPU de los routers. A medida que el ancho de banda de la red se volvió más asequible y el ruteo de paquetes basado en CPU relativamente lento evolucionó hacia un reenvío de paquetes de capa 3 más rápido en ASIC de hardware dedicado, disminuyó la importancia del tránsito de datos óptimo a través de segmentos de red multipunto. De forma predeterminada, la funcionalidad de redirección ICMP está habilitada en cada interfaz de capa 3. Sin embargo, sus intentos de notificar a los nodos de red en segmentos Ethernet multipunto acerca de las rutas de reenvío óptimas no siempre son entendidos por el personal de la red y sobre los que éste actúa. En redes con uso combinado de varios mecanismos de reenvío, como el enrutamiento estático, el enrutamiento dinámico y el enrutamiento basado en políticas, si deja habilitada la funcionalidad de redirección ICMP y no la supervisa correctamente, esto puede dar lugar a un uso no deseado de la CPU de los nodos de tránsito para controlar el tráfico de producción. Esto, a su vez, puede causar un impacto significativo tanto en los flujos de tráfico de producción como en la estabilidad del plano de control de la infraestructura de red.

En la mayoría de las redes, se considera una buena práctica deshabilitar de forma proactiva la funcionalidad de redirección ICMP en todas las interfaces de capa 3 de la infraestructura de red. Esto ayuda a evitar escenarios de tráfico de datos de producción que se manejan en la CPU de switches y routers de Capa 3 cuando hay una mejor trayectoria de reenvío a través de segmentos de red multipunto.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).