

Troubleshooting complejo del mensaje de error OSPF

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Problemas](#)

[Problema 1](#)

[Problema 2](#)

[Problema 3](#)

[Soluciones](#)

[Solución del problema 1](#)

[Tipo 2 LSA](#)

[Type-3 LSA](#)

[LSA tipos 5](#)

[Solución del problema 2](#)

[Solución del problema 3](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo resolver problemas los mensajes de error del Open Shortest Path First (OSPF) que se encuentran en las operaciones de la red normal y pudieron degradar la conectividad de red.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de los fundamentales OSPF.

Componentes Utilizados

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

hardware.

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.

Antecedentes

El protocolo OSPF es un Interior Gateway Protocol (IGP) extensamente desplegado en la empresa y las redes del proveedor de servicios.

Este protocolo era desarrollado debido a una necesidad en la comunidad de Internet de introducir las altas funciones, IGP NON-propietario para la familia de protocolos TCP/IP. Las discusiones para la creación de un interoperable común IGP para Internet comenzó en 1988 y no fueron formalizadas hasta 1991. En aquel momento, el Grupo de trabajo OSPF pidió que el OSPF esté considerado para que el adelanto elabore la norma de Internet.

El protocolo OSPF se basa en la tecnología de estado de link, que es una salida de los algoritmos basados en el vector de Botones-Ford que se utilizan en los Internet Routing Protocol tradicionales, tales como Routing Information Protocol (RIP).

Problemas

Esta sección describe tres problemas OSPF que pudieron degradar la conectividad de red.

Problema 1

Usted recibe el mensaje de error **OSPF-4-FLOOD_WAR**. La guerra de la inundación OSPF ocurre cuando el router recibe en varias ocasiones su propio anuncio del estado del link (LSA) y lo vacía de la red o envía una nueva versión de ella. Esto se significa para detectar los problemas con el Tipo 2 LSA cuando las direcciones IP duplicadas están presentes en la red, o con los LSA tipos 5 cuando hay un ID de router duplicado en diversas áreas OSPF.

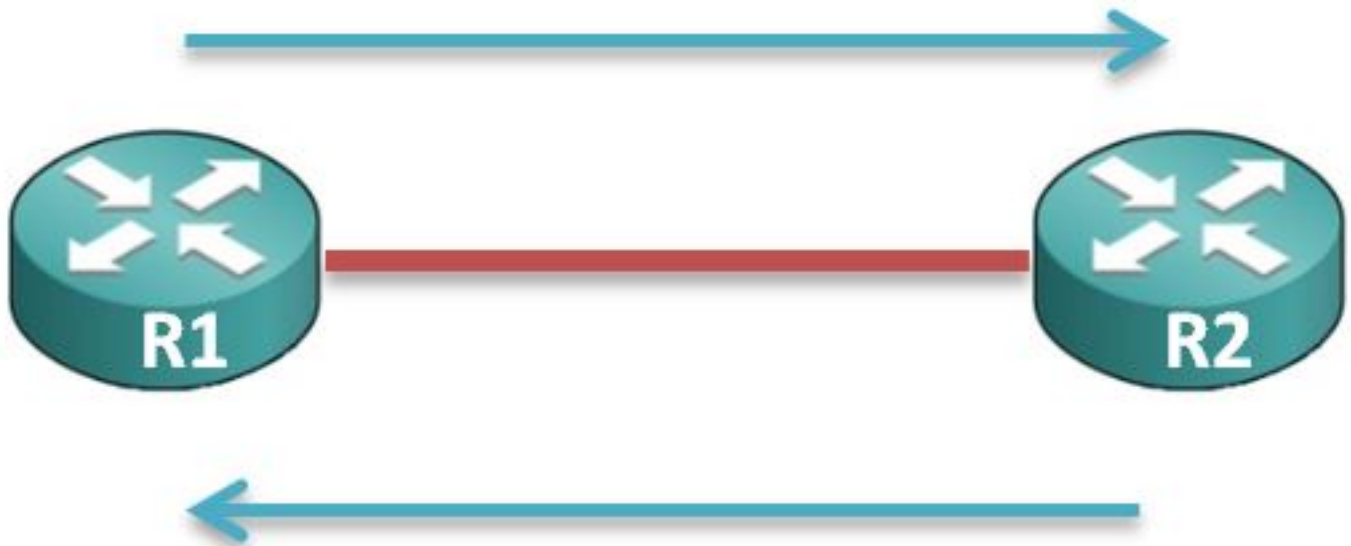
En un escenario típico, hay un router en la red que origina el LSA y a un segundo router que vacía el LSA.

Esta imagen ilustra las creaciones y los eventos rasantes entre el primer y segundo Routers (R1 Nombrado y r2, respectivamente):

1) Originates LSA Seq#N, age 1

3) Originates LSA Seq#N+1, age 1

5) Originates LSA Seq#N+2, age 1



2) Flushes LSA Seq#N, age 3600

4) Flushes LSA Seq#N+1, age 3600

Problema 2

Usted recibe el mensaje de error `%OSPF-4-CONFLICTING_LSAID`. Este mensaje de error indica que una creación LSA era prevenido debido a un conflicto con un LSA actual que tiene el mismo estado ID del link pero una diversa *máscara de subred*.

El algoritmo en el RFC 2328, el apéndice E se utiliza para resolver los conflictos cuando los LSA múltiples con el mismo prefijo y diversas máscaras se hacen publicidad. Cuando se utiliza este algoritmo, y se hacen publicidad las rutas del host, hay situaciones donde está imposible la resolución de conflicto y la ruta del host o el prefijo que está en conflicto no se hace publicidad.

Aquí está un snippet del ejemplo del mensaje de error:

```
%OSPF-4-CONFLICTING_LSAID: LSA origination prevented by existing LSA with same LSID  
but a different mask
```

```
Existing Type 5 LSA: LSID 192.168.1.0/31  
New Destination: 192.168.1.0/32
```

Problema 3

Usted configura el OSPF para utilizar la característica rápida de los paquetes de saludo, que causa CPU elevada. El soporte OSPF para la característica rápida de los paquetes de saludo no prohíbe a configuraciones tales que los paquetes de saludo están enviados en los intervalos menos que el segundo. Estos tipos de configuraciones dan lugar a una convergencia más rápida en una red OSPF.

Este comando se utiliza para fijar el intervalo durante el cual por lo menos un paquete de saludo debe ser recibido, o consideran al vecino abajo:

```
ip ospf dead-interval minimal hello-multipliermultiplier
```

Aquí tiene un ejemplo:

```
Router(config-if)# ip ospf dead-interval minimal hello-multiplier 5
```

En este ejemplo, el soporte OSPF para los paquetes de saludo rápidos se habilita con la especificación de la palabra clave **mínima**, de la palabra clave del hola-**multiplicador**, y del valor. Porque el multiplicador se fija a **5**, cinco paquetes de saludo se envían cada segundo.

Soluciones

Esta sección describe algunas Soluciones posibles a los problemas que se describen en la sección anterior.

Solución del problema 1

Es importante que usted entienda el mensaje de error durante las tentativas de resolver problemas los mensajes de la guerra de la inundación. Los mensajes aparecen diferentemente en las creaciones y el Routers rasante. Por este motivo, es crucial centrarse en el tipo LSA para quien el mensaje de la guerra de la inundación está señalado, pues resuelven problemas a cada tipo LSA diferentemente.

Aquí está un snippet del ejemplo del mensaje de la guerra de la inundación OSPF:

```
%OSPF-4-FLOOD_WAR: Process 1 re-originates LSA ID 172.16.254.25 type-2 adv-rtr  
172.16.253.1 in area 0
```

```
%OSPF-4-FLOOD_WAR: Process 1 flushes LSA ID 172.16.254.25 type-2 adv-rtr  
172.16.253.1 in area 0
```

Aquí están los componentes del mensaje descritos:

- **Proceso** – Éste es el proceso OSPF que señala el error.
- **re-origina** o los **rubores** – Esto indica si este router *origina* o *vacía* el LSA.
- **LSA ID** – Éste es el LSA ID para el cual se detecta la guerra de la inundación.
- **Tipo** – Éste es el tipo LSA.

Nota: La guerra de la inundación para cada LSA tiene una diversa causa raíz.

- **adv-RTR** – Éste es el router de anuncio que origina el LSA.
- **Área** – Ésta es el área a la cual el LSA pertenece.

Tipo 2 LSA

Nota: Refiera al [RFC 2328](#) (capítulo 13.4, el caso 3) para la información adicional si la guerra de la inundación se imprime para un Tipo 2 LSA.

Si un router recibe una red LSA del Tipo 2 cuyo LSA ID esté lo mismo que la dirección IP para una de las interfaces que se asocian a ese router, después el router debe vaciar el LSA. La causa raíz en este escenario es las dirección IP duplicadas en las creaciones y el Routers rasante.

Para resolver este problema, configurar de nuevo el IP Address en una de las interfaces o apagar la interfaz que tiene la dirección IP duplicada.

Nota: Esta comprobación para las dirección IP duplicadas se realiza en las interfaces que están abajo también. La interfaz debe ser en el modo *admin-abajo* para desviar el control. En algunos casos que ocurres sólo fuera de los parámetros de funcionamiento normales, la guerra de la inundación también está señalada para una interfaz administrativo apagada, así que la solución permanente es quitar las dirección IP duplicadas en la red.

Type-3 LSA

Es raro encontrar los problemas de la guerra de la inundación para un Type-3 LSA. Los mensajes de error de la guerra de la inundación para Type-3 LSA se han registrado en los escenarios en los cuales la subred IP de un link inestable se propaga pesadamente en el dominio OSPF.

Cisco recomienda que usted abre un caso de soporte con el Centro de Asistencia Técnica de Cisco (TAC) si usted encuentra los problemas de la guerra de la inundación debido a Type-3 LSA.

LSA tipos 5

Las guerras de la inundación debido a los LSA tipos 5 ocurren cuando hay ID de routers duplicados en el Routers que está situado en diversas áreas. Es obligatorio cambiar el Router ID en uno del Routers.

Otro caso de las guerras tipas 5 de la inundación es cuando hay dos Routers que tiene la misma declaración de la red del Border Gateway Protocol (BGP) y ambo Routers redistribuir esas redes de BGP en el OSPF. Si cualquiera de esos routers BGP alcanza la red con el OSPF, después una guerra de la inundación OSPF debido a un LSA tipo 5 está señalada.

En resumen, asegúrese de que el router ID no sea lo mismo, y la redistribución correcta del LSA externo debe prevenir los problemas de la guerra de la inundación debido a los LSA tipos 5.

Solución del problema 2

El paso inicial que usted debe tomar con las tentativas de resolver el mensaje de error **OSPF-CONFLICTING_LSAID** es localizar el prefijo que no se hace publicidad así como el prefijo que está en conflicto.

Para localizar éstos, ingrese la **ruta de IP de la demostración** y los comandos **show ip ospf database** en el CLI. El administrador debe seguir el origen del **nuevo destino: 192.168.1.0/32**, tal y como se muestra en el Caso de ejemplo descrito en la sección del [problema 2](#), y corrigen a la máscara de subred de la red.

El caso usual de LSA en conflicto ID se registra después de un cambio reciente en el OSPF y se resuelve después de que usted corrija la configuración de las máscaras de subred en las declaraciones de la red OSPF.

Solución del problema 3

CPU elevada los casos se registran con el TAC de Cisco cuando los clientes despliegan el hellos rápido OSPF en los switches de la serie del Cisco Catalyst.

Nota: Cisco recomienda que usted no configura el hellos OSPF rápidamente.

El ® del Cisco IOS se ejecuta en un modelo no comprado de antemano, y la característica rápida del paquete de saludo requiere que el hellos OSPF esté procesado más con frecuencia que el Intervalo muerto del segundo. Pudo haber ocasiones que el OSPF no obtiene a los recursos requeridos en un sistema con otros procesos de larga duración. El dependiente sobre su entorno y los otros protocolos y aplicaciones que se configuran en el router, el uso de esta capacidad puede ser problemático.

El suplente del sub-second hola fue introducido con la detección bidireccional de la expedición (BFD), en donde el BFD se desarrolla para la detección rápida del vecino abajo. El BFD se ejecuta en el modo de la *interrupción* y no experimenta los problemas que se observan con el hellos OSPF rápidamente. Cisco recomienda que usted utiliza el BFD para una convergencia más rápida.

Aquí están dos defectos conocidos debido al hellos rápido OSPF:

- Id. de bug Cisco [CSCut14044](#): *Hola rápido 333msec WS-C3750X-48/OSPF/descenso/15.0(2)SE6 de la adyacencia*
- Id. de bug Cisco [CSCsd17835](#): *las adyacencias rápidas del hola OSPF/del hsrp están agitando continuamente*

Información Relacionada

- [Resolver problemas los ID de routers duplicados con el OSPF](#)
- [Soporte y descargas – Cisco Systems](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)