Solução de problemas de mensagens de erro complexas do OSPF

Contents

Introduction

Este documento descreve como solucionar problemas de mensagens de erro de Open Shortest Path First (OSPF) que são encontrados em operações de rede normal e podem reduzir a conectividade de rede.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento dos fundamentos OSPF.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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

Informações de Apoio

O protocolo OSPF é um IGP (Interior Gateway Protocol, Protocolo de gateway interno) amplamente implantado em redes corporativas e de provedor de serviços.

Esse protocolo foi desenvolvido devido a uma necessidade na comunidade da Internet de introduzir uma alta funcionalidade, IGP não proprietário para a família de protocolos TCP/IP. As discussões para a criação de um IGP interoperável comum para a Internet começaram em 1988 e não foram formalizadas até 1991. Naquela época, o grupo de trabalho do OSPF solicitou que o OSPF fosse considerado para o avanço do Draft Internet Standard.

O protocolo OSPF é baseado na tecnologia link-state, que é um desvio dos algoritmos baseados em vetor da Bellman-Ford usados nos protocolos tradicionais de roteamento da Internet, como o Routing Information Protocol (RIP).

Problemas

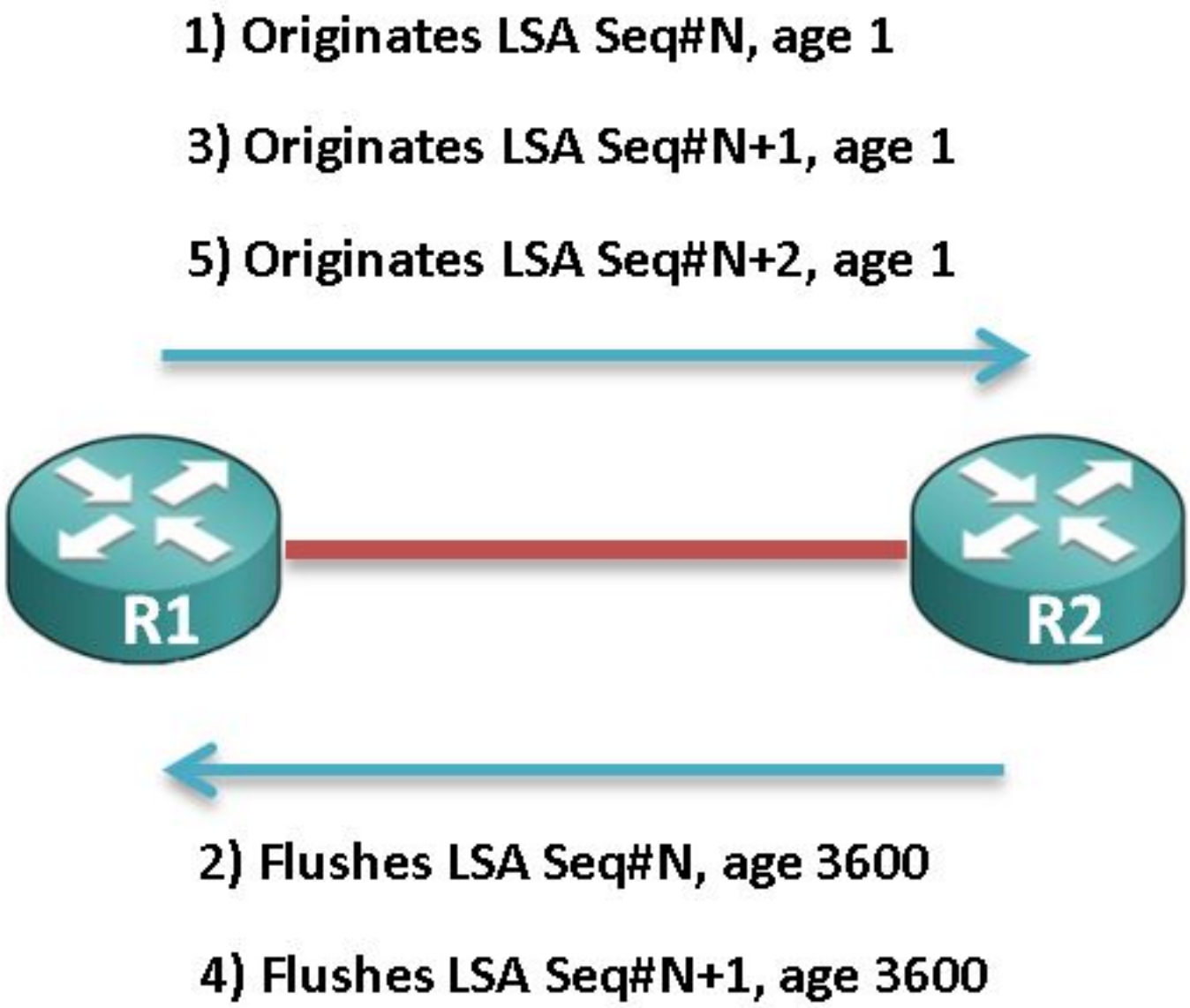
Esta seção descreve os três problemas do OSPF que podem prejudicar a conectividade de rede.

Problema 1

Você recebe a mensagem de erro **OSPF-4-FLOOD_WAR.** O flood war do OSPF ocorre quando o roteador recebe repetidamente seu próprio LSA (Link State Advertisement) e libera-o da rede ou envia uma nova versão dele. Isso serve para detectar problemas com LSAs tipo 2, quando endereços IP duplicados estão presentes na rede, ou com LSAs tipo 5, quando há uma ID de roteador duplicada em áreas de OSPF diferentes.

Em um cenário típico, há um roteador na rede que origina o LSA e um segundo roteador que libera o LSA.

Esta imagem ilustra os eventos de origem e liberação entre o primeiro e o segundo roteadores (denominados R1 e R2, respectivamente):



Problema 2

Você recebe a mensagem de erro **%OSPF-4-CONFLICTING_LSAID.** Essa mensagem de erro indica que uma origem de LSA foi impedida devido a um conflito com um LSA atual que possui a mesma ID de estado de link, mas uma diferente *máscara de sub-rede*.

O algoritmo no RFC 2328, Apêndice E, é usado para resolver conflitos quando vários LSAs com o mesmo prefixo e diferentes máscaras são anunciados. Quando esse algoritmo é usado e as rotas do host são anunciadas, há situações em que a resolução de conflitos é impossível e o roteador do host ou o prefixo conflitante não é anunciado.

Aqui está um exemplo de trecho de código da mensagem de erro:

```
%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

Configure o OSPF para usar o recurso de pacotes de identificação rápida, provocando a alta utilização da CPU. O suporte do OSPF para o recurso de pacotes de identificação rápida permite configurações de modo que esses pacotes sejam enviados em intervalos com menos de um segundo. Esses tipos de configurações resultam em uma convergência mais rápida em uma rede OSPF.

Este comando é usado para definir o intervalo durante o qual pelo menos um pacote de identificação deve ser recebido, ou o vizinho é considerado inativo:

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

Aqui está um exemplo:

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

Neste exemplo, o suporte do OSPF para pacotes de identificação rápida está ativado com a especificação da palavra-chave **minimal**, da palavra-chave **hello-multiplier e do valor.** Como o multiplicador está definido como **5**, cinco pacotes de identificação são enviados a cada segundo.

Soluções

Esta seção descreve algumas soluções possíveis para os problemas que estão descritos na seção anterior.

Solução do problema 1

Éimportante que você entenda a mensagem de erro durante as tentativas de solucionar problemas de mensagens de flood war. As mensagens aparecem de forma diferente na origem e liberam roteadores. Por esse motivo, é crucial concentrar-se no tipo de LSA para o qual a mensagem de flood war é relatada, já que cada tipo de LSA é problemático de maneira diferente.

Aqui está um exemplo de trecho de código da mensagem de flood war do 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
```

Aqui estão os componentes de mensagem descritos:

- **Process – É o processo OSPF que informa o erro.**
- **re-originates ou flushes – Indica se este roteador origina ou libera o LSA.**
- **LSA ID – É a ID LSA na qual o flood war é detectado.**

- **Type – É o tipo de LSA.**
  Note: O flood war de cada LSA tem uma causa do problema diferente.
- **adv-rtr – É o roteador de anúncio que origina o LSA.**

- **Area – É a área à qual o LSA pertence.**

LSAs tipo 2

> **Note**: Consulte RFC 2328 (Capítulo 13.4, caso 3) para obter mais informações se o flood war é impresso para um LSA tipo 2.

Se um roteador recebe um LSA de rede tipo 2 cuja ID LSA é igual ao endereço IP de uma das interfaces associadas a esse roteador, em seguida, o roteador deve liberar o LSA. A causa do problema neste cenário refere-se aos endereços IP duplicados nos roteadores de origem e liberação.

Para resolver esse problema, reconfigure o endereço IP em uma das interfaces ou encerre a interface que tem o endereço IP duplicado.

> **Note**: Essa verificação de endereços IP duplicados também é realizada em interfaces que estão desativadas. A interface deve estar no modo *admin-down para ignorar a verificação.* Em alguns casos, o flood war também é relatado para uma interface de encerramento administrativo, portanto, a solução permanente é remover os endereços IP duplicados na rede.

LSAs tipo 3

Éraro encontrar problemas de flood war em um LSA tipo 3. Mensagens de erro de flood war para LSAs tipo 3 foram registradas em cenários nos quais a sub-rede IP de um link altamente flexível é propagada no domínio OSPF.

A Cisco recomenda que você abra um caso de suporte com o Cisco Technical Assistance Center (TAC) quando há problemas de flood war devido a LSAs tipo 3.

LSAs tipo 5

Os flood wars devido a LSAs tipo 5 ocorrem quando há IDs de roteador duplicados em roteadores localizados em áreas diferentes. É obrigatório alterar a ID do roteador em um dos roteadores.

Outra ocorrência de flood wars tipo 5 é quando há dois roteadores que têm a mesma declaração de rede do protocolo BGP e ambos os roteadores redistribuem essas redes BGP no OSPF. Se qualquer um desses roteadores BGP atingir a rede através do OSPF, um flood war do OSPF devido ao LSA tipo 5 será relatado.

Em resumo, verifique se as IDs do roteador não são iguais, e a redistribuição correta de LSAs externos deve evitar problemas de flood war devido a LSAs tipo 5.

Solução do problema 2

A etapa inicial que você deve executar com tentativas de resolver a mensagem de erro OSPF-CONFLICTING_LSAID é localizar o prefixo que não é anunciado, bem como o prefixo conflitante.

Para localizá-los, insira os comandos **show ip route e show ip ospf database na CLI.** O administrador deve controlar a origem do **Novo destino: 192.168.1.0/32**, conforme mostrado no exemplo descrito na seção Problema 2 e corrigir a máscara de sub-rede da rede.

O caso usual de IDs de LSA em conflito é registrado após uma alteração recente no OSPF e é resolvido depois que você corrige a configuração das máscaras de sub-rede nas instruções de rede do OSPF.

Solução do problema 3

Os casos de alta utilização da CPU são registrados com o Cisco TAC quando os clientes implantam identificações rápidas do OSPF nos Cisco Catalyst Series Switches.

> **Note**: A Cisco recomenda que você não configure identificações rápidas do OSPF.

O Cisco IOS® é executado em um modelo não preemptivo, e o recurso de pacote de identificação rápida requer que a identificação do OSPF seja processada com mais frequência do que o intervalo inativo de um segundo. Pode haver chances de que o OSPF não obtenha os recursos necessários em um sistema com outros processos de execução longa. Dependendo do ambiente e dos outros protocolos e aplicativos configurados no roteador, o uso desse recurso pode ser problemático.

A alternativa da identificação de sub-segundo foi introduzida através da detecção de encaminhamento bidirecional (BFD), em que a BFD é desenvolvida para detecção rápida de vizinho inativo. A BFD é executada no modo de *interrupção e não sofre os problemas que são observados com a identificação rápida do OSPF.* A Cisco recomenda que você use a BFD para uma convergência mais rápida.

Aqui estão dois defeitos conhecidos devido à identificação rápida do OSPF:

- Cisco bug ID CSCut14044: *WS-C3750X-48 / OSPF Fast hello 333msec / adjacency drop / 15.0(2)SE6*
- Cisco bug ID CSCsd17835: *ospf/hsrp fast hello adjacencies are flapping continuously*

Informações Relacionadas

- Solução de problemas de IDs de roteador duplicadas com o OSPF
- Suporte e downloads – Cisco Systems
- Suporte técnico e documentação - Cisco Systems