

# Dépannage d'un message d'erreur complexe OSPF

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Problèmes](#)

[Problème 1](#)

[Problème 2](#)

[Problème 3](#)

[Solutions](#)

[Solution au problème 1](#)

[Déclarations d'état de liaison de type 2](#)

[Déclarations d'état de liaison de type 3](#)

[Déclarations d'état de liaison de type 5](#)

[Solution au problème 2](#)

[Solution au problème 3](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment dépanner les messages d'erreur OSPF (Open Shortest Path First) qui surviennent lors de l'exploitation normale du réseau et qui peuvent entraver la connectivité.

## Conditions préalables

### Conditions requises

Cisco vous recommande de connaître les principes fondamentaux de l'OSPF.

### Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

## Informations générales

Le protocole OSPF est un protocole IGP (Interior Gateway Protocol) largement utilisé par les réseaux d'entreprise et les fournisseurs de services.

Ce protocole a été développé pour répondre au besoin de la communauté pour un IGP de haute fonctionnalité et non propriétaire pour la famille de protocoles TCP/IP. Les discussions en vue de la création d'un IGP interopérable commun pour l'Internet ont commencé en 1988 et n'ont été officialisées qu'en 1991. C'est à ce moment que le groupe de travail a demandé que l'OSPF soit pris en considération pour passer à l'étape d'ébauche de norme Internet.

Le protocole OSPF est basé sur la technologie d'état de liaison, qui diverge des algorithmes vectoriels Bellman-Ford utilisés dans les protocoles de routage Internet traditionnels, comme le Routing Information Protocol (RIP).

## Problèmes

Cette section décrit trois problèmes OSPF qui pourraient entraver la connectivité du réseau.

### Problème 1

Vous recevez le message d'erreur **OSPF-4-FLOOD\_WAR**. Cette erreur se produit lorsque le routeur reçoit à plusieurs reprises sa propre déclaration d'état de liaison (Link State Advertisement ou LSA) et l'élimine du réseau ou envoie une nouvelle version de celle-ci. Ceci sert à détecter les problèmes avec les déclarations d'état de liaison de type 2 lorsque des adresses IP dupliquées sont présentes dans le réseau, ou avec les déclarations de type 5 lorsqu'il y a un ID de routeur dupliqué dans différentes zones OSPF.

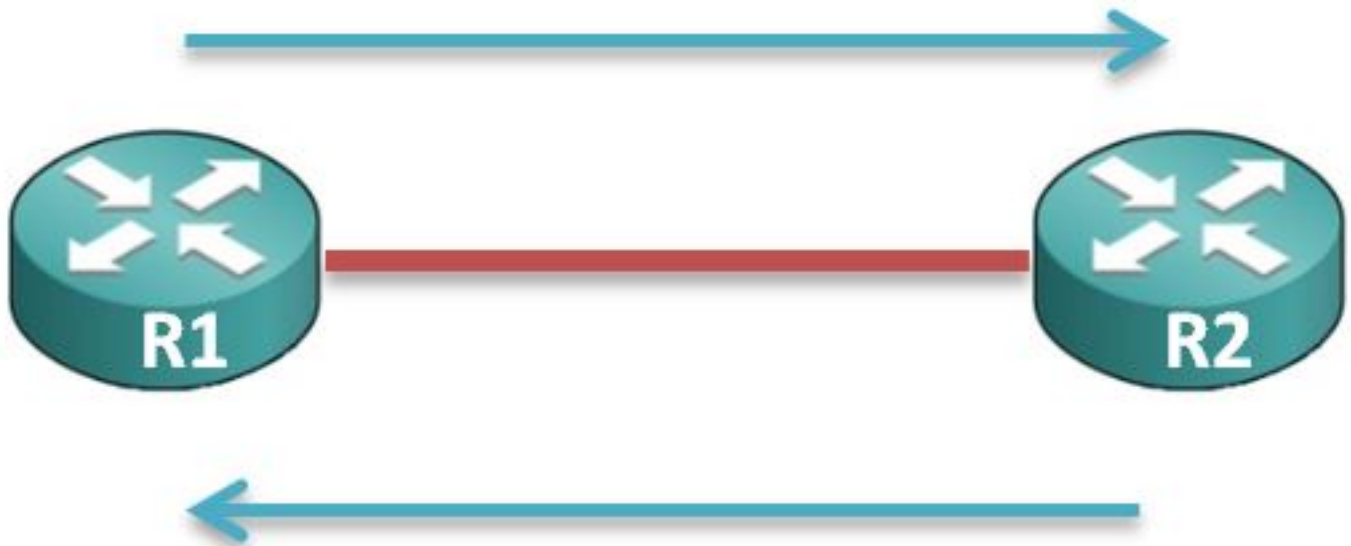
En général, il y a un routeur dans le réseau qui est à l'origine de la déclaration et un deuxième routeur qui l'élimine.

Cette image illustre les événements d'origine et d'élimination entre les deux routeurs (représentés par R1 et R2) :

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

## Problème 2

Vous recevez le message d'erreur **%OSPF-4-CONFLICTING\_LSaid**. Ce message d'erreur indique que l'envoi d'une déclaration d'état de liaison a été bloqué en raison d'un conflit avec une déclaration existante qui a le même identifiant mais un *masque de sous-réseau différent*.

L'algorithme de l'annexe E de la RFC 2328 est utilisé pour résoudre les conflits lorsque plusieurs déclarations avec le même préfixe et des masques différents sont déclarés. Lorsque cet algorithme est utilisé et que les routages de l'hôte sont déclarés, il y a des situations où la résolution de conflit est impossible et où le routage de l'hôte ou le préfixe de conflit n'est pas déclaré.

Voici un extrait d'un tel message d'erreur :

```
%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
```

## Problème 3

Vous configurez OSPF afin d'utiliser la fonction « Fast Hello Packets », qui engendre une utilisation élevée de l'unité centrale. La prise en charge de cette fonction par l'OSPF permet des configurations dans lesquelles les paquets Hello sont envoyés par intervalles de moins d'une seconde. Ces types de configurations permettent une convergence plus rapide dans un réseau OSPF.

La commande suivante est utilisée pour définir l'intervalle pendant lequel au moins un paquet Hello doit être reçu, ou le voisin est considéré comme en panne :

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

Voici un exemple :

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

Dans cet exemple, la fonction « Fast Hello Packets » est activée avec les mots-clés « **minimal** » et « **hello-multiplier** » et la **valeur de multiplication**. Puisque cette valeur est de **5**, cinq paquets Hello sont envoyés chaque seconde.

## Solutions

Cette section décrit quelques solutions possibles aux problèmes décrits dans la section précédente.

### Solution au problème 1

Il est important que vous compreniez le message d'erreur lorsque vous tentez de régler un déluge de déclarations. Ces messages sont différents, selon qu'ils proviennent du routeur d'origine ou d'élimination. Pour cette raison, il est crucial de déterminer le type de la déclaration pour laquelle le message d'erreur est envoyé, car chaque type est résolu différemment.

Voici un extrait d'un message d'erreur lors d'un déluge de déclarations 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
```

Voici la description de chacun des éléments de ces messages :

- **Process** – Le processus OSPF qui signale l'erreur.
- **reoriginates** ou **flushes** – Indique si ce routeur est à l'origine (**reoriginates**) d'une déclaration d'état de liaison, ou s'il l'élimine (**flushes**).
- **LSA ID** – L'identifiant de la déclaration qui provoque le déluge.

- **Type** – Le numéro de type de la déclaration qui provoque le déluge.  
**Note:** La cause première de chaque déluge est différente.
- **adv-rtr** – L'adresse du routeur à l'origine de la déclaration.
  
- **Area** – La zone à laquelle appartient la déclaration.

## Déclarations d'état de liaison de type 2

**Note:** Reportez-vous au document [RFC 2328 \(chapitre 13.4, cas 3\)](#) pour plus d'informations en cas de déluge de déclarations de type 2.

Si un routeur reçoit une déclaration d'état de liaison de type 2 dont l'identifiant est identique à l'adresse IP d'une des interfaces associées à ce routeur, le routeur doit éliminer cette déclaration. La cause première de ce scénario est le dédoublement des adresses IP sur les routeurs d'origine et d'élimination.

Pour résoudre ce problème, reconfigurez l'adresse IP de l'une des interfaces ou fermez l'interface qui possède l'adresse IP en double.

**Note:** Cette vérification des adresses IP en double est également effectuée sur les interfaces qui sont hors service. L'interface doit être en mode « *admin-down* » afin de contourner cette vérification. Dans certains cas, un déluge est signalé pour une interface fermée par l'administrateur; la solution consiste alors à supprimer de façon permanente les adresses IP en double dans le réseau.

## Déclarations d'état de liaison de type 3

Il est rare que des déclarations d'état de liaison de type 3 provoquent un déluge. Cela peut survenir lorsque le sous-réseau IP d'une liaison ballottante se propage dans le domaine OSPF.

Nous vous recommandons d'ouvrir un dossier auprès du Centre d'assistance technique Cisco (TAC) si vous rencontrez un problème de déluge pour des déclarations de type 3.

## Déclarations d'état de liaison de type 5

Un déluge de déclarations de type 5 peut se produire lorsqu'il y a des identifiants de routeurs en double sur des routeurs situés dans des zones différentes. Vous devez alors modifier l'identifiant d'un des routeurs.

Une telle situation peut aussi se produire lorsqu'il y a deux routeurs qui ont le même protocole de réseau BGP (Border Gateway Protocol) et que les deux routeurs redistribuent ces réseaux dans l'OSPF. Un déluge de déclarations de type 5 se produira si l'un de ces routeurs BGP atteint le réseau par OSPF.

En somme, vous pouvez prévenir les déluges de déclarations de type 5 en vous assurant que les routeurs ont tous un identifiant unique.

## Solution au problème 2

Si vous tentez de résoudre le message d'erreur « OSPF-CONFLICTING\_LSAID », vous devriez commencer en identifiant le préfixe qui n'est pas déclaré, ainsi que le préfixe en conflit.

Vous pouvez retrouver ces préfixes avec les commandes **show ip route** et **show ip ospf database**. Dans l'extrait de message d'erreur donné à la fin du « Problème 2 », vous devriez donc trouver l'origine du message en consultant la ligne « **New Destination: 192.168.1.0/32** », comme indiqué dans le cas de exemple indiqué dans le [2 Problème section et corriger le masque de sous-réseau du réseau](#).

En général, un tel conflit se produit après un changement dans OSPF. Pour le résoudre, il faut corriger la configuration des masques de sous-réseau dans les instructions de réseau dans OSPF.

## Solution au problème 3

Selon notre centre d'assistance, ce problème survient lorsque des clients déploient la fonction OSPF « Fast Hello Packets » sur les commutateurs Cisco Catalyst;

**Note:** nous vous recommandons donc de ne pas déployer cette fonction.

Cisco IOS® fonctionne sur un modèle non préventif, et la fonction « Fast Hello Packet » nécessite que les paquets « Hello » soient traités plus fréquemment que l'intervalle hors service (1 seconde). Il se peut que OSPF n'obtienne pas les ressources nécessaires sur un système doté d'autres processus persistants. Selon votre environnement et les autres protocoles et applications qui sont configurés sur le routeur, l'utilisation de cette capacité peut être problématique.

La détection bidirectionnelle de transfert (Bidirectional Forwarding Detection ou BFD) constitue une solution de rechange aux paquets « Hello », car elle a été conçue pour détecter les voisins hors service en moins d'une seconde. Le BFD exécute dans *interrupt mode et undergo pas les problèmes qui sont observés avec Hellos OSPF rapide*. Cisco vous recommande d'utiliser la BFD pour une convergence plus rapide.

Voici deux problèmes associés aux paquets « Fast Hello » OSPF que nous avons répertorié :

- Identifiant de bogue cisco [CSCut14044](#) : *WS-C3750X-48 / OSPF Fast hello 333msec / adjacency drop / 15.0(2)SE6*
- Identifiant de bogue cisco [CSCsd17835](#) : *ospf/hsrp fast hello adjacencies are flapping continuously*

## Informations connexes

- [Dépannage des ID de routeur dupliqués avec OSPF](#)
- [Support and Downloads – Cisco Systems](#)
- [Assistance technique et documentation - Cisco Systems](#)