OSPF Complex Error Message Troubleshooting

Document ID: 118880

Contributed by Mohammed Muddasir Khan, Cisco TAC Engineer.
Apr 01, 2015

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Problems
Issue 1
Issue 2
Issue 3
Solutions
Issue 1 Solution
Type−2 LSAs
Type−3 LSAs
Type−5 LSAs
Issue 2 Solution
Issue 3 Solution
Related Information

Introduction

This document describes how to troubleshoot Open Shortest Path First (OSPF) error messages that are encountered in normal network operations and might degrade network connectivity.

Prerequisites

Requirements

Cisco recommends that you have knowledge of OSPF fundamentals.

Components Used

This document is not restricted to specific software and hardware versions.

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.

Background Information

The OSPF protocol is a widely deployed Interior Gateway Protocol (IGP) in Enterprise and Service Provider networks.

This protocol was developed due to a need in the Internet community to introduce a high functionality, non−proprietary IGP for the TCP/IP protocol family. Discussions for the creation of a common interoperable IGP for the Internet started in 1988 and was not formalized until 1991. At that time, the OSPF Working Group requested that OSPF be considered for advancement to Draft Internet Standard.

The OSPF protocol is based on link−state technology, which is a departure from the Bellman−Ford vector−based algorithms that are used in the traditional Internet routing protocols, such as Routing Information Protocol (RIP).

Problems

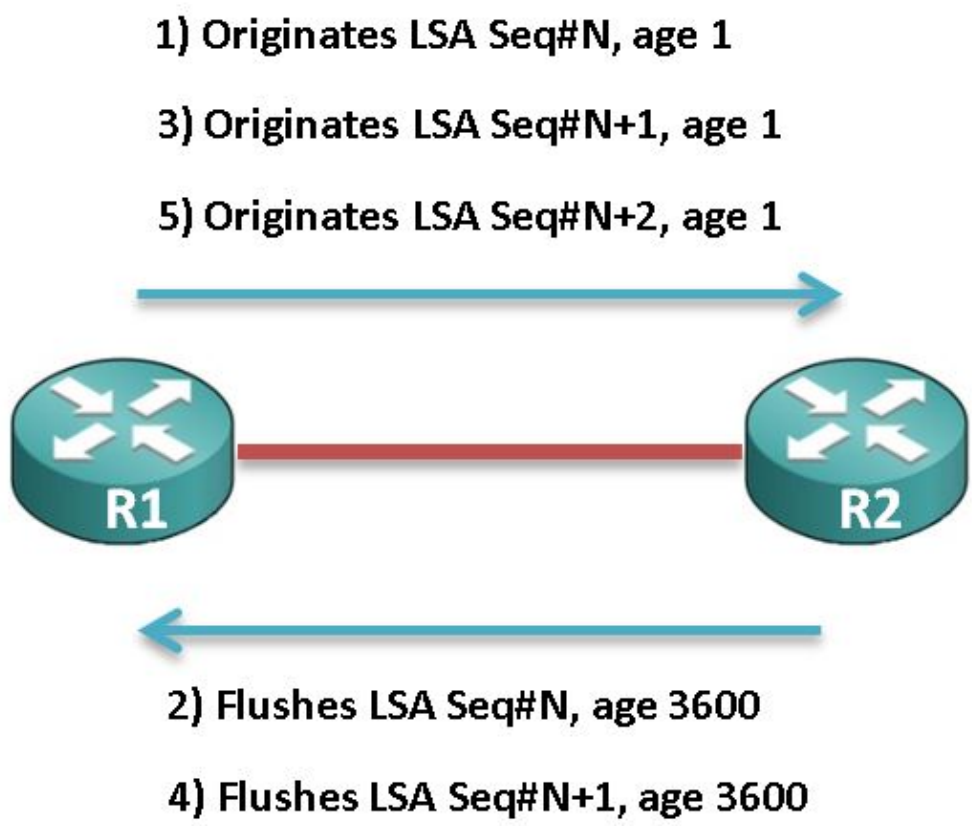
This section describes three OSPF issues that might degrade network connectivity.

Issue 1

You receive the ***OSPF−4−FLOOD_WAR*** error message. The OSPF flood war occurs when the router repeatedly receives its own Link State Advertisement (LSA) and flushes it from the network or sends a new version of it. This is meant to detect issues with Type−2 LSAs when duplicate IP addresses are present in the network, or with Type−5 LSAs when there is a duplicate router ID in different OSPF Areas.

In a typical scenario, there is one router in the network that originates the LSA and a second router that flushes the LSA.

This image illustrates the origination and flush events between the first and second routers (named R1 and R2, respectively):



Issue 2

You receive the ***%OSPF−4−CONFLICTING_LSAID*** error message. This error message indicates that an LSA origination was prevented due to a conflict with a current LSA that has the same Link State ID but a different *subnet mask*.

The algorithm in RFC 2328, Appendix E is used in order to resolve conflicts when multiple LSAs with the same prefix and different masks are advertised. When this algorithm is used, and the host routes are advertised, there are situations where conflict resolution is impossible and either the host route or the prefix that conflicts is not advertised.

Here is an example snippet of the error message:

```
%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
```

Issue 3

You configure OSPF in order to use the Fast Hello Packets feature, which causes high CPU. The OSPF Support for the Fast Hello Packets feature allows configurations such that the Hello packets are sent in intervals less than one second. These types of configurations result in faster convergence in an OSPF network.

This command is used in order to set the interval during which at least one Hello packet must be received, or the neighbor is considered down:

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

Here is an example:

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

In this example, the OSPF Support for Fast Hello Packets is enabled with the specification of the ***minimal*** keyword, the ***hello−multiplier*** keyword, and the value. Because the multiplier is set to ***5***, five Hello packets are sent every second.

Solutions

This section describes some possible solutions to the problems that are described in the previous section.

Issue 1 Solution

It is important that you understand the error message during attempts to troubleshoot flood war messages. The messages appear differently on the origination and flush routers. For this reason, it is crucial to focus on the LSA type for which the flood war message is reported, as each LSA type is troubleshot differently.

Here is an example snippet of the OSPF flood war message:

```
%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
```

Here are the message components described:

- ***Process*** This is the OSPF process that reports the error.
- ***re−originates*** or ***flushes*** This indicates whether this router *originates* or *flushes* the LSA.
- ***LSA ID*** This is the LSA ID for which the flood war is detected.
- ***Type*** This is the LSA type.

  Note: The flood war for every LSA has a different root cause.
- ***adv−rtr*** This is the Advertising router that originates the LSA.
- ***Area*** This is the area to which the LSA belongs.

Type−2 LSAs

Note: Refer to RFC 2328 (Chapter 13.4, Case 3) for additional information if the flood war is printed for a Type−2 LSA.

If a router receives a Type−2 network LSA whose LSA ID is the same as the IP address for one of the interfaces that are associated with that router, then the router should flush the LSA. The root cause in this scenario is the duplicate IP addresses on the origination and flush routers.

In order to resolve this issue, reconfigure the IP address on one of the interfaces or shutdown the interface that has the duplicate IP address.

Note: This check for duplicate IP addresses is performed on interfaces that are down as well. The interface must be in *admin−down* mode in order to bypass the check. In some corner cases, the flood war is also reported for an administratively shut down interface, so the permanent solution is to remove the duplicate IP addresses in the network.

Type−3 LSAs

It is rare to encounter flood war issues for a Type−3 LSA. Flood war error messages for Type−3 LSAs have been recorded in scenarios in which the IP subnet of a heavily flapping link is propagated in the OSPF domain.

Cisco recommends that you open a support case with the Cisco Technical Assistance Center (TAC) if you encounter flood war issues due to Type−3 LSAs.

Type−5 LSAs

Flood wars due to Type−5 LSAs occur when there are duplicate router IDs on routers that are located in different Areas. It is compulsory to change the router ID on one of the routers.

Another instance of Type−5 flood wars is when there are two routers that have the same Border Gateway Protocol (BGP) network statement and both routers redistribute those BGP networks into the OSPF. If either of those BGP routers reach the network through OSPF, then an OSPF flood war due to a Type−5 LSA is reported.

In summary, ensure that the router IDs are not the same, and the correct redistribution of external LSAs should prevent flood war issues due to Type−5 LSAs.

Issue 2 Solution

The initial step that you should take with attempts to resolve the ***OSPF−CONFLICTING_LSAID*** error message is to locate the prefix that is not advertised as well as the prefix that conflicts.

In order to locate these, enter the ***show ip route*** and ***show ip ospf database*** commands into the CLI. The administrator must track the origin of the ***New Destination: 192.168.1.0/32***, as shown in the example case described in the Issue 2 section, and correct the subnet mask of the network.

The usual case of conflicted LSA IDs is logged after a recent change in OSPF and is resolved after you correct the subnet masks configuration in the OSPF network statements.

Issue 3 Solution

High CPU cases are logged with the Cisco TAC when customers deploy OSPF fast Hellos on Cisco Catalyst Series switches.

Note: Cisco recommends that you do not configure OSPF fast Hellos.

Cisco IOS® runs on a nonpreemptive model, and the Fast Hello Packet feature requires that the OSPF Hellos be processed more frequently than the one−second dead interval. There might be chances that OSPF does not obtain the required resources on a system with other long−running processes. Dependent upon your environment and the other protocols and applications that are configured on the router, the use of this capability can be problematic.

The alternate of sub−second Hello was introduced through Bi−Directional Forwarding Detection (BFD), wherein BFD is developed for fast neighbor down detection. The BFD runs in *interrupt* mode and does not undergo the problems that are observed with OSPF fast Hellos. Cisco recommends that you use BFD for faster convergence.

Here are two known defects due to OSPF fast Hellos:

- 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*

Related Information

- ***Troubleshooting Duplicate Router IDs with OSPF***
- ***Support and Downloads Cisco Systems***
- ***Technical Support & Documentation Cisco Systems***

Updated: Apr 01, 2015 Document ID: 118880