

OSPF 复杂错误消息故障排除

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[背景信息](#)

[问题](#)

[问题 1](#)

[问题 2](#)

[问题 3](#)

[解决方案](#)

[问题 1 解决方案](#)

[第 2 类 LSA](#)

[第 3 类 LSA](#)

[第 5 类 LSA](#)

[问题 2 解决方案](#)

[问题 3 解决方案](#)

[Related Information](#)

Introduction

本文档介绍如何对正常网络运营中遇到的可能降低网络连接性能的开放最短路径优先 (OSPF) 错误消息进行故障排除。

Prerequisites

Requirements

思科建议您掌握 OSPF 基础知识。

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.

背景信息

OSPF 协议是企业 and 运营商网络中广泛部署的内部网关协议 (IGP)。

此协议是由于互联网社区中需要为 TCP/IP 协议系列引入功能丰富的非专有 IGP 而开发的。1988 年，人们就开始讨论为互联网创建一个通用的互通 IGP，但直到 1991 年仍未正式制定该协议。当时，OSPF 工作小组要求考虑将 OSPF 发展为互联网标准草案。

OSPF 协议基于链路状态技术，这与路由信息协议 (RIP) 等传统互联网路由协议中使用的基于矢量的贝尔曼-福特算法相违背。

问题

此部分介绍可能降低网络连接性能的三个 OSPF 问题。

问题 1

您收到 **OSPF-4-FLOOD_WAR** 错误消息。当路由器反复收到自己的链路状态通告 (LSA) 并从网络中清除它或发送它的新版本时，即会发生 OSPF 泛洪。这是为了检测网络中存在重复的 IP 地址时出现的第 2 类 LSA 问题或不同 OSPF 区域中存在重复的路由器 ID 时出现的第 5 类 LSA 问题。

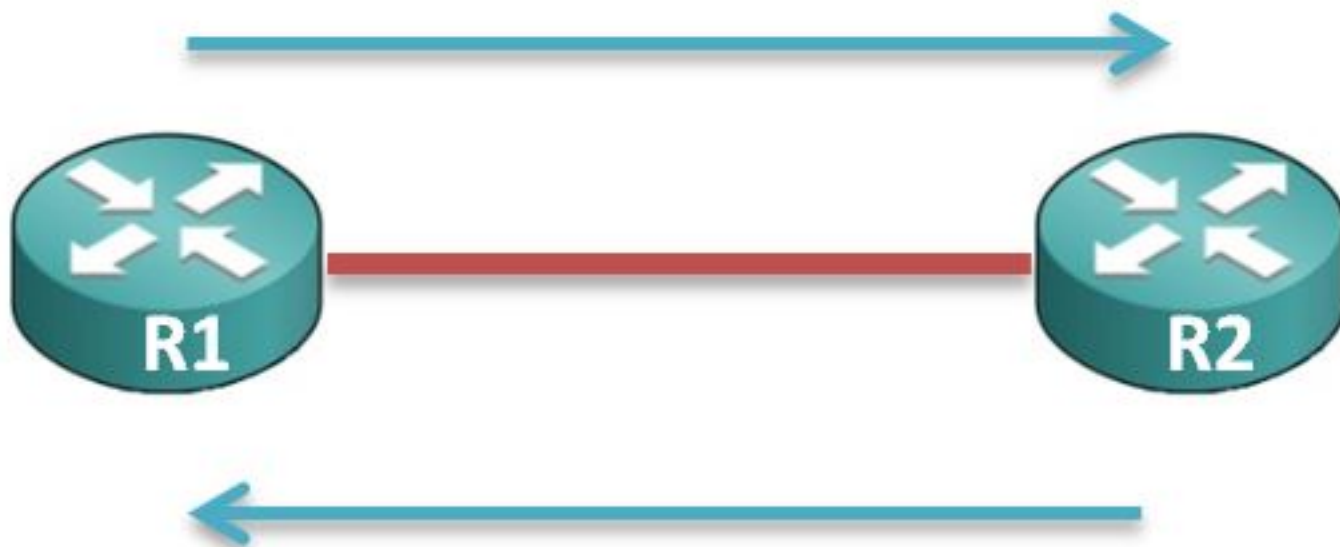
在典型场景中，网络中有一台路由器发出 LSA，另一台路由器清除 LSA。

下图显示了第一台和第二台路由器（分别名为 R1 和 R2）之间发出和清除 LSA 的事件：

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

问题 2

您收到 %OSPF-4-CONFLICTING_LS Aid 错误消息。此错误消息表示发出 LSA 受到阻止，原因是与具有相同链路状态 ID 但子网掩码不同的当前 LSA 冲突。

为了在通告前缀相同而掩码不同的多个 LSA 时解决冲突问题，使用了 RFC 2328 附录 E 中的算法。当使用此算法并通告主机路由时，在某些情况下不可能解决冲突，因此也就不会通告主机路由或相冲突的前缀。

以下是该错误消息的代码片段示例：

```
%OSPF-4-CONFLICTING_LS Aid: LSA origination prevented by existing LSA with same LS ID  
but a different mask
```

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

问题 3

您为了使用快速 Hello 数据包功能而配置了 OSPF，结果导致了 CPU 使用率高的问题。OSPF 对快速 Hello 数据包功能的支持允许您进行配置，以便按小于一秒的间隔发送 Hello 数据包。此类配置导致 OSPF 网络中的收敛速度加快。

我们使用以下命令来设置间隔，在此间隔时间内至少必须收到一个 Hello 数据包，否则就认为邻居出现故障：

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

示例如下：

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

在此示例中，通过指定 **minimal** 关键字、**hello-multiplier** 关键字和值启用 OSPF 对快速 Hello 数据包的支持。由于乘数设置为 **5**，因此每秒将发送五个 Hello 数据包。

解决方案

此部分介绍可能解决上一部分所述问题的一些解决方案。

问题 1 解决方案

在尝试对泛洪消息进行故障排除期间，了解错误消息很重要。发出和清除 LSA 的路由器上显示的消息不同。因此，关注报告的是哪一类 LSA 的泛洪消息成为关键，因为每一类 LSA 的故障排除方式不同。

以下是 OSPF 泛洪消息的代码片段示例：

```
%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
```

以下是对消息的各个组成部分的介绍：

- **Process** - 这是报告错误的 OSPF 进程。
- **re-originates** 或 **flushes** - 这表示此路由器是发出还是清除 LSA。
- **LSA ID** - 这表示检测到的是该 LSA ID 的泛洪。
- **Type** - 这是 LSA 类型。
Note:每一类 LSA 的泛洪都有不同的根本原因。
- **adv rtr** - 这是发出 LSA 的通告方路由器。
- **Area** - 这是 LSA 所属的区域。

第 2 类 LSA

Note: 如果为第 2 类 LSA 发表泛洪，请参阅 [RFC 2328](#) (第 13.4 章第 3 种情况) 了解其他信息。

如果路由器收到第 2 类网络 LSA，其 LSA ID 与该路由器关联的一个接口的 IP 地址相同，则该路由器应清除此 LSA。此场景中的根本原因是发出和清除 LSA 的路由器的 IP 地址重复。

为了解决此问题，请重新配置其中一个接口的 IP 地址或关闭 IP 地址重复的接口。

Note: 在关闭的接口上也要执行此项重复 IP 地址检查。接口必须处于 *admin-down* 模式才能绕过此检查。在某些极端情况下，也会报告管理性关闭接口的泛洪，因此删除网络中的重复 IP 地址才是一劳永逸的解决方案。

第 3 类 LSA

第 3 类 LSA 很少遇到泛洪问题。根据记录，曾经出现过第 3 类 LSA 泛洪错误消息的场景是剧烈摆动的链路的 IP 子网在 OSPF 域中传播时。

如果您遇到第 3 类 LSA 造成的泛洪问题，思科建议您向思科技术支持中心 (TAC) 提交支持请求。

第 5 类 LSA

当位于不同区域的路由器上的路由器 ID 重复时，即会发生第 5 类 LSA 造成的泛洪。必须更改其中一台路由器上的路由器 ID。

第 5 类泛洪的另一种情况是，两台路由器的边界网关协议 (BGP) network 语句相同，且两台路由器都将这些 BGP 网络重新分发到 OSPF 中。如果其中任一台 BGP 路由器通过 OSPF 访问网络，则会报告第 5 类 LSA 造成的 OSPF 泛洪。

总之，确保路由器 ID 不同并正确地重新分发外部 LSA 应该可以防止第 5 类 LSA 造成的泛洪问题。

问题 2 解决方案

要尝试解决 `OSPF-CONFLICTING_LSAID` 错误消息，首先应当采取的措施是找到未通告的前缀以及冲突的前缀。

为了找到这些前缀，请在 CLI 中输入 `show ip route` 和 `show ip ospf database` 命令。管理员必须跟踪 `New Destination:192.168.1.0/32` 的源，如 [问题 2](#) 部分所述的示例中所示，并更正该网络的子网掩码。

LSA ID 发生冲突的常见情况已记录到近期更改后的 OSPF 中，并可在更正 OSPF network 语句中的子网掩码配置后得到解决。

问题 3 解决方案

客户在思科 Catalyst 系列交换机上部署 OSPF 快速 Hello 功能时，已向思科 TAC 报告并记录 CPU

使用率高的情况。

Note:思科建议您不要配置 OSPF 快速 Hello。

思科 IOS® 以非先占模式运行，而快速 Hello 数据包功能要求 OSPF Hello 数据包的处理频率高于一秒 dead 间隔。在具有长期运行的其他进程的系统上，OSPF 有可能无法获得所需的资源。根据您的具体环境和路由器上配置的其他协议和应用，此功能的使用可能存在问题。

通过双向转发检测 (BFD) 引入了亚秒级 Hello 的替代方案，其中 BFD 是为快速检测邻居故障而开发的。BFD 以 *中断*模式运行，不会遇到我们在 OSPF 快速 Hello 中发现的问题。思科建议您使用 BFD 来加快收敛速度。

以下是 OSPF 快速 Hello 造成的两个已知缺陷：

- 思科漏洞 ID [CSCut14044](#) : *WS-C3750X-48 / OSPF Fast hello 333msec / adjacency drop / 15.0(2)SE6*
- 思科漏洞 ID [CSCsd17835](#) : *ospf/hsrp fast hello adjacencies are flapping continuously*

Related Information

- [OSPF 中重复路由器 ID 故障排除](#)
- [支持和下载 - 思科系统公司](#)
- [Technical Support & Documentation - Cisco Systems](#)