**交换机产品OSPF router ID重复日志告警问题**

**排查云图**



1. **开始**

OSPF作为常用的网络路由协议，广泛用于各类网络中。在实际的开局实施与设备运行过程中，设备打印Duplicate router ID xx.xx.xx的告警为现网比较常见的一类故障，本云图排思路适用于Comware V7交换机产品打印Duplicate router ID类的故障问题。

具体排查步骤如下：

**步骤1：**查看设备日志，确认重复Router ID的报文来源。

**步骤2：**排查是否存在环路。

**步骤3：**排查是否存在设备弹包。

**步骤4：**排查是否网络中其他设备配置错误。

**步骤5：**收集故障信息及上述排查结果，拨打400电话寻求帮助。

1. **流程图相关操作说明**
2. **查看设备日志，确认重复Router ID的报文来源**

当设备收到与自身Router ID重复的OSPF报文时，设备会打印Duplicate router ID的日志，通过查看设备打印的日志里的sourced from IP address可以判断冲突Router ID的OSPF报文的来源。

以如下日志为例，设备打印OSPF进程1收到了重复的router ID为1.1.1.1的OSPF报文，冲突报文的来源为10.0.0.1.

%Apr 6 14:59:42:106 2024 H3C OSPF/6/OSPF\_DUP\_RTRID\_NBR: OSPF 1 Duplicate router ID 1.1.1.1 on interface Vlan-interface1, sourced from IP address 10.0.0.1.

%Apr 6 15:00:15:067 2024 H3C OSPF/6/OSPF\_DUP\_RTRID\_NBR: OSPF 1 Duplicate router ID 1.1.1.1 on interface Vlan-interface1, sourced from IP address 10.0.0.1.

知道冲突报文来源的IP之后，就需要判断收到的OSPF报文属于自身发出的报文被重新发回了网络，还是网络中有其他网络设备配置了相同的router ID。如果是自身发出的报文被重新发回了网络中，则进行第2步与第3步的排查；如果是网络中有其他设备配置了相同的router ID，则进行第4步排查。

通过display ospf，确认来源的地址是否属于本地接口的地址。如果为本地地址，则为自身发出的报文被重新发回了网络中，不为本地地址则是网络中有其他设备配置了相同的router ID。

display ospf

 OSPF Process 1 with Router ID 1.1.1.1

 OSPF Protocol Information

 RouterID: 1.1.1.1 Router type:

 Route tag: 0

 Multi-VPN-Instance is not enabled

 Ext-community type: Domain ID 0x5, Route Type 0x306, Router ID 0x107

 Domain ID: 0.0.0.0

 Opaque capable

 Area: 0.0.0.0 (MPLS TE not enabled)

 Authentication type: None Area flag: Normal

 SPF scheduled count: 2

 ExChange/Loading neighbors: 0

 Interface: 10.0.0.2 (Vlan-interface1)

 Cost: 1 State: Waiting Type: Broadcast MTU: 1500

 Cost source: Default

 Priority: 1

 Designated router: 0.0.0.0

 Backup designated router: 0.0.0.0

 Timers: Hello 10, Dead 40, Poll 40, Retransmit 5, Transmit Delay 1

 FRR backup: Enabled

 Enabled by network configuration

1. **排查是否存在环路。**

1）通过display mac-address查看设备上是否有大量MAC地址漂移，如有则确认网络中有环路，消除环路之后再看是否还会报router ID重复。

2）UP的接口流统，确认是否有接口收到对应源ip的地址发的OSPF报文。（部分设备上CPU的报文统计不到）

流统的ACL如下：

rule permit ospf source xx.xx.xx 0

如排查确认没有环路产生，但是确实收到了自身发出的OSPF报文，则需确认是否网络中有弹包，进行第3步排查。

1. **排查是否存在设备弹包。**

部分互联设备弹包也会导致设备收到自己发出的OSPF报文，此类情况可以通过抓包进行确认，通过抓取本端接口与本端接口互联设备对应端口的流量，确认是否有弹包。

如有网络弹包，则需确认对应设备弹包的原因。

常见的配置错误导致设备弹包的情况有互联设备配置port bridge enable开启桥转发功能后，设备从收到报文的接口将报文发出，可先排查是否存在此类情况。

1. 排查是否网络中其他设备配置错误。

如果收到的OSPF的报文为其他设备发出，则登录对应源地址的设备，确认是否ospf配置错误，修改对应的配置。

在对应的设备上display ospf，确认router ID是否符合预期，如为冲突的id，修改ID即可。如router ID不冲突，我司设备进行第5步排查。

display ospf

 OSPF Process 1 with Router ID 1.1.1.1

 OSPF Protocol Information

 RouterID: 1.1.1.1 Router type:

 Route tag: 0

 Multi-VPN-Instance is not enabled

 Ext-community type: Domain ID 0x5, Route Type 0x306, Router ID 0x107

 Domain ID: 0.0.0.0

1. **收集故障信息及上述排查结果，拨打400电话寻求帮助。**

收集前面几个步骤的信息以及替换测试的说明描述，联系400热线求助。