某局点拆堆叠升级过程中IPV6地址冲突典型案例分析

域间策略/安全域 孔凡安 2023-05-04 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

某局点拆堆叠升级完成后发现子接口下IPV6地址显示冲突，导致经过该防火墙的IPV6业务异常。

```
<H3C>dis ipv int b
*down: administratively down
(s): spoofing
Interface                              Physical Protocol IPv6 Address
LoopBack2                              up       up(s)    Unassigned
Reth1                                  up       up       Unassigned
Reth1.2001                             up       up       2409:8028:3810:19::200A [DUPLICATE]
Reth2                                  up       up       Unassigned
Reth2.1001                             up       up       2409:8028:3810:19::5003 [DUPLICATE]
Reth3                                  up       up       Unassigned
<H3C>dis ip int b
*down: administratively down
(s): spoofing  (l): loopback
Interface                Physical Protocol IP Address      Description
Loop2                    up       up(s)    --              --
Reth1                    up       up       --              internal
Reth1.2001               up       up       210.0.2.5       SDN_SUBIF_Reth...
Reth2                    up       up       --              external
Reth2.1001               up       up       188.103.189.129 SDN_SUBIF_EXT_...
Reth3                    up       up       210.0.5.3       management
<H3C>
```

过程分析

根据故障截图可以看出该地址的状态显示【DUPLICATE】,一般来说接口下的IPV6地址有以下几种状态:

> 接口上配置的全球单播地址
> 可能的IPv6地址状态及含义如下:
> · TENTATIVE:该状态为地址初始化状态,此时该地址可能正在进行DAD检测或准备进行DAD检测,处于该状态的地址不能作为报文的源地址或者目的地址
> · DUPLICATE:该状态表明地址DAD检测已经结束,由于该地址在链路上不唯一,因此不能使用
> · PREFERRED:该状态表明地址处于首选生命期以内。该状态的地址可以作为报文的源地址或者目的地址。为该状态时,不显示地址的状态标识
> · DEPRECATED:该状态表明地址超过首选生命期,但是在有效生命期以内。该状态地址有效,但不应作为新建连接报文的源地址,目的地址是该地址的报文还可以被正常处理
> 如果地址来源不为手工配置的全球单播地址,则会标记地址来源。可能的地址来源及含义如下:
> · AUTOCFG:表示无状态自动配置的全球单播地址
> · DHCP:表示DHCPv6服务器分配的全球单播地址
> · EUI-64:表示手工配置的EUI-64格式全球单播地址
> · RANDOM:表示自动生成的临时地址
> 如果地址为手工配置的任播地址,则会标记ANYCAST

虽然配置成功下发,但是接口IPV6地址状态为【DUPLICATE】,配置实际是不生效的,设备无法收发数据包。但是检查该链路的地址实际未发现IPV6地址冲突。
经过分析拆堆叠过程的日志,发现堆叠分裂的情况下,两框的接口存在同时UP的情况,对应的IPV6地址冲突的日志如下:

```
%Mar 22 01:13:57:364 2023 H3C ND/6/ND_DUPADDR:
 Duplicate address: 2409:8028:3810:19::200a on the interface Reth1.2001

%Mar 22 01:13:57:863 2023 H3C ND/6/ND_DUPADDR:
 Duplicate address: 2409:8028:3810:19::5003 on the interface Reth2.1001
```

原因在于现场在拆堆叠升级的过程中,业务切换时候FW02端口打开的时间早于FW01端口关闭的时间。在这一段时间范围内,主备防火墙业务接口都是UP状态,IPV6地址冲突。
原理分析:当接口获取到一个IPv6地址后,需要使用重复地址检测功能确定该地址是否已被其他节点使用。此接口会通过ND协议向被检测节点发送NS消息,地址冲突的节点会向此接口返回NA消息,接口收到NA消息后认为此IPv6地址是重复的。此IPv6地址在这个接口上被标识为duplicate状态,无法被用于通信。由于接口不会自动为被标识为duplicate状态的IPv6地址使用重复地址检测功能,因此即便地址不再冲突,被标识为duplicate状态的IPv6地址也不会自动恢复到正常状态。因此FW01接口IPV6地址没有生效,无法正常处理业务。

解决方法

恢复方法：重新配置IPV6地址或者shutdown，undo shutdown接口可以恢复。

优化建议：拆堆叠时候先关闭FW02业务端口，再打开FW01业务端口，避免业务端口同时UP。

其他优化建议：配置开启IPv6地址冲突自恢复功能，对应命令：ipv6 address duplicate-detect enable

。