某局点S7600 VRRP双主1秒业务中断20分钟问题案例（11752-陆世叶）

VRRP　陆世叶　2020-02-26 发表

组网及说明

S7610侧与S12508F-AF都作为三层转发设备承载用户业务，其中S7610侧为两台做VRRP，12508F-AF上静态路由下一跳指向VRRP虚地址。

问题描述

S7610交换机出现两VLAN VRRP双主，双主时间1秒不到，但实际业务中断近20分钟，后自动恢复

过程分析

问题一：VRRP双主

1. 首先分析S7610 VRRP侧双主原因。通过对设备的日志分析，故障开始时间，16:26:37备侧出现VRRP心跳报文超时，S7610两台交换机interface vlan 10、20出现VRRP双主，后在1秒内恢复VRRP状态

```
%Dec 20 16:26:37:652 2019 ZJHZ-PA-WGDCN-SW92-SQ5#3F-S7610 VRRP4/6/VRRP_STATUS_CHANGE:
The status of IPv4 virtual router 20 (configured on Vlan-interface20) changed from Backup to Master: Master-down-timer expired.

%Dec 20 16:26:37:660 2019 ZJHZ-PA-WGDCN-SW92-SQ5#3F-S7610 VRRP4/6/VRRP_STATUS_CHANGE:
The status of IPv4 virtual router 10 (configured on Vlan-interface10) changed from Backup to Master: Master-down-timer expired.

%Dec 20 16:26:38:110 2019 ZJHZ-PA-WGDCN-SW92-SQ5#3F-S7610 VRRP4/6/VRRP_STATUS_CHANGE:
The status of IPv4 virtual router 20 (configured on Vlan-interface20) changed from Master to Backup: VRRP packet received.

%Dec 20 16:26:38:657 2019 ZJHZ-PA-WGDCN-SW92-SQ5#3F-S7610 VRRP4/6/VRRP_STATUS_CHANGE:
The status of IPv4 virtual router 10 (configured on Vlan-interface10) changed from Master to Backup: VRRP packet received.
```

2. 通过设备上记录信息来看，S7610 VRRP备侧3秒内无法收到主的VRRP心跳报文从而超时。而具体的原因是备S7610侧slot 0槽位板卡CPU收到大量VRRP报文（主S7610侧slot 0也有记录），报文超过slot 0板卡的CPU的softcar限速，导致正常的VRRP主发来的心跳报文也被丢弃，丢弃3个报文后VRRP出现双主

```
[ZJHZ-PA-WGDCN-SW92-SQ5#3F-S7610-probe]debug rx
[ZJHZ-PA-WGDCN-SW92-SQ5#3F-S7610-probe]debug rxtx softcar  attack_rcd  SLOT 0

 sflow totalpps: 0 0
 thrd pps    inque memfail    mbuffail    nullptr    qfull      head       tail
 0    0      0     0          0           0          0          0          0
 1    0      0     0          0           0          0          0          0
 2    0      0     0          0           0          0          0          0

 current:
 ID   Acltype   Port

 history:
 ID   Type     IfIndex    Acltype                 Time            Date
 1    action   0x8        ARP                     08:26:39:3023   12/20/2019
 2    action   0x8        VRRP                    08:26:39:12831   12/20/2019
 3    recover  0x8        VRRP                    08:28:19:19056   12/20/2019
 4    recover  0x8        ARP                     08:28:24:7982   12/20/2019
 5    action   0x8        ARP                     08:28:30:64049   12/20/2019
 6    action   0x8        VRRP                    08:28:30:20781   12/20/2019
 7    recover  0x8        VRRP                    08:33:21:14155   12/20/2019
 8    action   0x8        VRRP                    08:33:26:22123   12/20/2019
 9    recover  0x8        VRRP                    08:35:53:29999   12/20/2019
 10   action   0x8        VRRP                    08:36:01:51257   12/20/2019
 11   recover  0x8        VRRP                    08:37:23:49568   12/20/2019
 12   recover  0x8        ARP                     08:37:27:23489   12/20/2019

 Rxtx timeout history:
 ID   Time          Date  Timeout
```

通过debug port map确认slot 0槽位TG0/0/8口的IfIndex为0x8

```
  ====debug port mapping chassis 0 slot 0====

 [Interface]    [Unit] [Port] [Name] [Combo?] [Active?] [IfIndex]  [MID]   [Link]
 ==========================================================================
  XGE0/0/1          0      1      xe0     no        no       0x1         4      up
  XGE0/0/2          0      2      xe1     no        no       0x2         4      up
  XGE0/0/3          0      3      xe2     no        no       0x3         4      up
  XGE0/0/4          0      4      xe3     no        no       0x4         4      up
  XGE0/0/5          0      5      xe4     no        no       0x5         4      up
  XGE0/0/6          0      6      xe5     no        no       0x6         4      up
  XGE0/0/7          0      7      xe6     no        no       0x7         4      up
  XGE0/0/8          0      8      xe7     no        no       0x8         4      up
  XGE0/0/9          0      9      xe8     no        no       0x9         4      down
```

后从现场监控软件发现，备S7610的TG0/0/8故障时间点有异常流量进来，所以基本确认为网络攻击。

3. 从主备S7610侧业务监控记录来看，故障时间备S7610 VLAN30中的TG0/0/8口入方向有一股未知流量进来，最终从主侧S7610的TG0/0/8出去：

所以综合1、2、3可以确认VLAN 10、20 VRRP双主的原因是备S7610 slot 0的CPU收到VRRP超限速攻击导致。

问题二：为何业务中断近20分钟

4. 备S7610因超时成为VRRP主，所以其会发送虚IP的免费ARP到下行EOR-S12508F-AF，原本EOR-S12508F-AF上路由出口指向VRRP主，会因为收到VRRP备的免费ARP，从而EOR-S12508F-AF上路由出口会切换指向VRRP备。**从监控流量上看，流量确实也都切向了VRRP备侧TG0/0/3和TG0/0/4**

5. 流量发到VRRP备侧后，因为备侧VRRP状态在1秒内恢复正常，收到EOR-S12508F-AF发过来的流量需要二层转发给VRRP主。又因为心跳链路只经过EOR-S12508F-AF，VRRP备收到过来的流量无法沿原入接口再转发回去（交换机二层转发基本原理），因此导致丢包。所以只要EOR-S12508F-AF上对应S7610的VRRP虚IP的ARP老化时间内，流量会一直发给VRRP备导致被丢弃，这也是流量为什么会中断这么长时间的原因

解决方法

VRRP侧可配置周期发送免费ARP，这样使得VRRP状态恢复也能快速恢复业务