关于交换机NTP单播报文超速丢弃解决方案

丢包 张旭A 2021-12-21 发表

组网及说明

不涉及

问题描述

设备产生日志告警，NTP 报文超速丢弃，导致设备CPU较高。

PktType= UCAST_NTP , srcMAC=84c2-e4f9-2c7a, Drop From Interface=GigabitEthernet2/3/0/4 at Stage=63, StageCnt=107817, TotalCnt=2858049 %@377%Dec 4 20:53:55:944 2021 GK-S7503X-A/B DRVPLAT/4/SOFTCAR DROP: -Chassis=2-Slot=3; PktType= UCAST_NTP , srcMAC=84c2-e4e9-3ba7, Drop From Interface=GigabitEthernet2/3/0/6 at Stage=63, StageCnt=107835, TotalCnt=2858248 %@378%Dec 4 20:53:56:958 2021 GK-S7503X-A/B DRVPLAT/4/SOFTCAR DROP: -Chassis=2-Slot=3;

```
[HZB7-R1-S5130-PWR-probe]debug rxtx softcar show slot 1

ID  Type              RcvPps Rcv_All     DisPkt_All    Pps  Dyn Sw
74  UCAST_NTP            142  111557282      688       100   S
```

过程分析

当设备收到NTP 报文超过设备阈值后，会上CPU进行丢弃处理，如果是攻击报文会导致CPU升高，影响设备处理性能

通过debug rxtx softcar show chasis x slot x可以查询到对应UCAST_NTP报文的统计情况如下图：

```
HZB7-R1-S5130-PWR-probe]debug rxtx softcar show slot 1

D  Type              RcvPps Rcv_All      DisPkt_All    Pps  Dyn Sw
74 UCAST_NTP            142 111557282      688         100    S
```

RcvPps表示当前接收的UCAST_NTP接收的速率；Rcv_ALL表示接收的总NTP单播报数

DisPkt_ALL表示丢弃的总数；Pps表示设备限速值

通过如上设备数据数据统计可以确认 设备的RcvPps=142 > 设备UCAST_NTP限速Pps=100，所以产生NTP单播包丢弃日志

解决方法

1、通过日志中的MAC地址，确认是否是正常终端NTP同步单播报文，若是正常报文，建议调整NTP客户端发包速率。2、若是终端发送的攻击报文，建议排查攻击源，同时设备可以配置NTP报文acl列表，只允许NTPsever的报文通过，否则会直接丢弃。配置命令ntp-service peer acl xx，通过acl 将下行ntp client和上行 ntp server加入permit规则。向其他ntp sever发送报文直接丢弃。