S7506X 收到大量arp导致 CPU高

CPU 小王 2024-08-23 发表

组网及说明

设备做终端的网关

告警信息

ARP/5/ARP_PACKET_SPEEDLIMIT_ALARM: -MDC=1-Slot=0; ARP or ARP miss packets were sent at 802 pps, which exceeded the alarm threshold.

S7506X_OLT DRVPLAT/4/SOFTCAR DROP: -Slot=0;
PktType= ARP , srcMAC=0200-004a-67b2，Drop From Interface=Olt0/0/9 at Stage=7, StageCnt=381959, TotalCnt=1135172

问题描述

设备业务异常，终端不定时获取不到地址
slot0的cpu异常高，正常时不到10%
[OLT-probe]display cpu-usage
Slot 0 CPU 0 CPU usage:
70% in last 5 seconds
70% in last 1 minute
69% in last 5 minutes

Slot 1 CPU 0 CPU usage:
6% in last 5 seconds
7% in last 1 minute
8% in last 5 minutes

过程分析

[OLT]monitor process slot 0 //看到收包和arp相关进程高
290 processes; 318 threads; 593 fds
Thread states: 6 running, 312 sleeping, 0 stopped, 0 zombie
CPU states: 0.02% idle, 4.23% user, 77.96% kernel, 17.79% interrupt
Memory: 976M total, 344M available, page size 4K

JID	PID	PRI	State	FDs	MEM	HH:MM:SS	CPU	Name
187	187	120	R	0	0K	01:24:58	41.96%	[T_RT]
206	206	115	R	0	0K	00:38:55	16.07%	[bRX1]
346	346	115	R	0	0K	00:37:56	13.09%	[karp/1]
270	270	120	R	22	12352K	00:06:35	6.39%	diagd
198	198	111	D	0	0K	00:08:46	4.01%	[SC_CORE]
34	34	100	D	0	0K	00:04:32	3.27%	[RECV]
1	1	120	S	17	10432K	00:00:22	2.52%	scmd
93	93	115	D	0	0K	00:03:15	2.08%	[PRSC]
61	61	116	D	0	0K	00:01:53	1.63%	[bLK0]
204	204	120	D	0	0K	00:02:30	1.63%	[SCAR]

解决方法

debug rxtx softcar show slot 0 看上cpu是否有丢包

ID	Type	RcvPps	Rcv_All	DisPkt_All	Pps	Dyn	Swi	Hash	ACLmax
29	ARP	1211	13623388	725999	750	S	On	SMAC	8

限速750pps ，每秒1211，导致超过限速丢包
cpu高主要是arp报文冲击cpu引起的。
Probe视图执行下述命令，看看arp报文主要从哪个端口上来的，看看是否存在arp攻击
debug rxtx softcar 29 portdetail slot 0
可以看出各个接口arp报文收到的速度，确认是哪个接口收到异常大量的arp
[_S7506X_OLT-probe]debug rxtx softcar 29 portdetail slot 0

Softcar Type ARP PortStatusFetchCnt=11112

Port	Level	Attkd_time	Packet/s	DisPkt/s	Pack_tol	DisP_tol	Pps/P	Proprtn
0	0	0	0	0	25077	0	750	0 1 0
1	1	0	101	0	6074272	166723	750	0 1 0
2	0	0	0	0	15999	0	750	0 1 0
3	0	0	0	0	0	0	750	0 1 0

4 0 0 0 0 783 0 750 0 1 0
5 0 0 0 0 0 0 750 0 1 0
6 0 0 0 0 4685 0 750 0 1 0
7 0 0 0 0 0 0 750 0 1 0
8 5 -9 475 0 7576769 564567 750 1 1 1
9 0 0 0 0 1866 0 750 0 1 0

10 0 0 0 0 0 0 750 0 1 0

Port 8对应port maping 的name ge8 对应olt0/0/9
Port1 对应 port maping的 name ge1 对应0/0/2
[RHWGY_CORE_S7506X_OLT-probe]debug port mapping slot 0

[Interface] [Unit] [Port] [Name] [Combo?] [Active?] [IfIndex] [MID] [Link]
==========
OLT0/0/1 0 1 ge0 no no 0x1 4 up
OLT0/0/2 0 2 ge1 no no 0x2 4 up
OLT0/0/3 0 3 ge2 no no 0x3 4 up
OLT0/0/4 0 4 ge3 no no 0x4 4 down
OLT0/0/5 0 5 ge4 no no 0x5 4 up
OLT0/0/6 0 6 ge5 no no 0x6 4 down
OLT0/0/7 0 7 ge6 no no 0x7 4 up
OLT0/0/8 0 8 ge7 no no 0x8 4 up
OLT0/0/9 0 9 ge8 no no 0x9 4 up
OLT0/0/10 0 10 ge9 no no 0xa 4 up
OLT0/0/11 0 11 ge10 no no 0xb 4 up
OLT0/0/12 0 12 ge11 no no 0xc 4 up

OLT0/0/13 0 13 ge12 no no 0xd 4 up
这两个接口收到大量arp导致cpu高
使用如下功能防护

源MAC地址固定的ARP攻击检测功能简介

本特性根据ARP报文的源MAC地址对上送CPU的ARP报文进行统计，在5秒内，如果收到同一源MAC地址（源MAC地址固定）的ARP报文超过一定的阈值，则认为存在攻击，系统会将此MAC地址添加到攻击检测表项中。当开启了ARP日志信息功能（配置**arp source-mac log enable**命令），且在该攻击检测表项老化之前，如果设置的检查模式为过滤模式，则会打印日志信息并且将该源MAC地址发送的ARP报文过滤掉，同时，还会将源/目的MAC地址为该MAC地址的数据报文也过滤掉；如果设置的检查模式为监控模式，则只打印日志信息，不会将该源MAC地址发送的ARP报文过滤掉。关于ARP日志信息功能的详细描述，请参见“三层技术-IP业务配置指导”中的“ARP”。
切换源MAC地址固定的ARP攻击检查模式时，如果从监控模式切换到过滤模式，过滤模式马上生效；如果从过滤模式切换到监控模式，已生成的攻击检测表项，到表项老化前还会继续按照过滤模式处理。

对于网关或一些重要的服务器，可能会发送大量ARP报文，为了使这些ARP报文不被过滤掉，可以将这类设备的MAC地址配置成保护MAC地址，这样，即使该设备存在攻击也不会被检测或过滤。
开启源MAC地址固定的ARP攻击检测功能，并选择filter检查模式。

<Sysname> system-view

[Sysname] arp source-mac filter