

知 某局点S7506X leaf设备内存异常超阈值问题

ADCampus方案 内存 董智敏 2022-12-12 发表

组网及说明

现场AD campus解决方案，S7506X作为单leaf设备

问题描述

现场S7506X作为campus 单leaf场景分支用户的网关无法学习上连的对端设备的arp信息，有mac信息但是无法学习到arp，查看诊断信息，发现1框2槽，2框1槽，2框2槽板卡内存严重超阈值，且1框0槽，1框1槽和2框0槽上一次重启原因都是内存耗尽重启。

Chassis 1 Slot 2:

	Total	Used	Free	Shared	Buffers	Cached	FreeRatio
Mem:	1978236	1879852	98384	0	0	57240	5.0%
-/+ Buffers/Cache:	1822612	155624					
Swap:	0	0	0				

Chassis 2 Slot 1:

	Total	Used	Free	Shared	Buffers	Cached	FreeRatio
Mem:	1978236	1928116	50120	0	0	57364	2.6%
-/+ Buffers/Cache:	1870752	107484					
Swap:	0	0	0				

Chassis 2 Slot 2:

	Total	Used	Free	Shared	Buffers	Cached	FreeRatio
Mem:	1978236	1907484	70752	0	0	57236	3.6%
-/+ Buffers/Cache:	1850248	127988					
Swap:	0	0	0				

过程分析

1.查看日志里面内存超阈值告警里面主要是portsecd进程（认证相关）占用比较多

Free-memory thresholds:

Minor: 8%

Severe: 7%

Critical: 4%

Normal: 9%

Early-warning: 10%

Secure: 15%

Process info(KB):

JID	Used	Name
465	1688228	portsecd
268	67476	ifmgr
433	21448	laggd
464	20524	stpd
261	18144	devd

2.查看现场配置，发现没有把无线vlan 4093设置为free-vlan，导致无线流量进入交换机后会进行认证，认证服务器下发授权vlan。认证用户下发授权VLAN时，交换机单板需要对每个mac都下发硬件acl规则。正常解决方案配置下，认证用户应该都下发授权VSI，交换机单板对每VSI下发硬件acl规则，其下发的acl量远小于每个mac下发硬件acl量。

```
interface Bridge-Aggregation2
port link-type trunk port trunk permit vlan 1 to 4020 4022 to 4094
link-aggregation mode dynamic
stp tc-restriction
mac-based ac
mac-authentication
mac-authentication carry user-ip exclude-ip acl 2500
mac-authentication domain test
mac-authentication parallel-with-dot1x
port-security free-vlan 1 20 44 4094
#
```

3.现网在没有将无线vlan 4093设置为free-vlan的情况下，每个无线终端都会在交换机上进行认证下发授权vlan，占用单板大量的硬件acl资源，当单板下发acl使用的counter资源数量超过slice中counter资源总数后，硬件acl会一直反复进行扩展安装处理，引起硬件acl进程一直处于繁忙状态，此时，设备上又一直有认证终端在上下线动作，而接口板上portsecd进程直接接收主控板发来的消息，但是portsecd进程又由于硬件acl一直在繁忙状态而不能及时处理，所以消息堆积不断占用内存最终导致内存不足。

解决方法

该问题是因为现场无线业务开局过程中Leaf设备的不规范配置导致硬件acl繁忙，最终造成内存超阈值，标准配置中在leaf设备下行接口设置无线vlan 4093为免认证报文的标准配置可以规避此问题

```
port-security free-vlan 4093
```

