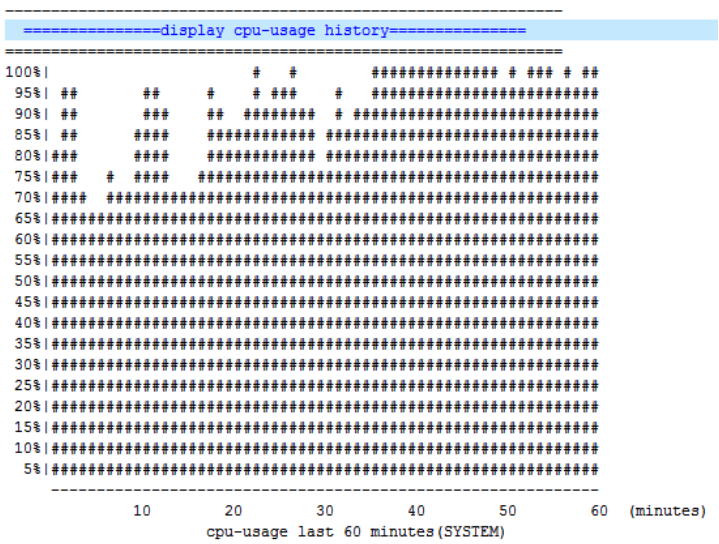
某局点PTTP进程导致CPU过高问题处理的经验案例

wlan接入 Portal 协议报文限速 邹鹏 2015-07-30 发表

局点反馈近期portal认证弹出页面较慢，并且IMC持续告警，AC的CPU利用率持续性过高。PTTP进程约占了30%。

IMC持续告警AC的CPU利用率过高，参考CPU高云图排查来获取CPU的相关信息。先确认近期没有发生过网络整改、增删配置、异常掉电等非常规动作，并且搜集下信息：
display cpu-usage history
隐藏模式下
display cpu-usage task
reset task-runtime-max
display task
通过查看近期CPU使用记录，发现AC上CPU使用率持续性过高，有时已达到100%，情况比较严重。如下图所示



再通过task任务列表，发现进程PTTP明显过高，已远远超出正常值10%，为CPU高的主要原因。如下表所示

==========running CPU usage information==========

===== Current CPU usage info =====
CPU Usage Stat. Cycle: 14 (Second)
CPU Usage : 100%
CPU Usage Stat. Time : 2015-07-16 17:06:50
CPU Usage Stat. Tick : 0x78111(CPU Tick High) 0x853ec8a0(CPU Tick Low)
Actual Stat. Cycle : 0x0(CPU Tick High) 0x39c339bc(CPU Tick Low)

TaskName	CPU	Runtime(CPU Tick High/CPU Tick Low)
CTLT	0%	0/ 70f63
VIDL	0%	0/ 8f51b9
TICK	0%	0/ 607bd6
STMR	0%	0/ 56db87
IPCT	0%	0/ 21981d
DrTC	0%	0/ 32b57f
DrTF	0%	0/ 22e2f3
MCIN	0%	0/ 544b
IPCB	0%	0/ 19e891
IPCD	0%	0/ ac6fe
RPCQ	0%	0/ 1a73c9
VP	0%	0/ 3f5
ADJ6	0%	0/ 45b6
IPCM	0%	0/ 1fc51b
INFO	10%	0/ 5c8bf3b
DHBK	0%	0/ 259d3

WIPS 0% 0/ 15ac3
WCFG 0% 0/ 29f1
WPMS 0% 0/ 2c8b
WPEE 0% 0/ 25d4
DEV 0% 0/ 399be
SOCK 0% 0/ 2bc6b2
ADJ4 0% 0/ b6af
SFLW 0% 0/ e88c
ACL 0% 0/ fc11
LAGG 0% 0/ 88b5
MSTP 0% 0/ 61dc
LLDP 0% 0/ 553e
PTMT 2% 0/ 152d4e3
PTTP 28% 0/10632cc1
ARP 5% 0/ 3575365
IP 0% 0/ 1be649
NQA 0% 0/ 2a95a1
FSLH 0% 0/ 43f9
FSLR 0% 0/ 3d28e
vt1 1% 0/ a8bc34
NTPT 0% 0/ 13927
VTYD 0% 0/ 4b1e5
DHCP 2% 0/ 12c4068
DHSE 1% 0/ b83c9f
VRRP 0% 0/ 99e10
V3RP 0% 0/ c9dd9
DHP6 0% 0/ 51c468
ND 2% 0/ 13122e6
AGNT 12% 0/ 73a3abc
TRAP 8% 0/ 4e4514d
DT1X 0% 0/ 5e4867
ACM 0% 0/ 26ddd2
LS 0% 0/ 32d95
RDSO 0% 0/ 5237a
RDS 0% 0/ 1c2947
SC 0% 0/ 37a128
IKE 0% 0/ 161b1e
MACA 0% 0/ 5850d5
WAPI 0% 0/ 70f32
PSEC 0% 0/ a589
ULOG 0% 0/ 34b0d
STND 0% 0/ 1869b
ROUT 0% 0/ 2eb074
WMAC 6% 0/ 40b0c93
WIDS 0% 0/ 393db
WRRM 0% 0/ 5687e
CWMS 0% 0/ be8f
LWPS 10% 0/ 62ddb2a
WVB 0% 0/ 57ee
WBKP 0% 0/ 33611
IACT 0% 0/ 523e
WBNJ 0% 0/ 3631b
IFNT 0% 0/ 7b0c
FTMT 0% 0/ 124cde
FTMC 0% 0/ 1240e1
vt3 0% 0/ 21055

进程PTTP一般应在10%以内，该进程为TCP仿冒进程和portal认证相关。在portal认证时AC阻断终端的访问请求后，由PTTP进程仿冒回应给终端，并实现AC的重定向。现场由于AP数量较多且人流量较大，无线网络又使用明文方式，众多无线终端虽然没有portal认证账号，但也会连接上该无线并且触发portal认证。过多的porta认证导致PTTP进程使用率过高。

由于PTTP是portal认证过程中TCP仿冒的进程，所以减少portal认证触发和控制TCP仿冒速率是解决问题的两种途径。

1、更改明文加密方式，设置接入密钥，控制接入网络的用户数量。

2、给portal触发配置点流量。正常情况下无线终端接入无线网络会自动触发portal认证，尤其是明文SSID情况下，所有接入的用户都会触发。这种情况下给portal认证触发配置一定的流量，可以减少部分portal认证的触发。

命令[H3C-Vlan-interface1]portal mac-trigger enable threshold

3、开启重定向报文限速，根据流限制每秒处理速率，限制PTTP处理速率，来降低PTTP的使用率。命令如下：

anti-attack protocol portal_syn enable //开启portal重定向报文总限速

anti-attack protocol portal_syn flow-threshold 1 100 //开启portal重定向报文流限速，每条流每秒1个, 每秒触发一百个

anti-attack enable //开启总限速

4、开启portal无感知认证，二次上线的用户将不会触发PTTP进程，继而减少PTTP的使用率。//推荐使用

5、更新版本，使用B109P43及以上版本，合入的web降噪功能将大幅度降低非法流量触发PTTP。