

5G-eLite-Core - 错误 #193

upf收到PCFP session modification request出现Segmentation fault

2020-07-25 09:10 - 徐红超

| | | | |
|-------|-----|---------|------------|
| 状态: | 已关闭 | 开始日期: | 2020-07-25 |
| 优先级: | 一般 | 计划完成日期: | |
| 指派给: | 徐红超 | % 完成: | 0% |
| 类别: | | 预期时间: | 0.00 小时 |
| 目标版本: | | 耗时: | 0.00 小时 |
| 问题归属: | | | |

```

描述
INFO[2020-07-25T02:42:48+08:00] /home/epc/go/src/free5gc/src/upf/src/n4/n4_pfc_handler.c:827 UpfN4HandleSessionModificationRequest()
[PCFP] Session Modification Response, ueip:60.60.0.4 UPF=Util
INFO[2020-07-25T02:42:49+08:00] /home/epc/go/src/free5gc/src/upf/src/n4/n4_dispatcher.c:133 UpfDispatcher() [PCFP] Handle PCFP session
modification request UPF=Util
INFO[2020-07-25T02:42:49+08:00] /home/epc/go/src/free5gc/src/upf/src/n4/n4_pfc_handler.c:827 UpfN4HandleSessionModificationRequest()
[PCFP] Session Modification Response, ueip:60.60.0.4 UPF=Util
INFO[2020-07-25T02:42:49+08:00] /home/epc/go/src/free5gc/src/upf/src/n4/n4_dispatcher.c:138 UpfDispatcher() [PCFP] Handle PCFP session
deletion request UPF=Util
!!! delete entry !!!
!!! delete entry !!!
!!! delete entry !!!
INFO[2020-07-25T02:42:49+08:00] /home/epc/go/src/free5gc/src/upf/src/n4/n4_pfc_handler.c:862 UpfN4HandleSessionDeletionRequest() [PCFP]
Session Deletion Response UPF=Util
INFO[2020-07-25T02:42:50+08:00] /home/epc/go/src/free5gc/src/upf/src/n4/n4_dispatcher.c:133 UpfDispatcher() [PCFP] Handle PCFP session
modification request UPF=Util
INFO[2020-07-25T02:42:50+08:00] /home/epc/go/src/free5gc/src/upf/src/n4/n4_pfc_handler.c:827 UpfN4HandleSessionModificationRequest()
[PCFP] Session Modification Response, ueip:60.60.0.4 UPF=Util
INFO[2020-07-25T02:42:50+08:00] /home/epc/go/src/free5gc/src/upf/src/n4/n4_dispatcher.c:133 UpfDispatcher() [PCFP] Handle UPF=Util
WARN[2020-07-25T02:42:50+08:00] /home/epc/go/src/free5gc/src/upf/lib/utlt/src/utlt_buff.c:197 BufBlkAlloc() Pool is empty UPF=Util
ERRO[2020-07-25T02:42:50+08:00] /home/epc/go/src/free5gc/src/upf/lib/utlt/src/utlt_buff.c:198 BufBlkAlloc() The pool of Buffer is empty UPF=Util

Thread 1 "free5gc-upfd" received signal SIGSEGV, Segmentation fault.
0x0000555555571f20 in _TlvBuildMessage (bufBlkPtr=0x7ffffffcd78, msg=0x7ffffffce1c, ieDescription=0x555555784e0f <ieDescriptionTable+2831>)
at /home/epc/go/src/free5gc/src/upf/lib/pfcp/src/pfcp_message.c:395
395     uint16_t *tagPtr = (uint16_t *) ((*bufBlkPtr)->buf);
(gdb)
(gdb) bt
#0 0x0000555555571f20 in _TlvBuildMessage (bufBlkPtr=0x7ffffffcd78, msg=0x7ffffffce1c,
ieDescription=0x555555784e0f <ieDescriptionTable+2831>) at /home/epc/go/src/free5gc/src/upf/lib/pfcp/src/pfcp_message.c:395
#1 0x000055555557242d in _PfcBuildBody (bufBlkPtr=0x7ffffffe298, msg=0x7ffffffce14, ieDescription=0x55555578a71c
<ieDescriptionTable+25628>)
at /home/epc/go/src/free5gc/src/upf/lib/pfcp/src/pfcp_message.c:452
#2 0x00005555555727f3 in PfcBuildMessage (bufBlkPtr=0x7ffffffe298, pfcpMessage=0x7ffffffce00)
at /home/epc/go/src/free5gc/src/upf/lib/pfcp/src/pfcp_message.c:522
#3 0x00005555555c720 in UpfN4BuildSessionModificationResponse (bufBlkPtr=0x7ffffffe298, type=53 '5',
session=0x5555556a544f8 <upfSessionPool+792504>, modifyRequest=0x555555cd6bd8 <bufPool8192+90328>, cause=1 '\001')
at /home/epc/go/src/free5gc/src/upf/src/n4/n4_pfc_build.c:84
#4 0x000055555555fb71 in UpfN4HandleSessionModificationRequest (session=0x5555556a544f8 <upfSessionPool+792504>,
xact=0x5555558e217b8 <pfcpXactPool+1592>, request=0x5555558cd6bd8 <bufPool8192+90328>)
at /home/epc/go/src/free5gc/src/upf/src/n4/n4_pfc_handler.c:814
#5 0x000055555555c26e in UpfDispatcher (event=0x7ffffffe380) at /home/epc/go/src/free5gc/src/upf/src/n4/n4_dispatcher.c:134
#6 0x00005555555583a0 in eventConsumer () at /home/epc/go/src/free5gc/src/upf/src/upf.c:87
#7 0x00005555555581c3 in main (argc=1, argv=0x7ffffffe4f8) at /home/epc/go/src/free5gc/src/upf/src/upf.c:31
(gdb)

```

历史记录

#1 - 2020-08-18 11:49 - 徐红超

- 状态从 新建 变更为 已解决

#2 - 2021-01-18 15:12 - 徐红超

- 状态从 已解决 变更为 已关闭