

上行大带宽 - 错误 #578

内存分配失败

2021-06-25 10:08 - 周磊

状态:	已解决	开始日期:	2021-06-25
优先级:	普通	计划完成日期:	
指派给:		% 完成:	0%
类别:		预期时间:	0.00 小时
目标版本:	Rel_2.1.6	耗时:	0.00 小时
问题归属:	DU	CPU类型:	
描述			
简述:内存分配失败 测试环境 : 246 测试版本 : rel2.1.6 测试问题 : 24h常保测试, 配置大上行, 内存分配失败, 导致du挂死			

历史记录

#1 - 2021-06-25 10:16 - 匿名用户

```
[06-25 05:17:33.782][DEBUG]NR_RACH_DBG: MSG3 RECVED is CCCH SDU!!!  
[06-25 05:17:33.782][ERROR]rgSCHLv1UtlAllocSBuf,Unable to Allocate the Buffer  
[06-25 05:17:33.782][ERROR]DBG_CELLID1 Scheduler handling failed rgSCHLv1CfgCellUeCtxtInIt for CRNTI17027
```

```
cmGetMemBlkSetForAlloc failed 2  
Failed to get the buffer of size 50616 file /root/DU/ran/DU_Alpha/src/cm/cm_mem_wl.c line 2504
```

```
(gdb) p ue  
$1 = (RgSchLv1UeCb *) 0x7ffe56502020  
(gdb) p ue->cell  
$2 = (RgSchLv1CellCb *) 0x0  
(gdb) p ue->ueld  
$3 = 0
```

长时间运行后, UE随机接入收到MSG3之后, 初始化UE在MAC的结构体时, 分配内存失败, 后续其他流程访问未保护, 导致访问到错误空地址从而挂死。

#2 - 2021-06-25 11:26 - 匿名用户

可能存在的情况：
1. 内存存在未释放的情况, 导致内存耗尽, 无法分配出内存给新的UE接入；
2. 内存分配的链表出现异常, 无法找到可用的内存。

#3 - 2021-06-25 18:15 - 匿名用户

huang xiwen 写到：

可能存在的情况：
1. 内存存在未释放的情况, 导致内存耗尽, 无法分配出内存给新的UE接入；
2. 内存分配的链表出现异常, 无法找到可用的内存。

已增加必要的log, 待问题复现后继续分析。

#4 - 2021-06-25 18:16 - 匿名用户

- 状态从新建变更为进行中

#5 - 2021-06-28 10:25 - 匿名用户

```
[06-27 07:00:37.968][DEBUG]NR_RACH_DBG: MSG3 RECVED !!!  
[06-27 07:00:37.968][DEBUG]NR_RACH_DBG: MSG3 RECVED is CCCH SDU!!!  
[06-27 07:00:37.968][DEBUG]cmGetMemBlkSetForAlloc: failed 2, listValidBktSet Cnt0  
[06-27 07:00:37.968][ERROR]rgSCHLv1UtlAllocSBuf,Unable to Allocate the Buffer  
[06-27 07:00:37.968][ERROR]DBG_CELLID1 Scheduler handling failed rgSCHLv1CfgCellUeCtxtInIt for CRNTI17036
```

周末跑的挂死情况也是内存分配失败导致, 从上面新添加log看, 是内存耗尽, 不是踩栈改变了内存管理链表。该处申请内存大小大于50000, 为最后一个内存bucket。

下一步只能走读代码，细致查看哪一处存在对该大内存bucket使用，但未释放的情况。

#6 - 2021-06-29 17:34 - 匿名用户

- 状态从进行中变更为转测试

huang xiwen 写到：

```
[06-27 07:00:37.968][DEBUG]NR_RACH_DBG: MSG3 RECVED !!!  
[06-27 07:00:37.968][DEBUG]NR_RACH_DBG: MSG3 RECVED is CCCH SDU!!!  
[06-27 07:00:37.968][DEBUG]cmGetMemBkSetForAlloc: failed 2, listValidBktSet Cnt0  
[06-27 07:00:37.968][ERROR]rgSCHLvl1UtilAllocSBuf,Unable to Allocate the Buffer  
[06-27 07:00:37.968][ERROR]DBG_CELLID1Scheduler handling failed rgSCHLvl1CfgCellUeCtxInit for CRNTI17036
```

周末跑的挂死情况也是内存分配失败导致，从上面新添加log看，是内存耗尽，不是踩栈改变了内存管理链表。
该处申请内存大小大于50000，为最后一个内存bucket。
下一步只能走读代码，细致查看哪一处存在对该大内存bucket使用，但未释放的情况。

经过对所有大小超过20000的内存进行走读，查看申请和释放是否正常；
经过排查发现，随机接入过程中，如果收到了MSG3，但CU未正常反馈rrc setup的情况下，内存释放异常，部分已申请内存未释放，且大小正好是超过20000的。

在该情况下，添加对未释放内存的释放操作，版本更新后，待测试验证。

#7 - 2021-07-12 11:13 - 匿名用户

经过4T4R添加大内存的分配和释放，发现了一个新的导致大内存未释放的问题；
填写PHY接口时，内存有一个暂存待后续释放的操作，但该暂存结构体记录包长的变量定义为U16，
从而导致超过65535的数据都无法被正确释放。

#8 - 2021-10-13 14:57 - 周磊

- 状态从转测试变更为已解决