FirstCall - 错误 #2866

RLC AM模式的发送端，收到状态报告，释放已经确认接收的数据包时，发生CRASH

2025-02-24 17:33 - 王 艳芳

状态:	已关闭	**开始日期:**	2025-02-24
优先级:	普通	**计划完成日期:**	
指派给:	王 艳芳	**% 完成:**	0%
类别:		**预期时间:**	0.00 小时
目标版本:		**耗时:**	0.00 小时

描述

X86环境下打桩测试RLC
AM重传，设置终端节点类型为IRN，当接收到打桩的状态报告进行释放已经确认接收的数据包时，发生CRASH。

历史记录

#1 - 2025-02-24 17:33 - 王 艳芳

- 状态 从 新建 变更为 进行中

#2 - 2025-02-27 09:36 - 王 艳芳

- 状态 从 进行中 变更为 已解决

【问题现象】GDB调试，CRASH行为wnRlcAmArqPrcsAckNack的1032行，调用ngPktFree释放nackInfo[0]
的nackSn之前的PKT，即sn=txNextAck的PKT时，会概率性CRASH
【问题原因】原因基本是该PKT的NEXT不为空，且为无效的NGPKT指针，释放是循环的，所以，当m=m->next时，由于m->next为无效指针，所以，出现CRASH。跟踪wnRlcAmAddToTxBuff函数里LCSDU指针及NEXT，确认NEXT是空，即SDU的初始内存指针没有问题，属于后面代码处理引入的问题。继续跟踪后续代码实现，定位为wnRlcAmTxPollHndlr传参错误，应该传入SDU的PKT的数据起始地址，但实际传入了SDU的PKT指针，导致PKT的头信息被修改，从而把NEXT指针信息从空指针修改为无效地址，引发了PKT释放时的CRASH(DPDK内存的管理和释放)
【问题验证】修改代码后，验证通过

#3 - 2025-03-08 15:18 - 王 艳芳

- 状态 从 已解决 变更为 已关闭

【测试结果】测试已通过