OsmoPCU - Bug #4756

osmo-pcu: assert hit

09/16/2020 04:38 PM - pespin

Status: Resolved
Priority: High
Assignee: pespin
Category: 
Target version: 
Spec Reference: 

Description

$ osmo-pcu --version
OsmoPCU version 0.8.0.199-2597

20200916182904116 DRLCMACMEAS qprs rlcmac_meas.cpp:108 MS(TLLI=0x9b2a715a, IMSI=000, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182904291 DRLCMACMEAS qprs rlcmac_meas.cpp:186 DL Bandwitdh of IMSI=901700000015254 / TLLI=0xd0176e02: 1915 KBits/s
20200916182904457 DRLCMACMEAS qprs rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -17 dBm
20200916182904656 DRLCMACMEAS qprs rlcmac_meas.cpp:108 MS(TLLI=0x9b2a715a, IMSI=000, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182904992 DRLCMACMEAS qprs rlcmac_meas.cpp:186 DL Bandwitdh of IMSI=000 / TLLI=0x9b2a715a: 108 KBits/s
20200916182905215 DRLCMACMEAS qprs rlcmac_meas.cpp:108 MS(TLLI=0x9b2a715a, IMSI=901700000015256, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182905292 DRLCMACMEAS qprs rlcmac_meas.cpp:186 DL Bandwitdh of IMSI=901700000015254 / TLLI=0xd0176e02: 1004 KBits/s
20200916182905374 DRLCMACMEAS qprs rlcmac_meas.cpp:46 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) Rx Measurement Report: NC1 Serv -52 dbm
20200916182905477 DRLCMACMEAS qprs rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -17 dBm
20200916182905334 DRLCMACMEAS qprs rlcmac_meas.cpp:108 MS(TLLI=0x9b2a715a, IMSI=901700000015256, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182908059 DRLCMACMEAS qprs rlcmac_meas.cpp:186 DL Bandwitdh of IMSI=901700000015256 / TLLI=0xe7daadb8: 207 KBits/s
20200916182906109 DRLCMACMEAS qprs rlcmac_meas.cpp:186 DL Bandwitdh of IMSI=901700000015256 / TLLI=0x9b2a715a: 207 KBits/s
20200916182906055 DRLCMACMEAS qprs rlcmac_meas.cpp:108 MS(TLLI=0x9b2a715a, IMSI=901700000015256, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182906109 DRLCMACMEAS qprs rlcmac_meas.cpp:186 DL Bandwitdh of IMSI=901700000015256 / TLLI=0x9b2a715a: 207 KBits/s
20200916182906492 DRLCMACMEAS qprs rlcmac_meas.cpp:186 DL Bandwitdh of IMSI=901700000015254 / TLLI=0xd0176e02: 968 KBits/s
20200916182906574 DRLCMACMEAS qprs rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -17 dBm
20200916182906618 DRLCMACMEAS qprs rlcmac_meas.cpp:108 MS(TLLI=0xe7daadb8, IMSI=901700000015256, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182907231 DRLCMACMEAS qprs rlcmac_meas.cpp:186 DL Bandwitdh of IMSI=901700000015256 / TLLI=0xe7daadb8: 145 KBits/s
20200916182907516 DRLCMACMEAS qprs rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -17 dBm
20200916182907753 DRLCMACMEAS qprs rlcmac_meas.cpp:186 DL Bandwitdh of IMSI=901700000015254 / TLLI=0xd0176e02: 3270 KBits/s
20200916182908272 DRLCMACMEAS qprs rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -17 dBm
20200916182908869 DRLCMACMEAS qprs rlcmac_meas.cpp:186 DL Bandwitdh of IMSI=901700000015254 / TLLI=0xd0176e02: 728 KBits/s
20200916182909196 DRLCMACMEAS qprs rlcmac_meas.cpp:46 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) Rx Measurement Report: NC1 Serv -51 dbm
20200916182909436 DRLCMACMEAS qprs rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -17 dBm
20200916182909657 DTBF tbf.cpp:647 TBF(TFI=1 TLLI=0xe7daadb8 DIR=DL STATE=WAIT RELEASE EGPRS) T319 3 timeout expired, freeing TBF
20200916182909673 DTBFDL tbf dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 444, because the window is stalled.
20200916182909713 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=90170000015254, T A=0, 12/12, UL DL) UL RSSI: -17 dBm

20200916182909871 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=90170000015254 / TLLI=0xd0176e02: 7025 KBits/s

20200916182909949 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 508, because the window is stalled.

20200916182910111 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 508, because the window is stalled.

20200916182910158 DRLCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe7daadb8, IMSI=901700000015256, TA=0, 12/12,) Rx Measurement Report: NC1 Serv -48 dbm

20200916182910309 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 580, because the window is stalled.

20200916182910516 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -15 dBm

20200916182910609 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 660, because the window is stalled.

20200916182910849 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 708, because the window is stalled.

20200916182911156 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=901700000015254 / TLLI=0xd0176e02: 15819 KBits/s

20200916182911449 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 780, because the window is stalled.

20200916182911573 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -14 dBm

20200916182911731 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 924, because the window is stalled.

20200916182911892 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 924, because the window is stalled.

20200916182911971 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=901700000015254 / TLLI=0xd0176e02: 16733 KBits/s

20200916182912292 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -15 dBm

20200916182912409 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1068, because the window is stalled.

20200916182912594 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe7daadb8, IMSI=000, TA=0, 12/12, UL DL) UL RSSI: -11 dBm

20200916182912672 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1132, because the window is stalled.

20200916182912972 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=901700000015254 / TLLI=0xd0176e02: 19606 KBits/s

20200916182912991 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1210, because the window is stalled.

20200916182913036 DRLCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) Rx Measurement Report: NC1 Serv -51 dbm

20200916182913134 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe7daadb8, IMSI=000, TA=0, 12/12, UL DL) UL RSSI: -11 dBm

20200916182913215 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -15 dBm

20200916182913249 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182913411 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182913453 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=000 / TLLI=0xe7daadb8: 231 KBits/s

20200916182913572 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182913596 DTBF tbf.cpp:806 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1155778, TS=3 (curr FN 1155843)

20200916182913596 DTBF tbf.cpp:877 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Timeout for polling PACKET DOWNLINK ACK.

20200916182913596 DTBF tbf.cpp:1177 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Assignment was on PACCH

20200916182913596 DTBF tbf.cpp:1183 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC
K was received

20200916182914052 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182914533 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182914689 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182914719 DRLMAC pdch.cpp:480 EGPRS PACKET DOWNLINK ACK with unknown FN=1156077 TFI=1 (TX 0 TS 6)

20200916182914754 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182914851 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182915012 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182915156 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182915156 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182915492 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182915535 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182915535 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182915535 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182915535 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182915535 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.
polling PACKET DOWNLINK ACK.

20200916182915535 DTBF tfb.cpp:1177 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Assignment was on PACCH
20200916182915535 DTBF tfb.cpp:1183 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received
20200916182915650 DTBFDL tfb_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.
20200916182915811 DTBFDL tfb_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.
20200916182915936 DTBF tfb.cpp:806 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN 1156350)
20200916182915936 DTBF tfb.cpp:877 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Timeout for polling PACKET DOWNLINK ACK.
20200916182915936 DTBF tfb.cpp:1177 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Assignment was on PACCH
20200916182915936 DTBF tfb.cpp:1183 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received
20200916182915973 DTBFDL tfb_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.
20200916182916152 DTBFDL tfb_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.
20200916182916309 DTBFDL tfb_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.
20200916182916315 DTBF tfb.cpp:598 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) N3105 exceeded MAX (8)
20200916182916315 DTBF tfb.cpp:598 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) N3105 exceeded MAX (8)
20200916182916315 DTBF tfb.cpp:598 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) N3105 exceeded MAX (8)
20200916182916315 DTBF tfb.cpp:598 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) N3105 exceeded MAX (8)
20200916182916315 DTBF tfb.cpp:598 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) N3105 exceeded MAX (8)
20200916182916315 DTBF tfb.cpp:598 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) N3105 exceeded MAX (8)
20200916182920155 DRLCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe7daadb8, IMSI=000, TA=0, 12/12,) Rx Measurement Report: NCI Serv - 47 dbm
20200916182920777 DRLCMAC pdch.cpp:480 EGPRS PACKET DOWNLINK ACK with unknown FN=1156077 TFI=1 (TR X 0 TS 6)
20200916182921315 DTBF tfb.cpp:647 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=RELEASING EGPRS) T3195 timeout expired, freeing TBF
20200916182921315 DTBF tfb.cpp:1177 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=RELEASING EGPRS) Assignment was on PACCH
20200916182921315 DTBF tfb.cpp:1183 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=RELEASING EGPRS) Downlink AC K was received
20200916182921315 DTBF tfb.cpp:598 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) N3105 exceeded MAX (8)
20200916182921434 DBSSGP gprs_bssgp_bss.c:64 BSSGP (BVC='0') Tx SUSPEND (TLLI=0xe7daadb8)

09/17/2022
Program received signal SIGABRT, Aborted.
0x000007ffff5a46615 in raise () from /usr/lib/libc.so.6
(gdb) bt
#0 0x000007ffff5a46615 in raise () from /usr/lib/libc.so.6
#1 0x000007ffff5a2f862 in abort () from /usr/lib/libc.so.6
#2 0x00007ffff6a019c2 in osmo_panic_default (fmt=0x5555558a3940 "Assert failed \%s \%s:%d\n", args=0x7fffffffff340) at /git/libosmocore/src/panic.c:49
#3 0x00007ffff6a01afe in osmo_panic (fmt=0x5555558a3940 "Assert failed \%s \%s:%d\n") at /git/libosmocore/src/panic.c:84
#4 0x000055555557f2da5 in gen_freq_params (freq_params=0x6340005408cc, tbf=0x7fffffff9860) at /git/osmo-pcu/src/encoding.cpp:562
#5 0x000055555557f4d04 in Encoding::write_packet_uplink_assignment (block=0x634000540860, old_tfi=1 '001', old_downlink=0 '000', tlli=349196418, use_tlli=1 '001', tbf=0x7fffffff9860, poll=1 '001', rrbp=0 '000', alpha=0 '000', gamma=0 '000', ta_idx=-1 '377', use_egprs=true) at /git/osmo-pcu/src/encoding.cpp:678
#6 0x000055555557a1c9 in gprs_rlcmac_tbf::create_ul_ass (this=0x7fffffff9860, fn=1164080, ts=7 'a') at /git/osmo-pcu/src/tbf.cpp:1372
#7 0x000055555557b7153 in sched_select_ctrl_msg (trx=0 '000', ts=7 'a', fn=1164080, block_nr=2 '002', pdch=0x555555b11800 <s_bts+4320>, ul_ass_tbf=0x7fffffff9860, dl_ass_tbf=0x0, ul_ack_tbf=0x0) at /git/osmo-pcu/src/gprs_rlcmac_sched.cpp:215
#8 0x000055555557b7267 in gprs_rlcmac_rcv_rts_block (bts=0x555555b10728 <s_bts+8>, trx=0 '000', ts=7 'a', fn=1164080, block_nr=2 '002') at /git/osmo-pcu/src/gprs_rlcmac_sched.cpp:427
#9 0x000055555557b4d3 in pcu_rx_rts_req_pduch (trx=0 '000', ts=7 'a', fn=1164080, block_nr=2 '002') at /git/osmo-pcu/src/pcu_l1_if.cpp:386
#10 0x000055555557c756 in pcu_rx_rts_req (rts_req=0x7fffffffffda4) at /git/osmo-pcu/src/pcu_l1_if.cpp:420
#11 0x000055555557b5b86 in pcu_rx (msg_type=16 '020', pcu_prim=0x7fffffffffda0) at /git/osmo-pcu/src/pcu_l1_if.cpp:765
#12 0x000055555557b1937f in pcu_sock_read (bfd=0x555555b1a3e0 <pcu_sock_state>) at /git/osmo-pcu/src/omsbots_sock.cpp:141
#13 0x000055555557b196c6 in pcu_sock_cb (bfd=0x555555b1a3e0 <pcu_sock_state>, flags=1) at /git/osmo-pcu/src/omsbots_sock.cpp:196
#14 0x000007ffffff9b90a in osmo_fd Disp_fds (_rsset=0x7fffffffffddc0, _wsset=0x7fffffffffde60, _eset=0x7fffffffff00) at /git/libosmocore/src/select.c:227
#15 0x000007ffffff9b654 in osmo_select_main (polling=0) at /git/libosmocore/src/select.c:265
#16 0x000007ffffff9b741 in osmo_select.main (polling=0) at /git/libosmocore/src/select.c:274
--Type <RET> for more, q to quit, c to continue without paging--
#17 0x00005555555748196 in main (argc=7, argv=0x7fffffffef8) at /git/osmo-pcu/src/pcu_main.cpp:357

The assert failing:

/* Prepare to be encoded Frequency Parameters IE (see Table 12.8.1) */
static void gen_freq_params(Frequency_Parameters_t *freq_params,
    const struct gprs_rlcmac_tbf *tbf)
{
    const struct gprs_rlcmac_pdch *pdch;
    Direct_encoding_1_t fh_params;

    /* Check one PDCH, if it's hopping then all other should too */

09/17/2022
pdch = tbf->pdch[tbf->first_ts];
OSMO_ASSERT(pdch != NULL);

It happened a few seconds after stopping osmo-bts-trx with gdb.

(gdb) print tbf->first_ts
$2 = 2 '\002'  
(gdb) print tbf->pdch
$3 = {0x0, 0x0, 0x0, 0x555555b10ea0 <s_bts+1920>, 0x0, 0x0, 0x0, 0x0}

Happened again, during a call, probably because the PDCH TS where the MS was laying was deleted (because I have all TS set as dynamic TCH_H/TCH_F/PDCH).

Assert failed pdch != NULL /git/osmo-pcu/src/encoding.cpp:562
backtrace() returned 21 addresses
/build/new/out/lib/libosmocore.so.16(+0x146c2e) [0x7ffff6a01c2e]
/build/new/out/lib/libosmocore.so.16(osmo_generate_backtrace+0x18) [0x7ffff6a01ffd]

History
#1 - 09/16/2020 04:50 PM - pespin
Program received signal SIGABRT, Aborted.
0x00007fff5a46615 in raise () from /usr/lib/libc.so.6
(gdb) bt
#0 0x00007fff5a46615 in raise () from /usr/lib/libc.so.6
#1 0x00007fff5a2f862 in abort () from /usr/lib/libc.so.6
#2 0x00007ffff6a019c2 in osmo_panic_default (fmt=0x5555558a3940 "Assert failed %s %s:%d
", args=0x7fffffffdd40) at /git/libosmocore/src/panic.c:49
#3 0x00007ffff6a01afe in osmo_panic (fmt=0x5555558a3940 "Assert failed %s %s:%d
") at /git/libosmocore/src/panic.c:84
#4 0x00005555557f2da5 in gen_freq_params (freq_params=0x6340003608cc, tbf=0x7fffff21bb860) at /git/osmo-pcu/src/encoding.cpp:562
#5 0x00005555557f4d04 in Encoding::write_packet_uplink_assignment (block=0x634000360860, old_tfi=1 \"001\", old_downlink=0 \"000\", tlli=3641136890, use_tlli=1 \"001\", rrbp=0 \"000\", alpha=0 \"000\", gamma=0 \"000\", ta_idx=\"377\", use_egprs=true) at /git/osmo-pcu/src/encoding.cpp:678
#6 0x00005555557ac19c in gprs_rlcmac_tbf::create_ul_ass (this=0x7fffff21bb860, fn=561734, ts=7 \"a\") at /git/osmo-pcu/src/tbf.cpp:1372
#7 0x0000555555827153 in sched_select_ctlr_msg (trx=0 \"000\", ts=7 \"a\", fn=561734, block_nr=7 \"a\", pdcch=0x555555b11800 <s_bts+4320>, ul_ass_tbf=0x7fffff21bb860, dl_ass_tbf=0x0, ul_ack_tbf=0x0) -- Type RET for more, q to quit, c to continue without paging-- at /git/osmo-pcu/src/gprs_rlcmac_sched.cpp:215
#8 0x0000555555829267 in gprs_rlcmac_rcv_rts_block (bts=0x555555b10728 <s_bts+8>, trx=0 \"000\", ts=7 \"a\", fn=561734, block_nr=7 \"a\") at /git/osmo-pcu/src/gprs_rlcmac_sched.cpp:427
#9 0x00005555557bd63 in pcu_rx_rts_reg_pdtch (trx=0 \"000\", ts=7 \"a\", fn=561734, block_nr=7 \"a\") at /git/osmo-pcu/src/pcu_rx_rts_reg_pdtch.cpp:386
#10 0x00005555557c756 in pcu_rx_rts_reg_rts (rts_req=0x7fffffffdfaf4) at /git/osmo-pcu/src/pcu_rx_rts_reg.cpp:420
#11 0x00005555557b8b8 in pcu_rx (mag_type=16 \"020\", pcu_prim=0x7fffffffdfaf0) at /git/osmo-pcu/src/pcu_rx.cpp:1765
#12 0x000055555581937f in pcu_sock_read (bfd=0x5555555b1a3e0 <pcu_sock_state>) at /git/osmo-pcu/src/osmobts_sock.cpp:141
#13 0x0000555555819a6c in pcu_sock_ch (bfd=0x5555555b1a3e0 <pcu_sock_state>, flags=1) at /git/osmo-pcu/src/osmobts_sock.cpp:196
#14 0x00007fffff69b90a in osmo_fd_disp_fds (_reset=0x7fffffffddc0, _wset=0x7fffffffdefe60, _reset=0x7fffffffeed00) at /git/libosmocore/src/select.c:227
#15 0x00007fffff69b9654 in osmo_pcu_select_main (polling=0) at /git/libosmocore/src/select.c:227
#16 0x00007fffff69b9741 in osmo_pcu_select_main (polling=0) at /git/libosmocore/src/select.c:274
-- Type RET for more, q to quit, c to continue without paging--
#17 0x0000555555748196 in main (argc=7, argv=0x7fffffffef8) at /git/osmo-pcu/src/pcu_main.cpp:357
I confirm I can reproduce this by placing a call between 2 MS whenever all timeslots are set to TCH/F_TCH/H_PDCH.

1- MS are GPRS attached to the network, probably doing data transfers
2- call MO_MT between them
3- Take the call, leave it for a few seconds and hang the call
4- pcu crashes.

This is very interesting, because we used to dereference that pointer without any checks before my hopping patches:

```cpp
void Encoding::write_packet_uplink_assignment(...) {
  // ...
  /* Frequency Parameters IE */
  fp->TSC = tbf->tsc(); // Training Sequence Code (TSC)
  fp->UnionType = 0x00;  // Single ARFCN
  fp->u.ARFCN = tbf->trx->arfcn;
}
```

here is the definition of tbf->tsc():

```cpp
uint8_t gprs_rlcmac_tbf::tsc() const {
  return trx->pdch[first_ts].tsc;
}
```

so I am pretty sure we had this bug, but never noticed it?

I'll try to implement a TTCN-3 test case, so we can see if the problem does exist in the 'latest'.

Unfortunately, I was not able to reproduce the problem, neither in GPRS nor in EGPRS mode.

So as a reminder, I have TS=CCCH+SDCCH4, TS1..5=TCH/F_TCH/H_PDCH, TS6..7=PDCH. I also have "channel allocator descending", which means TS 4 and 5 are switched to TCH to handle the call, which means they get deactivated in PCU. That's working fine. I also added a VTY command to verify during the call the TS are marked as disabled in PCU.
Now, I added some more debugging during chan allocation:

20200922184517883 DTBF tbf.cpp:997 Allocating UL TBF: MS_CLASS=12/12
20200922184517883 DTBF tbf.cpp:1009 TBF(TFI=0 TLLI=0x00000000 DIR=UL STATE=NULL EGPRS) Enabled EGPRS, mode EGP RS
20200922184517883 DRLCMAC gprs_rlcmac_ts_alloc.cpp:895 [UL] algo B <multi> (suggested TRX: 0): reserved slots: ul=0x0c dl=0x0e, first_common_ts=ffffffff
20200922184517883 DRLCMAC gprs_rlcmac_ts_alloc.cpp:904 [UL] algo B <multi> (suggested TRX: 0): first_ts=2
20200922184517883 DRLCMAC gprs_rlcmac_ts_alloc.cpp:929 [UL] algo B <multi> (suggested TRX: 0): first_common_ts =3
20200922184517883 DRLCMAC gprs_rlcmac_ts_alloc.cpp:941 [UL] algo B <multi> (suggested TRX: 0): using 1/1 slots (0x08)
20200922184517883 DRLCMAC gprs_rlcmac_ts_alloc.cpp:807 - Assigning UL TS 3
20200922184517883 DTBFUL tbf_ul.cpp:613 TBF(TFI=1 TLLI=0xf99b124d DIR=UL STATE=ASSIGN EGPRS) setting EGPRS UL window size to 64, base(slots) = 0, ws_pdch(0)
20200922184517893 DTBF tbf.cpp:1379 TBF(TFI=1 TLLI=0xf99b124d DIR=UL STATE=ASSIGN EGPRS) start Packet Uplink Assignment (PACCH)

Not seen in the text above, but in the pcap file in debug I see (so available TS in C are correct): 1,2,3,7,8:

63499 18:45:17.883736890 127.0.0.1 34946 127.0.0.1 4729 GSMTAP 189 - Possible DL/UL sl ots: (TS=0)".CCC..CC"(TS=7)

Then, after doing the calculations it decides the available slots are: reservation slots: ul=0x0c dl=0x0e so 00001100 and 00001110. From there, it selects fn_first=2, and (only seen in debug pcap), afterwards it says "- Skipping TS 2, because num TBFs 1 > 0" and immediately after sets fn_common_first=3. Later it calculates the amount of slots to 1. So if you sum all the points above, there's only 1 TS being selected for this PDCH, yet fn_first and fn_common_first differ, which makes no sense to me. The issue seems to come from UL TBF branch calling allocate_usf() in alloc_algorithm_b(), which updates "reserved_ul_slots" and "ul_slots" later passed to update_ms_reserved_slots and assign_ul_tbf_slots, but forgets to update first_ts accordingly.

#8 - 09/22/2020 06:41 PM - pespin
- % Done changed from 0 to 90

Should be fixed by:
https://gerrit.osmocom.org/c/osmo-pcu/+/20254 Fix crash accessing NULL tbf->pdch[first_ts]

AFAICT this bug has been there since Jan 31 2018.

#9 - 09/30/2020 08:03 PM - laforge
- Status changed from Feedback to Resolved