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

---

20200916182904116 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0x9b2a715a, IMSI=000, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182904291 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=901700000015254 / TLLI=0x0d0176e02: 1915 KBits/s
20200916182904457 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0x0d0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -17 dBm
20200916182904656 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=901700000015254 / TLLI=0xd0176e02: 1004 KBits/s
20200916182904992 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182905215 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0x9b2a715a, IMSI=901700000015256, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182905292 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=901700000015254 / TLLI=0xd0176e02: 1004 KBits/s
20200916182905374 DRLCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0x0d0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) Rx Measurement Report: NCI Serv -52 dbm
20200916182905734 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0x0d0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -17 dBm
20200916182906055 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0x9b2a715a, IMSI=901700000015256, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182906109 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=901700000015256 / TLLI=0x9b2a715a: 207 KBits/s
20200916182906492 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=901700000015254 / TLLI=0xd0176e02: 968 KBits/s
20200916182906574 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0x0d0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -17 dBm
20200916182906618 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe7daadb8, IMSI=901700000015256, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182907231 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=901700000015256 / TLLI=0xe7daadb8: 145 KBits/s
20200916182907516 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0x0d0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -17 dBm
20200916182907753 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=901700000015254 / TLLI=0xd0176e02: 3270 KBits/s
20200916182908272 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0x0d0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) UL RSSI: -17 dBm
20200916182908869 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=901700000015254 / TLLI=0xd0176e02: 728 KBits/s
20200916182909196 DRLCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0x0d0176e02, IMSI=901700000015254, TA=0, 12/12, UL DL) Rx Measurement Report: NCI Serv -51 dbm
20200916182909436 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0x0d0176e02, 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.

---

08/08/2021 1/9
20200916182909713 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=90170000015254, TA=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.
20200916182910842 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=90170000015254 / TLLI=0xd0176e02: 15819 KBits/s
20200916182911150 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 708, because the window is stalled.
20200916182911342 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe7daadb8, IMSI=901700000015256, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182911573 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=90170000015254, TA=0, 12/12, UL DL) UL RSSI: -14 dBm
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.
20200916182912042 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 924, because the window is stalled.
20200916182912292 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=90170000015254 / TLLI=0xd0176e02: 16733 KBits/s
20200916182912594 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe7daadb8, IMSI=000, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182912720 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xd0176e02, IMSI=90170000015254, TA=0, 12/12, UL DL) UL RSSI: -11 dBm
20200916182912972 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwidth of IMSI=90170000015254 / TLLI=0xd0176e02: 19606 KBits/s
20200916182913249 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe7daadb8, IMSI=000, TA=0, 12/12, UL DL) UL RSSI: -15 dBm
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 DTBFDL tbf_dl.cpp:806 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1155778, TS=3 (curr FN 1155843)
20200916182913596 DTBFDL tbf_dl.cpp:877 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Timeout for polling PACKET DOWNLINK ACK.
20200916182913596 DTBFDL tbf_dl.cpp:1177 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Assignment was on PACCH
20200916182913596 DTBFDL tbf_dl.cpp:1183 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC
polling PACKET DOWNLINK ACK.

Assignment was on PACCH

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

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

DTBF tbf.cpp:1177 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

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

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

TBF(TFI=0 TLLI=0 xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0 xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0 xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0 xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0 xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0 xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0 xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0 xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0 xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0 xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)

TBF(TFI=0 TLLI=0 xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN=1156350)
Program received signal SIGABRT, Aborted.
0x0000007fff5a46615 in raise () from /usr/lib/libc.so.6
(gdb) bt
#0 0x0000007fff5a46615 in raise () from /usr/lib/libc.so.6
#1 0x0000007fff5a2f662 in abort () from /usr/lib/libc.so.6
#2 0x0000007fff6a019c2 in osmo_panic_default (fmt=0x5555558a3940 "Assert failed \%s \%s:%d\n", args=0x7fffffff6f340) at /git/libosmocore/src/panic.c:49
#3 0x0000007fff6a01afe in osmo_panic (fmt=0x5555558a3940 "Assert failed \%s \%s:%d\n") at /git/libosmocore/src/panic.c:84
#4 0x000000555555557f2da5 in gen_freq_params (freq_params=0x6340005408cc, tbf=0x7fffff1ee9860) at /git/osmo-pcu/src/encoding.cpp:562
#5 0x000000555555557f4d04 in Encoding::write_packet_uplink_assignment (block=0x634000540860, old_tfi=1 '\001', old_downlink=0 '\000', tlli=349196418, use_tlli=1 '\001', tbf=0x7fffff1ee9860, 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 0x000000555555557f4ac9 in gprs_rlcmac_tbf::create_ul_ass (this=0x7fffff1ee9860, fn=1164080, ts=7 '\a') at /git/osmo-pcu/src/tbf.cpp:1372
#7 0x000000555555557f2153 in sched_select_ctrl_msg (trx=0 '\000', ts=7 '\a', fn=1164080, block_nr=2 '\002', pdch=0x5555555b11800 <s_bts+4320>, ul_ass_tbf=0x7fffff1ee9860, 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 0x000000555555557f2267 in gprs_rlcmac_rcv_rts_block (bts=0x5555555b10728 <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 0x000000555555557f7d63 in pcu_rx_rts_req_pdch (trx=0 '\000', ts=7 '\a', fn=1164080, block_nr=2 '\002') at /git/osmo-pcu/src/pcu_l1_if.cpp:386
#10 0x000000555555557f7c7e in pcu_rx_rts_req (rts_req=0x7fffffffdfaf4) at /git/osmo-pcu/src/pcu_l1_if.cpp:420
#11 0x000000555555557f78b6 in pcu_rx (msg_type=16 '\020', pcu_prim=0x7fffffffdfaf0) at /git/osmo-pcu/src/pcu_l1_if.cpp:765
#12 0x000000555555557f1937 in pcu_sock_read (bfd=0x5555555b1a3e0 <pcu_sock_state>) at /git/osmo-pcu/src/osmobs_sock.cpp:141
#13 0x000000555555557f1937 in pcu_sock_cb (bfd=0x5555555b1a3e0 <pcu_sock_state>, flags=1) at /git/osmo-pcu/src/osmobs_sock.cpp:196
#14 0x0000007fffffff90a in osmo_fd_disp_fds (_rset=0x7fffffff6f2c0, _wset=0x7fffffff6f000, _eset=0x7fffffff6f00) at /git/libosmocore/src/select.c:227
#15 0x0000007fffffff9654 in osmo_select_main (polling=0) at /git/libosmocore/src/select.c:265
#16 0x0000007fffffff9741 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 0x000000555555557f819e in main (argc=7, argv=0x7fffffffef18) 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 */
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}

History
#1 - 09/16/2020 04:50 PM - pespin

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).

20200916184620436 DRLCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe37fcdf2, IMSI=901700000015256, TA=0, 12/12,) Rx Measurement Report: NCI Serv -50 dbm

20200916184620598 DRLCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xd90756fa, IMSI=901700000015254, TA=0, 12/12,) Rx Measurement Report: NCI Serv -49 dbm

20200916184621657 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe37fcdf2, IMSI=901700000015256, TA=0, 12/12, UL) UL RSSI: -12 dbm

20200916184625518 DRLCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe37fcdf2, IMSI=901700000015256, TA=0, 12/12,) Rx Measurement Report: NCI Serv -50 dbm

20200916184631961 DBSSGP gprs_bssgp_bss.c:64 DBSSGP (BVCID=0) Tx SUSPEND (TLLI=0x0d90756fa)

20200916184638476 DTBF tbf.cpp:806 TBF(TFI=0 TLLI=0xd90756fa DIR=DL STATE=ASSIGN EGPRS) poll timeout for FN=54 9952, TS=2 (curr FN 550017)

20200916184638476 DTBF tbf.cpp:856 TBF(TFI=0 TLLI=0xd90756fa DIR=DL STATE=ASSIGN EGPRS) Timeout for polling PACKET CONTROL ACK for PACKET DOWNLINK ASSIGNMENT.

20200916184638476 DTBF tbf.cpp:1177 TBF(TFI=0 TLLI=0xd90756fa DIR=DL STATE=ASSIGN EGPRS) Assignment was on PAC CH

20200916184638476 DTBF tbf.cpp:1185 TBF(TFI=0 TLLI=0xd90756fa DIR=DL STATE=ASSIGN EGPRS) No downlink ACK received yet

20200916184639256 DTBF tbf.cpp:806 TBF(TFI=0 TLLI=0xd90756fa DIR=DL STATE=ASSIGN EGPRS) poll timeout for FN=55 0038, TS=2 (curr FN 550099)

20200916184639634 DTBF tbf.cpp:806 TBF(TFI=0 TLLI=0xd90756fa DIR=DL STATE=ASSIGN EGPRS) poll timeout for FN=55 0121, TS=2 (curr FN 550186)

20200916184640036 DTBF tbf.cpp:806 TBF(TFI=0 TLLI=0xd90756fa DIR=DL STATE=ASSIGN EGPRS) poll timeout for FN=55 0207, TS=2 (curr FN 550268)

20200916184640036 DTBF tbf.cpp:806 TBF(TFI=0 TLLI=0xd90756fa DIR=DL STATE=ASSIGN EGPRS) poll timeout for FN=55 0230, TS=2 (curr FN 550355)

20200916184640085 DTBF tbf.cpp:1136 TBF(TFI=0 TLLI=0xd90756fa DIR=DL STATE=ASSIGN EGPRS) releasing due to PACC H assignment timeout.

20200916184640085 DTBF tbf.cpp:856 TBF(TFI=0 TLLI=0xd90756fa DIR=DL STATE=ASSIGN EGPRS) Timeout for polling PACKET CONTROL ACK for PACKET DOWNLINK ASSIGNMENT.

20200916184640085 DTBF tbf.cpp:1177 TBF(TFI=0 TLLI=0xd90756fa DIR=DL STATE=ASSIGN EGPRS) Assignment was on PAC CH

20200916184640408 DTBF tbf.cpp:806 TBF(TFI=0 TLLI=0xd90756fa DIR=DL STATE=ASSIGN EGPRS) No downlink ACK received yet

20200916184643396 DTBF tbf.cpp:856 TBF(TFI=0 TLLI=0xe37fcdf2 DIR=DL STATE=ASSIGN EGPRS) Timeout for polling PACKET CONTROL ACK for PACKET DOWNLINK ASSIGNMENT.

20200916184643396 DTBF tbf.cpp:856 TBF(TFI=0 TLLI=0xe37fcdf2 DIR=DL STATE=ASSIGN EGPRS) Assignment was on PAC CH

20200916184643396 DTBF tbf.cpp:1136 TBF(TFI=0 TLLI=0xe37fcdf2 DIR=DL STATE=ASSIGN EGPRS) releasing due to PACC H assignment timeout.

20200916184643396 DTBF tbf.cpp:1177 TBF(TFI=0 TLLI=0xe37fcdf2 DIR=DL STATE=ASSIGN EGPRS) Assignment was on PAC CH

20200916184643396 DTBF tbf.cpp:806 TBF(TFI=0 TLLI=0xe37fcdf2 DIR=DL STATE=ASSIGN EGPRS) poll timeout for FN=55 1104, TS=2 (curr FN 551165)

20200916184644176 DTBF tbf.cpp:806 TBF(TFI=0 TLLI=0xe37fcdf2 DIR=DL STATE=ASSIGN EGPRS) poll timeout for FN=55 1187, TS=2 (curr FN 551252)

20200916184644556 DTBF tbf.cpp:806 TBF(TFI=0 TLLI=0xe37fcdf2 DIR=DL STATE=ASSIGN EGPRS) poll timeout for FN=55 1273, TS=2 (curr FN 551334)

20200916184644956 DTBF tbf.cpp:806 TBF(TFI=0 TLLI=0xe37fcdf2 DIR=DL STATE=ASSIGN EGPRS) poll timeout for FN=55 1356, TS=2 (curr FN 551421)

20200916184645029 DTBF tbf.cpp:1136 TBF(TFI=0 TLLI=0xe37fcdf2 DIR=DL STATE=ASSIGN EGPRS) releasing due to PACC H assignment timeout.

20200916184645029 DTBF tbf.cpp:856 TBF(TFI=0 TLLI=0xe37fcdf2 DIR=DL STATE=ASSIGN EGPRS) FIXME: Software error: Pending downlink assignment in state GPRS_RLCMAC_DL_ASS_WAIT_ACK. This may not happen, because the assignment message never gets transmitted. Please be sure not to free in this state. PLEASE FIX!

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) [0x7ffff6a01ff0]

08/08/2021 6/9
Program received signal SIGABRT, Aborted.
0x0000000000000000 in raise () from /usr/lib/libc.so.6
(gdb) bt
#0 0x00007fffffa46d15 in raise () from /usr/lib/libc.so.6
#1 0x00007fffffa46d2 in abort () from /usr/lib/libc.so.6
#2 0x00007fffffa39ad in osmo_panic_default (fmt=0x5555558a3f40 "Assert failed %s %s:%d\n", args=0x7fffffffdd0)
at /git/libosmocore/src/panic.c:49
#3 0x00007fffffa39a8 in osmo_panic (fmt=0x5555558a3f40 "Assert failed %s %s:%d\n")
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 0x00005555557f2d41 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=-1 \377, use_egprs=true)
at /git/osmo-pcu/src/encoding.cpp:678
#6 0x00005555557f2d41 in gprs_rlcmac_tbf::create_ul_ass (this=0x7fffff21bb860, fn=561734, ts=7 \001)
at /git/osmo-pcu/src/tbf.cpp:1372
#7 0x00005555557f2d41 in sched_select_ctrl_msg (trx=0 \000, ts=7 \001, a", fn=561734, block_nr=7 \001"

--Type <RET> for more, q to quit, c to continue without paging--
at /git/osmo-pcu/src/gprs_rlcmac_sched.cpp:215
#8 0x00005555557f2d41 in gprs_rlcmac_rcv_rts_block (bts=0x555555b10728 \000, txr=0 \000, ts=7 \001, fn=561734, block_nr=7 \001"
at /git/osmo-pcu/src/gprs_rlcmac_sched.cpp:427
#9 0x00005555557f2d41 in pcu_rx_rts_reg_pdtch (trx=0 \000, ts=7 \001, a", fn=561734, block_nr=7 \001"
at /git/osmo-pcu/src/pcu11_if.cpp:386
#10 0x00005555557f2d41 in pcu_rx_rts_reg (rts_reg=0x7fffffffdf04)
at /git/osmo-pcu/src/pcu11_if.cpp:420
#11 0x00005555557f2d41 in pcu_rx (mag_type=16 \020, pcu_prm=0x7fffffffdf0)
at /git/osmo-pcu/src/pcu11_if.cpp:765
#12 0x00005555557f2d41 in pcu_sock_read (bdfd=0x555555b1a3e0 \000, flags=1)
at /git/osmo-pcu/src/osmotts_sock.cpp:141
#13 0x00005555557f2d41 in pcu_sock cb (bdfd=0x555555b1a3e0 \000, flags=1)
at /git/osmo-pcu/src/osmotts_sock.cpp:196
#14 0x00005555557f2d41 in osmo_fd disp fds (_reset=0x7fffffffdd0, _reset=0x7fffffffdd0)
at /git/libosmocore/src/select.c:227
#15 0x00005555557f2d41 in osmo_select_main (polling=0)
at /git/libosmocore/src/select.c:265
#16 0x00005555557f2d41 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 0x00005555557f2d41 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:

```c
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():

```c
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 EGPRS
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
20200922184517883 DRLCMAC gprs_rlcmac_ts_alloc.cpp:807 - Assigning UL TS 3
20200922184517883 DTBF tbf.cpp:539 TBF(TFI=1 TLLI=0xf99b124d DIR=UL STATE=NULL EGPRS) Allocating: trx = 0, ul_slots = 08, dl_slots = 00
20200922184517883 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 slots: (TS=0)".CCC..CC" (TS=7)
```

Then, after doing the calculations it decides the available slots are: reserved 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 PDCCH, 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