$ osmo-pcu --version
OsmoPCU version 0.8.0.199-2597
20200916182913698 DRLCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe7daadb8, IMSI=000, TA=0, 12/12, UL DL) UL RSSI: -11 dBm

20200916182913729 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182913974 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182913974 DTBFDL tbf_dl.cpp:806 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1155947, TS=3 (curr FN 1156012)

20200916182913974 DTBFDL tbf_dl.cpp:877 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Timeout for polling PACKET DOWNLINK ACK.

20200916182913974 DTBFDL tbf_dl.cpp:1177 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Assignment was on PACCH

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.

20200916182914137 DBSSGP gprs_bssgp_bss.c:64 BSSGP (BVCI=0) Tx SUSPEND (TLLI=0xd0176e02)

20200916182914209 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182914371 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182914375 DTBFDL tbf_dl.cpp:806 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1155947, TS=3 (curr FN 1156012)

20200916182914375 DTBFDL tbf_dl.cpp:877 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Timeout for polling PACKET DOWNLINK ACK.

20200916182914375 DTBFDL tbf_dl.cpp:1177 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Assignment was on PACCH

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.

20200916182914592 DRLCMACMEAS gprs_rlcmac_meas.cpp:186 DL Bandwitdh of IMSI=000 / TLLI=0xe7daadb8: 254 KBits/s

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

20200916182914754 DTBFDL tbf_dl.cpp:806 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156033, TS=3 (curr FN 1156094)

20200916182914754 DTBFDL tbf_dl.cpp:877 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Timeout for polling PACKET DOWNLINK ACK.

20200916182914754 DTBFDL tbf_dl.cpp:1177 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Assignment was on PACCH

20200916182914881 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:806 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156116, TS=3 (curr FN 1156181)

20200916182915156 DTBFDL tbf_dl.cpp:877 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Timeout for polling PACKET DOWNLINK ACK.

20200916182915156 DTBFDL tbf_dl.cpp:1177 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Assignment was on PACCH

20200916182915156 DTBFDL tbf_dl.cpp:1183 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

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.

20200916182915333 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:806 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156202, TS=3 (curr FN 1156263)

20200916182915535 DTBFDL tbf_dl.cpp:877 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Timeout for polling PACKET DOWNLINK ACK.

20200916182915535 DTBFDL tbf_dl.cpp:1177 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Assignment was on PACCH

20200916182915535 DTBFDL tbf_dl.cpp:1183 TBF(TFI=0 TLLI=0x0d176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

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

20200916182915535 DTBF tbf.cpp:1183 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

20200916182915650 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182915811 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182915936 DTBF tbf.cpp:806 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1156285, TS=3 (curr FN 1156350)

20200916182915936 DTBF tbf.cpp:877 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Timeout for polling PACKET DOWNLINK ACK.

20200916182915936 DTBF tbf.cpp:1177 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Assignment was on PACCH

20200916182915936 DTBF tbf.cpp:1183 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Downlink AC K was received

20200916182915973 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182916152 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182916309 DTBFDL tbf_dl.cpp:438 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) Restarting at BSN 1274, because the window is stalled.

20200916182916315 DTBF tbf.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 tbf.cpp:647 TBF(TFI=0 TLLI=0xd0176e02 DIR=DL STATE=FLOW EGPRS) T3195 timeout expired, freeing TBF

20200916182921434 DBSSGP gprs_bssgp_bss.c:64 BSSGP (BVCI=0) Tx SUSPEND (TLLI=0xe7daadb8) Assert failed pdch != NULL /git/osmo-pcu/src/encoding.cpp:562 backtrace() returned 21 addresses

/usr/lib/libc.so.6(__libc_start_main+0xf2) [0x7ffff5a31152]
/build/new/out/bin/osmo-pcu(main+0x2bb6) [0x555555748196]
/usr/lib/libc.so.6(__libc_start_main+0xf2) [0x7ffff5a31152]
The assert failing:

```c
/* 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_rlmac_tbf *tbf)
{
    const struct gprs_rlmac_pdch *pdch;
    Direct_encoding_1_t fh_params;

    /* Check one PDCH, if it's hopping then all other should too */
```
It happened a few seconds after stopping osmo-bts-trx with gdb.

```
(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 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe37fcdf2, IMSI=90170000015256, TA=0, 12/12,) Rx Measurement Report: NCI Serv -50 dbm
20200916184620598 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xd90756fa, IMSI=901700000015254, TA=0, 12/12,) Rx Measurement Report: NCI Serv -49 dbm
20200916184621657 DLRCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe37fcdf2, IMSI=901700000015256, TA=0, 12/12, UL) UL RSSI: -12 dbm
```

```
20200916184620436 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe37fcdf2, IMSI=90170000015256, TA=0, 12/12,) Rx Measurement Report: NCI Serv -50 dbm
20200916184620598 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xd90756fa, IMSI=901700000015254, TA=0, 12/12,) Rx Measurement Report: NCI Serv -49 dbm
20200916184621657 DLRCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe37fcdf2, IMSI=901700000015256, TA=0, 12/12, UL) UL RSSI: -12 dbm
```

```
20200916184620436 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe37fcdf2, IMSI=90170000015256, TA=0, 12/12,) Rx Measurement Report: NCI Serv -50 dbm
20200916184620598 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xd90756fa, IMSI=901700000015254, TA=0, 12/12,) Rx Measurement Report: NCI Serv -49 dbm
20200916184621657 DLRCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe37fcdf2, IMSI=901700000015256, TA=0, 12/12, UL) UL RSSI: -12 dbm
```

```
20200916184620436 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe37fcdf2, IMSI=90170000015256, TA=0, 12/12,) Rx Measurement Report: NCI Serv -50 dbm
20200916184620598 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xd90756fa, IMSI=901700000015254, TA=0, 12/12,) Rx Measurement Report: NCI Serv -49 dbm
20200916184621657 DLRCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe37fcdf2, IMSI=901700000015256, TA=0, 12/12, UL) UL RSSI: -12 dbm
```

```
20200916184620436 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe37fcdf2, IMSI=90170000015256, TA=0, 12/12,) Rx Measurement Report: NCI Serv -50 dbm
20200916184620598 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xd90756fa, IMSI=901700000015254, TA=0, 12/12,) Rx Measurement Report: NCI Serv -49 dbm
20200916184621657 DLRCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe37fcdf2, IMSI=901700000015256, TA=0, 12/12, UL) UL RSSI: -12 dbm
```

```
20200916184620436 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe37fcdf2, IMSI=90170000015256, TA=0, 12/12,) Rx Measurement Report: NCI Serv -50 dbm
20200916184620598 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xd90756fa, IMSI=901700000015254, TA=0, 12/12,) Rx Measurement Report: NCI Serv -49 dbm
20200916184621657 DLRCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe37fcdf2, IMSI=901700000015256, TA=0, 12/12, UL) UL RSSI: -12 dbm
```

```
20200916184620436 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe37fcdf2, IMSI=90170000015256, TA=0, 12/12,) Rx Measurement Report: NCI Serv -50 dbm
20200916184620598 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xd90756fa, IMSI=901700000015254, TA=0, 12/12,) Rx Measurement Report: NCI Serv -49 dbm
20200916184621657 DLRCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe37fcdf2, IMSI=901700000015256, TA=0, 12/12, UL) UL RSSI: -12 dbm
```

```
20200916184620436 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe37fcdf2, IMSI=90170000015256, TA=0, 12/12,) Rx Measurement Report: NCI Serv -50 dbm
20200916184620598 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xd90756fa, IMSI=901700000015254, TA=0, 12/12,) Rx Measurement Report: NCI Serv -49 dbm
20200916184621657 DLRCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe37fcdf2, IMSI=901700000015256, TA=0, 12/12, UL) UL RSSI: -12 dbm
```

```
20200916184620436 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe37fcdf2, IMSI=90170000015256, TA=0, 12/12,) Rx Measurement Report: NCI Serv -50 dbm
20200916184620598 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xd90756fa, IMSI=901700000015254, TA=0, 12/12,) Rx Measurement Report: NCI Serv -49 dbm
20200916184621657 DLRCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe37fcdf2, IMSI=901700000015256, TA=0, 12/12, UL) UL RSSI: -12 dbm
```

```
20200916184620436 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xe37fcdf2, IMSI=90170000015256, TA=0, 12/12,) Rx Measurement Report: NCI Serv -50 dbm
20200916184620598 DLRCMACMEAS gprs_rlcmac_meas.cpp:46 MS(TLLI=0xd90756fa, IMSI=901700000015254, TA=0, 12/12,) Rx Measurement Report: NCI Serv -49 dbm
20200916184621657 DLRCMACMEAS gprs_rlcmac_meas.cpp:108 MS(TLLI=0xe37fcdf2, IMSI=901700000015256, TA=0, 12/12, UL) UL RSSI: -12 dbm
```
Program received signal SIGABRT, Aborted.
0x00007ffff5a46615 in raise () from /usr/lib/libc.so.6
(gdb) bt
#0 0x00007ffff5a46615 in raise () from /usr/lib/libc.so.6
#1 0x00007ffff5a2f862 in abort () from /usr/lib/libc.so.6
#2 0x00007ffff6a019c2 in osmo_panic_default (fmt=0x5555558a3940 "Assert failed %s %s:%d
", args=0x7fffffffdd340) 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=-1 '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/libosmocore/src/panic.c:1372
#7 0x0000555555827153 in sched_select_ctlr_msg (trx=0 '000', ts=7 'a', fn=561734, block_nr=7 'a', pdcch=0x5555555b11800 <s_bts+4320>, ul_ass_tbf=0x7fffff21bb860, dl_ass_tbf=0x0, ul_ack_tbf=0x0) -- Type <RET> for more, c to quit, c to continue without paging-- at /git/osmo-pcu/src/gprs_rlcmac_sched.cpp:427
#8 0x00005555558229267 in gprs_rlcmac_rcv_rts_block (bts=0x5555555b10728 <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_req_pdtch (trx=0 '000', ts=7 'a', fn=561734, block_nr=7 'a') at /git/osmo-pcu/src/pcu_l1_if.cpp:386
#10 0x00005555557c756 in pcu_rx_rts_req (rts_req=0x7fffffffdfaf4) at /git/osmo-pcu/src/pcu_l1_if.cpp:420
#11 0x0000555555785ba8 in pcu_rx (mag_type=16 '020', pcu_prim=0x7fffffffdfaf0) at /git/osmo-pcu/src/pcu_l1_if.cpp:765
#12 0x000055555581937f in pcu_sock_read (bfid=0x5555555b1a3e0 <pcu_sock_state>) at /git/osmo-pcu/src/osmobts_sock.cpp:141
#13 0x0000555555819a6c in pcu_sock_cb (bfid=0x5555555b1a3e0 <pcu_sock_state>, flags=1) at /git/osmo-pcu/src/osmobts_sock.cpp:196
#14 0x00007fffffff9d0a in osmo_fd_disp_fds (_reset=0x7fffffffdd0, __reset=0x7fffffffdd00) at /git/libosmocore/src/select.c:227
#15 0x00007fffffff9654 in osmo_select_main (polling=0) at /git/libosmocore/src/select.c:227
#16 0x00007fffffff9741 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 0x0000555555748196 in main (argc=7, argv=0x7fffffffef8) at /git/osmo-pcu/src/pcu_main.cpp:357

03/09/2022 0/9/2022 7/9
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;
}
```

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.

I have been looking at this for a while and there's definitely a bug with TS allocation producing a later crash, but I'm still unsure at what's exactly the issue.

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 DRLCMAC gprs_rlcmac_ts_alloc.cpp:225 Attaching TBF tbf->pdch[3] = 0x555555b1e360
20200922184517884 DTBF tbf.cpp:539 TBF(TFI=1 TLLI=0x00000000 DIR=UL STATE=NULL EGPRS) Setting Control TS 3
20200922184517884 DTBF tbf.cpp:952 TBF(TFI=1 TLLI=0xf99b124d DIR=UL STATE=ASSIGN EGPRS) Allocated: trx = 0, ul_slots = 08, dl_slots = 00
20200922184517893 DTBFUL tbf_ul.cpp:613 TBF(TFI=1 TLLI=0xf99b124d DIR=UL STATE=NULL EGPRS) setting EGPRS UL window size to 64, base(64) slots(1) ws_pdch(0)
```

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