When osmo-bts-trx is started with option `-i` (osmo-bts-trx -c ./osmo-bts.cfg -i 127.0.0.1), then it fails with SIGABRT (or Segmentation Fault without GDB). The problem is most likely related to an msgb that is too small.
Mon Aug 15 14:43:21 2022 <0006> l1sap.c:1942 (bts=0,trx=0,ts=7,ss=0) Activating channel PDCH on TS7
Mon Aug 15 14:43:21 2022 <0006> scheduler.c:1099 (bts=0,trx=0,ts=7,ss=0) Activating PDTCH
Mon Aug 15 14:43:21 2022 <0006> scheduler.c:1099 (bts=0,trx=0,ts=7,ss=0) Activating PTCCH
Mon Aug 15 14:43:21 2022 <0006> lchan.c:271 (bts=0,trx=0,ts=7,ss=0) state NONE -> ACTIVE
Mon Aug 15 14:43:21 2022 <0006> l1sap.c:837 (bts=0,trx=0,ts=7,ss=0) activate confirm chan_nr=PDCH on TS7 trx=0
Mon Aug 15 14:43:21 2022 <0000> rsl.c:1389 (bts=0,trx=0,ts=7,ss=0) not sending CHAN ACT ACK
Mon Aug 15 14:43:21 2022 <0011> input/ipa.c:139 127.0.0.1:3002 connected write
Mon Aug 15 14:43:21 2022 <0009> pcu_sock.c:680 Data request received: sapi=PDTCH arfcn=868 block=11 data=
msgb(0x55555558a3a30): Not enough tailroom msgb_put (allocated 52904, head at 0, len 16, tailroom 53024 < want tailroom 1432604448)
backtrace() returned 22 addresses
/usr/local/lib/libosmocore.so.19(osmo_generate_backtrace+0x18) [0x7ffff7e15e23]
/usr/local/lib/libosmocore.so.19(osmo_panic+0xca) [0x7ffff7e15bd0]
/usr/local/lib/libosmocore.so.19(gsmtap_make_msg_ex+0x110) [0x7ffff7e1533f]
/usr/local/lib/libosmocore.so.19(gsmtap_send_ex+0x88) [0x7ffff7e1563e]
/usr/local/lib/libosmocore.so.19(gsmtap_send+0x79) [0x7ffff7e156fa]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xeb) [0x7ffff7c1309b]
/usr/local/bin/osmo-bts-trx(+0x5a5f1) [0x5555555ae5f1]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0x1eb) [0x7ffff7c1309b]
/lib/local/bin/osmo-bts-trx(+0x1d4a) [0x55555556114a]
Program received signal SIGABRT, Aborted.
__GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
50 ..//sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb)

History
#1 - 08/30/2022 09:33 AM - pespin
Mon Aug 15 14:43:21 2022 <0009> pcu_sock.c:680 Data request received: sapi=PDTCH arfcn=868 block=11 data=
msgb(0x55555558a3a30): Not enough tailroom msgb_put (allocated 52904, head at 0, len 16, tailroom 53024 < want tailroom 1432604448)

Looks like something is wrong with that size 1432604448. This size should be rejected even before trying to allocate a msgb for it. So the problem is not the msgb being too small, it's a size totally unrealistic being passed. Maybe a negative number converted to unsigned?

#2 - 08/30/2022 09:35 AM - pespin
dexter can you provide more information on the versions, setup, etc. you were using when having this crash?

09/22/2022 2/2