OsmoBSC - Bug #3744

include/osmocom/bsc/gsm_data.h: OSMO_ASSERT(conn->lchan); failed in conn_get_bts()

12/30/2018 10:39 AM - fixeria

Status:	New	**Start date:**	12/30/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

Please see the core dumps and logs attached.

```
(gdb) bt
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
#1  0x00007f762ea0a51a in __GI_abort () at abort.c:118
#2  0x00007f762f3e6100 in osmo_panic_default (args=0x7ffd827b4328, fmt=0x564cf83183c2 "Assert fail
ed %s %s:%d\n")
    at ../../../src/libosmocore/src/panic.c:49
#3  osmo_panic (fmt=fmt@entry=0x564cf83183c2 "Assert failed %s %s:%d\n") at ../../../src/libosmoco
re/src/panic.c:84
#4  0x0000564cf82a6ff9 in conn_get_bts (conn=<optimized out>) at ../../../../src/osmo-bsc/include/
osmocom/bsc/gsm_data.h:1276
#5  0x0000564cf8303c54 in conn_get_bts (conn=0x564cf9720650) at ../../../../src/osmo-bsc/src/osmo-
bsc/osmo_bsc_bssap.c:417
#6  bssmap_handle_cipher_mode (conn=conn@entry=0x564cf9720650, payload_length=payload_length@entry
=12, msg=<optimized out>)
    at ../../../../src/osmo-bsc/src/osmo-bsc/osmo_bsc_bssap.c:479
#7  0x0000564cf83053e6 in bssmap_rcvmsg_dt1 (length=12, msg=0x564cf96e8f50, conn=0x564cf9720650)
    at ../../../../src/osmo-bsc/src/osmo-bsc/osmo_bsc_bssap.c:880
#8  bsc_handle_dt (conn=conn@entry=0x564cf9720650, msg=0x564cf96e8f50, len=14) at ../../../../src/
osmo-bsc/src/osmo-bsc/osmo_bsc_bssap.c:1005
#9  0x0000564cf830c27a in handle_data_from_msc (msg=<optimized out>, conn=0x564cf9720650)
    at ../../../../src/osmo-bsc/src/osmo-bsc/osmo_bsc_sigtran.c:134
#10 sccp_sap_up (oph=0x564cf96e8fd8, _scu=<optimized out>) at ../../../../src/osmo-bsc/src/osmo-bs
c/osmo_bsc_sigtran.c:245
#11 0x00007f762f3e0553 in _osmo_fsm_inst_dispatch (fi=0x564cf971e4d0, event=11, data=data@entry=0x
564cf9768960,
    file=file@entry=0x7f762efa1668 "../../../src/libosmo-sccp/src/sccp_scoc.c", line=line@entry=16
70) at ../../../src/libosmocore/src/fsm.c:580
#12 0x00007f762ef918fc in sccp_scoc_rx_from_scrc (inst=inst@entry=0x564cf9672200, xua=xua@entry=0x
564cf9768960)
    at ../../../src/libosmo-sccp/src/sccp_scoc.c:1670
#13 0x00007f762ef8f452 in scrc_rx_mtp_xfer_ind_xua (inst=inst@entry=0x564cf9672200, xua=0x564cf976
8960)
    at ../../../src/libosmo-sccp/src/sccp_scrc.c:457
#14 0x00007f762ef924c5 in mtp_user_prim_cb (oph=0x564cf976d058, ctx=0x564cf9672200) at ../../../sr
c/libosmo-sccp/src/sccp_user.c:176
#15 0x00007f762ef8a802 in m3ua_rx_xfer (xua=0x564cf9726b40, asp=0x564cf9629350) at ../../../src/li
bosmo-sccp/src/m3ua.c:586
#16 m3ua_rx_msg (asp=asp@entry=0x564cf9629350, msg=msg@entry=0x564cf975ffc0) at ../../../src/libos
mo-sccp/src/m3ua.c:739
#17 0x00007f762ef9873b in xua_cli_read_cb (conn=0x564cf96720b0) at ../../../src/libosmo-sccp/src/o
smo_ss7.c:1607
#18 0x00007f762e2323db in osmo_stream_cli_read (cli=0x564cf96720b0) at ../../../src/libosmo-netif/
src/stream.c:192
#19 osmo_stream_cli_fd_cb (ofd=<optimized out>, what=1) at ../../../src/libosmo-netif/src/stream.c
:276
#20 0x00007f762f3dc8ae in osmo_fd_disp_fds (_eset=0x7ffd827b5890, _wset=0x7ffd827b5810, _rset=0x7f
fd827b5790)
    at ../../../src/libosmocore/src/select.c:217
```

```
#21 osmo_select_main (polling=<optimized out>) at ../../../src/libosmocore/src/select.c:257
#22 0x0000564cf82a7c77 in main (argc=<optimized out>, argv=<optimized out>) at ../../../../src/osm
o-bsc/src/osmo-bsc/osmo_bsc_main.c:932
```

Files

osmo_bsc_6655.dump.gz	449 KB	12/30/2018	fixeria
osmo_bsc_22008.dump.gz	466 KB	12/30/2018	fixeria
osmo-bsc.18-12-29--23-02-43.log	681 KB	12/30/2018	fixeria
osmo-bsc.18-12-29--23-32-54.log	676 KB	12/30/2018	fixeria