libosmocore - Bug #1760

LAPD: segfault in T200 call-back

07/03/2016 02:18 PM - laforge

Status:	Closed	**Start date:**	07/03/2016
Priority:	Normal	**Due date:**	
Assignee:	laforge	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

```
<001c> input/lapd.c:628 LAPD DL-RELEASE indication TEI=62 SAPI=62
<001c> lapd_core.c:378 sending MDL-ERROR-IND cause 1
Program received signal SIGSEGV, Segmentation fault.
0xb7f87783 in lapd_dl_flush_hist (dl=<optimized out>, dl=<optimized out>) at lapd_core.c:162
162                     if (dl->tx_hist[i].msg) {
(gdb) p dl
$1 = <optimized out>
(gdb) bt
#0  0xb7f87783 in lapd_dl_flush_hist (dl=<optimized out>, dl=<optimized out>) at lapd_core.c:162
#1  0xb7f892cd in lapd_t200_cb (data=0x8194230) at lapd_core.c:581
#2  0xb7f5a99b in osmo_timers_update () at timer.c:244
#3  0xb7f5b0e3 in osmo_select_main (polling=0) at select.c:188
#4  0x0804d575 in main (argc=3, argv=0xbffffd44) at bsc_hack.c:375
```

further inspection discovers:

- dl->tx_hist == NULL
- dl->range_hist = 2

Related issues:

Related to OsmoBSC - Bug #1761: LAPD: segfault when bootstrapping Nokia InSite	**Resolved**	**07/03/2016**
Related to libosmocore - Bug #1762: Review LAPD code for race conditions rega...	**New**	**07/03/2016**
Related to libosmocore - Bug #4646: SEGV when bringing up Nokia InSite	**Resolved**	**07/04/2020**

History

#1 - 07/03/2016 02:20 PM - laforge

- Status changed from New to In Progress

So it seems T200 is expiring, but the tx_hist array is NULL at that point.

tx_hist is allocated in lapd_dl_init() and set to NULL in lapd_dl_exit().

The latter appears to be executed before the crash:

```
Breakpoint 1, lapd_dl_exit (dl=0x8194230) at lapd_core.c:319
319     {
(gdb) bt
#0  lapd_dl_exit (dl=0x8194230) at lapd_core.c:319
#1  0xb7f257d3 in lapd_sap_free (sap=0x8194220) at input/lapd.c:249
#2  0xb7f26996 in send_dlsap (dp=0xbffffa14, lctx=0x8194254) at input/lapd.c:629
#3  0xb7f892ba in send_dl_l3 (msg=<optimized out>, lctx=<optimized out>, op=<optimized out>, prim=<optimized o
ut>) at lapd_core.c:359
#4  send_dl_simple (lctx=<optimized out>, op=<optimized out>, prim=<optimized out>) at lapd_core.c:368
#5  lapd_t200_cb (data=0x8194230) at lapd_core.c:577
#6  0xb7f5a99b in osmo_timers_update () at timer.c:244
#7  0xb7f5b0e3 in osmo_select_main (polling=0) at select.c:188
#8  0x0804d575 in main (argc=3, argv=0xbffffd44) at bsc_hack.c:375
```

#2 - 07/03/2016 04:52 PM - laforge

- File flush.diff added

- % Done changed from 0 to 50

attached diff fixes the crash, but I'm facing other LAPD related issues, not submitting until it is clear.

#3 - 07/03/2016 06:48 PM - laforge

- Status changed from In Progress to Closed

- % Done changed from 50 to 100

submitted as https://gerrit.osmocom.org/451

#4 - 07/03/2016 08:17 PM - laforge

- Related to Bug #1761: LAPD: segfault when bootstrapping Nokia InSite added

#5 - 07/03/2016 08:20 PM - laforge

- Related to Bug #1762: Review LAPD code for race conditions regarding state, particularly in RELEASE added

#6 - 07/04/2020 08:44 AM - laforge

- Related to Bug #4646: SEGV when bringing up Nokia InSite added

Files

flush.diff	378 Bytes	07/03/2016	laforge