libosmocore - Bug #1982

LAPD: segfault in lapd_est_req function

03/14/2017 02:54 PM - kluchnikov

Status:	Resolved	**Start date:**	03/14/2017
Priority:	Normal	**Due date:**	
Assignee:	laforge	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

This issue occurs once a day on one of loaded BTS (osmo-bts-trx is used).
It seems that this issue is related with #1760#1761#1762.
As you can see it crashes in lapd_est_req funtion on line:

```
lapd_core.c 1769: dl->tx_hist[0].msg = lapd_msgb_alloc(msg->len, "HIST");
```

because dl->tx_hist = 0x0 at this point.

The cause of this issue is not obvious for me, so any help will be appreciated.

See full backtrace below.

```
#0  0x00007f46ecd99aa5 in lapd_est_req (dp=<optimized out>, lctx=0x7f46ed80b8b8) at lapd_core.c:17
69
        dl = 0x7f46ed80b888
        msg = 0x7f46eeab4940
        nctx = {dl = 0x7f46ed80b888, n201 = 20, cr = 1 '\001', sapi = 3 '\003', tei = 0 '\000', lp
d = 0 '\000', format = 3 '\003', p_f = 1 '\001', n_send = 0 '\000',
          n_recv = 0 '\000', s_u = 7 '\a', length = 0, more = 0 '\000'}
#1  0x00007f46ecd9dda8 in rslms_rx_rll_est_req (msg=msg@entry=0x7f46eeab4940, dl=dl@entry=0x7f46ed
80b888) at lapdm.c:845
        rllh = <optimized out>
        chan_nr = <optimized out>
        link_id = <optimized out>
        sapi = <optimized out>
        tv = {lv = {{len = 0, val = 0x0} <repeats 256 times>}}
        length = 0 '\000'
        n201 = 20 '\024'
        dp = {oph = {sap = 0, primitive = 2, operation = PRIM_OP_REQUEST, msg = 0x7f46eeab4940}, u
 = {error_ind = {cause = 1 '\001'}, rel_req = {mode = 1 '\001'}}}
#2  0x00007f46ecd9fc03 in rslms_rx_rll (lc=0x7f46ed80b398, msg=0x7f46eeab4940) at lapdm.c:1157
        rllh = <optimized out>
        msg_type = 4
        dl = 0x7f46ed80b888
        sapi = 3 '\003'
        le = <optimized out>
        rc = 0
#3  lapdm_rslms_recvmsg (msg=0x7f46eeab4940, lc=0x7f46ed80b398) at lapdm.c:1223
        rslh = <optimized out>
#4  0x00007f46ed63773d in rsl_rx_rll (msg=<optimized out>, trx=<optimized out>) at rsl.c:2178
        rh = <optimized out>
        lchan = <optimized out>
#5  down_rsl (trx=<optimized out>, msg=<optimized out>) at rsl.c:2541
        rslh = <optimized out>
        ret = 0
#6  0x00007f46ed641529 in sign_link_cb (msg=<optimized out>) at abis.c:169
        link = <optimized out>
#7  0x00007f46ec54b111 in ipaccess_bts_read_cb (link=0x7f46eeab4940, msg=0x0) at input/ipaccess.c:
807
```

```
        hh = 0x1
        e1i_ts = <optimized out>
        sign_link = <optimized out>
        ret = -290764341
#8  0x00007f46ec548a8e in ipa_client_read (link=0x7f46ee26ae30) at input/ipa.c:74
        ofd = 0x7f46ee25ce18
        msg = 0x7f46eeab4940
        ret = <optimized out>
#9  ipa_client_fd_cb (ofd=<optimized out>, what=1) at input/ipa.c:137
        link = 0x7f46ee26ae30
        error = -290764480
        ret = <optimized out>
        len = 4
#10 0x00007f46ecfc726f in osmo_fd_disp_fds (_eset=0x7ffe7a9fcd20, _wset=0x7ffe7a9fcca0, _rset=0x7f
fe7a9fcc20) at select.c:167
        flags = 1
        ufd = 0x7f46ee25ce18
        tmp = 0x7f46ee25d3f0
        work = 1
#11 osmo_select_main (polling=polling@entry=0) at select.c:207
        readset = {__fds_bits = {0 <repeats 16 times>}}
        writeset = {__fds_bits = {0 <repeats 16 times>}}
        exceptset = {__fds_bits = {0 <repeats 16 times>}}
        rc = <optimized out>
        no_time = {tv_sec = 0, tv_usec = 0}
#12 0x00007f46ed63fc25 in bts_main (argc=5, argv=<optimized out>) at main.c:359
        btsb = 0x7f46ee22f6b0
        trx = <optimized out>
        line = <optimized out>
        rc = <optimized out>
        i = <optimized out>
#13 0x00007f46ebd76f45 in __libc_start_main (main=0x7f46ed61b120 <main>, argc=5, argv=0x7ffe7a9fcf
18, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>,
    stack_end=0x7ffe7a9fcf08) at libc-start.c:287
        result = <optimized out>
        unwind_buf = {cancel_jmp_buf = {{jmp_buf = {0, 4313346456460387904, 139942607040805, 14073
0955714320, 0, 0, -4314201601083251136, -4228385196325935552}, mask_was_saved = 0}},
          priv = {pad = {0x0, 0x0, 0x7ffe7a9fcf48, 0x7f46ed60f1c8}, data = {prev = 0x0, cleanup =
0x0, canceltype = 2057293640}}}
        not_first_call = <optimized out>
#14 0x00007f46ed61b14e in _start ()

(gdb) print *dl
$2 = {send_dlsap = 0x7f46ecd9e600 <send_rslms_dlsap>, send_ph_data_req = 0x7f46ecd9e3f0 <lapdm_sen
d_ph_data_req>, update_pending_frames = 0x7f46ecd9dad0 <update_pending_frames>, cr = {
    loc2rem = {cmd = 1 '\001', resp = 0 '\000'}, rem2loc = {cmd = 0 '\000', resp = 1 '\001'}}, mod
e = LAPD_MODE_NETWORK, use_sabme = 0, reestablish = 0, n200 = 23, n200_est_rel = 5,
  lctx = {dl = 0x7f46ed80b888, n201 = 20, cr = 0 '\000', sapi = 3 '\003', tei = 0 '\000', lpd = 0
'\000', format = 0 '\000', p_f = 0 '\000', n_send = 0 '\000', n_recv = 0 '\000',
    s_u = 0 '\000', length = 0, more = 0 '\000'}, maxf = 200, k = 1 '\001', v_range = 8 '\b', v_se
nd = 3 '\003', v_ack = 2 '\002', v_recv = 0 '\000', state = 4, seq_err_cond = 0,
  own_busy = 0 '\000', peer_busy = 0 '\000', t200_sec = 1, t200_usec = 0, t203_sec = 0, t203_usec
= 0, t200 = {node = {rb_parent_color = 139942619707121, rb_right = 0x7f46ee23f158,
      rb_left = 0x0}, list = {next = 0x7f46ed80b918, prev = 0x7f46ed80b918}, timeout = {tv_sec = 1
489476828, tv_usec = 792795}, active = 0, cb = 0x7f46ecd9acb0 <lapd_t200_cb>,
    data = 0x7f46ed80b888}, t203 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, l
ist = {next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0}, active = 0,
    cb = 0x7f46ecd996c0 <lapd_t203_cb>, data = 0x7f46ed80b888}, retrans_ctr = 5 '\005', tx_queue =
 {next = 0x7f46ed80b9a8, prev = 0x7f46ed80b9a8}, send_queue = {next = 0x7f46ed80b9b8,
    prev = 0x7f46ed80b9b8}, send_buffer = 0x0, send_out = 49, tx_hist = 0x0, range_hist = 2 '\002'
, rcv_buffer = 0x0, cont_res = 0x0}
```

Related issues:

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**
Related to OsmoBSC - Bug #1761: LAPD: segfault when bootstrapping Nokia InSite	**Resolved**	**07/03/2016**

History

#1 - 03/14/2017 03:40 PM - laforge

can you please specify which particular git versions of libosmocore and
osmo-bts were used while observing this issue?

#2 - 03/15/2017 07:58 AM - kluchnikov

libosmocore: (Feb 7, 2017) 6b986c24228a4cc83b22e1d8aae22b94fe36e6f2 [lapd_core: Fix MDL-ERROR ind after RELEASE ind]

osmo-bts: (Feb 20, 2017) 64d16028eb7d38bb442591c6c0224ae28eb3e2be [oml: Fix incorrect usage of const variable abis_nm_att_tlvdef_ipa]

#3 - 03/15/2017 09:09 AM - laforge

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

#4 - 03/15/2017 09:15 AM - laforge

In general, the problem you're encountering means that lapd_est_req
(i.e. an ESTABLISH REQUEST) is called on a LAPD data link which has not
been initialized before (via lapd_dl_init()).

lapd_dl_init() allocates the dl_hist[] array, and lapd_dl_exit()
releases the associated memory.

From the direction (BSC->BTS) and the SAPI value you can see that it is
establishment for SMS, in the MT direction.

So it seems that somehow somebody calls lapdm_channel_exit() or
lapdm_entity_exit() or lapd_dl_exit() before attempting to establish a
SAPI=3 in donwlink.

OsmoBTS calls lapdm_channel_exit() from rsl_tx_rf_rel_ack(), so
basically it means that we get an RSL "RF CHANNEL RELEASE" and process
that before receiving an RLL EST REQ (SAPI=3) on Abis, which is of
course invalid.

Nevertheles, the lapd_core code should be extended with a new state
(one even efore LAPD_STATE_NULL), so that the STATE_NULL is only entered
when lapd_dl_init() was successful, and that all function calls will
first check if the state is >= LAPD_STATE_NULL?

It would of course be super-awesome if somebody actually went for
osmo_fsm conversion of lapd_core, but that might be a bit too much
effort for "just" fixing the bug.

#5 - 07/18/2019 05:49 AM - laforge

- Priority changed from Normal to High

#6 - 12/01/2019 10:14 AM - laforge

- Status changed from New to Stalled

- Assignee set to laforge

- Priority changed from High to Normal

#7 - 07/04/2020 08:21 AM - laforge

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

#8 - 07/14/2020 06:18 PM - laforge

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

#9 - 07/14/2020 06:19 PM - laforge

- Status changed from Stalled to Resolved

- % Done changed from 0 to 100

addressed by https://gerrit.osmocom.org/c/libosmocore/+/19130