OsmoBTS - Bug #3702

osmo-bts-sysmo crash

11/21/2018 09:29 PM - msuraev

Status:	Resolved	**Start date:**	11/21/2018
Priority:	Normal	**Due date:**	
Assignee:	msuraev	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

Hit the following with latest nightly sysmocom-core-image-sysmobts-v2-20181121054638.rootfs.ubi on sysmobts:

```
#0  llist_count (head=head@entry=0xb6c9ad50) at /usr/include/osmocom/core/linuxlist.h:394
#1  queue_limit_to (prefix=0xa91e0 "(bts=0,trx=0,ts=1,ss=0)", queue=queue@entry=0xb6c9ad50, limit=
1)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/common/l1sap.c:152
#2  0x0003a47c in l1sap_rtp_rx_cb (rs=rs@entry=0x1240d0, rtp_pl=0xb6c3c734 "\330 \242\341ZP", rtp_
pl_len=rtp_pl_len@entry=33,
    seq_number=<optimized out>, timestamp=898524770, marker=false)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/common/l1sap.c:1444
#3  0xb6fe8c60 in recv_with_cb (rs=0x1240d0)
    at /usr/src/debug/libosmo-abis/0.5.1+gitrAUTOINC+de5758d307-r0.18.0/git/src/trau/osmo_ortp.c:1
85
#4  osmo_rtp_socket_poll (rs=0x1240d0)
    at /usr/src/debug/libosmo-abis/0.5.1+gitrAUTOINC+de5758d307-r0.18.0/git/src/trau/osmo_ortp.c:2
02
#5  0x000387cc in l1sap_tch_rts_ind (l1sap=0x1271a4, rts_ind=0x1271b4, rts_ind=0x1271b4, trx=0xb6c
7b038)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/common/l1sap.c:931
#6  l1sap_up (trx=trx@entry=0xb6c7b038, l1sap=0x1271a4)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/common/l1sap.c:1351
#7  0x00015dbc in handle_ph_data_ind (l1p_msg=<optimized out>, data_ind=<optimized out>, fl1=<opti
mized out>)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/osmo-bts-sysmo/l1_if.c:98
7
#8  l1if_handle_ind (fl1=<optimized out>, msg=0x1270e0)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/osmo-bts-sysmo/l1_if.c:11
09
#9  0x00016b74 in l1if_handle_l1prim (wq=wq@entry=1, fl1h=<optimized out>, msg=<optimized out>)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/osmo-bts-sysmo/l1_if.c:11
66
#10 0x000211b4 in read_dispatch_one (queue=1, msg=<optimized out>, fl1h=<optimized out>)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/osmo-bts-sysmo/l1_transp_
hw.c:191
#11 l1if_fd_cb (ofd=0x1070a8, what=<optimized out>)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/osmo-bts-sysmo/l1_transp_
hw.c:231
#12 0x45c87d48 in osmo_fd_disp_fds (_eset=0xbefffb10, _wset=0xbefffa90, _rset=0xbefffa10)
    at /usr/src/debug/libosmocore/0.12.1+gitrAUTOINC+c8772517d9-r0/git/src/select.c:217
#13 osmo_select_main (polling=polling@entry=0)
    at /usr/src/debug/libosmocore/0.12.1+gitrAUTOINC+c8772517d9-r0/git/src/select.c:257
#14 0x0003b384 in bts_main (argc=<optimized out>, argv=<optimized out>)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/common/main.c:354
#15 0x455f7c18 in __libc_start_main (main=0xbefffd54, argc=1165112320, argv=0x455f7c18 <__libc_sta
rt_main+276>,
    init=<optimized out>, fini=0x3e92c <__libc_csu_fini>, rtld_fini=0x455b07d0 <_dl_fini>, stack_e
nd=0xbefffd54)
    at /usr/src/debug/glibc/2.25-r0/git/csu/libc-start.c:295
#16 0x00014280 in _start () at ../sysdeps/arm/start.S:124
```

```
Backtrace stopped: previous frame identical to this frame (corrupt stack?)
```

Not sure how reliable is the trace though.
Just in case, extended version:

```
#0  llist_count (head=head@entry=0xb6c9ad50) at /usr/include/osmocom/core/linuxlist.h:394
        entry = 0x0
        i = 0
#1  queue_limit_to (prefix=0xa91e0 "(bts=0,trx=0,ts=1,ss=0)", queue=queue@entry=0xb6c9ad50, limit=
1)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/common/l1sap.c:152
        count = <optimized out>
#2  0x0003a47c in l1sap_rtp_rx_cb (rs=rs@entry=0x1240d0, rtp_pl=0xb6c3c734 "\330 \242\341ZP", rtp_
pl_len=rtp_pl_len@entry=33,
    seq_number=<optimized out>, timestamp=898524770, marker=false)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/common/l1sap.c:1444
        lchan = 0xb6c9a88c
        msg = 0x126b10
#3  0xb6fe8c60 in recv_with_cb (rs=0x1240d0)
    at /usr/src/debug/libosmo-abis/0.5.1+gitrAUTOINC+de5758d307-r0.18.0/git/src/trau/osmo_ortp.c:1
85
        payload = 0xb6c3c734 "\330 \242\341ZP"
        mblk = 0xb6c3cd38
        plen = 33
#4  osmo_rtp_socket_poll (rs=0x1240d0)
    at /usr/src/debug/libosmo-abis/0.5.1+gitrAUTOINC+de5758d307-r0.18.0/git/src/trau/osmo_ortp.c:2
02
No locals.
#5  0x000387cc in l1sap_tch_rts_ind (l1sap=0x1271a4, rts_ind=0x1271b4, rts_ind=0x1271b4, trx=0xb6c
7b038)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/common/l1sap.c:931
        resp_msg = <optimized out>
        resp_l1sap = <optimized out>
        empty_l1sap = {oph = {sap = 1171262076, primitive = 1165112320, operation = PRIM_OP_RESPON
SE, msg = 0x126ee0}, u = {
            data = {link_id = 40 '(', chan_nr = 54 '6', fn = 58, rssi = -52 '\314', ber10k = 0, {t
a_offs_qbits = 0,
                ta_offs_256bits = 0}, lqual_cb = 0, pdch_presence_info = PRES_INFO_BOTH}, tch = {c
han_nr = 40 '(', fn = 58,
              rssi = -52 '\314', marker = 1 '\001', ber10k = 0, lqual_cb = 0}, rach_req = {ra = 40
 '(', ta = 54 '6',
              tx_power = 114 'r', is_combined_ccch = 69 'E', offset = 58}, rach_ind = {chan_nr = 4
0 '(', ra = 17778,
              acc_delay = 58 ':', fn = 460, is_11bit = 0 '\000', burst_type = 7, rssi = 0 '\000',
ber10k = 0,
              acc_delay_256bits = 0}, conn_ind = {fn = 1165112872}, info = {type = 1165112872, u =
 {time_ind = {fn = 58},
                meas_ind = {chan_nr = 58 ':', fn = 460, ber10k = 0, {ta_offs_qbits = 0, ta_offs_25
6bits = 0}, c_i_cb = 7,
                  is_sub = 0 '\000', inv_rssi = 0 '\000'}, act_req = {chan_nr = 58 ':', sacch_only
 = 0 '\000'}, act_cnf = {
                  chan_nr = 58 ':', cause = 0 '\000'}, ciph_req = {chan_nr = 58 ':', downlink = 0
'\000', uplink = 0 '\000'}}}}}
        chan_nr = 9 '\t'
        marker = 0 '\000'
        fn = 22152
        g_time = {fn = 22152, t1 = 16, t2 = 0 '\000', t3 = 18 '\022', tc = 2 '\002'}
        lchan = 0xb6c9a88c
        rc = <optimized out>
#6  l1sap_up (trx=trx@entry=0xb6c7b038, l1sap=0x1271a4)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/common/l1sap.c:1351
        msg = 0x1270e0
        rc = 0
```

```
#7  0x00015dbc in handle_ph_data_ind (l1p_msg=<optimized out>, data_ind=<optimized out>, fl1=<opti
mized out>)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/osmo-bts-sysmo/l1_if.c:98
7
        chan_nr = <optimized out>
        l1sap = <optimized out>
        fn = <optimized out>
        link_id = <optimized out>
        sap_msg = <optimized out>
        g_time = {fn = 412, t1 = 7, t2 = 0 '\000', t3 = 0 '\000', tc = 4 '\004'}
        rc = <optimized out>
#8  l1if_handle_ind (fl1=<optimized out>, msg=0x1270e0)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/osmo-bts-sysmo/l1_if.c:11
09
        l1p = 0x1271a4
        rc = 0
#9  0x00016b74 in l1if_handle_l1prim (wq=wq@entry=1, fl1h=<optimized out>, msg=<optimized out>)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/osmo-bts-sysmo/l1_if.c:11
66
        l1p = <optimized out>
        wlc = <optimized out>
        rc = <optimized out>
#10 0x000211b4 in read_dispatch_one (queue=1, msg=<optimized out>, fl1h=<optimized out>)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/osmo-bts-sysmo/l1_transp_
hw.c:191
No locals.
#11 l1if_fd_cb (ofd=0x1070a8, what=<optimized out>)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/osmo-bts-sysmo/l1_transp_
hw.c:231
        i = 1
        rc = <optimized out>
        prim_size = 216
        count = 2
        iov = {{iov_base = 0x126fd4, iov_len = 216}, {iov_base = 0x1271a4, iov_len = 216}, {iov_ba
se = 0x127374, iov_len = 216}}
        msg = {0x126f10, 0x1270e0, 0x1272b0}
#12 0x45c87d48 in osmo_fd_disp_fds (_eset=0xbefffb10, _wset=0xbefffa90, _rset=0xbefffa10)
    at /usr/src/debug/libosmocore/0.12.1+gitrAUTOINC+c8772517d9-r0/git/src/select.c:217
        flags = <optimized out>
        ufd = <optimized out>
        tmp = <optimized out>
        exceptset = <optimized out>
        work = <optimized out>
        readset = <optimized out>
        writeset = <optimized out>
#13 osmo_select_main (polling=polling@entry=0)
    at /usr/src/debug/libosmocore/0.12.1+gitrAUTOINC+c8772517d9-r0/git/src/select.c:257
        readset = {__fds_bits = {0 <repeats 32 times>}}
        writeset = {__fds_bits = {0 <repeats 32 times>}}
        exceptset = {__fds_bits = {0 <repeats 32 times>}}
        rc = <optimized out>
        no_time = {tv_sec = 0, tv_usec = 0}
#14 0x0003b384 in bts_main (argc=<optimized out>, argv=<optimized out>)
    at /usr/src/debug/osmo-bts/0.8.1+gitAUTOINC+36a61df7a6-r1.18/git/src/common/main.c:354
        trx = <optimized out>
        line = <optimized out>
        rc = <optimized out>
#15 0x455f7c18 in __libc_start_main (main=0xbefffd54, argc=1165112320, argv=0x455f7c18 <__libc_sta
rt_main+276>,
    init=<optimized out>, fini=0x3e92c <__libc_csu_fini>, rtld_fini=0x455b07d0 <_dl_fini>, stack_e
nd=0xbefffd54)
    at /usr/src/debug/glibc/2.25-r0/git/csu/libc-start.c:295
        self = <optimized out>
        result = <optimized out>
        unwind_buf = {cancel_jmp_buf = {{jmp_buf = {415430329, -480087707, 256204, 0, 82516, 0, 0,
 0, 1163722752, 0,
                -1090519912, 1163725492, 9, -1225449864, 1, 0, 1, 1163725144, -1225440604, -122475
```

```
3056, 0, 1163590284,
                -1227512208, 1, 1, 0, -1090519912, 1163805748, 1163725584, 1163725144, -1, 348572,
 1163837700, -1224751664,
                -1090519700, 1163722752, 0, 1163590284, -1227513488, 1, 1, 0, 1, -1225438124, 1163
722752, -1225449864, 0,
                413812, 0, -1227509600, 0, 1163722752, 0, 1163590284, -1225449864, 1, 1, 0, -12251
00144, 1163837700,
                1174014448, 0, 0, 82516}, mask_was_saved = 0}}, priv = {pad = {0x0, 0x0, 0x0,
              0x455b66a0 <_dl_runtime_resolve+24>}, data = {prev = 0x0, cleanup = 0x0, canceltype
= 0}}}
        not_first_call = <optimized out>
#16 0x00014280 in _start () at ../sysdeps/arm/start.S:124
No locals.
Backtrace stopped: previous frame identical to this frame (corrupt stack?)
```

This happens when placing the call between 2 phones connected to the same bts right after it's answered. Nothing out of the ordinary in .pcap or configs/logs so far. Investigation is on-going.

History

#1 - 11/21/2018 09:31 PM - msuraev

On a related note - we don't have tests for llist_* functions in libosmocore. It might make sense to add couple of basic tests just to be on a safe side.

#2 - 11/22/2018 10:39 AM - pespin

- Status changed from New to Feedback

Cause of this crash is lchan->dl_tch_queue being NULL in l1sap_rtp_rx_cb.

I think it should be fixed by osmo-bts 6dacc35c751452f0e94acf15e6fd42ac774c8e53:
https://gerrit.osmocom.org/#/c/osmo-bts/+/11864/

Please msuraev give it a try with latest master, which already contains that commit.

#3 - 11/22/2018 10:45 AM - pespin

Sorry, I expressed myself incorrectly, lchan->dl_tch_queue is not NULL but uninitialized (that is, it's prev and next are NULL).

#4 - 12/18/2018 06:16 PM - msuraev

- Status changed from Feedback to Resolved

- % Done changed from 0 to 100

Fixed indeed.