OsmoBSC - Bug #3446

osmo-bsc hits assertion in osmo_bsc_sigtran.c:351

08/03/2018 01:22 PM - dexter

Status:	Resolved	**Start date:**	08/03/2018
Priority:	Normal	**Due date:**	
Assignee:	dexter	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

When osmo-bsc is started while the stp is unreachable and a phone tries to make an LU, than osmo-bsc crashes:

```
Fri Aug  3 14:20:51 2018 DMSC <0007> fsm.c:189 A-RESET(msc-0)[0x55ca2cae15e0]{DISC}: Timeout of T4
Fri Aug  3 14:20:51 2018 DMSC <0007> a_reset.c:106 A-RESET(msc-0)[0x55ca2cae15e0]{DISC}: (re)sendi
ng BSSMAP RESET message...
Fri Aug  3 14:20:51 2018 DMSC <0007> osmo_bsc_sigtran.c:92 Sending RESET to MSC: RI=SSN_PC,PC=0.23
.1,SSN=BSSAP
Fri Aug  3 14:20:51 2018 DLSS7 <001f> m3ua.c:507 XUA_AS(as-clnt-msc-0)[0x55ca2cae06d0]{AS_DOWN}: E
vent AS-TRANSFER.req not permitted
Fri Aug  3 14:20:51 2018 DMSC <0007> a_reset.c:110 A-RESET(msc-0)[0x55ca2cae15e0]{DISC}: state_chg
 to DISC
Fri Aug  3 14:20:52 2018 DRSL <0003> abis_rsl.c:1057 (bts=0,trx=0,ts=0,ss=0): meas_rep_count++=37
meas_rep_last_seen_nr=36
Fri Aug  3 14:20:52 2018 DRSL <0003> abis_rsl.c:1057 (bts=0,trx=0,ts=0,ss=1): meas_rep_count++=35
meas_rep_last_seen_nr=34
BTS 0 reported connected PCU version 0.5.0
Fri Aug  3 14:20:52 2018 DRSL <0003> abis_rsl.c:1057 (bts=0,trx=0,ts=0,ss=0): meas_rep_count++=38
meas_rep_last_seen_nr=37
Fri Aug  3 14:20:52 2018 DRSL <0003> abis_rsl.c:1057 (bts=0,trx=0,ts=0,ss=1): meas_rep_count++=36
meas_rep_last_seen_nr=35
Fri Aug  3 14:20:53 2018 DRSL <0003> abis_rsl.c:1057 (bts=0,trx=0,ts=0,ss=0): meas_rep_count++=39
meas_rep_last_seen_nr=38
Fri Aug  3 14:20:53 2018 DRSL <0003> abis_rsl.c:1057 (bts=0,trx=0,ts=0,ss=1): meas_rep_count++=37
meas_rep_last_seen_nr=36
Fri Aug  3 14:20:53 2018 DRSL <0003> abis_rsl.c:1057 (bts=0,trx=0,ts=0,ss=0): meas_rep_count++=40
meas_rep_last_seen_nr=39
Fri Aug  3 14:20:53 2018 DRSL <0003> abis_rsl.c:1057 (bts=0,trx=0,ts=0,ss=1): meas_rep_count++=38
meas_rep_last_seen_nr=37
Fri Aug  3 14:20:53 2018 DMSC <0007> fsm.c:189 A-RESET(msc-0)[0x55ca2cae15e0]{DISC}: Timeout of T4
Fri Aug  3 14:20:53 2018 DMSC <0007> a_reset.c:106 A-RESET(msc-0)[0x55ca2cae15e0]{DISC}: (re)sendi
ng BSSMAP RESET message...
Fri Aug  3 14:20:53 2018 DMSC <0007> osmo_bsc_sigtran.c:92 Sending RESET to MSC: RI=SSN_PC,PC=0.23
.1,SSN=BSSAP
Fri Aug  3 14:20:53 2018 DLSS7 <001f> m3ua.c:507 XUA_AS(as-clnt-msc-0)[0x55ca2cae06d0]{AS_DOWN}: E
vent AS-TRANSFER.req not permitted
Fri Aug  3 14:20:53 2018 DMSC <0007> a_reset.c:110 A-RESET(msc-0)[0x55ca2cae15e0]{DISC}: state_chg
 to DISC
Fri Aug  3 14:20:54 2018 DRSL <0003> abis_rsl.c:1057 (bts=0,trx=0,ts=0,ss=0): meas_rep_count++=41
meas_rep_last_seen_nr=40
Fri Aug  3 14:20:54 2018 DRSL <0003> abis_rsl.c:1057 (bts=0,trx=0,ts=0,ss=1): meas_rep_count++=39
meas_rep_last_seen_nr=38
Fri Aug  3 14:20:54 2018 DRSL <0003> abis_rsl.c:1057 (bts=0,trx=0,ts=0,ss=0): meas_rep_count++=42
meas_rep_last_seen_nr=41
Fri Aug  3 14:20:54 2018 DRSL <0003> abis_rsl.c:1057 (bts=0,trx=0,ts=0,ss=1): meas_rep_count++=40
meas_rep_last_seen_nr=39
Fri Aug  3 14:20:54 2018 DMSC <0007> bsc_subscr_conn_fsm.c:631 SUBSCR_CONN[0x55ca2caf1d30]{INIT}:
state_chg to CLEARING
Assert failed conn->sccp.msc osmo_bsc_sigtran.c:351
backtrace() returned 12 addresses
/usr/local/lib/libosmocore.so.11(osmo_panic+0xbb) [0x7ff2f4cad67b]
```

```
/usr/local/bin/osmo-bsc(+0x72684) [0x55ca2bade684]
/usr/local/bin/osmo-bsc(+0x3526c) [0x55ca2baa126c]
/usr/local/bin/osmo-bsc(+0x5d553) [0x55ca2bac9553]
/usr/local/lib/libosmocore.so.11(_osmo_fsm_inst_dispatch+0x113) [0x7ff2f4ca7ba3]
/usr/local/bin/osmo-bsc(+0x28fd1) [0x55ca2ba94fd1]
/usr/local/lib/libosmoabis.so.6(ipaccess_fd_cb+0x112) [0x7ff2f4a8aba2]
/usr/local/lib/libosmocore.so.11(osmo_select_main+0x1de) [0x7ff2f4ca448e]
/usr/local/bin/osmo-bsc(+0x154a7) [0x55ca2ba814a7]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf1) [0x7ff2f42be2b1]
/usr/local/bin/osmo-bsc(+0x154fa) [0x55ca2ba814fa]
signal 6 received
talloc report on 'vty' (total 258190 bytes in 14537 blocks)
    save_cwd                       contains     33 bytes in   1 blocks (ref 0) 0x55ca2c90cdc0
    vty_command                    contains 155283 bytes in 8554 blocks (ref 0) 0x55ca2c8fa080
    vty_vector                     contains 102874 bytes in 5981 blocks (ref 0) 0x55ca2c8fa010
full talloc report on 'osmo-bsc' (total 453755 bytes in 354 blocks)
    telnet_connection              contains      1 bytes in   1 blocks (ref 0) 0x55ca2cac2350
    struct osmo_ss7_instance       contains   3521 bytes in  27 blocks (ref 0) 0x55ca2cacfff0
        struct osmo_sccp_instance      contains    190 bytes in   3 blocks (ref 0) 0x55ca2cae1360
            struct osmo_sccp_user          contains     86 bytes in   2 blocks (ref 0) 0x55ca2cae1
430
                msc-0                          contains      6 bytes in   1 blocks (ref 0) 0x55ca2
cae14f0
        struct osmo_ss7_asp            contains   1044 bytes in  11 blocks (ref 0) 0x55ca2cae0b10
            struct osmo_fsm_inst           contains    351 bytes in   4 blocks (ref 0) 0x55ca2cae1
050
                struct xua_asp_fsm_priv        contains    104 bytes in   1 blocks (ref 0) 0x55ca2
cae1290
                XUA_ASP(asp-clnt-msc-0)[0x55ca2cae1050] contains     40 bytes in   1 blocks (ref 0
) 0x55ca2cae1200
                asp-clnt-msc-0                 contains     15 bytes in   1 blocks (ref 0) 0x55ca2
cae1180
            struct osmo_stream_cli         contains    224 bytes in   1 blocks (ref 0) 0x55ca2cae0
f00
            struct osmo_fsm_inst           contains    262 bytes in   4 blocks (ref 0) 0x55ca2cae0
cc0
                struct lm_fsm_priv             contains      8 bytes in   1 blocks (ref 0) 0x55ca2
cae0e90
                xua_default_lm(asp-clnt-msc-0)[0x55ca2cae0cc0] contains     47 bytes in   1 blocks
 (ref 0) 0x55ca2cae0df0
                asp-clnt-msc-0                 contains     15 bytes in   1 blocks (ref 0) 0x55ca2
cae0a90
            asp-clnt-msc-0                 contains     15 bytes in   1 blocks (ref 0) 0x55ca2cae0
c40
        struct osmo_ss7_as             contains    586 bytes in   6 blocks (ref 0) 0x55ca2cae0500
```

History

#1 - 08/03/2018 01:40 PM - dexter

- % Done changed from 0 to 50

I think I found the reason for this crash. The FSM tries to send data through an SCCP connection but we never had one, thats why the asserition is hit.

Normally this should be prevented by gscon_sigtran_send(). This function avoids sending data when the ST_INIT or ST_WAIT_CC. When someone calls gscon_lchan_releasing() at a random point in time, the function forces the FSM to ST_CLEARING, and this state is not covered by by gscon_sigtran_send() so it tries to send the data even though there is no connection.

My idea is no to check in gscon_lchan_releasing() if we are already in ST_CLEARING. If not we just go to ST_CLEARING but before we call gscon_bssmap_clear(). If there is a connection it will be cleared then, if we are still in ST_INIT or ST_WAIT_CC nothing happens. If we are already in ST_CLEARING nothing happens at all.

In general I think its not a very good idea to allow other entities to do random state changes. I think its better when the FSM makes the state changes by itsself based on the events it receives.

#2 - 08/03/2018 02:24 PM - dexter

- Status changed from New to In Progress

- % Done changed from 50 to 100

I have now pushed the fix, but in the End I think this does not really cut it. It solves the problem, but the FSM should certainly know better about its connected state. Maybe gscon_lchan_releasing() can send an event to the FSM so that the FSM can decide consciously if it is appropriate to send the BSSMAP CLEAR REQUEST or not.

https://gerrit.osmocom.org/#/c/osmo-bsc/+/10333 GSCON: avoid sending clear when not connected

#3 - 08/13/2018 08:14 AM - dexter

- Status changed from In Progress to Resolved