OsmoMSC - Bug #2794

msc crashing 34c3

12/29/2017 09:48 PM - lynxis

Status:	Rejected	**Start date:**	12/29/2017
Priority:	Urgent	**Due date:**	
Assignee:	lynxis	**% Done:**	0%
Category:			
Target version:			
Resolution:			

Description

```
(gdb) bt
#0  0x00007f0293ce7c20 in _osmo_fsm_inst_dispatch (fi=0x5636065c63a0, event=event@entry=3, data=0x
5636065c62a0, file=file@entry=0x563604b7ebcc "msc_mgcp.c", line=line@entry=1068) at fsm.c:433
#1  0x0000563604b63008 in msc_mgcp_call_release (trans=trans@entry=0x5636065c5de0) at msc_mgcp.c:1
068
#2  0x0000563604b59491 in _gsm48_cc_trans_free (trans=0x5636065c5de0) at gsm_04_08.c:1338
#3  0x0000563604b65fc5 in trans_free (trans=0x5636065c5de0) at transaction.c:124
#4  0x0000563604b55cae in gsm48_cc_rx_release_compl (trans=0x5636065c5de0, msg=<optimized out>) at
 gsm_04_08.c:2223
#5  0x0000563604b5a514 in gsm0408_rcv_cc (msg=0x5636066bcad0, conn=0x5636065c3bf0) at gsm_04_08.c:
3186
#6  gsm0408_dispatch (conn=conn@entry=0x5636065c3bf0, msg=msg@entry=0x5636066bcad0) at gsm_04_08.c
:3296
#7  0x0000563604b6708d in msc_dtap (conn=0x5636065c3bf0, link_id=<optimized out>, msg=0x5636066bca
d0) at osmo_msc.c:108
#8  0x0000563604b68490 in gsm0408_rcvmsg_iucs (network=0x56360558f200, msg=0x5636066bcad0, lac=0x0
) at iucs.c:181
#9  0x00007f0292ae6811 in ranap_handle_co_dt (ies=0x7ffdcc137a88, ctx=0x5636065c3b50) at iu_client
.c:408
#10 cn_ranap_handle_co (ctx=0x5636065c3b50, message=0x7ffdcc137a80) at iu_client.c:542
#11 0x00007f0292ae4043 in ranap_cn_rx_co (cb=cb@entry=0x7f0292ae6310 <cn_ranap_handle_co>, ctx=0x5
636065c3b50, data=<optimized out>, len=<optimized out>) at ranap_common_cn.c:307
#12 0x00007f0292ae5b2c in sccp_sap_up (oph=0x5636066bc428, _scu=0x5636056343c0) at iu_client.c:795
#13 0x00007f0293ce7d8d in _osmo_fsm_inst_dispatch (fi=0x5636065bf0b0, event=11, data=data@entry=0x
5636066bc000, file=file@entry=0x7f02931d635d "sccp_scoc.c", line=line@entry=1581) at fsm.c:450
#14 0x00007f02931c6a1c in sccp_scoc_rx_from_scrc (inst=inst@entry=0x563605638a00, xua=xua@entry=0x
5636066bc000) at sccp_scoc.c:1581
#15 0x00007f02931c4670 in scrc_rx_mtp_xfer_ind_xua (inst=inst@entry=0x563605638a00, xua=0x5636066b
c000) at sccp_scrc.c:449
#16 0x00007f02931c7545 in mtp_user_prim_cb (oph=0x5636066b5d98, ctx=0x563605638a00) at sccp_user.c
:176
#17 0x00007f02931bf402 in m3ua_rx_xfer (xua=0x5636066a2190, asp=0x5636056380c0) at m3ua.c:586
#18 m3ua_rx_msg (asp=asp@entry=0x5636056380c0, msg=msg@entry=0x5636066a5f50) at m3ua.c:738
#19 0x00007f02931ca51b in xua_cli_read_cb (conn=<optimized out>) at osmo_ss7.c:1590
#20 0x00007f0291abd46b in osmo_stream_cli_read (cli=0x5636056384c0) at stream.c:192
#21 osmo_stream_cli_fd_cb (ofd=<optimized out>, what=1) at stream.c:276
#22 0x00007f0293ce495e in osmo_fd_disp_fds (_eset=0x7ffdcc138240, _wset=0x7ffdcc1381c0, _rset=0x7f
fdcc138140) at select.c:216
#23 osmo_select_main (polling=<optimized out>) at select.c:256
#24 0x0000563604b4e1fc in main (argc=5, argv=<optimized out>) at msc_main.c:552
```

History

#1 - 01/04/2018 10:35 AM - laforge

- Assignee set to lynxis

- Priority changed from Normal to Urgent

#2 - 01/07/2018 05:37 PM - neels

This is obviously related to the new MGCP FSM https://gerrit.osmocom.org/4980

We observed crashes both with GERAN and UTRAN. Unfortunately I was not able to obtain detailed logging leading up to the crash.

The crash didn't happen continuously, so it appears to be related to a call release situation that's not too common. Maybe the user hanging up right away? Maybe some radio failure?

If I were spending time on this, I would probably add voice call tests to the msc_vlr_tests suite in osmo-msc, could also be a candidate for ttcn3 tests... With tests like these I uncovered various tear down / free problems in the subscriber connection and VLR FSMs. It's not trivial to do proper cleanup in all situations.

#3 - 02/15/2018 10:18 PM - neels

- File call_establishment_and_call_end.pcapng added

Now during testing, I hit the same error, and this time I can provide some log output and traces with it.

Notably the call didn't work, I see RTP traffic only from one call leg coming through.
The cause for the failing call is most certainly that I was using a setup running osmo-bsc_mgcp as MGW for the MSC, with current osmo-msc master which expects osmo-mgw instead.
The call not working is besides the point, the interesting bit here is the MSC crash. Maybe an MGW problem is a prerequisite for the crash occuring?

log leading up to the crash and backtrace:

```
Thu Feb 15 22:45:01 2018 DLINP DEBUG ipa.c:56 127.0.0.1:4222 message received
Thu Feb 15 22:45:01 2018 DLGSUP DEBUG gsup_client.c:201 GSUP receiving PONG
Thu Feb 15 22:45:20 2018 DLINP DEBUG stream.c:275 connected read
Thu Feb 15 22:45:20 2018 DLINP DEBUG stream.c:189 message received
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG osmo_ss7.c:1551 asp-asp-clnt-OsmoMSC-A-Iu: xua_cli_read_cb(): sctp_recvms
g() returned 48 (flags=0x80)
Thu Feb 15 22:45:20 2018 DLM3UA DEBUG m3ua.c:721 asp-asp-clnt-OsmoMSC-A-Iu: Received M3UA Message (XFER:DATA)
Thu Feb 15 22:45:20 2018 DLM3UA DEBUG m3ua.c:541 asp-asp-clnt-OsmoMSC-A-Iu: m3ua_rx_xfer
Thu Feb 15 22:45:20 2018 DLM3UA DEBUG m3ua.c:580 asp-asp-clnt-OsmoMSC-A-Iu: m3ua_rx_xfer(): M3UA data header:
opc=187=0.23.3 dpc=185=0.23.1
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG osmo_ss7_hmrt.c:274 m3ua_hmdc_rx_from_l2(): found dpc=185=0.23.1 as local
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG sccp_scrc.c:442 scrc_rx_mtp_xfer_ind_xua:  HDR=(CO:CODT,V=0,LEN=0),
    PART(T=Destination Reference,L=4,D=00000005),
    PART(T=Segmentation,L=4,D=00000000),
    PART(T=Data,L=8,D=010005032502e090)
Thu Feb 15 22:45:20 2018 DLSCCP DEBUG sccp_scoc.c:1548 Received CO:CODT for local reference 5
Thu Feb 15 22:45:20 2018 DLSCCP DEBUG sccp_scoc.c:1581 SCCP-SCOC(5)[0x555555b5f030]{ACTIVE}: Received Event RC
OC-DT1.ind
Thu Feb 15 22:45:20 2018 DLSCCP DEBUG sccp_user.c:156 Delivering N-DATA.indication to SCCP User 'OsmoMSC-A'
Thu Feb 15 22:45:20 2018 DBSSAP DEBUG a_iface.c:552 N-DATA.ind(5, 01 00 05 03 25 02 e0 90 )
Thu Feb 15 22:45:20 2018 DMSC DEBUG a_iface_bssap.c:85 Looking for A subscriber: conn_id 5
Thu Feb 15 22:45:20 2018 DBSSAP DEBUG a_iface_bssap.c:93 (subscr MSISDN:101, conn_id 5) Found A subscriber for
 conn_id 5
Thu Feb 15 22:45:20 2018 DBSSAP DEBUG a_iface_bssap.c:594 (subscr MSISDN:101, conn_id 5) Rx DTAP 01 00 05 03 2
5 02 e0 90
Thu Feb 15 22:45:20 2018 DRLL DEBUG gsm_04_08.c:3462 Dispatching 04.08 message GSM48_MT_CC_DISCONNECT (0x3:0x2
5)
Thu Feb 15 22:45:20 2018 DCC DEBUG gsm_04_08.c:1306 (ti 08 sub MSISDN:101) new state ACTIVE -> DISCONNECT_IND
Thu Feb 15 22:45:20 2018 DMNCC DEBUG gsm_04_08.c:1358 transmit message MNCC_DISC_IND
Thu Feb 15 22:45:20 2018 DCC DEBUG gsm_04_08.c:1381 Sending 'MNCC_DISC_IND' to MNCC.
Thu Feb 15 22:45:20 2018 DMNCC DEBUG mncc_builtin.c:311 (call 80000001) Received message MNCC_DISC_IND
Thu Feb 15 22:45:20 2018 DMNCC DEBUG mncc_builtin.c:216 (call 80000001) Releasing call with cause 16
Thu Feb 15 22:45:20 2018 DMNCC DEBUG gsm_04_08.c:2974 receive message MNCC_REL_REQ
Thu Feb 15 22:45:20 2018 DCC DEBUG gsm_04_08.c:3148 (ti 08 sub 101) Received 'MNCC_REL_REQ' from MNCC in state
 12 (DISCONNECT_IND)
Thu Feb 15 22:45:20 2018 DCC DEBUG gsm_04_08.c:1625 starting timer T308 with 10 seconds
```

```
Thu Feb 15 22:45:20 2018 DCC DEBUG gsm_04_08.c:1306 (ti 08 sub MSISDN:101) new state DISCONNECT_IND -> RELEASE
_REQ
Thu Feb 15 22:45:20 2018 DMSC DEBUG msc_ifaces.c:53 msc_tx 6 bytes to MSISDN:101 via RAN_GERAN_A
Thu Feb 15 22:45:20 2018 DBSSAP DEBUG a_iface.c:155 (subscr MSISDN:101, conn_id 5) Passing DTAP message from M
SC to BSC
Thu Feb 15 22:45:20 2018 DBSSAP DEBUG a_iface.c:169 (subscr MSISDN:101, conn_id 5) N-DATA.req([])
Thu Feb 15 22:45:20 2018 DLSCCP DEBUG sccp_scoc.c:1615 Received SCCP User Primitive N-DATA.request)
Thu Feb 15 22:45:20 2018 DLSCCP DEBUG sccp_scoc.c:1657 SCCP-SCOC(5)[0x555555b5f030]{ACTIVE}: Received Event N-
DATA.req
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG sccp_scrc.c:391 sccp_scrc_rx_scoc_conn_msg:  HDR=(CO:CODT,V=0,LEN=0),
    PART(T=Routing Context,L=4,D=00000000),
    PART(T=Destination Reference,L=4,D=00000006),
    PART(T=Data,L=9,D=010006832d0802e090)
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG osmo_ss7_hmrt.c:278 m3ua_hmdc_rx_from_l2(): dpc=187=0.23.3 not local, mes
sage is for routing
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG osmo_ss7_hmrt.c:227 Found route for dpc=187=0.23.3: pc=0=0.0.0 mask=0x0=0
.0.0 via AS as-clnt-OsmoMSC-A-Iu proto=m3ua
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG osmo_ss7_hmrt.c:233 rt->dest.as proto is M3UA for dpc=187=0.23.3
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG m3ua.c:507 XUA_AS(as-clnt-OsmoMSC-A-Iu)[0x5555558c0100]{AS_ACTIVE}: Recei
ved Event AS-TRANSFER.req
Thu Feb 15 22:45:20 2018 DMNCC DEBUG mncc_builtin.c:225 (call 1) Disconnecting remote with cause 16
Thu Feb 15 22:45:20 2018 DMNCC DEBUG gsm_04_08.c:2974 receive message MNCC_DISC_REQ
Thu Feb 15 22:45:20 2018 DCC DEBUG gsm_04_08.c:3148 (ti 00 sub 102) Received 'MNCC_DISC_REQ' from MNCC in stat
e 10 (ACTIVE)
Thu Feb 15 22:45:20 2018 DCC DEBUG gsm_04_08.c:1625 starting timer T306 with 30 seconds
Thu Feb 15 22:45:20 2018 DCC DEBUG gsm_04_08.c:1306 (ti 00 sub MSISDN:102) new state ACTIVE -> DISCONNECT_IND
Thu Feb 15 22:45:20 2018 DMSC DEBUG msc_ifaces.c:53 msc_tx 5 bytes to MSISDN:102 via RAN_GERAN_A
Thu Feb 15 22:45:20 2018 DBSSAP DEBUG a_iface.c:155 (subscr MSISDN:102, conn_id 6) Passing DTAP message from M
SC to BSC
Thu Feb 15 22:45:20 2018 DBSSAP DEBUG a_iface.c:169 (subscr MSISDN:102, conn_id 6) N-DATA.req([])
Thu Feb 15 22:45:20 2018 DLSCCP DEBUG sccp_scoc.c:1615 Received SCCP User Primitive N-DATA.request)
Thu Feb 15 22:45:20 2018 DLSCCP DEBUG sccp_scoc.c:1657 SCCP-SCOC(6)[0x555555c95130]{ACTIVE}: Received Event N-
DATA.req
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG sccp_scrc.c:391 sccp_scrc_rx_scoc_conn_msg:  HDR=(CO:CODT,V=0,LEN=0),
    PART(T=Routing Context,L=4,D=00000000),
    PART(T=Destination Reference,L=4,D=00000007),
    PART(T=Data,L=8,D=010005032502e090)
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG osmo_ss7_hmrt.c:278 m3ua_hmdc_rx_from_l2(): dpc=187=0.23.3 not local, mes
sage is for routing
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG osmo_ss7_hmrt.c:227 Found route for dpc=187=0.23.3: pc=0=0.0.0 mask=0x0=0
.0.0 via AS as-clnt-OsmoMSC-A-Iu proto=m3ua
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG osmo_ss7_hmrt.c:233 rt->dest.as proto is M3UA for dpc=187=0.23.3
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG m3ua.c:507 XUA_AS(as-clnt-OsmoMSC-A-Iu)[0x5555558c0100]{AS_ACTIVE}: Recei
ved Event AS-TRANSFER.req
Thu Feb 15 22:45:20 2018 DMM DEBUG subscr_conn.c:354 Subscr_Conn(790009884)[0x555555b5f410]{SUBSCR_CONN_S_COMM
UNICATING}: Received Event SUBSCR_CONN_E_COMMUNICATING
Thu Feb 15 22:45:20 2018 DMM DEBUG osmo_msc.c:63 Subscr_Conn(790009884)[0x555555b5f410]{SUBSCR_CONN_S_COMMUNIC
ATING}: Received Event SUBSCR_CONN_E_BUMP
Thu Feb 15 22:45:20 2018 DMM DEBUG subscr_conn.c:164 Subscr_Conn(790009884)[0x555555b5f410]{SUBSCR_CONN_S_COMM
UNICATING}: bump: connection still has active transaction: CC
Thu Feb 15 22:45:20 2018 DLINP DEBUG stream.c:279 connected write
Thu Feb 15 22:45:20 2018 DLINP DEBUG stream.c:204 sending data
Thu Feb 15 22:45:20 2018 DLINP DEBUG stream.c:279 connected write
Thu Feb 15 22:45:20 2018 DLINP DEBUG stream.c:204 sending data
Thu Feb 15 22:45:20 2018 DLINP DEBUG stream.c:279 connected write
Thu Feb 15 22:45:20 2018 DLINP DEBUG stream.c:204 sending data
Thu Feb 15 22:45:20 2018 DLINP DEBUG stream.c:275 connected read
Thu Feb 15 22:45:20 2018 DLINP DEBUG stream.c:189 message received
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG osmo_ss7.c:1551 asp-asp-clnt-OsmoMSC-A-Iu: xua_cli_read_cb(): sctp_recvms
g() returned 44 (flags=0x80)
Thu Feb 15 22:45:20 2018 DLM3UA DEBUG m3ua.c:721 asp-asp-clnt-OsmoMSC-A-Iu: Received M3UA Message (XFER:DATA)
Thu Feb 15 22:45:20 2018 DLM3UA DEBUG m3ua.c:541 asp-asp-clnt-OsmoMSC-A-Iu: m3ua_rx_xfer
Thu Feb 15 22:45:20 2018 DLM3UA DEBUG m3ua.c:580 asp-asp-clnt-OsmoMSC-A-Iu: m3ua_rx_xfer(): M3UA data header:
opc=187=0.23.3 dpc=185=0.23.1
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG osmo_ss7_hmrt.c:274 m3ua_hmdc_rx_from_l2(): found dpc=185=0.23.1 as local
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG sccp_scrc.c:442 scrc_rx_mtp_xfer_ind_xua:  HDR=(CO:CODT,V=0,LEN=0),
    PART(T=Destination Reference,L=4,D=00000006),
    PART(T=Segmentation,L=4,D=00000000),
    PART(T=Data,L=5,D=010002832d)
Thu Feb 15 22:45:20 2018 DLSCCP DEBUG sccp_scoc.c:1548 Received CO:CODT for local reference 6
Thu Feb 15 22:45:20 2018 DLSCCP DEBUG sccp_scoc.c:1581 SCCP-SCOC(6)[0x555555c95130]{ACTIVE}: Received Event RC
OC-DT1.ind
Thu Feb 15 22:45:20 2018 DLSCCP DEBUG sccp_user.c:156 Delivering N-DATA.indication to SCCP User 'OsmoMSC-A'
Thu Feb 15 22:45:20 2018 DBSSAP DEBUG a_iface.c:552 N-DATA.ind(6, 01 00 02 83 2d )
Thu Feb 15 22:45:20 2018 DMSC DEBUG a_iface_bssap.c:85 Looking for A subscriber: conn_id 6
```

```
Thu Feb 15 22:45:20 2018 DBSSAP DEBUG a_iface_bssap.c:93 (subscr MSISDN:102, conn_id 6) Found A subscriber for
 conn_id 6
Thu Feb 15 22:45:20 2018 DBSSAP DEBUG a_iface_bssap.c:594 (subscr MSISDN:102, conn_id 6) Rx DTAP 01 00 02 83 2
d
Thu Feb 15 22:45:20 2018 DRLL DEBUG gsm_04_08.c:3462 Dispatching 04.08 message GSM48_MT_CC_RELEASE (0x3:0x2d)
Thu Feb 15 22:45:20 2018 DCC DEBUG gsm_04_08.c:1346 stopping pending timer T306
Thu Feb 15 22:45:20 2018 DMSC DEBUG msc_ifaces.c:53 msc_tx 2 bytes to MSISDN:102 via RAN_GERAN_A
Thu Feb 15 22:45:20 2018 DBSSAP DEBUG a_iface.c:155 (subscr MSISDN:102, conn_id 6) Passing DTAP message from M
SC to BSC
Thu Feb 15 22:45:20 2018 DBSSAP DEBUG a_iface.c:169 (subscr MSISDN:102, conn_id 6) N-DATA.req([])
Thu Feb 15 22:45:20 2018 DLSCCP DEBUG sccp_scoc.c:1615 Received SCCP User Primitive N-DATA.request)
Thu Feb 15 22:45:20 2018 DLSCCP DEBUG sccp_scoc.c:1657 SCCP-SCOC(6)[0x555555c95130]{ACTIVE}: Received Event N-
DATA.req
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG sccp_scrc.c:391 sccp_scrc_rx_scoc_conn_msg:  HDR=(CO:CODT,V=0,LEN=0),
    PART(T=Routing Context,L=4,D=00000000),
    PART(T=Destination Reference,L=4,D=00000007),
    PART(T=Data,L=5,D=010002032a)
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG osmo_ss7_hmrt.c:278 m3ua_hmdc_rx_from_l2(): dpc=187=0.23.3 not local, mes
sage is for routing
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG osmo_ss7_hmrt.c:227 Found route for dpc=187=0.23.3: pc=0=0.0.0 mask=0x0=0
.0.0 via AS as-clnt-OsmoMSC-A-Iu proto=m3ua
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG osmo_ss7_hmrt.c:233 rt->dest.as proto is M3UA for dpc=187=0.23.3
Thu Feb 15 22:45:20 2018 DLSS7 DEBUG m3ua.c:507 XUA_AS(as-clnt-OsmoMSC-A-Iu)[0x5555558c0100]{AS_ACTIVE}: Recei
ved Event AS-TRANSFER.req
Thu Feb 15 22:45:20 2018 DMNCC DEBUG gsm_04_08.c:1358 transmit message MNCC_REL_IND
Thu Feb 15 22:45:20 2018 DCC DEBUG gsm_04_08.c:1381 Sending 'MNCC_REL_IND' to MNCC.
Thu Feb 15 22:45:20 2018 DMNCC DEBUG mncc_builtin.c:311 (call 1) Received message MNCC_REL_IND
Thu Feb 15 22:45:20 2018 DMNCC DEBUG mncc_builtin.c:241 (call 1) Releasing remote with cause 0
Thu Feb 15 22:45:20 2018 DMNCC DEBUG mncc_builtin.c:51 (call 1) Call removed.
Thu Feb 15 22:45:20 2018 DMNCC DEBUG gsm_04_08.c:2974 receive message MNCC_REL_REQ
Thu Feb 15 22:45:20 2018 DCC DEBUG gsm_04_08.c:3148 (ti 08 sub 101) Received 'MNCC_REL_REQ' from MNCC in state
 19 (RELEASE_REQ)
Thu Feb 15 22:45:20 2018 DCC DEBUG gsm_04_08.c:3157 Message unhandled at this state.
Thu Feb 15 22:45:20 2018 DCC DEBUG gsm_04_08.c:1306 (ti 00 sub MSISDN:102) new state DISCONNECT_IND -> NULL

Program received signal SIGSEGV, Segmentation fault.
_osmo_fsm_inst_dispatch (fi=0x7fffdea25bc0, event=event@entry=3, data=0x555555cdc990, file=file@entry=0x555555
58ffe8 "../../../../src/osmo-msc/src/libmsc/msc_mgcp.c", line=line@entry=1066)
    at ../../../src/libosmocore/src/fsm.c:463
463         fsm = fi->fsm;
(gdb) bt
#0  _osmo_fsm_inst_dispatch (fi=0x7fffdea25bc0, event=event@entry=3, data=0x555555cdc990, file=file@entry=0x55
555558ffe8 "../../../../src/osmo-msc/src/libmsc/msc_mgcp.c", line=line@entry=1066)
    at ../../../src/libosmocore/src/fsm.c:463
#1  0x000055555557507d in msc_mgcp_call_release (trans=trans@entry=0x555555b6fa00) at ../../../../src/osmo-msc
/src/libmsc/msc_mgcp.c:1066
#2  0x000055555556b141 in _gsm48_cc_trans_free (trans=0x555555b6fa00) at ../../../../src/osmo-msc/src/libmsc/g
sm_04_08.c:1418
#3  0x0000555555578415 in trans_free (trans=0x555555b6fa00) at ../../../../src/osmo-msc/src/libmsc/transaction
.c:123
#4  0x0000555555567bb1 in gsm48_cc_rx_release (trans=0x555555b6fa00, msg=<optimized out>) at ../../../../src/o
smo-msc/src/libmsc/gsm_04_08.c:2229
#5  0x000055555556c4dc in gsm0408_rcv_cc (msg=0x555555e37ed0, conn=0x555555c95360) at ../../../../src/osmo-msc
/src/libmsc/gsm_04_08.c:3285
#6  gsm0408_dispatch (conn=conn@entry=0x555555c95360, msg=msg@entry=0x555555e37ed0) at ../../../../src/osmo-ms
c/src/libmsc/gsm_04_08.c:3490
#7  0x00005555555794ad in msc_dtap (conn=0x555555c95360, link_id=<optimized out>, msg=0x555555e37ed0) at ../..
/../../src/osmo-msc/src/libmsc/osmo_msc.c:107
#8  0x0000555555562d74 in rx_dtap (scu=0x7ffff754a900 <hexd_buff>, a_conn_info=0x7fffffffe0c0, a_conn_info=0x7
fffffffe0c0, msg=<optimized out>) at ../../../../src/osmo-msc/src/libmsc/a_iface_bssap.c:600
#9  a_sccp_rx_dt (scu=scu@entry=0x5555558ea700, a_conn_info=a_conn_info@entry=0x7fffffffe0f0, msg=<optimized o
ut>) at ../../../../src/osmo-msc/src/libmsc/a_iface_bssap.c:622
#10 0x0000555555560f24 in sccp_sap_up (oph=0x555555e37f58, _scu=0x5555558ea700) at ../../../../src/osmo-msc/sr
c/libmsc/a_iface.c:553
#11 0x00007ffff7333e7f in _osmo_fsm_inst_dispatch (fi=0x555555c95130, event=11, data=data@entry=0x555555cdc960
, file=file@entry=0x7ffff6cb14a8 "../../../src/libosmo-sccp/src/sccp_scoc.c", line=line@entry=1581)
    at ../../../src/libosmocore/src/fsm.c:481
#12 0x00007ffff6ca1985 in sccp_scoc_rx_from_scrc (inst=inst@entry=0x5555558e8150, xua=xua@entry=0x555555cdc960
) at ../../../src/libosmo-sccp/src/sccp_scoc.c:1581
#13 0x00007ffff6c9f67b in scrc_rx_mtp_xfer_ind_xua (inst=inst@entry=0x5555558e8150, xua=0x555555cdc960) at ../
../../src/libosmo-sccp/src/sccp_scrc.c:449
#14 0x00007ffff6ca2555 in mtp_user_prim_cb (oph=0x555555a2bf48, ctx=0x5555558e8150) at ../../../src/libosmo-sc
cp/src/sccp_user.c:176
#15 0x00007ffff6c9a393 in m3ua_rx_xfer (xua=0x555555ce9c80, asp=0x5555558c0550) at ../../../src/libosmo-sccp/s
rc/m3ua.c:586
```

```
#16 m3ua_rx_msg (asp=asp@entry=0x5555558c0550, msg=msg@entry=0x555555932c80) at ../../../src/libosmo-sccp/src/
m3ua.c:738
#17 0x00007ffff6ca5553 in xua_cli_read_cb (conn=<optimized out>) at ../../../src/libosmo-sccp/src/osmo_ss7.c:1
592
#18 0x00007ffff55bf3fb in osmo_stream_cli_read (cli=0x5555558e59a0) 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 0x00007ffff7330a71 in osmo_fd_disp_fds (_eset=0x7fffffffe500, _wset=0x7fffffffe480, _rset=0x7fffffffe400)
at ../../../src/libosmocore/src/select.c:216
#21 osmo_select_main (polling=<optimized out>) at ../../../src/libosmocore/src/select.c:256
#22 0x000055555555f46c in main (argc=1, argv=<optimized out>) at ../../../../src/osmo-msc/src/osmo-msc/msc_mai
n.c:533

(gdb) l
458                 " FSM instance!\n", event);
459             osmo_log_backtrace(DLGLOBAL, LOGL_ERROR);
460             return -ENODEV;
461         }
462
463         fsm = fi->fsm;
464         OSMO_ASSERT(fi->state < fsm->num_states);
465         fs = &fi->fsm->states[fi->state];
466
467         LOGPFSMSRC(fi, file, line,
(gdb) p fi
$1 = (struct osmo_fsm_inst *) 0x7fffdea25bc0
(gdb) p *fi
Cannot access memory at address 0x7fffdea25bc0
(gdb) frame 1
#1  0x000055555557507d in msc_mgcp_call_release (trans=trans@entry=0x555555b6fa00) at ../../../../src/osmo-msc
/src/libmsc/msc_mgcp.c:1066
1066        osmo_fsm_inst_dispatch(mgcp_ctx->fsm, EV_TEARDOWN, mgcp_ctx);
(gdb) l
1061         * all context information immediately */
1062        mgcp_ctx->free_ctx = true;
1063
1064        /* Initaite teardown, regardless of which state we are currently
1065         * in */
1066        osmo_fsm_inst_dispatch(mgcp_ctx->fsm, EV_TEARDOWN, mgcp_ctx);
1067
1068        /* Prevent any further operation that is triggered from outside by
1069         * overwriting the context pointer with NULL. The FSM will now
1070         * take care for a graceful shutdown and when done it will free
(gdb) p mgcp_ctx
$2 = <optimized out>
(gdb) p mgcp_ctx->fsm
value has been optimized out
(gdb)
```

Find logs of all the other core network components in the pcap trace (includes gsmtap_log). Note that each program sends gsmtap_log to a different 127.0.0.N address, so it is possible to filter by program using the destination IP, e.g. "gsmtap_log && ip.dst == 127.0.0.9" is osmo-msc's log.

#4 - 04/10/2018 02:37 PM - lynxis

- Status changed from New to Rejected

Since the last crash we have to many changes and now new tests.

Files

call_establishment_and_call_end.pcapng	1 MB	02/15/2018	neels