OsmoSGSN - Bug #3727

SGSN segfaults on network type change

12/12/2018 11:29 PM - manatails

Status:	New	**Start date:**	12/12/2018
Priority:	Normal	**Due date:**	
Assignee:	lynxis	**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

When the phone changes its network type between GSM and UMTS osmo-sgsn crashes with the following log:

<0012> gprs_llc_parse.c:81 LLC SAPI=1 C U GEA0 IOV-UI=0x000000 FCS=0x760d06 CMD=UI DATA
<0002> gprs_gmm.c:1609 -> GMM RA UPDATE REQUEST type="RA updating"
<0002> gprs_gmm.c:1685 MM Looked up by matching TLLI and P_TMSI. BSSGP TLLI: b99cab1e, P-TMSI: f99cab1e (00000000), TLLI: 00000000 (00000000), RA: 450-09-1-1

Program received signal SIGSEGV, Segmentation fault.
0x0000000000409667 in gsm48_gmm_authorize (ctx=0x758600) at gprs_gmm.c:1051
1051 if (ctx->ran_type == MM_CTX_T_UTRAN_Iu && !ctx->iu.ue_ctx->integrity_active) {
(gdb)

History

#1 - 12/13/2018 12:07 AM - manatails

ctx->iu.ue_ctx is null at the time of crash

#2 - 04/09/2019 11:17 AM - laforge

- Assignee set to lynxis

#3 - 04/11/2019 04:13 AM - lynxis

Can you create a backtrace when this problem happens (gdb cli: bt). It would be also nice if you can provide a pcap trace.
I would guess this problem happens when a MS/UE moves from 3G to 2G. Not sure if the SGSN also crashs the other way around :).

I should write a TTCN-3 test first to cover this.

#4 - 04/15/2019 07:26 AM - laforge

#5 - 05/03/2019 09:25 AM - manatails

lynxis wrote:

> Can you create a backtrace when this problem happens (gdb cli: bt). It would be also nice if you can provide a pcap trace.
> I would guess this problem happens when a MS/UE moves from 3G to 2G. Not sure if the SGSN also crashs the other way around :).
>
> I should write a TTCN-3 test first to cover this.

```
Program received signal SIGSEGV, Segmentation fault.
0x000000000040ad17 in gsm48_gmm_authorize (ctx=0x764350) at gprs_gmm.c:1058
1058            if (ctx->ran_type == MM_CTX_T_UTRAN_Iu && !ctx->iu.ue_ctx->integrity_active) {
(gdb) bt
#0  0x000000000040ad17 in gsm48_gmm_authorize (ctx=0x764350) at gprs_gmm.c:1058
#1  0x000000000040b6c5 in gsm48_rx_gmm_ra_upd_req (mmctx=0x764350, mmctx@entry=0x0, msg=msg@entry=0x760690, ll
me=llme@entry=0x762430) at gprs_gmm.c:1800
#2  0x000000000040c45e in gsm0408_rcv_gmm (mmctx=mmctx@entry=0x0, msg=msg@entry=0x760690, llme=llme@entry=0x76
2430, drop_cipherable=drop_cipherable@entry=false) at gprs_gmm.c:2008
#3  0x000000000040d352 in gsm0408_gprs_rcvmsg_gb (msg=msg@entry=0x760690, llme=0x762430, drop_cipherable=drop_
```

```
cipherable@entry=false) at gprs_gmm.c:2933
#4  0x000000000041c10b in gprs_llc_rcvmsg (msg=0x760690, tv=<optimized out>) at gprs_llc.c:997
#5  0x0000000000415ead in bssgp_prim_cb (oph=oph@entry=0x1, ctx=ctx@entry=0x0) at sgsn_main.c:125
#6  0x00007ffff7758ec0 in bssgp_rx_ul_ud (ctx=<optimized out>, ctx=<optimized out>, tp=<optimized out>, msg=<o
ptimized out>) at gprs_bssgp.c:414
#7  bssgp_rx_ptp (bctx=<optimized out>, tp=<optimized out>, msg=<optimized out>) at gprs_bssgp.c:873
#8  bssgp_rcvmsg (msg=0x760690) at gprs_bssgp.c:1096
#9  0x00007ffff7752cea in gprs_ns_rx_unitdata (msg=0x760690, nsvc=0x761380) at gprs_ns.c:1139
#10 gprs_ns_process_msg (nsi=nsi@entry=0x73a040, msg=msg@entry=0x760690, nsvc=nsvc@entry=0x7fffffffe260) at gp
rs_ns.c:1774
#11 0x00007ffff775482a in gprs_ns_rcvmsg (nsi=nsi@entry=0x73a040, msg=msg@entry=0x760690, saddr=saddr@entry=0x
7fffffffe2c0, ll=ll@entry=GPRS_NS_LL_UDP) at gprs_ns.c:1523
#12 0x00007ffff7754995 in handle_nsip_read (bfd=0x73a070) at gprs_ns.c:1989
#13 nsip_fd_cb (bfd=0x73a070, what=1) at gprs_ns.c:2022
#14 0x00007ffff7303e37 in osmo_fd_disp_fds (_eset=0x7fffffffe430, _wset=0x7fffffffe3b0, _rset=0x7fffffffe330)
at select.c:223
#15 osmo_select_main (polling=polling@entry=0) at select.c:263
#16 0x0000000000405097 in main (argc=2, argv=<optimized out>) at sgsn_main.c:524
(gdb)
```

Sorry for late reply,

Here is the backtrace took when going from 3G->2G.

Moving from 2G-3G causes the crash as well.

```
Program received signal SIGSEGV, Segmentation fault.
gsm48_parse_ra (raid=raid@entry=0x7636c8, buf=buf@entry=0x0) at gsm48.c:788
788     {
(gdb) bt
#0  gsm48_parse_ra (raid=raid@entry=0x7636c8, buf=buf@entry=0x0) at gsm48.c:788
#1  0x00007ffff7758639 in bssgp_parse_cell_id (raid=raid@entry=0x7636c8, buf=0x0) at gprs_bssgp.c:239
#2  0x000000000040b705 in gsm48_rx_gmm_ra_upd_req (mmctx=0x763670, mmctx@entry=0x0, msg=msg@entry=0x767d60, ll
me=llme@entry=0x0) at gprs_gmm.c:1756
#3  0x000000000040c45e in gsm0408_rcv_gmm (mmctx=0x0, msg=0x767d60, llme=0x0, drop_cipherable=<optimized out>)
 at gprs_gmm.c:2008
#4  0x00007ffff60b2e1e in ranap_handle_co_initial_ue (ies=<optimized out>, ctx=0x7fffffffdf80) at iu_client.c:
373
#5  cn_ranap_handle_co_initial (ctx=0x7fffffffdf80, message=<optimized out>) at iu_client.c:517
#6  0x00007ffff60b1908 in ranap_cn_rx_co (cb=cb@entry=0x7ffff60b2af0 <cn_ranap_handle_co_initial>, ctx=ctx@ent
ry=0x7fffffffdf80, data=<optimized out>, len=<optimized out>) at ranap_common_cn.c:307
#7  0x00007ffff60b379a in sccp_sap_up (oph=0x766f98, _scu=0x760550) at iu_client.c:803
#8  0x00007ffff73086b7 in _osmo_fsm_inst_dispatch (fi=0x766cf0, event=5, data=data@entry=0x7611d0, file=file@e
ntry=0x7ffff639711d "sccp_scoc.c", line=line@entry=1677) at fsm.c:818
#9  0x00007ffff6387059 in sccp_scoc_rx_from_scrc (inst=inst@entry=0x760350, xua=xua@entry=0x7611d0) at sccp_sc
oc.c:1677
#10 0x00007ffff638444a in scrc_node_6 (inst=inst@entry=0x760350, xua=xua@entry=0x7611d0, called=0x7fffffffe130
, called=0x7fffffffe130) at sccp_scrc.c:348
#11 0x00007ffff6384b8d in scrc_rx_mtp_xfer_ind_xua (inst=inst@entry=0x760350, xua=0x7611d0) at sccp_scrc.c:468
#12 0x00007ffff6387c45 in mtp_user_prim_cb (oph=0x765d58, ctx=0x760350) at sccp_user.c:176
#13 0x00007ffff637fbff in m3ua_rx_xfer (xua=0x760b40, asp=0x75f030) at m3ua.c:586
#14 m3ua_rx_msg (asp=asp@entry=0x75f030, msg=msg@entry=0x764fe0) at m3ua.c:739
#15 0x00007ffff638e30b in xua_cli_read_cb (conn=0x75fe70) at osmo_ss7.c:1650
#16 0x00007ffff50bede3 in osmo_stream_cli_read (cli=0x75fe70) at stream.c:213
#17 osmo_stream_cli_fd_cb (ofd=<optimized out>, what=1) at stream.c:297
#18 0x00007ffff7303e37 in osmo_fd_disp_fds (_eset=0x7fffffffe430, _wset=0x7fffffffe3b0, _rset=0x7fffffffe330)
at select.c:223
#19 osmo_select_main (polling=polling@entry=0) at select.c:263
#20 0x0000000000405097 in main (argc=2, argv=<optimized out>) at sgsn_main.c:524
(gdb)
```

2G->3G backtrace

#6 - 05/03/2019 09:32 AM - manatails