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
<br><0002> gprs_gmm.c:1609 -> GMM RA UPDATE REQUEST type="RA updating"
<br><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
<br>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) {
<br>(gdb)
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) {
<br>(gdb) bt
#0 0x00000000000040ad17 in gsm48_gmm_authorize (ctx=0x764350) at gprs_gmm.c:1058

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 crashes the other way around :).
I should write a TTCN-3 test first to cover this.

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 crashes 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) {
<br>(gdb) bt
#0 0x00000000000040ad17 in gsm48_gmm_authorize (ctx=0x764350) at gprs_gmm.c:1058
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

(gdb) bt
#0 gsm48_parse_ra (raid=raid@entry=0x7636c8, buf=buf@entry=0x0) at gsm48.c:788
#1 0x00000000007758639 in bssgp_parse_cell_id (raid=raid@entry=0x7636c8, buf=0x0) at gprs_bssgp.c:239
#2 0x000000000076d6b0 in gsm48_rx_gmm_ra_upd_req (mmctx=0x7676d60, llme=llme@entry=0x0) at gmm_rmm.c:2008
#3 0x000000000076d6b0 in gsm0408_rcv_gmm (mmctx=0x0, msg=0x7676d60, llme=llme@entry=0x0) at gmm_rmm.c:2933
#4 0x000000000076d6b0 in gsm0408_gprs_rcvmsg_gb (msg=0x7676d60, llme=llme@entry=0x0) at gprs_gmm.c:1800
#5 0x000000000076d6b0 in gprs_llc_rcvmsg (msg=0x760690, tv=<optimized out>) at gprs_llc.c:997
#6 0x000000000076d6b0 in bssgp_prim_cb (oph=oph@entry=0x1, ctx=ctx@entry=0x0) at sgn_main.c:125
#7 0x000000000076d6b0 in bssgp_rx_ul_ud (ctx=ctx@entry=0x0, msg=<optimized out>, tp=<optimized out>) at gprs_bssgp.c:414
#8 bssgp_rx_ptp (ctx=ctx@entry=0x0, msg=<optimized out>) at gprs_bssgp.c:873
#9 bssgp_rcvmsg (msg=0x760690) at gprs_bssgp.c:1096
#10 gprs_ns_rx_unitdata (msg=0x760690, nsvc=0x761380) at gprs_ns.c:1139
#11 gprs_ns_process_msg (nsi=nsi@entry=0x73a040, msg=msg@entry=0x760690, nsvc=nsvc@entry=0x7fffffffe260) at gprs_ns.c:1774
#12 gprs_ns_rcvmsg (nsi=nsi@entry=0x73a040, msg=msg@entry=0x760690, saddr=saddr@entry=0x7fffffffe2c0, ll=ll@entry=GPRS_NS_LL_UDP) at gprs_ns.c:1523
#13 handle_nsip_read (bfd=0x73a070) at gprs_ns.c:1989
#14 nsip_fd_cb (bfd=0x73a070, what=1) at gprs_ns.c:2022
#15 osmo_fd_disp_fds (_eset=0x7fffffffe430, _wset=0x7fffffffe3b0, _rset=0x7fffffffe330) at select.c:223
#16 osmo_select_main (polling=polling@entry=0) at select.c:263

2G->3G backtrace

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

#7 - 07/18/2019 05:02 AM - laforge

- Priority changed from Normal to High
I've tested the ttcn3 branch laforge/iu, rebased it and pushed to gerrit as lynxis/sgsn_iu
Next step is writing a testcase:

- do a gmm attach vi geran
- do a LU via iups

#9 - 07/18/2019 04:42 PM - lynxis
- Status changed from New to In Progress

#10 - 08/12/2019 03:21 PM - lynxis

GMM Attach via Iu succeed (with a connection close patch).

#11 - 08/12/2019 03:36 PM - lynxis

I could reproduce the crash geran -> utran

#12 - 08/13/2019 04:59 AM - fixeria

IMHO, gsm48_rx_gmm_ra_upd_req() needs to be refactored. It does not check whether the received msgb actually contains any data (like we do in
OsmoMSC), so sending an incorrect / incomplete message would crash OsmoSGSN.

#13 - 08/13/2019 04:12 PM - lynxis
- Related to Bug #3995: OsmoSGSN doesn't close SCCP connection after successful LU over IuPS added

#14 - 09/04/2019 09:12 AM - laforge

is there any status update on this one? How did you handle this at CCCamp2019? I think this is a rather important bug to resolve, if possible without
rewriting all of the SGSN :)

#15 - 09/04/2019 09:44 AM - pespin

I think I saw some related patches in osmo-sgsn.git branch "cccamp2019" and they will be submitted soon, probably after refactoring patches are
merged.

#16 - 09/12/2019 12:50 AM - lynxis

I've started refactoring those patches to be mergable.
https://gerrit.osmocom.org/q/topic:%22upstream_camp%22+(status:open%20OR%20status:merged)

#17 - 09/15/2019 11:18 PM - lynxis
- % Done changed from 0 to 50

#18 - 09/16/2019 07:38 PM - lynxis
- Related to Bug #1977: 3G IuPS is unreliable added

#19 - 01/08/2020 10:38 PM - laforge
- Status changed from In Progress to Stalled
- Assignee changed from lynxis to sysmocom

#20 - 01/21/2020 02:45 PM - pespin

Hi lynxis, can you write a short summary on the status of what you did here?
From what I understand, all patches you shared link with are merged except this one which is not ready yet:
https://gerrit.osmocom.org/c/osmo-sgsn/+/15487
You added SGSN_Tests_Iu to osmo-ttcn3-hacks.git, and it currently is running only one test (TC_iu_attach) in jenkins dockerized setup, which is passing fine.

I see then that there's also more tests not enabled by default in SGSN_Tests_Iu.ttcn's control(), which probably are the tests you were using to test the patch that was yet not merged and which is expected to support ran swapping:
TC_iu_attach_geran_rau
TC_geran_attach_iu_rau

Can you share your thoughts if I'm missing something?

#21 - 01/21/2020 05:32 PM - daniel

I looked at the patches mentioned and I think the one that would fix this issue is:
https://gerrit.osmocom.org/c/osmo-sgsn/+/15487 which is still WIP

#22 - 01/21/2020 06:19 PM - lynxis

pespin The only parts missing, is resolv your comments and take a look if the outcommend test cases now succeed.

#23 - 01/21/2020 06:46 PM - daniel

- Status changed from Stalled to In Progress
- Assignee changed from sysmocom to daniel

Okay, I cherry-picked it to master and am testing with the disabled tests now. Will look at the review comments as well.

#24 - 01/21/2020 07:08 PM - daniel

Some improvements - the SGSN doesn't crash anymore and one of the tests passes:

```
<testcase classname='SGSN_Tests_Iu' name='TC_iu_attach_geran_rau' time='2.081220'/>
<testcase classname='SGSN_Tests_Iu' name='TC_geran_attach_iu_rau' time='2.093987'>
  <error type='DTE'/></error>
</testcase>
```

#25 - 01/22/2020 05:34 PM - daniel

- % Done changed from 50 to 60

Both tests pass sometimes. The failure seems to be an issue with shutting down the test. Sometimes the RAU Accept is being sent on a closed port/connection after the test has passed. It seems when getting a SecurityModeCmd the function f_routing_area_update doesn't wait for the RAU accept, but returns after receiving the Command.

05/15/2020
A bit back and forth about the proper way to address this issue, but there is progress.

See https://gerrit.osmocom.org/q/topic:%22OS%25233727%22+(status:open%20OR%20status:merged) for a list of changes related to this issue

#27 - 02/07/2020 09:30 AM - daniel
- Status changed from In Progress to Resolved
- % Done changed from 80 to 100

The important patches, notably https://gerrit.osmocom.org/c/osmo-sgsn/+/15487 got merged.

The one remaining change https://gerrit.osmocom.org/c/osmo-sgsn/+/17080 is not really relevant to this segfault, so closing this issue.