OsmoSGSN - Bug #4602

SGSN crash with "Assert failed mm->gb.llme == NULL gprs_sgsn.c:358"

06/08/2020 06:22 PM - laforge

Status:	Feedback	**Start date:**	06/08/2020
Priority:	Normal	**Due date:**	
Assignee:	lynxis	**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

In a test lab installation using a non-osmocom BSS + 3G RAN, the SGSN every so often crashes with the following last lines:

The SGSN is crashing from time to time with:

```
Jun 08 15:23:56 osmo-cn osmo-sgsn[4976]: <0018> iu_client.c:547 handle_co_initial(dir=1, proc=19)
Jun 08 15:23:56 osmo-cn osmo-sgsn[4976]: <0018> iu_client.c:174 New RNC 1203 at RI=2,PC=1204,SSN=1
42
Jun 08 15:23:56 osmo-cn osmo-sgsn[4976]: <0018> iu_client.c:257 RNC 1203: new LAC 123 RAC 1
Jun 08 15:23:56 osmo-cn osmo-sgsn[4976]: <0002> gprs_gmm.c:1561 MM(---/ffffffff) -> GMM RA UPDATE
REQUEST type="periodic updating"
Jun 08 15:23:56 osmo-cn osmo-sgsn[4976]: <0002> gprs_gmm.c:1636 MM(901700000040778/fa8d76a4) Looke
d up by matching TLLI and P_TMSI. BSSGP TLLI: 00000000, P-TMSI: fa8d76a4 (00000000), TLLI: fa8d76a
4 (fa8d76a4), RA: 901-70-123-1
Jun 08 15:23:56 osmo-cn osmo-sgsn[4976]: <0002> gprs_gmm_fsm.c:170 MM_STATE_Gb(3572395996)[0x55d97
cd93740]{Standby}: Event E_MM_IMPLICIT_DETACH not permitted
Jun 08 15:23:56 osmo-cn osmo-sgsn[4976]: <0002> gprs_gmm.c:1099 GMM(gmm_fsm)[0x55d97cd93610]{Commo
nProcedureInitiated}: Event E_GMM_COMMON_PROC_INIT_REQ not permitted
Jun 08 15:23:57 osmo-cn osmo-sgsn[4976]: <0018> iu_client.c:570 handle_co(dir=2, proc=6)
Jun 08 15:23:57 osmo-cn osmo-sgsn[4976]: <0002> gprs_gmm.c:1430 MM(901700000040778/fa8d76a4) <- RO
UTING AREA UPDATE ACCEPT
Jun 08 15:23:57 osmo-cn osmo-sgsn[4976]: <0018> iu_client.c:570 handle_co(dir=1, proc=20)
Jun 08 15:23:57 osmo-cn osmo-sgsn[4976]: <0002> gprs_gmm.c:1757 MM(901700000040778/fa8d76a4) -> RO
UTING AREA UPDATE COMPLETE
Jun 08 15:23:57 osmo-cn osmo-sgsn[4976]: <0002> gprs_gmm.c:1765 MM_STATE_Iu[0x55d97cd97350]{Detach
ed}: Event E_PMM_RA_UPDATE not permitted
Jun 08 15:25:50 osmo-cn osmo-sgsn[4976]: <0018> iu_client.c:570 handle_co(dir=1, proc=11)
Jun 08 15:25:50 osmo-cn osmo-sgsn[4976]: <0018> iu_client.c:570 handle_co(dir=2, proc=1)
Jun 08 15:25:50 osmo-cn osmo-sgsn[4976]: <0002> gprs_ranap.c:135 MM(901700000040778/fa8d76a4) IU r
elease for imsi 901700000040778
Jun 08 15:28:15 osmo-cn osmo-sgsn[4976]: <0002> gprs_gmm.c:1021 MM(901700000040778/fa8d76a4) Cance
lled, deleting context silently
Jun 08 15:28:15 osmo-cn osmo-sgsn[4976]: <0002> gprs_gmm.c:193 MM(901700000040778/fa8d76a4) Cleani
ng MM context due to access cancelled
Jun 08 15:28:15 osmo-cn osmo-sgsn[4976]: Assert failed mm->gb.llme == NULL gprs_sgsn.c:358
```

any ideas?

I will of course try to create better traces (combined pcap with GSMTAP libosmocore logs) but this may take some time.

Related issues:

Related to OsmoSGSN - Bug #4604: Lots of "Unusual event"	**New**	**06/08/2020**
Related to OsmoSGSN - Bug #4605: GMM_ATTACH_REQ_FSM: Event E_AUTH_RESP_RECV_S...	**New**	**06/08/2020**
Related to OsmoSGSN - Bug #3964: SIGSEGV in sndcp_sm_deactivate_ind()	**New**	**04/29/2019**

History

#1 - 06/08/2020 07:02 PM - laforge

- Related to Bug #4604: Lots of "Unusual event" added

#2 - 06/08/2020 07:05 PM - laforge

- Related to Bug #4605: GMM_ATTACH_REQ_FSM: Event E_AUTH_RESP_RECV_SUCCESS not permitted added

#3 - 06/08/2020 07:06 PM - pespin

If I'm correct in the setup 2G and 3G are being used at the same time, so to me it looks like some context first done over 2G afterwards registers through 3G and previous 2G mmctx was not cleaned up properly.

#4 - 06/08/2020 07:12 PM - fixeria

- Related to Bug #3964: SIGSEGV in sndcp_sm_deactivate_ind() added

#5 - 06/11/2020 03:48 PM - lynxis

From the log I think the GPRS Suspend does the problem. AFAIK GPRS Suspend happens in our setup only in 2G when a calls comes in.

EDIT: We don't have ttcn3 tests for this.