OsmoMSC - Feature #3615

Feature # 2583 (Resolved): SGsAP Interface for LTE/ePC CSFB Support

SGs subscriber state machine

10/02/2018 04:48 PM - laforge

Status:	Resolved	**Start date:**	10/02/2018
Priority:	High	**Due date:**	
Assignee:	dexter	**% Done:**	100%
Category:	SGs Interface		
Target version:			
Resolution:			

Description

3GPP TS 29.118 section 4.2.2 describes the SGs state machine for each subscriber in the VLR (in our case OsmoMSC). We need to implement that state machine as osmo_fsm.

Related issues:

Related to OsmoMSC - Bug #3704: When Paging request for SMS is unanswered, os...	**Resolved**	**11/22/2018**

History

#1 - 10/02/2018 05:55 PM - laforge

- Priority changed from Normal to High

#3 - 10/10/2018 08:42 PM - laforge

- Status changed from New to In Progress

- Assignee set to laforge

- % Done changed from 0 to 20

initial code for the osmo-msc side is at http://git.osmocom.org/osmo-msc/log/?h=laforge/sgsap

The completely untested code contains:

- data structures for SGs connection, SGs MME, SGs per-UE context
- FSM for managing the VLR reset procedure to a given MME
- SGs server over SCTP using libosmo-netif, listening for MME connections
- per-UE FSM described in 3GPP spec
- message encoding/decoding helper functions
- VTY for configuring SGs interface related settings (ip/port, timers, vlr name, ...)

#4 - 10/24/2018 02:52 PM - dexter

Note: I have had a look at laforge/sgsap and on laforge/sgs in osmo-ttcn3-hacks. I checked the fsm, the events and states match what is in the spec. We should discuss the next steps. I think having a TTCN3 test that sends a RESET IND and expects a RESET ACK from osmo-msc could be a first milestone.

#5 - 10/24/2018 03:30 PM - laforge

Hi Philipp,

I want to have that reset procedure test hopefully working today, and then merge
the related libosmocore + TTCN3 code.

Feel free to review osmo-msc in the context of adding a new SGs "ran type", and how
you would go about that in general.

Regards,
Harald

#6 - 10/28/2018 11:26 PM - laforge

- Status changed from In Progress to Stalled

#7 - 11/01/2018 05:07 PM - dexter

- Status changed from Stalled to In Progress

- Assignee changed from laforge to dexter

I have done some clean ups and split ups to the existing code as the long c-file got difficult to read. There is now an vlr_sgs_fsm.c in /vlr that contains the FSM that is allocated with each subscriber. I have kept the sgs_iface.c outside the HLR and probably we should leave it there but I am not sure with it.

I also have parts of the LU now running. When the TTCN3 test sends an LU, a function in hlr.c/hlr.h is called. This function searches/creates the subscriber by its IMSI and dispatches a signal to the FSM. The FSM then initiates the LU with the HLR. I can already see the response in GSUB and the VLR knows that it is for an SGs LU because the FSM is in SGS_UE_ST_LA_UPD_PRES at that moment. The FSM in the spec says that the transition has to happen when the LU ACCEPT or LU REJECT is sent. We could do the transition early once we got the response from the HLR and trigger the sending from the message from the SGs FSM, but that would violate the spec and it would also not be sensitive to errors that may happen on the SCTP. What I have in mind is to give the function that triggers the SGs LU a callback, that then controls the sending of the ACCEPT/REJECT messages in sgs_iface.c. Also sgs_iface.c will then take care that the relevant signals are dispatched to vlr_sgs_fsm.c. This closes the loop then.

From the logs I can see that that my LU that is triggered from TTCN3 is apparently accepted. However, I am still not sure which members I must populate before performing the LU, but for now I think it looks to me like I am on the right way.

The changes I made can be found on pmaier/sgsap

#8 - 11/02/2018 05:23 PM - dexter

I have now the LU working, but I think its not quite right yet. The HLR gets requested and the response is handled, but I think I am not yet populating the struct members of vlr_subscriber correctly yet. I also do not get a TMSI yet. I have also some open questions about the LU and the DETACH, we should discuss those next week. However, all of the existing TTCN3 tests are now passing so I think we need some more test coverage now.

#9 - 11/12/2018 04:37 PM - dexter

Since the last update I have improved the paging so that it updates the internal states properly and handles Ts5. In TTCN3 I introduced CTRL-Iface to the MSC tests so that the tests can observe the state of the SGs association, which I think is important because the association state is an integral part of the whole feature. As far as the paging is concerned I am currently only testing failure cases since a success case would mean to respond with a service request and do real stuff. At the moment I am working on improving the LU. The TTCN3 tests now check for the presence of a TMSI in the LU-Accept. If there is a TMSI a TMSI REALLOCATION COMPLETE is sent. The MSC already receives this message but is not processing it yet. The TTCN3 test passes so far.

#10 - 11/16/2018 06:02 PM - dexter

- % Done changed from 20 to 30

The TMSI reallocation process should now work. The TMSI is kept in vsup->tmsi_new until the TMSI reallocation completes. If the MME does not respond with a TMSI reallocation for some reason the TMSI is considered as deallocated.

I focused now on MT SMS. I am now at the point where I can trigger an SMS via the VTY. Then TTCN3 sees the paging via SGs and responds with a SERVICE REQUEST. The MSC then sends unit-data through the SGs interface. However, I am not yet able to answer in TTCN3 and there is also no receive function for unit-data on the SGs interface yet. I can already see that the paging is stopped on the MSC side. Probably we need to do something about the paging anyway because at the moment the MSC trys to page multiple times as there is no answer. To my understanding it should be exactly once and then Ts5 starts running.

I am currently somewhat stuck on the TTCN3 side. The templates for the unit-data require octetstrings for the dtap/nas messages so I am having difficulties to use the L3 templates there.

#11 - 11/19/2018 10:00 PM - dexter

I managed to resolve the problems I had on the TTCN3 side. There is indeed a mechanism implemented to get the NAS message container (that holds the DTAP message) directly decoded via SGsAP.receive and SGsAP.send works the same way, just like with BSSAP.send/receive. I did not immediately realize that such a mechanism was in place so I expected the wrong templates in my code but now since I use the right templets things seem to be fine.

There seems to be indeed an SMS transfered between osmo-msc and TTCN3 but something is not quite right, somehow the msc tries to deliver the SMS again. I guess I either messed up some state machine here or the MSC has problems to understand the messages that TTCN3 sends. I think the first is true. I think I will have to learn more about how osmo-msc handles subscribers and connections, especially the put/get mechanism that is supposed to detect when a conn is no longer in use.

#12 - 11/21/2018 06:00 PM - dexter

- % Done changed from 30 to 50

I have nor MO and MT SMS working. The testcases look good so far, also on the MSC side everything looks fine now. Also the Release messages from the MSC are now where they should be, which basically means that the ref-counting is now correct. However, I discovered that I still have a ref-counting problem in the VLR so this needs to be fixed and I also need more testcoverage regarding paging and unit-data transfers to check some odd cases. Once that is done I think we are good to focus on the CSFB voice call scenario.

I have pushed the current state of osmo-msc to gerrit, the ttcn3 tests are not yet updated but the current statue can be found at pmaier/sgsap

#13 - 11/21/2018 06:31 PM - fixeria

BTW, I just accidentally noticed a potential copy-paste error in pmaier/sgsap:

https://git.osmocom.org/osmo-msc/diff/src/libmsc/gsm_09_11.c?h=pmaier/sgsap&id=a928b204202d64e0b813f87c0381777c695c139b

```
trans->paging_request = subscr_request_conn(vsub,
    &handle_paging_event, trans, "GSM 09.11 SS/USSD",
    SGSAP_SERV_IND_SMS); // !!!
```

GSM 09.11 is not about SMS, it's about SS/USSD. I couldn't find the definition
of SGSAP_SERV_IND_*, but it seems there should be something like SGSAP_SERV_IND_SS_USSD.

#14 - 11/26/2018 09:24 AM - dexter

- Related to Bug #3704: When Paging request for SMS is unanswered, osmo-msc sends infinit number of paging requests added

#15 - 11/26/2018 06:11 PM - dexter

I am currently working out some edge cases for SMS in TTCN3, this is important to see if the the MSC recovers properly from failed SMS deliveries etc. While doing this I stumbled upon a problem with the SMS queue and the paging behavior. More infos can be found at in task #3704. Since SGs allows to actively reject paging request we need to be able to make paging stop.

#16 - 12/03/2018 05:10 PM - dexter

There was quite a log refactoring going on on the current master of osmo-msc. I have rebased my sgsap branch. Unfortunately I had some trouble but now all TTCN3 tests (except TC_sgsap_mt_sms_and_nothing, which is known) tests pass. Since the SMS/Paging problems are now repaired I am confident to get TC_sgsap_mt_sms_and_nothing passing as well soon.

#17 - 12/07/2018 05:19 PM - dexter

- % Done changed from 50 to 80

Now the SMS tests work as they should. In case the MME does not respond to any paging, the MSC/VLR will try a few times and then give up. I also added a first test for a CSFB call. This also works so far, but there is still some extension of the test coverage needed.

On the MSC side I did some improvements, a few use-after free bugs are fixed and the VLR ref-counting was a little bit messed up as well. This is now clean. I also cleaned up a lot of other minor things. Technically the patchset would build now in jenkins, but since I have decided to separate some parts (generator functions) out to libosmocore it currently does not build but this is not a problem.

All changes can be found in the gerrit review as well as on my private pmaier/sgsap branches in libosmocore.git, and omso-msc.git as well as in osmo-ttcn3-hacks.git.

Form the technical perspective the patch-sets are developed far enough so that an interop test with a real MME would make sense.

#18 - 12/10/2018 08:27 AM - dexter

The related libosmocore patches are now merged to master, so there is no need anymore to checkout pmaier/sgsap for libosmocore. osmo-msc will compile just fine against a current master libosmocore. I will delete the pmaier/sgsap on libosmocore soon.

#19 - 12/17/2018 04:26 PM - dexter

- % Done changed from 80 to 90

I have increased the test coverage of the TTCN3 tests. We now execute a few BSSAP operations after each SGSAP related test. This way we make sure that the MSC does not end up in a malfunctioning state once an SGSAP operation has been performed.

Also I checked back on the CSFB call test that was only working before re regular BSSAP LU was executed. I was assuming that this is related to missing authentication tuples in the VLR, but after inspection it turned out to be just a problem with the HLR flags. This is now corrected and I added functionality to the VTY to inspect those flags. We now have a test with BSSAP LU in the beginning and one without. Both work fine.

In SGSAP in may happen that the VLR sends a paging and the MME responds with an LU instead of a service request. This is rare, but can happen when MME and VLR loose sync (e.g. the VLR was reset). In those cases the VLR must go through the LU and check Ts5 (SGs paging timeout) when done. When Ts5 is not expired, then the VLR should resend the paging. I have added a TTCN3 test that simulates this behavior and added the missing bits to the MSC so that this corner case can be handled.

I also fixed smaller bugs here and there while testing. While studying the spec I noticed that there is also an MM Info message on SGSAP. This is not implemented yet. Unfortunately our TTCN3 testsuite seems not to support/test this on BSSMAP.

#20 - 12/21/2018 05:25 PM - dexter

I have now also integrated the sending of MM Info after a successful LU, like we already have it for the regular RANs (2G, 3G). Also the TTCN3 tests now check if the MM Info that is sent by the MSC contains consistent data.

The pmaier/sgsap branches on osmo-ttcn3-hacks and osmo-msc are rebased to current master and up to date.

#21 - 01/15/2019 11:03 AM - dexter

I have gone through all current review issues and fixed them now. Everything is rebased to current master, also the pmaier/sgsap branches are up to date now.

#22 - 01/21/2019 04:24 PM - dexter

The review process is still ongoing. At the moment I am through with the second row of review issues and I am waiting for feedback.

#23 - 02/11/2019 04:26 PM - dexter

- Status changed from In Progress to Resolved

- % Done changed from 90 to 100

The review process is done now. I think we can close this now and process follow up issues in separate tasks. See also #3614 and #3778