OsmoMSC - Bug #3122

fix subscr_conn fsm: safely catch all compl-l3 failures, properly handle all release situations

03/28/2018 01:58 PM - neels

Status:	Resolved	**Start date:**	03/28/2018
Priority:	High	**Due date:**	
Assignee:	neels	**% Done:**	100%
Category:			
Target version:			
Resolution:		**Spec Reference:**	

Description

Various reports and patches pop up with various people about the MSC's subscr_conn FSM not handling specific corner cases properly.

- If anything goes wrong during compl-l3, the FSM might think that it is busy with auth+ciph. Need a separate state for auth+ciph; then at the end of msc_compl_l3() discard any conn that is still in state 'NEW'.
- For failure situations causing premature conn release, properly handle release messages and receive responses in a separate 'RELEASING' state.

- In the course of that, it may make sense to refactor:
  - closely tie the FSM with the struct gsm_subscriber_connection. Historically, the ownership was shared between libbsc and libmsc, complicating the ref-count in that the FSM was a separate entity. It should be possible to refactor the conn struct and the FSM as "a single entity", triggering a release event by the ref-count reaching zero, instead of needing explicit "release if unused" events.
  - ~~CM Service Requests may actually overlap. The conn >received_cm_service_request however is a boolean, which means that we possibly lose the pending-ness of a second CM Service Request if a first one concludes at just the wrong time, or if two come in "consecutively".~~ -> #3156

That's a lot to ask for in a single issue, but it makes sense to tie all of these items into a refactoring of the subscr_conn FSM.

Related issues:

Related to OsmoMSC - Bug #3062: osmo-msc crash while running osmo-gsm-tester ...	**Resolved**	**03/13/2018**
Related to OsmoMSC - Bug #3125: testcase for fixed "osmo-msc crashes while ha...	**New**	**03/29/2018**

History

#1 - 03/28/2018 01:59 PM - neels

- Related to Bug #3062: osmo-msc crash while running osmo-gsm-tester voice:nanobts added

#2 - 03/29/2018 03:34 PM - pespin

- Related to Bug #3125: testcase for fixed "osmo-msc crashes while handling a call" added

#3 - 04/03/2018 12:12 AM - neels

- Status changed from New to In Progress

- % Done changed from 0 to 60

#4 - 04/09/2018 01:15 AM - neels

Testing against the current ttcn3 test suite yields 6 tests being fixed (proper Clear Request / Clear Complete messages now).
But a corner case (#3062) is re-raised by the changes, still need to address that (shouldn't be too hard). It should also be part of the ttcn3 (or at least some) test suite.
I would like to get this merged sooner rather than later and get back to inter-bsc HO, but #3062 shows that I need to be patient enough to not break things that had workarounds before.

Also still trying to reproduce #3125 in ttcn3, see there. Took me a lot of time to get a simple MNCC REL REQ case going (mostly log interpretation retard: this time I got mixed up between MNCC Alerting vs. DTAP CC Alerting, and then it took forever to figure out that I need to expect an IPACC DLCX + ACK to not run into T_guard...) -- now it still needs to actually trigger the bug instead of succeeding, so that I can see whether the new code fixes the bug.

#5 - 04/11/2018 11:51 AM - neels

- Subject changed from fix subscr_conn fsm: safely catch all compl-l3 failures, properly handle all release situations, handle overlapping CM Service Requests to fix subscr_conn fsm: safely catch all compl-l3 failures, properly handle all release situations

- Description updated

- % Done changed from 60 to 90

waiting for CR on https://gerrit.osmocom.org/#/q/status:open+project:osmo-msc+branch:master+topic:fsm_refactor

I think handling overlapping CM Service Requests should be a separate issue -> #3156

#6 - 04/15/2018 08:57 PM - neels

- Status changed from In Progress to Resolved

- % Done changed from 90 to 100

all patches are merged now