After issuing the reset of the BTS, something goes wrong.

Relevant end of the log:

```
<0004> bts_nokia_site.c:1693 ABIS_OM_MDISC_FOM
<0004> bts_nokia_site.c:1521 (0x81) NOKIA_BTS_ACK
<0004> bts_nokia_site.c:1553 ACK = 1
<0014> input/lapd.c:541 LAPD DL-RELEASE request TEI=1 SAPI=62
<0014> lapd_core.c:2243 Message DL-RELEASE-REQUEST received in state LAPD_STATE_MF_EST (dl=0x91171c8)
<0014> lapd_core.c:237 new state LAPD_STATE_MF_EST -> LAPD_STATE_IDLE (dl=0x91171c8)
<0014> lapd_core.c:230 stop T203 (dl=0x91171c8)
<0014> input/lapd.c:656 LAPD DL-RELEASE confirm TEI=1 SAPI=62
<0014> input/lapd.c:274 LAPD Freeing SAP for SAPI=62 / TEI=1 (dl=0x91171c8, sap=0x91171b8)
<0014> lapd_core.c:310 Resetting LAPDm instance
<0014> lapd_core.c:237 new state LAPD_STATE_IDLE -> LAPD_STATE_IDLE (dl=0x91171c8)
<0014> lapd_core.c:237 new state LAPD_STATE_IDLE -> LAPD_STATE_NULL (dl=0x91171c8)
<0014> lapd_core.c:1681 we are busy, send RNR (dl=0x91171c8)
Segmentation fault
```

So right after freeing the SAP, we try to send a RNR on the dl that was just freed so obviously this doesn't workout ...

I couldn't really generate a backtrace, gdb didn't give anything meaningful even on a binary with debug symbols.

Related issues:
- Related to OsmoBSC - Bug #1761: LAPD: segfault when bootstrapping Nokia InSite
  - Status: In Progress
  - Due date: 07/03/2016
- Related to OsmoBSC - Feature #4514: OM2000 Support for Ericsson RBS6000 / DUG 20
  - Status: In Progress
  - Due date: 04/27/2020

History

#1 - 05/04/2019 11:57 AM - laforge

On Sat, May 04, 2019 at 11:14:10AM +0000, tnt [REDMINE] wrote:

    So right after freeing the SAP, we try to send a RNR on the dl that was just freed so obviously this doesn't workout ...

The RNR is generated from the lapd_rx_i() function, which seems to suggest we receive an I frame on a LAPD instance (dl) that had just been free'd?

#2 - 05/04/2019 12:20 PM - tnt

With breakpoints I captured that during the same call chain to process the received LAPD message, we first free the SAP instance and a bit later we try to send a RNR over it.

```
lapd_core.c:1604 - This will trigger the SAP release
lapd_core.c:1683 - This tries to send a RNR
```

Breakpoint 1, lapd_sap_free (sap=0x822f1b8) at input/lapd.c:271
warning: Source file is more recent than executable.
271 {
#3 - 05/08/2019 03:14 PM - tnt
- Related to Bug #1761: LAPD: segfault when bootstrapping Nokia InSite added

#4 - 07/18/2019 06:00 AM - laforge
- Assignee set to laforge

#5 - 04/27/2020 08:23 PM - laforge
- Related to Feature #4514: OM2000 Support for Ericsson RBS6000 / DUG 20 added

#7 - 05/11/2020 05:22 AM - tnt
- Status changed from New to Closed
That’s fixed actually.