Description

Type "apropos word" to search for commands related to "word"...

Reading symbols from /usr/bin/osmo-sgsn...done.

```
[New LWP 22489]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Core was generated by `/usr/bin/osmo-sgsn -c /etc/osmocom/osmo-sgsn.cfg'.
Program terminated with signal SIGSEGV, Segmentation fault.
#0 0x0000560fba77e920 in do_act_pdp_req (mmctx=mmctx@entry=0x560fba7acfb0, msg=msg@entry=0x560fba9489f0, delete=delete@entry=0x7fff093b068f) at ../../../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:2826
#1 0x0000560fba76c677 in gsm48_rx_gsm_act_pdp_req (_msg=0x560fba9489f0, mmctx=0x560fba7acfb0) at ../../../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:2939
#2 0x0000560fba7acbe70 in gsm0408_gprs_rcvmsg_gb (msg=msg@entry=0x560fba9489f0, lme=llme@entry=0x7fff093b068f) at ../../../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:3188
#3 0x0000560fba76e98d in gprs_llc_rcvmsg (msg=0x560fba9489f0, tv=<optimized out>) at ../../../../../src/libosmocore/src/gb/gprs_llc.c:1003
#4 0x0000560fba76a9cd in ?? ()
#5 0x0000560fba762ebd08 in do_act_pdp_req (mmctx=mmctx@entry=0x560fba7acfb0, msg=msg@entry=0x560fba9489f0, delete=delete@entry=0x7fff093b068f) at ../../../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:2826
#6 0x0000560fba76c677 in gsm48_rx_gsm_act_pdp_req (_msg=0x560fba9489f0, mmctx=0x560fba7acfb0) at ../../../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:2939
#7 0x0000560fba7acbe70 in gsm0408_gprs_rcvmsg_gb (msg=msg@entry=0x560fba9489f0, lme=llme@entry=0x7fff093b068f) at ../../../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:3188
#8 0x0000560fba7acbe70 in gsm0408_gprs_rcvmsg_gb (msg=msg@entry=0x560fba9489f0, lme=llme@entry=0x7fff093b068f) at ../../../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:3188
```

(gdb) bt
```
#0 0x0000560fba77e920 in do_act_pdp_req (mmctx=mmctx@entry=0x560fba7acfb0, msg=msg@entry=0x560fba9489f0, delete=delete@entry=0x7fff093b068f) at ../../../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:2826
#1 0x0000560fba76c677 in gsm48_rx_gsm_act_pdp_req (_msg=0x560fba9489f0, mmctx=0x560fba7acfb0) at ../../../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:2939
#2 0x0000560fba7acbe70 in gsm0408_gprs_rcvmsg_gb (msg=msg@entry=0x560fba9489f0, lme=llme@entry=0x7fff093b068f) at ../../../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:3188
```
{gdb} print
The history is empty.
{gdb} print mmctx
$1 = (struct sgsn_mm_ctx *) 0x560fba7acfb0
{gdb} frame 0
0 gsm48_tx_gsm_act_pdp_acc (pdp=0x560fba776920) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:2535
2535 msgb_v_put(msg, pdp->lib->radio_PRI);
{gdb} p pdp
$2 = (struct sgsn_pdp_ctx *) 0x560fba776920
{gdb} p pdp->lib
$3 = (struct pdp_t *) 0x0
$4 = (struct pdp_t *) 0x0
{gdb} p mmctx->pmm_state
$6 = MM_READY

Associated revisions
Revision 424628d5 - 09/06/2019 07:34 PM - pespin
sgsn: Reject PdpActReq if no GTP pdp ctx exists

It could happen that SGSN drops GTP side of a pdp ctx (pdp->lib=NULL) while still maintaing the other side (to notify about the entire pdp ctx being torn down). If a PdpActReq arrives during that time, we need to account for that situation, otherwise osmo-sgsn crashes accessing pdp->lib.
If no pdp->lib is found at that time, let's reject the request and expect at some point later in time the entire pdp context will be destroyed and reestablished.

Related: OS#4173
Change-Id: I6dd87557ebb26fdbd280504abde10d976acecf64

History
#1 - 08/29/2019 12:45 PM - pespin
- Status changed from New to Feedback
- Assignee set to lynxis

I submitted this patch, assigning to lynxis for him to review it.
https://gerrit.osmocom.org/c/osmo-sgsn/+/15330 sgsn: Reject PdpActReq if no GTP pdp ctx exists

#2 - 09/09/2019 09:13 AM - pespin

Patch has been merged. lynxis please have a look and close the ticket if fine for you.

#3 - 09/10/2019 12:56 PM - lynxis
- Status changed from Feedback to Closed

LGTM.

#4 - 09/15/2019 11:28 PM - lynxis
- % Done changed from 0 to 100