# OsmoGGSN (former OpenGGSN) - Bug #4172

## osmoggsn crashes when stopping

08/23/2019 10:00 PM - lynxis

| | | | |
|---|---|---|---|
| **Status:** | New | **Start date:** | 08/23/2019 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | | **% Done:** | 0% |
| **Category:** | | | |
| **Target version:** | | | |
| **Spec Reference:** | | | |

**Description**

on the cccamp 2019 the ggsn crashed.
Direct before that, the sgsn crashed.

```
(gdb) bt
#0  gtp_delete_context_req2 (gsn=0x0, pdp=0x7f9e66094138, cbp=0x0, teardown=1)
    at ../../../src/osmo-ggsn/gtp/gtp.c:2449
#1  0x000055702696abf6 in pool_close_all_pdp (pool=0x557027b1ed90) at ../../../src/osmo-ggsn/ggsn/
ggsn.c:111
#2  0x000055702696cc17 in apn_stop (apn=0x557027b1eaa0) at ../../../src/osmo-ggsn/ggsn/ggsn.c:124
#3  0x000055702696ce60 in ggsn_stop (ggsn=0x557027b1e650) at ../../../src/osmo-ggsn/ggsn/ggsn.c:11
82
#4  0x0000557026968a16 in ggsn_stop (ggsn=0x557027b1e650) at ../../../src/osmo-ggsn/ggsn/ggsn.c:11
77
#5  main (argc=3, argv=0x7fffd20cd068) at ../../../src/osmo-ggsn/ggsn/ggsn.c:1319
```

### History

**#1 - 08/29/2019 10:34 AM - pespin**

*- Subject changed from osmoggsn crashs when stopping to osmoggsn crashes when stopping*

**#2 - 08/29/2019 11:35 AM - pespin**

This one looks really weird. pdp->gsn should never be NULL, since pdp is always related to a gsn_t. In no place pdp->gsn is set to NULL, and actually only place where pdp->gsn is set is in gtp_pdp_newpdp():

```
(*pdp)->gsn = gsn;
```

And gsn cannot be NULL there because it's deferred to get access to pdpa before in the same function:

```
struct pdp_t *pdpa = gsn->pdpa;
```

However, pdp_freepdp() does this:

```
memset(pdp, 0, sizeof(struct pdp_t));
```

So only way pdp->gsn is NULL is that pdp_freepdp was already called on that pdp context.

osmo-ggsn only makes use of pdp_freepdp() in one place and it's not triggered here: cb_conf(type=GTP_DELETE_PDP_REQ), basically because we free the pdp context before that point whenever we do a DeletePdpReq in osmo-ggsn. For other cases, osmo-ggsn calls gtp_freepdp_teardown() which would call the delete_ctx cb and appropiatelly remove it from ippool.

libgtp never calls pdp_freepdp() (which does not call delete_ctx cb), and it should only do it when the user/app doesn't have knowledge abot that pdp context (so no associated structures are managed).

Would be great to know which commit/version was this one running when the crash appeared.

Some log file would have been great too, it would be a lot more clear to understand what happened.