# OsmoSGSN - Bug #3466

## gprs_gb_parse_dtap does not handle "DEACT PDP ACK"

08/16/2018 10:38 AM - stsp

| | | | |
|---|---|---|---|
| **Status:** | Feedback | **Start date:** | 08/16/2018 |
| **Priority:** | Low | **Due date:** | |
| **Assignee:** | lynxis | **% Done:** | 90% |
| **Category:** | osmo-gbproxy | | |
| **Target version:** | | | |
| **Spec Reference:** | | | |

**Description**

While investigating issue #3178, we found that gprs_gb_parse_dtap() is logging unhandled messages:

```
<0011> gprs_gb_parse.c:384 Unhandled GSM 04.08 message type unknown 0x47 for protocol discriminato
r SM
```

The meaning of message type 0x47 is "DEACT PDP ACK"

From osmo-sgsn's gsm_04_08_gprs.h:

```
/* Table 10.4a, GPRS Session Management (GSM) */
#define GSM48_MT_GSM_ACT_PDP_REQ        0x41
#define GSM48_MT_GSM_ACT_PDP_ACK        0x42
#define GSM48_MT_GSM_ACT_PDP_REJ        0x43
#define GSM48_MT_GSM_REQ_PDP_ACT        0x44
#define GSM48_MT_GSM_REQ_PDP_ACT_REJ    0x45
#define GSM48_MT_GSM_DEACT_PDP_REQ      0x46
#define GSM48_MT_GSM_DEACT_PDP_ACK      0x47
```

This happened with a Sony Ericsson "Cyber Shot" phone (I cannot look up the exact model number right now, unfortunately) using an On-Waves test SIM (if in doubt ask pespin for details). The message appears after setting up a data connection profile in the phone's settings menu (select PS connection type, put in an arbitrary APN/user/password), and then trying to visit any website with the phone's browser (labeled "Internet" on the phone's main menu screen).

Browsing websites does not work with this phone (this could be part of larger problem which might not be strictly related to "DEACT PDP ACK"). It shows a full screen error message which states that there was a connection problem. Note that the phone's default homepage is a WAP page that is no longer served by Sony, so I tried browsing www.sysmocom.de and saw the same error. However, browsing works with other phones, e.g. it works with a Samsung Galaxy S2 which doesn't seem to send "DEACT PDP ACK".

The base station was an On-Waves AU running current experimental ONW images (libosmocore 94c0031297abb0bb42a4ea23e68f944622f50469 and osmo-pcu 3df1532e97c5c774a4abefffc2d62b8cc2d468da). I don't know the exact commit of osmo-sgsn, but it is likely close to current master commit 9b5d7f6398295af2ea33493f72917f161e8048de.

In any case, it is obvious that the switch statement in gprs_gb_parse_dtap() does not yet have a case for "DEACT PDP ACK" messages. We still need to determine whether this is an actual problem and if so how it could be fixed.

Please keep in mind that when investigating this issue we might also want to consider other message types which are not yet handled by gprs_gb_parse_dtap() and possibly file issues for any of those other cases as well.

### History

**#1 - 08/16/2018 10:49 AM - stsp**

stsp wrote:

> I don't know the exact commit of osmo-sgsn, but it is likely close to current master commit 9b5d7f6398295af2ea33493f72917f161e8048de.

Ooops, the osmo-sgsn tree I was looking at was a bit out of date.
9b5d7f6398295af2ea33493f72917f161e8048de is from July 16 2018
c503f0acd9668a50529f473492ce4c42de8b882a from Aug 7 is likely a closer match.

#### #2 - 02/23/2019 02:45 PM - laforge

*- Priority changed from Normal to Low*

#### #3 - 04/09/2019 11:23 AM - laforge

*- Assignee changed from sysmocom to lynxis*

#### #4 - 04/14/2019 03:40 AM - lynxis

*- Category set to osmo-gbproxy*

*- Status changed from New to Feedback*

*- Assignee changed from lynxis to daniel*

I don't know the gbproxy well enough. The missing case is not a problem, except the warning.
I've added REQ + ACK messages to the case in https://gerrit.osmocom.org/#/c/osmo-sgsn/+/13628/

daniel as said in the review, please validate my expectations.

#### #5 - 04/14/2019 03:40 AM - lynxis

*- % Done changed from 0 to 90*

#### #6 - 04/18/2019 11:54 AM - daniel

*- Assignee changed from daniel to lynxis*

Looking at the other message types handled in the function only GSM48_MT_GSM_ACT_PDP_REQ seems relevant.

There the apn_ie is extracted and future llc frames might patch the apn. We could set parse_ctx->apn_ie{,_len} back to 0 if we see a GSM48_MT_GSM_DEACT_PDP_ACK, but I don't think that it's necessary.

Any other thoughts?