# OsmoSGSN - Bug #1882

## xid is not re-transmitted on pdp-ctx-ack retransmission

12/19/2016 12:20 PM - dexter

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 12/19/2016 |
| **Priority:** | Low | **Due date:** | |
| **Assignee:** | dexter | **% Done:** | 100% |
| **Category:** | | | |
| **Target version:** | | | |
| **Spec Reference:** | | | |

**Description**

When a pdp-context is established, usually a xid is sent. This works the first time, but when the pdp-ctx-ack is retransmitted from do_act_pdp_req() in gprs_gmm.c the xid negotiation should also be repeated.

### History

**#1 - 02/27/2017 01:45 PM - dexter**

*- Status changed from New to In Progress*

The xid is set off from send_act_pdp_cont_acc() in sgsn_libgtp.c.

```
Fri Dec 23 19:45:34 2016 <000f> gprs_sgsn.c:868 Checking for inactive LLMEs, time = 1579985
Fri Dec 23 19:45:37 2016 <0011> gprs_bssgp.c:797 BSSGP BVCI=23 Rx Flow Control BVC
Fri Dec 23 19:45:38 2016 <0011> gprs_bssgp.c:379 BSSGP TLLI=0xe97ce9c2 Rx UPLINK-UNITDATA
Fri Dec 23 19:45:38 2016 <0012> gprs_llc_parse.c:74 LLC SAPI=1 C   FCS=0x239aa1CMD=UI DATA
Fri Dec 23 19:45:38 2016 <0002> gprs_gmm.c:2251 MM(001010000000002/e97ce9c2) -> ACTIVATE PDP CONTEXT REQ: SAPI
=3 NSAPI=5 IETF IPv4
Fri Dec 23 19:45:38 2016 <0002> gprs_sgsn.c:832 MM(001010000000002/e97ce9c2) Found GGSN 0 for APN 'internet' (
requested 'internet')
Fri Dec 23 19:45:38 2016 <0002> gprs_gmm.c:2142 MM(001010000000002/e97ce9c2) Using GGSN 0
Fri Dec 23 19:45:38 2016 <000f> sgsn_libgtp.c:148 Create PDP Context
Fri Dec 23 19:45:38 2016 <000f> sgsn_libgtp.c:590 libgtp cb_conf(type=16, cause=128, pdp=0x7f2a7cf2b880, cbp=0
x1a877e0)
Fri Dec 23 19:45:38 2016 <000f> sgsn_libgtp.c:365 PDP(001010000000002/0) Received CREATE PDP CTX CONF, cause=1
28(Request accepted)
Fri Dec 23 19:45:38 2016 <0013> gprs_sndcp.c:486 SNSM-ACTIVATE.ind (lle=0x1a855f0 TLLI=e97ce9c2, SAPI=3, NSAPI
=5)
Fri Dec 23 19:45:38 2016 <000f> gprs_gmm.c:2023 PDP(001010000000002/0) <- ACTIVATE PDP CONTEXT ACK
Fri Dec 23 19:45:38 2016 <0012> gprs_llc.c:334 Sending XID request to modem...
Fri Dec 23 19:45:47 2016 <0011> gprs_bssgp.c:797 BSSGP BVCI=23 Rx Flow Control BVC
Fri Dec 23 19:45:57 2016 <0010> gprs_ns.c:582 NSEI=23 Timer expired in mode tns-test (30 seconds)
Fri Dec 23 19:45:57 2016 <0010> gprs_ns.c:515 NSEI=23 Tx NS ALIVE (NSVCI=23)
Fri Dec 23 19:45:57 2016 <0010> gprs_ns.c:554 NSEI=23 Starting timer in mode tns-alive (3 seconds)
Fri Dec 23 19:45:57 2016 <0010> gprs_ns.c:528 NSEI=23 Tx NS ALIVE_ACK (NSVCI=23)
Fri Dec 23 19:45:57 2016 <0010> gprs_ns.c:554 NSEI=23 Starting timer in mode tns-test (30 seconds)
Fri Dec 23 19:45:57 2016 <0011> gprs_bssgp.c:797 BSSGP BVCI=23 Rx Flow Control BVC
Fri Dec 23 19:46:04 2016 <000f> gprs_sgsn.c:868 Checking for inactive LLMEs, time = 1580015
Fri Dec 23 19:46:07 2016 <0011> gprs_bssgp.c:797 BSSGP BVCI=23 Rx Flow Control BVC
Fri Dec 23 19:46:09 2016 <0011> gprs_bssgp.c:379 BSSGP TLLI=0xe97ce9c2 Rx UPLINK-UNITDATA
Fri Dec 23 19:46:09 2016 <0012> gprs_llc_parse.c:74 LLC SAPI=1 C   FCS=0xbdeff1CMD=UI DATA
Fri Dec 23 19:46:09 2016 <0002> gprs_gmm.c:2251 MM(001010000000002/e97ce9c2) -> ACTIVATE PDP CONTEXT REQ: SAPI
=3 NSAPI=5 IETF IPv4
Fri Dec 23 19:46:09 2016 <000f> gprs_gmm.c:2023 PDP(001010000000002/0) <- ACTIVATE PDP CONTEXT ACK
Fri Dec 23 19:46:09 2016 <0011> gprs_bssgp.c:506 BSSGP BVCI=23 TLLI=e97ce9c2 Rx LLC DISCARDED
Fri Dec 23 19:46:10 2016 <0011> gprs_bssgp.c:379 BSSGP TLLI=0xe97ce9c2 Rx UPLINK-UNITDATA
Fri Dec 23 19:46:10 2016 <0012> gprs_llc_parse.c:74 LLC SAPI=3 C   FCS=0x2188e4CMD=XID DATA
Fri Dec 23 19:46:10 2016 <0012> gprs_llc.c:284 Received XID indication from modem.
Fri Dec 23 19:46:10 2016 <0012> gprs_llc_xid.c:255 XID: type=6, data_len=2, data=05f0
Fri Dec 23 19:46:10 2016 <0012> gprs_llc_xid.c:255 XID: type=5, data_len=2, data=05f0
```

If we review the log output, we see that there are no log messages from sgsn_libgtp.c This is no proof, but leads to the suspicion that the second time, things work a little different. If have a look at send_act_pdp_cont_acc() in sgsn_libgtp.c, we see that gsm48_tx_gsm_act_pdp_acc() is called. Grepping for that function we see that gsm48_tx_gsm_act_pdp_acc() is also called from gprs_gmm.c:

```
/* This apparently is a re-transmission of a PDP CTX
 * ACT REQ (our ACT ACK must have got dropped) */
```

```
return gsm48_tx_gsm_act_pdp_acc(pdp);
```

Our call to sndcp_sn_xid_req() is oviously in the wrong place. send_act_pdp_cont_acc() is called from the libgtp side, when the GGSN has created the context. Resending is not the GGSN's business. This happens internally. And thats the reason why it only works the first time, but not the second time.

#### #2 - 02/27/2017 01:46 PM - dexter

*- % Done changed from 0 to 40*

#### #3 - 02/27/2017 05:08 PM - dexter

*- Status changed from In Progress to Resolved*

*- % Done changed from 40 to 100*

Added code that triggers the sending of the XID messages also for pdp-context-ack resends: https://gerrit.osmocom.org/1931

#### #4 - 02/28/2017 05:33 PM - laforge

*- Status changed from Resolved to Closed*