

## OsmoPCU - Bug #1742

### Regression in egprs patch series

06/02/2016 11:39 AM - pierre.baudry

<b>Status:</b> New	<b>Start date:</b> 06/02/2016
<b>Priority:</b> High	<b>Due date:</b>
<b>Assignee:</b> lynxis	<b>% Done:</b> 0%
<b>Category:</b>	
<b>Target version:</b>	
<b>Spec Reference:</b>	
<b>Description</b>	
Original mailing list thread : <a href="http://lists.osmocom.org/pipermail/openbsc/2016-May/009125.html">http://lists.osmocom.org/pipermail/openbsc/2016-May/009125.html</a> / <a href="http://lists.osmocom.org/pipermail/openbsc/2016-June/009329.html">http://lists.osmocom.org/pipermail/openbsc/2016-June/009329.html</a>	
I haven't been able to use gprs service since egprs merge (4f8438a6cd0f34bb22493b13154e382983bbda01).	
The first issue is the T6169 timeout during TBF assignment. A bisection showed that commit f1a7b8fc6651f92a8b7f3f27b7ca05d07f4e44e0 introduced this specific bug ; but even with this commit reverted, the gprs service is still unreliable.	
I am now bisecting d87e1d6ab747423d3668c74d16201a5d967accf0..f1a7b8fc6651f92a8b7f3f27b7ca05d07f4e44e0 and testing at each step connection and reliability on a end user device.	
un-duplicating issues:	
<ul style="list-style-type: none"><li>• Please refer to <a href="#">#1756</a> for why the WAIT_ASSIGN state in f1a7b8fc66 breaks GPRS completely.</li><li>• Discuss reliability after revert of f1a7b8fc66 here.</li></ul>	
<b>Related issues:</b>	
Related to OsmoPCU - Bug #1756: regression: "tbf: Add state WAIT_ASSIGN"	<b>New</b> <b>06/16/2016</b>
Related to OsmoGSMTester - Feature #2820: test GPRS with two (or more) subscr...	<b>Resolved</b> <b>01/07/2018</b>
Related to OsmoPCU - Bug #2890: OsmoPCU TTCN-3 test suite not executed by jen...	<b>Resolved</b> <b>01/27/2018</b>

### History

#### #1 - 06/24/2016 12:03 PM - neels

- Related to Bug #1756: regression: "tbf: Add state WAIT\_ASSIGN" added

#### #2 - 06/24/2016 12:55 PM - neels

- Description updated

Pierre, do you have any details on how the GPRS becomes unreliable even after the revert?

I did see some unreliability as well, in that GPRS is connected but initially not working. This happens particularly when I leave the CN running after testing with the WAIT\_ASSIGN state added to the PCU. When the phone reconnects again, problems seem to be gone.

With clean restarts of the entire CN + BTS + PCU, I don't see reliability problems AFAICT.

So it might be that the GPRS unreliability is still some erratic state stuck after the WAIT\_ASSIGN state testing. Might be an indication of the SGSN state not being cleaned up properly?

Here are some randomly picked log messages I see:

- SGSN log:

```
<0011> gprs_bssgp.c:797 BSSGP BVCI=1800 Rx Flow Control BVC
<000f> sgsn_libgtp.c:514 GTP DATA IND from GGSN, length=52
<0011> gprs_bssgp.c:379 BSSGP TLLI=0xb6400413 Rx UPLINK-UNITDATA
```

```

<0012> gprs_llc_parse.c:74 LLC SAPI=1 C FCS=0xd20b72CMD=UI DATA
<0012> gprs_llc.c:203 LLC RX: unknown TLLI 0xb6400413, creating LLME on the fly
<0011> gprs_bssgp.c:797 BSSGP BVCI=1800 Rx Flow Control BVC
<0011> gprs_bssgp.c:506 BSSGP BVCI=1800 TLLI=b6400413 Rx LLC DISCARDED
<0011> gprs_bssgp.c:379 BSSGP TLLI=0xda9df0d3 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=1 C FCS=0xbcd739CMD=UI DATA
<0011> gprs_bssgp.c:797 BSSGP BVCI=1800 Rx Flow Control BVC
<0011> gprs_bssgp.c:379 BSSGP TLLI=0xda9df0d3 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=1 C FCS=0xc327a2CMD=UI DATA
<000f> gprs_gmm.c:1603 PDP (274018000000012/0) <- ACTIVATE PDP CONTEXT ACK
<000f> gprs_sgsn.c:790 Checking for inactive LLMEs, time = 5710
<0011> gprs_bssgp.c:797 BSSGP BVCI=1800 Rx Flow Control BVC
<0011> gprs_bssgp.c:379 BSSGP TLLI=0xda9df0d3 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=3 C FCS=0x2188e4CMD=XID DATA
<0011> gprs_bssgp.c:379 BSSGP TLLI=0xda9df0d3 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=3 C FCS=0x2188e4CMD=XID DATA
<0011> gprs_bssgp.c:379 BSSGP TLLI=0xda9df0d3 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=3 C FCS=0xb94f37CMD=UI DATA
<0013> gprs_sndcp.c:537 Message for non-existing SNDCP Entity (lle=0x1dc7760, TLLI=da9df0d3, SAPI=3, NSAPI=5)
<0011> gprs_bssgp.c:379 BSSGP TLLI=0xda9df0d3 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=3 C FCS=0xd6848eCMD=UI DATA
<0013> gprs_sndcp.c:537 Message for non-existing SNDCP Entity (lle=0x1dc7760, TLLI=da9df0d3, SAPI=3, NSAPI=5)
<0011> gprs_bssgp.c:379 BSSGP TLLI=0xda9df0d3 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=3 C FCS=0x2188e4CMD=XID DATA
<0011> gprs_bssgp.c:797 BSSGP BVCI=1800 Rx Flow Control BVC
<0011> gprs_bssgp.c:379 BSSGP TLLI=0xda9df0d3 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=3 C FCS=0x2188e4CMD=XID DATA
<0011> gprs_bssgp.c:379 BSSGP TLLI=0xda9df0d3 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=3 C FCS=0x9039adCMD=UI DATA
<0013> gprs_sndcp.c:537 Message for non-existing SNDCP Entity (lle=0x1dc7760, TLLI=da9df0d3, SAPI=3, NSAPI=5)
<0011> gprs_bssgp.c:379 BSSGP TLLI=0xda9df0d3 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=3 C FCS=0xa4027eCMD=UI DATA
<0013> gprs_sndcp.c:537 Message for non-existing SNDCP Entity (lle=0x1dc7760, TLLI=da9df0d3, SAPI=3, NSAPI=5)
<0011> gprs_bssgp.c:797 BSSGP BVCI=1800 Rx Flow Control BVC
<000f> gprs_sgsn.c:790 Checking for inactive LLMEs, time = 5740
<0011> gprs_bssgp.c:797 BSSGP BVCI=1800 Rx Flow Control BVC
<0011> gprs_bssgp.c:379 BSSGP TLLI=0xda9df0d3 Rx UPLINK-UNITDATA
<0012> gprs_llc_parse.c:74 LLC SAPI=3 C FCS=0x5b6c32CMD=UI DATA
<0013> gprs_sndcp.c:537 Message for non-existing SNDCP Entity (lle=0x1dc7760, TLLI=da9df0d3, SAPI=3, NSAPI=5)

```

• BTS + PCU log:

```

<0006> oml.c:1450 Successful deactivation of L1 SAPI SACCH on TS 0
<0006> oml.c:723 (bts=0,trx=0,ts=0,ss=1) End of queue encountered. Now empty? 1
<0002> tbf.cpp:484 TBF(TFI=0 TLLI=0xcd310fdd DIR=DL STATE=FLOW) poll timeout for FN=24999, TS=6 (curr FN 25012)
<0002> tbf.cpp:556 - Timeout for polling PACKET DOWNLINK ACK.
<0002> tbf.cpp:888 - Assignment was on PACCH
<0002> tbf.cpp:894 - Downlink ACK was received
<0006> ll_if.c:874 Rx PH-DATA.ind SDCCH (hL2 000001bb): 01 00 4d 06 16 03 30 58 86 20 0b 60 14 04 2f 65 13 b8 80 0d 21 00 54 , Meas: RSSI -53.71 dBm, Qual 19.11 dB, BER 0.00, Timing -2
<0000> rsl.c:1766 (bts=0,trx=0,ts=0,ss=1) Fwd RLL msg DATA_IND from LAPDm to A-bis
<0002> tbf.cpp:484 TBF(TFI=0 TLLI=0xcd310fdd DIR=DL STATE=FLOW) poll timeout for FN=25029, TS=6 (curr FN 25042)
<0002> tbf.cpp:556 - Timeout for polling PACKET DOWNLINK ACK.
<0002> tbf.cpp:888 - Assignment was on PACCH
<0002> tbf.cpp:894 - Downlink ACK was received
<0002> tbf.cpp:484 TBF(TFI=0 TLLI=0xcd310fdd DIR=DL STATE=FLOW) poll timeout for FN=25059, TS=6 (curr FN 25077)
<0002> tbf.cpp:556 - Timeout for polling PACKET DOWNLINK ACK.
<0002> tbf.cpp:888 - Assignment was on PACCH
<0002> tbf.cpp:894 - Downlink ACK was received
<0006> ll_if.c:874 Rx PH-DATA.ind SDCCH (hL2 000001bb): 01 22 53 06 60 4a 40 00 03 50 ca ab 54 1a 95 5a a2 29 20 c1 12 00 06 , Meas: RSSI -53.50 dBm, Qual 18.92 dB, BER 0.00, Timing -2
<0002> tbf.cpp:484 TBF(TFI=0 TLLI=0xcd310fdd DIR=DL STATE=FLOW) poll timeout for FN=25094, TS=6 (curr FN 25107)
<0002> tbf.cpp:556 - Timeout for polling PACKET DOWNLINK ACK.

```

```
<0002> tbf.cpp:888 - Assignment was on PACCH
<0002> tbf.cpp:894 - Downlink ACK was received
<0002> tbf.cpp:484 TBF(TFI=0 TLLI=0xcd310fdd DIR=DL STATE=FLOW) poll timeout for FN=25124, TS=6 (curr FN 2
5137)
<0002> tbf.cpp:556 - Timeout for polling PACKET DOWNLINK ACK.
<0002> tbf.cpp:888 - Assignment was on PACCH
<0002> tbf.cpp:894 - Downlink ACK was received
<0006> ll_if.c:874 Rx PH-DATA.ind SDCCH (hL2 000001bb): 01 53 01 f5 a7 b3 19 8b 18 6a ed 82 a4 0f a3 89 2c
5d cd 7d 7e 71 f9 , Meas: RSSI -53.47 dBm, Qual 19.27 dB, BER 0.00, Timing -3
<0000> rsl.c:1766 (bts=0,trx=0,ts=0,ss=1) Fwd RLL msg REL_IND from LAPDm to A-bis
<0000> rsl.c:1847 (bts=0,trx=0,ts=0,ss=1) Rx RSL RF_CHAN_REL
<0007> llsap.c:1095 deactivating channel chan_nr=28 trx=0
```

**#3 - 06/24/2016 12:55 PM - neels**

- Description updated

**#4 - 10/29/2017 06:43 PM - laforge**

- Priority changed from Normal to High

**#5 - 03/03/2018 09:45 PM - laforge**

- Assignee set to sysmocom

**#6 - 04/10/2018 05:34 PM - laforge**

- Assignee changed from sysmocom to lynxis

**#7 - 10/02/2018 03:46 PM - laforge**

**#9 - 10/17/2018 10:24 AM - laforge**

- Assignee changed from lynxis to msuraev

**#10 - 10/24/2018 10:11 AM - msuraev**

One way to approach this would be to convert TBF to use proper osmo\_fsm for state transitions. Old implementation is cumbersome to maintain and modify as shown by this and related bugs. We'll need working TTCN3 tests before that though to avoid regressions during transition.

**#11 - 10/30/2018 01:40 PM - msuraev**

- Related to Feature #2820: test GPRS with two (or more) subscribers added

**#12 - 11/01/2018 05:00 PM - msuraev**

- Related to Bug #2890: OsmoPCU TTCN-3 test suite not executed by jenkins added

**#13 - 04/15/2019 07:47 AM - laforge**

- Assignee changed from msuraev to lynxis