

## OsmoPCU - Bug #4844

### do not resent DL assignment on RACH

11/04/2020 02:24 AM - lynxis

<b>Status:</b> Feedback	<b>Start date:</b> 11/04/2020
<b>Priority:</b> Normal	<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>	
<p>When a MS wants to send data without a TBF present, it sends a RACH, get's an immediate assign, moves over to the PDCH and receives a UL assignment.</p> <p>However if the MS misses either the immediate assign or the UL assignment, the PCU tries to assign using the TLLI 0x0, which seems to be wrong.</p> <p>The PCU uses TLLI 0x0, even it can't know the TLLI of the MS. It only knows it by the first UL data.</p> <pre>MS      PCU RACH -&gt;       X- IMM assign (MS never receive IMM assign)       ---- PCU have a UL timeout and doesn't know the TLLI       &lt;- UL TBF Assignment TLLI for 0x00000000.</pre>	

### History

#### #1 - 11/04/2020 05:04 AM - fixeria

This is a very confusing ticket description:

do not resent DL assignment on RACH

RACH is an Uplink-only unidirectional channel, so how can a Downlink assignment be sent on Uplink?

When a MS wants to send data without a TBF present, it sends a RACH, get's an immediate assign, moves over to the PDCH and receives a UL assignment.

It actually receives an Uplink resource assignment in the Rest Octets of (RR) Immediate Assignment.

However if the MS misses either the immediate assign or the UL assignment, the PCU tries to assign using the TLLI 0x0, which seems to be wrong.  
The PCU uses TLLI 0x0, even it can't know the TLLI of the MS. It only knows it by the first UL data.

Yep, more specifically a new TBF is always allocated with TLLI=0x00000000. I am not sure if 0x00000000 or 0xffffffff is a valid TLLI; the specs. do not mention any reserved values. On the other hand, in osmo-ttcn-hack we do have TLLI\_UNUSED := 'FFFFFFFF'...

#### #2 - 11/05/2020 02:30 PM - laforge

On Wed, Nov 04, 2020 at 05:04:09AM +0000, fixeria [REDMINE] wrote:

Yep, more specifically a new TBF is always allocated with TLLI=0x00000000. I am not sure if 0x00000000 or 0xffffffff is a valid TLLI; the specs. do not mention any reserved values. On the other hand, in osmo-ttcn-hack we do have TLLI\_UNUSED := 'FFFFFFFF'...

TLLI is derived from TMSI, and TMSI 0xffffffff is reserved for "not valid TLLI". the reason for that is that EF.TMSI - like all files on smart cards - are 0xffffffff in erased state.

#### #3 - 11/08/2020 06:39 AM - fixeria

I have not (yet) tested this change, and didn't run ttcn3-pcu-test against it:

<https://gerrit.osmocom.org/c/osmo-pcu/+/21073> TLLI 0x00000000 is a valid TLLI, use 0xffffffff instead

so let's keep it WIP for now.

**#4 - 11/08/2020 06:47 AM - fixeria**

P.S. BEWARE! Opening huge diffs in Gerrit may lead to OOM!

**#5 - 12/17/2020 01:04 AM - lynxis**

- Assignee set to fixeria

**#6 - 02/17/2021 02:16 PM - fixeria**

- Status changed from New to Feedback

- Assignee changed from fixeria to lynxis

I still do not understand what's the problem here, please clarify ticket description.

However if the MS misses either the immediate assign or the UL assignment, the PCU tries to assign using the TLLI 0x0, which seems to be wrong. The PCU uses TLLI 0x0, even it can't know the TLLI of the MS. It only knows it by the first UL data.

What do you expect to happen if the MS does not respond to the assignment?

**#7 - 02/19/2021 12:57 PM - lynxis**

- Description updated

**#8 - 02/19/2021 12:57 PM - lynxis**

- Assignee changed from lynxis to fixeria

- % Done changed from 0 to 60

**#9 - 02/20/2021 05:37 PM - fixeria**

I am sorry, but it's still not clear what's wrong and what do you expect. I am inclined to reject it.

```
RACH ->
X- IMM assign (MS never receive IMM assign)
---- PCU have a UL timeout and doesn't know the TLLI
<- UL TBF Assignment TLLI for 0x00000000.
```

Why would there be another assignment (last packet in your diagram)? Yes, osmo-pcu would create an Uplink TBF with a special TLLI (0xffffffff in the recent versions), which would simply expire after a timeout. Other than the first assignment in Immediate Assignment, nothing else will be sent.

I created a very simple test case that confirms my understanding:

<https://git.osmocom.org/osmo-ttcn3-hacks/commit/?h=fixeria/OS4844&id=46cf8242d2be9f49f035bd4970cb33cdcf6e9dd2>

Feel free to change this test case in order to demonstrate the problem, or at least provide a proper explanation.

**#10 - 02/20/2021 05:37 PM - fixeria**

- Assignee changed from fixeria to lynxis

- % Done changed from 60 to 0