

OsmoPCU - Bug #4844

do not resent DL assignment on RACH

11/04/2020 02:24 AM - lynxis

Status: New	Start date: 11/04/2020
Priority: Normal	Due date:
Assignee: fixeria	% Done: 0%
Category:	
Target version:	
Spec Reference:	
Description	
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.	
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.	

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