OsmoSGSN - Bug #4506

MediaTek MT6*** will not initiate Packet Access

04/20/2020 04:01 AM - keith

Status:	Closed	**Start date:**	04/20/2020
Priority:	Normal	**Due date:**	
Assignee:	keith	**% Done:**	90%
Category:			
Target version:			
Spec Reference:			

Description

I'm filing this under PCU but i'm not convinced it does not have to do with another component.

With recent improvements to all the PS components PS performance is great with most UE I have tested, however not so with these:

htc Desire 628 dual sim (MT6753)

htc Desire 626G dual sim (MT6592)

What happens in the attached pcaps is the following:

- htc exits airplane mode, does GPRS MM attach.
- Activate mobile data, does PDP context activate, followed by some apps attempting data access, which is successful as long as the TBF from the PDP activate is still there.
- Normally here we would see some IP traffic for 30 seconds or a minute or so as apps update themselves, but in this trial case, IP traffic is rejected and ICMP unreachable is sent back. (firewalled at the ggsn)
- The TBF expires shortly after.
- At this point, I try to ping the ggsn IP from a shell on the htc, I try access from apps, browser etc. Nothing happens. I'm monitoring the uplink RF which is totally quiet. There is no RF transmission from the phone whatsoever.
- I ping the phone IP from the ggsn VM. We see paging, TBF establishment, once again, apps on the phone kick into gear. ping replies come back. I kill the ping. TBF expires.
- Rinse and repeat....

What else i've done:

- compared the MS Network caps and RA caps with those of the phones that work and looked up everything that stands out as distintive in the spec, but nothing would appear to have to do with this issue, certainly not in GPRS mode.

- tested the desire 628 on a commercial network with EGPRS from a user perspective, appear to work fine.

This is the only GPRS class 12 phone I have:

```
GPRS multislot class: Max Rx-Slot/TDMA:4 Max Tx-Slot/TDMA:4 Max-Sum-Slot/TDMA:5 Tta:2 Ttb:1 Tra:2
Trb:1 Type:1 (12)
```

UPDATE:

Debugging tools on the UE side show the following messages after DL TBF is released:

On requesting a DNS lookup and identifying the corresponding request from the upper layer in the trace, this is shortly followed by:

- MSG_ID_GRR_DATA_REQ <--- DNS request observed in payload
- MSG_ID_MAC_RMPC_PKT_ACCESS_REQ
- TBF: 0, Orig RES_REQ Status <RES_REQ_INVALID>, New REQ_RES Status <RES_REQ_RLC_IN_RACH_IDLE>
- rmpc call mac_fn_cell_status_hdlr: rel cause ACCESS_NOT_ALLOWED
- ACS_DENY_ACS_REQ_FOR_RP_OR_CTRL_CLASS_NOT_ALLOW

I went down a track originally of wondering if maybe the phone expects some kind of access class information (TS 144.060 7.1) but I didn't manage to figure out where I might experiment with PSI messages on PBCCH, if at all.

I programmed a SIM card [ACC] with access levels 0-7 on and also level 15, this had no affect.

In EGPRS mode there is something of note that happens quite often, which is that when there is no more IP traffic, the phone keeps sending a LLC block with no payload (that might not be the right terminology) This can go on for some time. (several hundred transmissions)
In the next session I will grab pcaps in EGPRS mode.

The pcap does not contain all levels and categories of bts/pcu log and gsmtap. Please ask for other cats/levels if desired, I can repeat the procedure.

Related issues:

Related to OsmoPCU - Bug #2455: MS will not be able to use data service if we...	**Closed**	**08/21/2017**
Related to OsmoPCU - Bug #2400: transmit SI13 on PACCH during long TBFs	**Stalled**	**07/25/2017**

History

#1 - 04/20/2020 04:05 AM - keith

Eventually, if no traffic comes from the network side, the htc will do an MM detach, reason given "powering off" <-- ??

Followed by a reattach + pdp activate.. and from there we go back to this loop.

#2 - 04/20/2020 04:56 AM - fixeria

#3 - 04/20/2020 05:07 AM - fixeria

#4 - 04/20/2020 02:56 PM - keith

A further note I should have added in the description. I did test this phone against a commercial network. in EGPRS mode. It did not exhibit this behaviour.

#5 - 04/20/2020 04:20 PM - keith

#6 - 04/21/2020 02:31 AM - keith

- Description updated

#7 - 04/24/2020 01:38 AM - keith

- File PRQ_TFI.pcap added

I have noticed that this MT6753 is sending PACKET_RESOURCE_REQUEST on PACCH without MS RA Cap, in fact the only significant values in the Chan Request Description (attached) would appear to be PEAK_THOUGHOUT_CLASS and RADIO_PRIORITY

At this point, (contention resolution phase is finished?) the Global TFI is included in place of the TFI. (IE is at TS 04.60 Table 11.2.16.1)

This means that in pdch.cpp:gprs_rlcmac_pdch::rcv_resource_request, we skip the entire block

```
if (request->ID.UnionType) {....} (1 being TLLI, 0 being TFI)
```

This leads to unimplemented handling at the end of this function in the

```
if (request->ID.u.Global_TFI.UnionType) {....} block where we log:
```

```
pdch.cpp:663 TBF(TFI=0 TLLI=0xe1ad00cb DIR=UL STATE=FLOW) RX: [PCU <- BTS] FIXME: Packet resource request
```

This whole procedure appears to be described in TS 44.060 8.1.1.1.2:

During an uplink packet transfer, upper layers may request to transfer another upper layer PDU with a different PFI, a different Radio Priority, a different peak throughput class or a different RLC mode than the one which is in transfer.

If the mobile station has not started the countdown procedure [.....] *and either a higher radio priority or the same radio priority but a higher peak throughput class, the mobile station shall immediately request a resource reallocation for uplink according to the new Radio Priority and peak throughput class of the new upper layer PDU by sending a PACKET RESOURCE REQUEST message on the PACCH and starting timer T3168*

I'm not sure if this is the clause that applies here, there are a number of similar ones, but anyway, later we have:

If the mobile station or the network does not support multiple TBF procedures, (I'm pretty sure this is the case here from looking at SI and various IEs) *upon expiry of timer T3168 the mobile station shall retransmit the PACKET RESOURCE REQUEST message unless the PACKET RESOURCE REQUEST message has already been transmitted four times in which case the mobile station shall perform an abnormal release with access retry*

This appears to be what I observe, certainly only 4 tries, I'm not sure about the accesss retry.

It is not fully clear to me what causes the upper layer to request to TX this PDU with different priority or class, I don't seem to be always able to provoke it and the described misbehaviour of this ticket seems to be always present anyway. But anyway this is needs to be dealt with even if it does not fix the Original Issue.

It's also not clear to me from TS 44.060 exactly what is supposed to happen. The long sentences with condition after condition is not so easy to parse.

I've tried to do a few different things in response to the Resource Request in rcv_resource_request() but I'm still getting my head around code paths in the PCU. I look forward to learning a lot from a solution if anybody else can do it!

#8 - 04/24/2020 02:59 AM - keith

Note: TS 44.160 8.2.2.1.2.2 On receipt of the PACKET RESOURCE REQUEST

#9 - 04/29/2020 09:08 AM - fixeria

Regarding the actual problem described in this ticket, you could try to send *PACKET ACCESS REJECT* message (see 3GPP 44.060, section 11.2.1). Not sure if it would help, but it's better than sending nothing. See *Encoding::write_packet_access_reject()*. You would need to modify this function (or add some wrappers) in order to be able to specify the global TFI (the one that you received in the *PACKET RESOURCE REQUEST*) instead of TLLI.

#10 - 04/29/2020 11:24 AM - fixeria

> Regarding the actual problem described in this ticket, you could try to send PACKET ACCESS REJECT message

Here is an ugly hack implementing this: https://git.osmocom.org/osmo-pcu/log/?h=fixeria/reject_hack
keith could you please test and report back?

#11 - 05/03/2020 03:09 AM - keith

Thanks! testing, i see the REJECT in the trace. There is no difference in terms of the original issue described though.

Which is probably to be expected as really the issue appears before the phone even sends a first RESOURCE REQUEST, that is to say it goes "silent" as soon as the TBF that was used for the pdp context negotiation is finished. We should maybe have a separate ticket for this TFI Resource request issue.

#12 - 05/10/2020 08:52 PM - fixeria

Regarding the retransmissions:

> I finally came up with a (not yet published) TTCN-3 test case for this scenario
> and as it turns out osmo-pcu is doing everything correctly.

See https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/18187.

#13 - 09/03/2020 11:14 AM - keith

Tested this issue again with current latest.
The issue persists as described in the ticket description.

#14 - 09/03/2020 11:18 AM - keith

- Related to Bug #2455: MS will not be able to use data service if we let the MS idle about 30 seconds after PDP context activated added

#15 - 09/19/2020 09:38 AM - keith

- Related to Bug #2400: transmit SI13 on PACCH during long TBFs added

#16 - 09/19/2020 10:01 AM - keith

*- Subject changed from htc desire will not initiate Packet Access to MediaTek MT6*** will not initiate Packet Access*

- Description updated

- Status changed from New to In Progress

- % Done changed from 0 to 10

#17 - 09/20/2020 10:28 PM - keith

Pushed proposed fix: https://gerrit.osmocom.org/#/c/osmo-sgsn/+/20217/

#18 - 09/21/2020 06:40 AM - laforge

On Sat, Sep 19, 2020 at 09:38:19AM +0000, keith [REDMINE] wrote:

> I went down a track today of wondering if maybe the phone expects some kind of access class information (TS 144.060 7.1) but I didn't manage to figure out where I might experiment with PSI messages on PBCCH, if at all.

nobody has a PBCCH. Its mere existance has been removed from 3GPP specifications by now as a result of GSMA inquiring among operators that nobody use the PCCCH/PBCCH/... channels. Neither phones nor networks are required to support it.

#19 - 09/21/2020 08:13 AM - laforge

- % Done changed from 10 to 90

thanks, just merged. So I guess both sides were buggy. We encoded an invalid
priority for TOM8, but MTK should never check that TOM8 priority for TBFs
that are unrelated to tunneling of messages. According to TS 23.060 Section 6.10 this
is used for tunneling of non-3GPP messages such as TIA/EIA-136 (CDMA2000).

#20 - 09/21/2020 09:14 AM - keith

Yes, thanks for the two updates.

Just to note that I wrote that about "today" re the PBCCH back some months ago when originally writing the ticket. I'm well aware since then that PCCCH/PBCCH are not a thing, but it is good to have that firmly stated on the ticket to help not create confusion in the future. The number of references to PCCCH/PBCCH in the specs is really quite something, especially if you go looking for info on access class control!

So the actual bug that prevented access was not in the TOM8 priorty, but rather in the Radio Priority IE inside the PDP Context Activation. However, it seemed to make sense to also correct the TOM8 Priority (aka Radio Priority 2) in case that IE would cause a problem in the MTK also.

#21 - 10/19/2020 07:38 PM - keith

- Project changed from OsmoPCU to OsmoSGSN

- Status changed from In Progress to Closed

- Assignee set to keith

Moving to SGSN where the problem actually resided and closing due to consistent results showing fix works.

Files

bssgp.pcap	19.7 KB	04/20/2020	keith
gsmtap-log.pcap	388 KB	04/20/2020	keith
PRQ_TFI.pcap	121 Bytes	04/24/2020	keith