OsmoPCU - Bug #4506

htc desire will not initiate Packet Access

04/20/2020 04:01 AM - keith

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td></td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Spec Reference:</td>
<td></td>
</tr>
</tbody>
</table>

**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 this "htc desire 628 dual sim"

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:

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

The only exception to that is (maybe) that this is the only 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)

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.

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 level and categories of bts/pcu log and gsmtap. Please ask for other cats/levels if desired, I can repeat the procedure.

EDIT: According to GSM Arena, this is a [https://www.mediatek.com/products/smartphones/mt6753](https://www.mediatek.com/products/smartphones/mt6753)

**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.
Huh, this is probably unrelated, but I see multiple retransmissions on DL TBFs:

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Sequence</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>247 5.409157</td>
<td>127.0.0.1 → 127.0.0.1</td>
<td>GSMTAP 234 TBF(TFI=0 TLLI=0xee433fec DIR=DL STATE=FLOW) Scheduled Ack/Nack polling on FN=1022432, T8=6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>248 5.409203</td>
<td>127.0.0.1 → 127.0.0.1</td>
<td>GSM RLC/MAC 98 GPRS DL gsm_rlcmac.dl.tfi == 0 gsm_rlcmac.bsn ==</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>249 5.410058</td>
<td>127.0.0.1 → 127.0.0.1</td>
<td>GSM RLC/MAC 98 GPRS DL gsm_rlcmac.dl.tfi == 0 gsm_rlcmac.bsn ==</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>250 5.432305</td>
<td>127.0.0.1 → 127.0.0.1</td>
<td>GSM RLC/MAC 98 GPRS DL gsm_rlcmac.dl.tfi == 0 gsm_rlcmac.bsn ==</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>251 5.433037</td>
<td>127.0.0.1 → 127.0.0.1</td>
<td>GSM RLC/MAC 98 GPRS DL gsm_rlcmac.dl.tfi == 0 gsm_rlcmac.bsn ==</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>252 5.450729</td>
<td>127.0.0.1 → 127.0.0.1</td>
<td>GSM RLC/MAC 98 GPRS DL gsm_rlcmac.dl.tfi == 0 gsm_rlcmac.bsn ==</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>253 5.451474</td>
<td>127.0.0.1 → 127.0.0.1</td>
<td>GSM RLC/MAC 98 GPRS DL gsm_rlcmac.dl.tfi == 0 gsm_rlcmac.bsn ==</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>254 5.492250</td>
<td>127.0.0.1 → 127.0.0.1</td>
<td>GSM RLC/MAC 81 GPRS UL:PACKET_DOWNLINK_ACK_NACK gsm_rlcmac.dl.tfi == 0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As can be seen, a block with the same sequence number is retransmitted ~12 (!) times until the UL:PACKET_DOWNLINK_ACK_NACK is received. This is unacceptable. Are you using SDR? If so, what is the value of 'fn-advance' you’re using? We may want to create a separate ticket...

As can be seen, a block with the same sequence number is retransmitted ~12 (!) times
And this is what I see in the UL:PACKET_DOWNLINK_ACK_NACK:

```
0000 10.. = MESSAGE_TYPE (UL): PACKET_DOWNLINK_ACK_NACK (2)
.... ..00 000. .... = DL TFI: 0
Ack_Nack_Description
...0 .... = FINAL_ACK_INDICATION: False
.... 0001 000. .... = STARTING_SEQUENCE_NUMBER: 8
.... 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0111 1111. 111. .... = Received Block Bitmap: 255
```

```
--
0000 10.. = MESSAGE_TYPE (UL): PACKET_DOWNLINK_ACK_NACK (2)
.... ..00 000. .... = DL TFI: 0
Ack_Nack_Description
...0 .... = FINAL_ACK_INDICATION: False
.... 0001 001. .... = STARTING_SEQUENCE_NUMBER: 9
.... 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0011 1111 111. .... = Received Block Bitmap: 511
```

so the MS confirms reception of a block that was retransmitted so many times. In general, the network may (and should) send several blocks (BSN=N..N+M) during the polling timeout, and the MS would reflect all received blocks (BSN=N..N+M) in the bitmap.

**#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**

fixeria wrote:

> As can be seen, a block with the same sequence number is retransmitted ~12 (!) times

I've been seeing this kind of thing since some time ago.

I'm using a sysmoBTS.

**#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=0xelad00cb 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 access 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

As can be seen, a block with the same sequence number is retransmitted ~12 (!) times

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. If only one block is in the queue, and there are no other DL TBFs, osmo-pcu would (and should) retransmit it until the Ack is received. If several blocks are in the queue, then the whole sequence of blocks would be retransmitted until the Ack is received.

I guess in your case only one block was in the queue (ICMP Echo Request), so that's why we see those repeating transmissions of a block with the same BSN. This is expected. In any case, I will publish my test cases as soon as I have time to finish them.

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.

Files