

OsmoPCU - Bug #2400

transmit SI13 on PACCH during long TBFs

07/25/2017 02:48 PM - laforge

Status: Stalled	Start date: 07/25/2017
Priority: High	Due date:
Assignee: fixeria	% Done: 20%
Category:	
Target version:	
Spec Reference:	
Description	
5.5.1.3.3 SI13 reception failure If the mobile station has not received the SI13 or the PSI13 message within the last 60 s, a SI13 reception failure has occurred. An SI13 reception failure shall result in a cell reselection.	
5.5.2.1.3 System information on PACCH (and other logical channels)	
The network may broadcast PSI and SI messages on PACCH. In particular, if a mobile station is busy in packet transfer mode or MAC-Shared state and thus unable to receive the relevant blocks on the broadcast channels (PBCCH or BCCH) for a period longer than 15 seconds, the following requirements apply: [...] - If PBCCH is not present in the cell, the network may broadcast the PSI13 message on PACCH such that the mobile station may receive the PSI13 messages at least every 15 s.	
So basically this means that on a TBF that has a duration longer than 60s since the last SI13 was received on BCCH, a spec-compliant MS shall start cell re-selection, which will of course interrupt the transmission. We hence must periodically schedule SI13 in PACCH.	
Related issues:	
Related to OsmoPCU - Bug #3284: GPRS cell re-selection appears sticky in pack...	New 05/23/2018
Related to OsmoPCU - Bug #3472: GPRS connection is in a state where pdp-conte...	Closed 08/18/2018
Related to OsmoSGSN - Bug #4506: MediaTek MT6*** will not initiate Packet Access	Closed 04/20/2020

History

#1 - 07/28/2017 03:24 PM - laforge

- Description updated

#2 - 07/28/2017 03:24 PM - laforge

- Description updated

#3 - 08/10/2017 02:15 PM - mqng2

- Status changed from New to Feedback

I have seen an issue with the Lenovo A916 smartphone.

If the phone does not use Internet right after PDP context ACT, the phone will be unable to use the Internet.

It is also applied in case the phone waits for an amount of time after a Web page loaded 100%.

Do you think the problem with this phone is related to this issue?

#4 - 08/15/2017 05:54 PM - laforge

- Status changed from Feedback to New

mqng2 wrote:

Do you think the problem with this phone is related to this issue?

No, I don't think so, sorry.

#5 - 08/17/2017 06:43 AM - laforge

- Assignee set to msuraev

#6 - 08/18/2017 07:03 PM - mqng2

- Status changed from New to Feedback

laforge wrote:

mqng2 wrote:

Do you think the problem with this phone is related to this issue?

No, I don't think so, sorry.

Some input:

I wrote a small script to periodically ping the Lenovo A916 phone every 30 seconds. The phone does not go to state of unable to use the data service.

From this experiment, it looks like there is a timer expired somewhere that forces the phone into unable state...

#7 - 08/18/2017 08:15 PM - laforge

Hi Minh,

On Fri, Aug 18, 2017 at 07:03:35PM +0000, mqng2 [REDMINE] wrote:

I wrote a small script to periodically ping the Lenovo A916 phone every 30 seconds. The phone does not go to state of unable to use the data service.

From this experiment, it looks like there is a timer expired somewhere that forces the phone into unable state...

I'm not doubting that you are experiencing a problem. But it is clearly unrelated to this ticket, as this ticket is about TBFs that are established for longer than 15 seconds, i.e. when there is continuous data transfer so the TBF is never closed. If you ping every 30s, then for sure the TBF is closed after every ping and thus it is unrelated.

Feel free to file a different issue, preferably with protocol traces of Gb and Um (GSMTAP) as well as the detailed log output of osmo-pcu and indicating the specific version of the PCU using which the problem was observed.

#8 - 08/21/2017 01:51 PM - mqng2

laforge wrote:

Hi Minh,

On Fri, Aug 18, 2017 at 07:03:35PM +0000, mqng2 [REDMINE] wrote:

I wrote a small script to periodically ping the Lenovo A916 phone every 30 seconds. The phone does not go to state of unable to use the data service.

From this experiment, it looks like there is a timer expired somewhere that forces the phone into unable state...

I'm not doubting that you are experiencing a problem. But it is clearly unrelated to this ticket, as this ticket is about TBFs that are established for longer than 15 seconds, i.e. when there is continuous data transfer so the TBF is never closed. If you ping every 30s, then for sure the TBF is closed after every ping and thus it is unrelated.

Feel free to file a different issue, preferably with protocol traces of

Gb and Um (GSMTAP) as well as the detailed log output of osmo-pcu and indicating the specific version of the PCU using which the problem was observed.

A new ticket for this issue has created here <https://osmocom.org/issues/2455>

#9 - 08/22/2017 01:45 PM - msuraev

- Status changed from Feedback to New

#10 - 08/29/2017 10:41 AM - msuraev

- Status changed from New to In Progress

Note to self: spec references 3GPP TS 44.060 §5.5.2.1.3, §11.2.25 and 3GPP TS 44.018 §10.5.2.37b.

There's already PCU_IF_SAPI_BCCH and BTS-side code which updates SI13 with the data received from PCU (is this even spec compliant?) but no PCU-side code.

The difference between SI13 and PSI13 is 2-bit PAGE_MODE field in the beginning of the PSI13 message (which is ignored by MS on PACCH) - the SI13 has H (CSN1) value so it could be copied as is.

#11 - 08/31/2017 12:52 PM - msuraev

- Checklist item [] propagate SI13 from BTS to PCU added
Checklist item [] periodically schedule SI13 for busy TBF added
- % Done changed from 0 to 20

#12 - 08/31/2017 01:39 PM - msuraev

- Status changed from In Progress to Feedback

Does "mobile station is busy in packet transfer mode" in the spec refers to UL, DL or both?

#13 - 09/01/2017 12:47 PM - msuraev

- Checklist item deleted (propagate SI13 from BTS to PCU)
Checklist item [x] send SI13: BTS added
Checklist item [] recv SI13: PCU added

#14 - 09/01/2017 02:41 PM - msuraev

- Checklist item [] check that SI13 is removed from PCU after GPRS being disabled at BSC added
Checklist item [x] recv SI13: PCU set to Done

#15 - 10/11/2017 08:27 AM - laforge

- Priority changed from Normal to High

#16 - 12/03/2017 10:58 AM - laforge

- Status changed from Feedback to In Progress

If it's not explicitly specified, it of course applies to both uplink or downlink transfer mode. It's quite clear: Is it busy in packet transfer, or is it idle? Please avoid re-assigning tickets to "feedback" for bogus questions. Thanks.

#17 - 12/11/2017 02:56 PM - msuraev

- Status changed from In Progress to Stalled

#18 - 03/01/2018 11:14 PM - laforge

- Assignee changed from msuraev to sysmocom

#19 - 04/10/2018 05:34 PM - laforge

- Assignee changed from sysmocom to lynxis

#20 - 05/23/2018 10:15 AM - laforge

- Related to Bug #3284: GPRS cell re-selection appears sticky in packet transfer / packet idle mode added

#21 - 10/02/2018 03:45 PM - laforge

#22 - 10/17/2018 10:28 AM - laforge

- Assignee changed from lynxis to msuraev

#23 - 05/19/2019 07:42 AM - laforge

- Assignee changed from msuraev to lynxis

#24 - 09/10/2019 11:50 AM - laforge

[lynxis](#), is this something that [osmith](#) could take over from you?

#25 - 09/10/2019 11:58 AM - lynxis

- Assignee changed from lynxis to osmith

Sure. Btw. I'ven't seen this problematic in my test cases. But for sure, it only covers one particular firmware and phone.

#26 - 10/04/2019 10:27 PM - fixeria

- File *gprs_packet_serving_cell_data.pcapng.gz* added

5.5.2.1.3 System information on PACCH (and other logical channels)

I think I have seen something in my RLC/MAC captures from a commercial network, please see the attachment.

Unfortunately, Wireshark is not able to decode those PACKET_SERVING_CELL_DATA messages, but I already have a draft change implementing that. The payload of a PACKET_SERVING_CELL_DATA message consists of segments:

- one such message may contain one or more segments;
- every segment has a small header with PD (Protocol Discriminator) and the length field;
- a segment may be continued in the next message (if it doesn't fit):
 - special length value '11111'B indicates that;
- PACKET_SERVING_CELL_DATA has a fixed length of 19 octets,
 - after the last segment there can be a terminator (another segment with length 0) and optional '2B'O padding.

#27 - 10/04/2019 10:39 PM - fixeria

Wireshark bug report: https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=16105

#28 - 01/22/2020 11:41 AM - fixeria

- Related to Bug #3472: GPRS connection is in a state where pdp-context is active, but data TX cannot initiate from Network side. added

#29 - 05/12/2020 12:19 PM - laforge

- Assignee changed from osmith to fixeria

#30 - 09/19/2020 09:38 AM - keith

- Related to Bug #4506: MediaTek MT6*** will not initiate Packet Access added

Files

gprs_packet_serving_cell_data.pcapng.gz	883 Bytes	10/04/2019	fixeria
---	-----------	------------	---------