OpenBSC - Bug #3059

System Information on SACCH missing L2 Pseudo-Length

03/11/2018 11:03 PM - laforge

Status:	Resolved	**Start date:**	03/11/2018
Priority:	High	**Due date:**	
Assignee:	laforge	**% Done:**	100%
Category:			
Target version:			
Resolution:		**Spec Reference:**	

Description

Something seems odd about our SI5/SI6 messages.

The message on the downlink SACCH is structured as follows:

- two octets L1 header
- two octets "LAPDm B4" frame format: Address + Control Octet
- 23-4=19 octets of L3 payload (as specified in TS 44.018), consisting of
  - one octet L2 pseudo-length
  - 18 octets of actual L3 message

It appears that the messages that we send from the Osmocom stack are missing the L2 pseudo-length. This maybe related to https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14105

Related issues:

Related to OsmoBTS - Bug #3057: OsmoBTS fails to schedule SACCH filling like SI5	**Resolved**	**03/11/2018**
Related to Cellular Network Infrastructure - Bug #2963: Measurement Reports c...	**Resolved**	**02/19/2018**

History

#1 - 03/11/2018 11:03 PM - laforge

- Related to Bug #3057: OsmoBTS fails to schedule SACCH filling like SI5 added

#2 - 03/11/2018 11:03 PM - laforge

- Related to Bug #2963: Measurement Reports cease to be useful some time into a voice call / after handover (not sure which project has the bug / bugs yet) added

#3 - 03/11/2018 11:13 PM - laforge

- Status changed from New to In Progress

- % Done changed from 0 to 10

the interesting question is: how does the format look on Abis? According to my reading of the specs:

- L3 Info TLV length given by TS 48.058 for SACCH FILLING is "22", where 1 byte is tag, and 2 bytes are length, i.e. 19 bytes left for actual payload
  - this indicates the full 19 bytes *including pseudo-length* are to be included
- The actual SI5 / SI6 definitions in TS 44.018 also include the L2 pseodo length as part of the SI message

I also found some old pcap files of a proprietary ip.access BSC, which confirms that assumption.

So it seems to me that

- OsmoBSC is lacking the L2 pseudo-length field as first byte of the L3 INFO
- the wireshark packet-rsl.c decoder is broken as it assumes no l2 plen
- we impleemnted our code to comply with wireshark, inheriting the bug
- the wireshark LAPDm decoder was "fixed" by me to also comply with that broken assumption

So now, wiershark RSL, wiershark GSMTAP/LAPDm and OsmoBSC are all broken. yay. :(

#4 - 03/11/2018 11:19 PM - laforge

This appears to be the root of all evil:

```
commit 6f0e50c8337355eb59033903ede9ab6528890835
Author: Max <msuraev@sysmocom.de>
Date:   Wed Apr 12 15:30:54 2017 +0200

    Prepare for extended SI2quater support
```

as it overwrites the l2_plen just after it was written.

#5 - 03/11/2018 11:30 PM - laforge

- Assignee changed from laforge to neels

- % Done changed from 10 to 30

proposed (but yet untested) patch at https://gerrit.osmocom.org/7220

#6 - 03/11/2018 11:33 PM - laforge

- Project changed from Cellular Network Infrastructure to OsmoBSC

#7 - 03/12/2018 02:05 AM - neels

- Project changed from OsmoBSC to Cellular Network Infrastructure

- Assignee changed from neels to laforge

- % Done changed from 30 to 80

Just tested with this patch as well as https://gerrit.osmocom.org/#/c/7218/ (it's already merged to osmo-bts master, but let me mention that it was used in the test) and: YES! Finally the measurement reports survive a handover! No matter what I do, the neighbor lists are reliably populated. Excellent! Let me add a few percent there.

#8 - 03/12/2018 06:42 AM - fixeria

Hi Harald,

this is probably related to:

https://lists.osmocom.org/pipermail/openbsc/2017-December/011545.html

my plan is to revert the:

https://git.osmocom.org/osmocom-bb/commit/?id=1a8a80aeae4c2e5c870ae5b032d9a6ae60b67ac8

because I was referring an outdated spec version and the way of Osmocom stack.

#9 - 03/12/2018 10:16 AM - laforge

- Checklist item [ ] wireshark patch for RSL added
Checklist item [ ] wireshark patch for SACCH/LAPDm added

- Project changed from Cellular Network Infrastructure to OpenBSC

- % Done changed from 80 to 90

ok, have merged the related patch now. Let's abuse this ticket until wireshark patches are written + tested.

#10 - 03/12/2018 10:26 AM - laforge

- Checklist item [x] patch for legacy openbsc.git added

openbsc.git fix submitted in https://gerrit.osmocom.org/#/c/7226/

#11 - 03/12/2018 01:16 PM - fixeria

My question was lost because the 7226 was merged, but anyway,
laforge, what do you think about introducing a new structure with l2_plen?

#12 - 03/12/2018 01:50 PM - laforge

On Mon, Mar 12, 2018 at 01:16:53PM +0000, fixeria [REDMINE] wrote:

> My question was lost because the 7226 was merged, but anyway,

it wasn't lost, I read it ;)

> laforge, what do you think about introducing a new structure with l2_plen?

I don't think it's worth it. Too much confusion?

#13 - 04/07/2018 10:43 PM - laforge

- Checklist item [x] wireshark patch for RSL set to Done

#14 - 04/07/2018 10:43 PM - laforge

wireshark patch for RSL now proposed as https://code.wireshark.org/review/#/c/26797/

#15 - 04/07/2018 11:12 PM - laforge

- Checklist item [x] wireshark patch for SACCH/LAPDm set to Done

- Status changed from In Progress to Stalled

LAPDm patch submitted at https://code.wireshark.org/review/#/c/26798/1 - waiting for review.

#16 - 04/29/2018 08:35 AM - laforge

- Status changed from Stalled to Resolved

- % Done changed from 90 to 100

both wireshark patches merged.