OsmoBSC - Bug #3799

OsmoBSC send OML "Get Attributes" with wrong length value

02/12/2019 06:34 PM - laforge

Status:	Resolved		**Start date:**	02/12/2019
Priority:	High		**Due date:**	
Assignee:	laforge		**% Done:**	70%
Category:	A-bis OML			
Target version:				
Spec Reference:				

Description

When sending the OML "GET ATTRIBUTES" message to the "Baseband Transceiver", OsmoBSC is sending a wrong "length" field of the OML message. See attached pcap file.

```
80 80 00 07 81 04 00 00 ff 1a 00 02 1c 41
         ^  ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
         |  10 bytes following
         length octet stating len=7
```

Related issues:

Related to OsmoBSC - Bug #1614: better identification of BTS model / capabili...	**Stalled**	**02/23/2016**

Associated revisions

Revision 3933e930 - 02/12/2019 07:29 PM - laforge

OML: Work around OsmoBSC sending "GET ATTRIBUTES" with short length

OsmoBSC used to have a bug in encoding the "GET ATTRIBUTES" OML message, resulting in the actual message length being three bytes longer than the encoded length value.

As in Ib98f0d7c2cff9172714ed18667c02564540d65d7 we have introduced proper consistency checks on length values, all "GET ATTRIBUTES" from OsmoBSC version suntil today will fail. This patch introduces a work-around to remain compatible with old OsmoBSC while still keeping the consistency checks for all other messages.

Change-Id: Ifa24e9e2c71feb2c597557807d675438c2825b2d
Related: OS#3799

Revision 69b04a29 - 03/19/2019 01:44 PM - laforge

OML: Fix encoded length value of OML GET ATTRIBUTES

Before this patch, all OML GET ATTRIBUTES messages were encoded with an erroneous OML header length value. The length value was always three bytes less than the actual message length. This patch fixes the problem.

Change-Id: I56068de0bb14a99ec39be587e542e27cddb7d1df
Closes: OS#3799

History

#1 - 02/12/2019 06:38 PM - laforge

- Status changed from New to In Progress

- % Done changed from 0 to 10

will be working on a patch. The problem is that we have tons of old OsmoBSC versions around that do this wrong. This probably was wrong already in Change-Id I2b61131b9930afd03357c0b66947ee856d58cc46 merged in May 2017 - or possibly even longer than that...

#2 - 02/12/2019 06:39 PM - laforge

- Related to Bug #1614: better identification of BTS model / capabilities to BSC added

#3 - 02/12/2019 06:55 PM - laforge

- % Done changed from 10 to 70

A fix for OsmoBSC has been submitted as https://gerrit.osmocom.org/#/c/osmo-bsc/+/12890

A work-around for OsmoBTS has been submitted at https://gerrit.osmocom.org/#/c/osmo-bts/+/12891

#4 - 05/29/2019 02:12 PM - laforge

- Status changed from In Progress to Resolved

both patches merged quite some time ago.

Files

20190212-oml-get_attr.pcap	123 Bytes	02/12/2019	laforge