OsmoMSC - Bug #3805

OsmoMSC sends invalid BSSMAP length field on CSFB CLEAR COMMAND

02/18/2019 11:34 AM - laforge

Status:	Resolved	**Start date:**	02/18/2019
Priority:	High	**Due date:**	
Assignee:	laforge	**% Done:**	100%
Category:	A interface (general)		
Target version:			
Resolution:		**Spec Reference:**	

Description

When sending a BSSMAP CLEAR COMMAND with CSFB indicator, osmo-msc currently sends '0004200401098' where '04' is the length of the BSSMAP message which we follow with 5 bytes of IEs :(

Let's not only fix that one encoding bug but also add a general consistency checker in the BSSAP output path to ensure we catch sending invalid length fields inside osmo-msc (and osmo-bsc) itself.

See also: https://www.eclipse.org/forums/index.php/t/1097647/

Related issues:

Related to OsmoMSC - Feature #3778: Support CSFB "Fast Return"	**Resolved**	**02/03/2019**
Related to OsmoBSC - Bug #3806: OsmoBSC accepts BSSAP with wrong length field	**Stalled**	**02/18/2019**

Associated revisions

Revision 10ba47dd - 02/18/2019 01:11 PM - laforge

Fix BSSMAP length generated by gsm0808_create_clear_command2()

In Change-Id Id8a75e1da2d5f520064666e4ee413d1c91da6ae3 we recently
introduced adding the "CSFB INDICATOR" IE to the CLEAR COMMAND,
but we did so with a wrong length value.

Change-Id: I4d07d25fb03ca0f89fd7b94226c54309c77a010a
Closes: OS#3805
Related: OS#2778

Revision cf665fc6 - 02/18/2019 01:34 PM - laforge

gsm0808: Add unit tests for test_create_clear_command2()

Change-Id: Ie3f34b78edc91a013152742bebbd839586a787fe
Related: OS#3805

History

#1 - 02/18/2019 11:34 AM - laforge

- Related to Feature #3778: Support CSFB "Fast Return" added

#2 - 02/18/2019 11:35 AM - laforge

- Status changed from New to In Progress

#3 - 02/18/2019 12:59 PM - laforge

- % Done changed from 0 to 80

Actual encoding bug adressed in https://gerrit.osmocom.org/#/c/libosmocore/+/12924/

The bug only came about because

1. the related function gsm0808_create_clear_command2() was introduced without any unit test coverage.
2. the feature in osmo-msc was developed / added before having a TTCN-3 testcase in place

It saddens me a bit that >= 1.5 years after introducing test-driven development we still see those kind of issues slipping into master. We need to work together to improve our processes. This doesn't only affect the developer, but also the reviewers. We should have spotted the missing unit test

during review.

- https://gerrit.osmocom.org/#/c/libosmocore/+/12933/ adds the missing unit test
- https://gerrit.osmocom.org/#/c/osmo-msc/+/12928/ adds a generic "encoded length value" check to all BSSAP messages transmitted by osmo-msc.

#4 - 02/18/2019 01:13 PM - laforge

- Status changed from In Progress to Resolved

- % Done changed from 80 to 100

libosmocore patch merged, OsmoMSC now sends correct length values.

#5 - 02/18/2019 01:18 PM - laforge

- Related to Bug #3806: OsmoBSC accepts BSSAP with wrong length field added