libosmocore - Bug #4819

Wrong RLL ERR IND sent during LAPDm re-establishment procedures

10/19/2020 01:16 PM - laforge

Status:	Resolved	**Start date:**	10/19/2020
Priority:	Normal	**Due date:**	
Assignee:	pespin	**% Done:**	100%
Category:	libosmogsm		
Target version:			
Spec Reference:			

Description

In #4549 we-ve encountered a situation where a MS (by intention or by accident) sends a SABM with L=0 on a already fully established lchan. This currently triggers:

- an RLL ERROR IND "SABM frame with information not allowed in this state" (cause 14)
  - the cause value is even wrong, as there was no information field present ;)
- an UA response (i.e. the re-establishment actually happens

So somehow we send a RLL ERR IND that shouldn't be sent.

Related issues:

Related to OsmoBSC - Feature #4549: Emergency Call Priority / Pre-Emption	**Feedback**	**05/12/2020**

History

#1 - 10/19/2020 01:16 PM - laforge

- Related to Feature #4549: Emergency Call Priority / Pre-Emption added

#2 - 10/19/2020 01:21 PM - laforge

- Assignee set to pespin

we should create a TTCN3 test case as part of BTS_Tests_LAPDm that produces this scenario:

- establish a SDCCH like normal, transmit some data back and forth
- send a SABM with L=0 for SAPI=0 from the MS
- expect that the SABM is responded to with a UA
- expect no RLL ERROR IND on the BTS side. Rather, an "ESTABLISH IND", if at all.

#3 - 10/19/2020 01:29 PM - laforge

- Subject changed from Wring RLL ERR IND sent during LAPDm re-establishment procedures to Wrong RLL ERR IND sent during LAPDm re-establishment procedures

#4 - 10/19/2020 01:30 PM - laforge

the test should also verify that any L3 messages sent in uplink after the SABM/UA exchange are passed to the Abis/RSL side

#5 - 10/19/2020 06:22 PM - pespin

Test added here:
https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/20793 bts-lapdm: Introduce test TC_normal_reestablishment

However it's not triggering the issue seen in #4549 because lapdm state in BTS is not LAPD_STATE_TIMER_RECOV as in the initial case, but LAPD_STATE_MF_EST.

#6 - 10/20/2020 07:30 AM - laforge

On Mon, Oct 19, 2020 at 06:22:32PM +0000, pespin [REDMINE] wrote:

> However it's not triggering the issue seen in #4549 because lapdm state in BTS is not LAPD_STATE_TIMER_RECOV as in the initial case, but LAPD_STATE_MF_EST.

I think the TIMER_RECOV state just means there is some un-acknowledged data,
so if you send an I-frame from the Abis/RSL side, which has not yet been acknowledged
from the Um/L1CTL side (after T200 expiration, which is certainly < 1s), you should be in that state.

#7 - 10/20/2020 04:47 PM - pespin

- Status changed from New to Feedback

- % Done changed from 0 to 90

Bug is reproduced by this test:
https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/20805 bts-lapdm: Introduce test TC_normal_reestablishment_state_unacked

And fixed by (test passes after) this commit:
https://gerrit.osmocom.org/c/libosmocore/+/20807 lapdm: Allow SABM L=0 in Timer Recovery State

#8 - 10/21/2020 05:28 PM - pespin

- Status changed from Feedback to Resolved

- % Done changed from 90 to 100

Merged, and I also confirm the bug is fixed with a real modem.