OsmoBTS - Bug #3045

sysmoBTS: re-assigning an lchan to a different timeslot triggers activation of *all* SDCCH

03/08/2018 03:38 PM - neels

Status:	Rejected	**Start date:**	03/08/2018
Priority:	High	**Due date:**	
Assignee:	dexter	**% Done:**	90%
Category:			
Target version:			
Spec Reference:			

Description

edit: a fix is merged, we still want to test the fix on octphy and litecell-15

Scenario: two phones in a voice call on one sysmoBTS.
Issue 'assignment any' vty command to re-assign one TCH/F to a different lchan.
This triggers a cascade of all SDCCH being activated (RSL Chan Act, Chan Act Ack) followed by about as many failures to assign an SDDCH (since all are already activated).

(Details follow)

History

#1 - 03/08/2018 04:00 PM - neels

- File osmo-bts_sddch_act_flood2.pcapng added

This is with current master of osmo-bts-sysmo

```
===== osmo-bts =====
7eed026efc0b75608b37521147db140c06fca5b1

===== libosmocore =====
bf86d71f58f83f53e740d64e649884c91ee77c26

===== osmo-pcu =====
8343b4adbbe9afd4294232429696ee9736ec1004

===== layer1-api =====
7f0d5697b85340877b127a25e0c8f2a5f5fe66d7

===== libosmo-abis =====
61460fd6431d6ea62752d74ad05425f132d7abbe
```

In attached pcap, the call is established and up at packet 6862 (RTP and MGW logging is filtered out),
I issue an 'assignment any' command in the BSC VTY: packet 7125. (again later in 8653 with the same effect)
The Assignment first of all activates a TCH/F lchan in TS 4, as expected, which is acked and set up fine.

About .1 seconds after that is done, follows a BTS 0 CHAN RQD, reason "Location Updating", and we request to activate TS=0 lchan=1 (CCCH+SDCCH4 pchan).
Within .3 seconds the BSC receives more than 50 such CHAN RQD. Notably also one for reason "other" and one for reason "answer to paging" in between.
All available SDCCH lchans are activated and acked, followed by N "no resources for SDCCH".

The handover timer expires and handover is canceled.
The newly assigned TCH/F on TS=4 is released.

Three seconds after the SDCCH RQD flood, all the SDCCH are released in error, "no response to IMMEDIATE ASSIGN".

#2 - 03/08/2018 04:04 PM - neels

With the identical core net but running osmo-bts-sysmo 0.7.0.38-ef8c, the same procedure works like a charm.
Going to bisect now...

#3 - 03/08/2018 04:45 PM - neels

bisecting and testing leads me to this commit being the cause:

```
c2b4c668f3510b7b0baace749c5a310959010e90 is the first bad commit
commit c2b4c668f3510b7b0baace749c5a310959010e90
Author: Harald Welte <laforge@gnumonks.org>
Date:   Mon Feb 26 11:57:49 2018 +0100

    Move rach_busy counting above L1SAP

    In the past, rach_busy counting was performed below L1SAP, while
    reporting was handled above.  This lead to subtle differences between
    the BTS models, such as osmo-bts-trx missing to increment rach_busy.

    Let's move the rach_busy counting above L1SAP to share more code.

    This means we need libosmocore Change-Id
    I9439810c3a3ad89ea0302753617b850749af887c for the additional required
    parameters in ph_rach_ind_param, as well as libosmocore Change-id
    I2b1926a37bde860dcfeb0d613eb55a71271928c5 for osmo-bts-trx to determine
    the RACH bit error rate.

    Change-Id: I3b989580cb38082e3fd8fc50a11fedda13991092
    Closes: OS#3003
```

#4 - 03/08/2018 04:45 PM - neels

- Status changed from New to In Progress

- Assignee set to neels

- % Done changed from 0 to 20

#5 - 03/08/2018 05:00 PM - laforge

On Thu, Mar 08, 2018 at 03:38:58PM +0000, neels [REDMINE] wrote:

> Scenario: two phones in a voice call on one sysmoBTS.
> Issue 'assignment any' vty command to re-assign one TCH/F to a different lchan.
> This triggers a cascade of all SDCCH being activated (RSL Chan Act, Chan Act Ack) followed by about as many failures to assign an SDDCH (since all are already activated).

can we please try to reproduce this with osmo-bts-trx + trxcon or even straight away
in the BTS_Tests.ttcn test suite?

#6 - 03/08/2018 06:55 PM - neels

The difference between the successful and failing case is that before, the RACH was detected as a handover access burst in l1sap_ph_rach_ind(), while after above commit it is not, and ends up as a "RACH for RR access"; many of those flood in in close succession, each being mis-detected as "for RR access".

I added some printf()s to see what exactly is happening in l1sap_ph_rach_ind(), and in the successful code state, I see a rach_ind->chan_nr=0xa or =0xc; in the failing case, I see rach_ind->chan_nr=0x88. So something about that patch modifies the rach_ind->chan_nr.

Looking at handle_ph_ra_ind() in src/osmo-bts-sysmo/l1_if.c I add a printf() of ra_ind->hLayer2 at the top, where the lchan is determined before the patch, and another printf at the bottom, where the lchan is determined after the patch. The curious fact is that above, hLayer2 0x4bb, while at the bottom, hLayer2=0x2. Thus after the patch, the call to l1if_hLayer_to_lchan() never sees magic 0xbb and always returns NULL.

Now to find out what overwrites hLayer2.

#7 - 03/08/2018 08:18 PM - neels

- % Done changed from 20 to 80

A fix is in https://gerrit.osmocom.org/7169 -- but I tested only for sysmoBTS, octphy and litecell15 should still be verified to work now.

#8 - 03/09/2018 11:53 AM - laforge

I've merged the proposed patch now, but let's keep this open to check if we can move to a stack-based l1sap prim instead, which would be cleaner.

#9 - 03/09/2018 12:06 PM - ipse

I see that the merged patch doesn't touch osmo-bts-trx. Does this mean that it is not affected by this issue? We've seen something which has very similar symptoms in a network where we have handover enabled - all of a sudden all channels of a certain BTS get allocated by what looks like a RACH flood. We've never seen this in networks without handover. Our osmo-bts is quite old there but symptoms look too similar.

#10 - 03/09/2018 12:39 PM - neels

- Status changed from In Progress to Feedback

- Assignee changed from neels to dexter

- % Done changed from 80 to 90

The patch to fix this on sysmoBTS is already merged: https://gerrit.osmocom.org/7169

We should still verify that this patch has the desired result on litecell-15 (so similar to sysmoBTS that we might even not bother to test specifically), and on octphy (different enough to warrant a test).

dexter, could you please verify that an octphy build of osmo-bts master (with above patch included) works when doing 'assignment any' during a phone call? Thanks!

#11 - 03/09/2018 12:50 PM - neels

ipse wrote:

> I see that the merged patch doesn't touch osmo-bts-trx. Does this mean that it is not affected by this issue?

Exactly. The regression of accessing an ivalidated data structure was not introduced in the osmo-bts-trx code.

> We've seen something which has very similar symptoms in a network where we have handover enabled - all of a sudden all channels of a certain BTS get allocated by what looks like a RACH flood. We've never seen this in networks without handover. Our osmo-bts is quite old there but symptoms look too similar.

I understand the mechanism is that a Handover RACH gets misinterpreted as an RR RACH and causes allocation of an SDCCH channel. The handover RACH are repeated, each one misinterpreted, hence all SDCCH get allocated in close succession. If your old osmo-bts exhibits this, it is certainly not related to the regression introduced by the commit "Move rach_busy counting above L1SAP", because that one is barely two weeks old. Maybe moving to a newer osmo-bts-trx would help instead? (I must admit though I haven't tested handover on any model other than sysmoBTS yet.)

#12 - 03/09/2018 12:52 PM - neels

- Checklist item [x] test sysmoBTS added
Checklist item [ ] test litecell-15 added
Checklist item [ ] test octphy added

- Description updated

#13 - 03/09/2018 01:10 PM - laforge

On Fri, Mar 09, 2018 at 12:06:19PM +0000, ipse [REDMINE] wrote:

> I see that the merged patch doesn't touch osmo-bts-trx. Does this mean that it is not affected by this issue?

yes, it's not affected, as it was the only PHY that has received testing after the patch
introducing the bug was merged a few days ago, see
https://jenkins.osmocom.org/jenkins/view/TTCN3/job/ttcn3-bts-test/ for the nightly test runs. It uses
trxcon+fake_trx as well as an unmodified osmo-bts-trx.

> We've seen something which has very similar symptoms in a network where we have handover enabled - all of a sudden all channels of a certain BTS get allocated by what looks like a RACH flood. We've never seen this in networks without handover. Our osmo-bts is quite old there but symptoms look too similar.

I'm sure it's not the current issue, as this one was only introduced on February 26, 2018

#14 - 06/23/2018 06:51 PM - laforge

- Priority changed from Normal to High

#15 - 05/22/2019 02:33 PM - laforge

- Status changed from Feedback to Rejected

Files

osmo-bts_sddch_act_flood2.pcapng	2.34 MB	03/08/2018	neels