OsmoBTS - Bug #2674

osmo-bts-sysmo GPRS failing if running without "-M"

11/22/2017 01:58 PM - pespin

Status:	New	**Start date:**	11/22/2017
Priority:	Low	**Due date:**	
Assignee:	pespin	**% Done:**	0%
Category:	osmo-bts-sysmo		
Target version:			
Spec Reference:			

Description

In osmo-gsm-tester setup (CN+BSC running in main unit, BTS+PCU in sysmobts).

RUnning osmo-bts-sysmo with -M (pcu direct access to PHDATA) works fine.

If run without -M, then the phdata_ind packets are printed in uplink GSMTAP (by function to_gsmtap()), but never arrive to the osmo-pcu through the unix socket, and then osmo-pcu neves sends Attach Request to osmo-sgsn.

What I debugged so far:
The packets arrive to l1sap.c:l1sap_up():

```
    case OSMO_PRIM(PRIM_PH_DATA, PRIM_OP_INDICATION):
        to_gsmtap(trx, l1sap);
        rc = l1sap_ph_data_ind(trx, l1sap, &l1sap->u.data);
        break;
```

In there the packet is sent through GSMTAP, but l1sap_ph_data_ind() is returning -22 (EINVAL).

I verified that indeed that einval comes from l1sap.c:l1sap_ph_data_ind() code path which returns early and doesn't send content of the message through the unix socket:

```
static int l1sap_ph_data_ind(struct gsm_bts_trx *trx,
     struct osmo_phsap_prim *l1sap, struct ph_data_param *data_ind)
{
    struct msgb *msg = l1sap->oph.msg;
    uint8_t *data = msg->l2h;
    int len = msgb_l2len(msg);
    ...
    if (ts_is_pdch(&trx->ts[tn])) {
        ...
        /* don't send bad frames to PCU */
        if (len == 0) {
            LOGP(DL1P, LOGL_ERROR, "pespin: len==0, avoid send to pcu\n");
            return -EINVAL;
        }
        ...
        pcu_tx_data_ind(...)
        ...
    }
```

I see several possible issues there:
- In lower layers (l1) in osmo-bts-sysmo, we are not packing the indication correctly into the msgb.
- We are not doing the correct check in l1sap_ph_data_ind() and there's good information in the packets.
- We are not doing the correct check in to_gsmtap() if the packet is actually containing non correct data. We should avoid sending it and logging a NOTICE or similar instead.

History

#1 - 11/22/2017 02:09 PM - pespin

This is the print for each packet not sent to the PCU when created at the lower layers:

```
osmo-bts/src/osmo-bts-sysmo/l1_if.c:1137 Rx L1 prim PH-DATA.ind on queue 1
osmo-bts/src/common/l1sap.c:517 (bts=0,trx=0,ts=7,ss=0) MPH_INFO meas ind, ta_offs_qbits=0, ber10k=0, inv_rssi
=115
osmo-bts/src/osmo-bts-sysmo/l1_if.c:948 Rx PH-DATA.ind PDTCH 008662/06/04/43/06 (hL2 000700bb):
, Meas: RSSI -115.99 dBm,  Qual -4.72 dB,  BER 0.00,  Timing 0
osmo-bts/src/common/l1sap.c:999 Rx PH-DATA.ind 008662/06/04/43/06 chan_nr=0x0f link_id=0x00 len=0
osmo-bts/src/common/l1sap.c:1020 pespin: len==0, avoid send to pcu
osmo-bts/src/common/l1sap.c:1220 pespin: l1sap_ph_data_ind returned error rc=-22
```

#2 - 11/23/2017 12:29 PM - pespin

- Category set to osmo-bts-sysmo

- Assignee set to pespin

Using same environment (osmo-gsm-tester), osmo-bts-trx with osmo-pcu seems to be working fine (modems attaches), and of course that one doesn't support/use the -M option.

That means the issue only appears in osmo-bts-sysmo without -M option, and thus the issue is most probably in osmo-bts-sysmo specific code forwarding the packets to osmo-bts common code.

#3 - 07/18/2019 06:08 AM - laforge

- Priority changed from Normal to Low