As seen by a WIP ttcn3 test (branch pespin/pcu-cap-egprs), which sends a 8-bit RACH req and then tries to use Packet Resource Request to submit RA capabilities in order to get an EGPRS context, as explained in spec 3GPP TS 04.60 sec “7.1.3 TBF establishment using two phase access”.

```c
/* FIXME: properly encode RA (see TS 24.060, table 11.2.5.2) */
private function f_establish_tbf(out GsmRrMessage rr_imm_ass, uint8_t bts_nr := 0,
    uint16_t ra := oct2int('3A'O), uint8_t is_11bit := 0,
    PCUIF_BurstType burst_type := BURST_TYPE_0,
    TimingAdvance ta := 0)
runs on RAW_PCU_Test_CT return boolean {
    var uint32_t fn;
    /* FIXME: ask the BTS component to give us the current TDMA fn */
    fn := 1337 + ta;

    /* Send RACH.ind */
    log("Sending RACH.ind on fn=", fn, " with RA="r", ra, ", TA="t, ta);
    BTS.send(ts_PCUIF_RACH_IND(bts_nr := bts_nr, trx_nr := 0, ts_nr := 0,
        ra := ra, is_11bit := is_11bit,
        burst_type := burst_type,
        fn := fn, arfcn := 871,
        qta := ta * 4));

    /* Expect Immediate (TBF) Assignment on TS0/AGCH */
    return f_pcuif_rx_imm_ass(rr_imm_ass, tr_IMM_TBF_ASS(?r, ra, fn), bts_nr);
}
```

It fails during f_establish_tbf when using "egprs only" mode, because an Imm ass Reject is sent by PCU. gsmtap log:

```
.13.10 4729 GSMTAP 220 RACH request received: sapi=1 qta=0, ra=0x3a, fn=1337, cur_fn=4,
    is_11bit=0
.13.10 4729 GSMTAP 225 MS requests UL TBF on RACH, so we provide one: ra=0x3a Fn=1337
    qta=0 is_11bit=0
.13.10 4729 GSMTAP 193 Not accepting non-EGPRS phone in EGPRS-only mode
.13.10 4729 GSMTAP 211 No PDCH resource sending Immediate Assignment Uplink (AGCH) rej
ect
.13.10 4729 GSMTAP 289 Sending data request: trx=0 ts=0 sapi=2 arfcn=0 fn=0 cur_fn=4
```
Attached find the pcap generated by ttcn3 env.

So looking at osmo-pcu, the interesting parts seem to be located in bts.cpp BTS::rcv_rach(), which calls:

```cpp
sb = is_single_block(m_bts.force_two_phase, ra, burst_type, is_11bit);
```

which seems to decide whether a single block is required or not based on some information (force_two_phase is not set, but can be configured through VTY "two-phase-access"). In this case, a single block is not selected and fails later during call to tbf = tbf_alloc_ul_tbf(&m_bts, NULL, -1, 0, ms_class, true); which of course fails because egprs_ms_class passed is 0.

So as far as I understand from the spec reference listed above, it should be possible for this scenario to work. Maybe I need to send some specific value in the RACH request so that single block is selected in order to sent PACKET RESOURCE REQUEST? If that's not the case, then osmo-pcu needs to be fixed to accept the RACH request to allow the MS to upgrade its MS class afterwards.

---

**History**

**#1 - 04/23/2020 03:22 AM - fixeria**

If I remember correctly, keith reported a similar behavior in the IRC (not sure if there is any ticket).

... spec 3GPP TS 04.60 sec “7.1.3 TBF establishment using two phase access”.

TS 04.60 (or TS 44.060) mostly describes the establishment procedures for configurations where PBCCH (and thus PRACH) is present (despite it has been deprecated a while ago, and should not be used nowadays). I would recommend to additionally check out 3GPP TS 44.018, in particular section 3.5.2 "Packet access procedure using CCCH".

So as far as I understand from the spec reference listed above, it should be possible for this scenario to work.

Yep, I also think we should not reject phones just because egprs_ms_class is not known. Even in case of 11 bit EGPRS Packet Channel Request, egprs_ms_class is not always included (depending on its type). Maybe we should just do a regular GPRS assignment in that case? AH, damn, it's 'egprs-only' mode...

Maybe I need to send some specific value in the RACH request so that single block is selected in order to sent PACKET RESOURCE REQUEST?

See 3GPP TS 44.018, table 9.1.8.1 "CHANNEL REQUEST message content". The value '3A'O was picked randomly, because back then in September I had almost no knowledge about GPRS and its RLC/MAC. So '3A'O (00111010'B) is not even a valid packet Access Burst ;/ Looking at the table, it matches '0011xxxx'B - "Answer to paging".

So I would try sending '01110xxx'B (single block packet access), or one of '011110xx'B | '011110x0x'B | '01111xx0'B (one phase packet access). Good luck!

**#2 - 04/23/2020 03:35 PM - pespin**

Apparently we receive System Information 13 from BTS to PCU through the pcuif, so we can also gain information in osmo-pcu regarding what's allowed:

3GPP TS 04.08 version 7.21.0 "10.5.2.37b SI 13 Rest Octets"

Also in TS 04.60 (7.1.2.1 Initiation of the packet access procedure):

EGPRS TBF mode capable MSs shall monitor the GPRS Cell Options IE on the PBCCH (PSI1/PSI13) for the cell's EGPRS capability. In the GPRS Cell Options IE it is also indicated if the EGPRS PACKET CHANNEL REQUEST is supported by the cell.

**#3 - 04/24/2020 06:53 AM - laforge**

On Thu, Apr 23, 2020 at 03:35:22PM +0000, pespin [REDMINE] wrote:

Apparently we receive System Information 13 from BTS to PCU through the pcuif,

yes, this is among other things needed so we can send it to individual MS over PACCH once the TBF duration exceeds a certain time. This is required as the MS is not able to read SI13 from the BCCH while it is in an active TBF.

05/15/2020