OsmocomBB - Bug #1954

Motorola C188 with Osmocombb firmwre(RAM version) can't scan out any base stations

02/20/2017 11:58 AM - bbc250

Status:	In Progress	**Start date:**	02/20/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	90%
Category:			
Target version:			
Resolution:		**Spec Reference:**	

Description

Motorola C188 with Osmocombb firmwre (RAM version) can't scan out any base stations.
I tried to install Osmocombb on my single board computer (OrangePi Zero). By the way, There is not this problem on the virtual machine which bases on my x64 laptop.
When I try to upload the firmware to C118, no error

---
orangepi@orangepizero:/opt/osmocom-bb/src/host/osmocon$ sudo ./osmocon -p /dev/ttyUSB0 -m c123xor ../../target/firmware/board/compal_e88/layer1.compalram.bin
[sudo] orangepi □□□□
got 2 bytes from modem, data looks like: 04 81 ..
got 5 bytes from modem, data looks like: 1b f6 02 00 41 ....A
got 1 bytes from modem, data looks like: 01 .
got 1 bytes from modem, data looks like: 40 @
Received PROMPT1 from phone, responding with CMD
read_file(../../target/firmware/board/compal_e88/layer1.compalram.bin): file_size=54668, hdr_len=4, dnload_len=54675
got 1 bytes from modem, data looks like: 1b .
got 1 bytes from modem, data looks like: f6 .
got 1 bytes from modem, data looks like: 02 .
got 1 bytes from modem, data looks like: 00 .
got 1 bytes from modem, data looks like: 41 A
got 1 bytes from modem, data looks like: 02 .
got 1 bytes from modem, data looks like: 43 C
Received PROMPT2 from phone, starting download
handle_write(): 4096 bytes (4096/54675)
handle_write(): 4096 bytes (8192/54675)
handle_write(): 4096 bytes (12288/54675)
handle_write(): 4096 bytes (16384/54675)
handle_write(): 4096 bytes (20480/54675)
handle_write(): 4096 bytes (24576/54675)
handle_write(): 4096 bytes (28672/54675)
handle_write(): 4096 bytes (32768/54675)
handle_write(): 4096 bytes (36864/54675)
handle_write(): 4096 bytes (40960/54675)
handle_write(): 4096 bytes (45056/54675)
handle_write(): 4096 bytes (49152/54675)
handle_write(): 4096 bytes (53248/54675)
handle_write(): 1427 bytes (54675/54675)
handle_write(): finished
got 1 bytes from modem, data looks like: 1b .
got 1 bytes from modem, data looks like: f6 .
got 1 bytes from modem, data looks like: 02 .
got 1 bytes from modem, data looks like: 00 .
got 1 bytes from modem, data looks like: 41 A
got 1 bytes from modem, data looks like: 03 .
got 1 bytes from modem, data looks like: 42 B
Received DOWNLOAD ACK from phone, your code is running now!
battery_compal_e88_init: starting up

OSMOCOM Layer 1 (revision osmocon_v0.0.0-1351-g074c78a)
==========
Device ID code: 0xb4fb

Device Version code: 0x0000
ARM ID code: 0xfff3
cDSP ID code: 0x0128
Die ID code: 7cd81a308f439b0f ==========
REG_DPLL=0x2413
CNTL_ARM_CLK=0xf0a1
CNTL_CLK=0xff91
CNTL_RST=0xfff3
CNTL_ARM_DIV=0xfff9 ==========
Power up simcard:

THIS FIRMWARE WAS COMPILED WITHOUT TX SUPPORT!!!
Assert DSP into Reset
Releasing DSP from Reset
Installing DSP sniff patch
Setting some dsp_api.ndb values
Setting API NDB parameters
DSP Download Status: 0x0001
DSP API Version: 0x0000 0x0000
Finishing download phase
DSP Download Status: 0x0002
DSP API Version: 0x3606 0x0000
LOST 1131!
L1CTL_RESET_REQ: FULL!L1CTL_RESET_REQ: FULL!L1CTL_PM_REQ start=0 end=124
PM MEAS: ARFCN=0, 38 dBm at baseband, ~~99 dBm at RF~~
~~PM MEAS: ARFCN=1, 39 dBm at baseband, -98 dBm at RF~~
~~PM MEAS: ARFCN=2, 39 dBm at baseband, -98 dBm at RF~~
~~#....(some)....~~
~~PM MEAS: ARFCN=1023, 42 dBm at baseband, -96 dBm at RF~~
~~L1CTL_RESET_REQ: FULL!L1CTL_FBSB_REQ (arfcn=3, flags=0x7)~~
~~orangepi@orangepizero:/opt/osmocom-bb/src/host/osmocon$~~
~~----------~~

Then I opened a new terminal window, tried to scan base station, and got stuck at this notice.

---
orangepi@orangepizero:/opt/osmocom-bb/src/host/layer23/src/misc$ sudo ./cell_log -O
[sudo] orangepi □□□□
Copyright (C) 2010 Andreas Eversberg

License GPLv2+: GNU GPL version 2 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Failed to connect to '/tmp/osmocom_sap'.
Failed during sap_open(), no SIM reader
<000e> cell_log.c:864 Scanner initialized
Mobile initialized, please start phone now!
<000e> cell_log.c:443 Measure from 0 to 124
<000e> cell_log.c:443 Measure from 512 to 885
<000e> cell_log.c:443 Measure from 955 to 1023
<000e> cell_log.c:434 Measurement done
Layer2 socket failed

I lost my patience and removed connector from the USB port, and show a notification:"layer2 socket failed "
Before this step, I never had any errors. All steps were compiled successfully.

Environment:
Single board computer:OrangePi zero
Processor:Allwinner H2+(armhf)
OS:ArmBian Ubuntu 3.4.113 (xenial 16.04)

other useful information:
1.GnuArmToolchain:gnu-arm-build.3.sh(gcc-4.8.2/binutils-2.21.1a/newlib-1.19.0)
2.libosmocore osmocom-bb are both from the official git website.

In addition, my C188 had changed filters.

There are some other details that are not in it. But if you want to know, you can reply.
I am a new one in this website. Thank to everyone who can help me.:lol

History

#1 - 03/04/2017 11:30 AM - fixeria

Hi,

Motorola C188

Did you mean C118?

So, as I understand, you're losing L1CTL connection when the phone attempts to sync some BTS.
Please provide more information:

- Which branch are you using?
- What happens with phone after the L1CTL connection abort? It hangs?

Also, try to upgrade both libosmocore:

```
sudo make uninstall
make distclean
git pull --rebase

And then recompile it as usual.
```

and OsmocomBB:

```
make distclean
git pull --rebase

make
```

BTW: There is a problem with some toolchains: they compile the firmware, which hangs after synchronization attempt, so try to compile with this one: https://github.com/axilirator/gnu-arm-installer

#2 - 03/09/2017 04:51 PM - bbc250

- File untitled.png added

Hey,bro
I am sorry for replying too late.I am so busy for work.
Yeap,It is Motorola C118. just a small typing mistake

I tried what you said but it didn't work.
When I searched on the Internet, I found an article which metioned this issue.
(http://www.freebuf.com/sectool/107755.html)

At the seventh part,it said

If you use gnu-arm-build.2.sh and can't scan out any basestations, try to edit those files

vi osmocom-bb/src/target/firmware/board/compal/highram.lds
vi osmocom-bb/src/target/firmware/board/compal/ram.lds
vi osmocom-bb/src/target/firmware/board/compal_e88/flash.lds
vi osmocom-bb/src/target/firmware/board/compal_e88/loader.lds
vi osmocom-bb/src/target/firmware/board/mediatek/ram.lds

Find this sentence

KEEP(*(SORT(.ctors)))

Insert this after that

KEEP(*(SORT(.init_array)))

It look like the picture shows.

Edit all, save all, enter /osmocom-bb/src and rebuild it

make -e CROSS_TOOL_PREFIX=arm-none-eabi-

I have not tried. Just want to share this way
If it works, I will post

#3 - 03/09/2017 05:02 PM - bbc250

Branch:origin/luca/gsmmap

How can I see what happens with phone after the L1CTL connection abort? Which command is used?

I am new in this project. Can you give me some tips? Thank you so much

#4 - 03/24/2017 02:13 PM - bbc250

> (http://www.freebuf.com/sectool/107755.html)
>
> At the seventh part,it said
> ---
> If you use gnu-arm-build.2.sh and can't scan out any basestations, try to edit those files
>
> vi osmocom-bb/src/target/firmware/board/compal/highram.lds
> vi osmocom-bb/src/target/firmware/board/compal/ram.lds
> vi osmocom-bb/src/target/firmware/board/compal_e88/flash.lds
> vi osmocom-bb/src/target/firmware/board/compal_e88/loader.lds
> vi osmocom-bb/src/target/firmware/board/mediatek/ram.lds
>
> Find this sentence
>
> KEEP(*(SORT(.ctors)))
>
> Insert this after that
>
> KEEP(*(SORT(.init_array)))
>
> It look like the picture shows.
>
> Edit all, save all, enter /osmocom-bb/src and rebuild it
>
> make -e CROSS_TOOL_PREFIX=arm-none-eabi-

Thank everyone who follows this issues. It worked! Now my C118 can work successfully on RapsberryPi3. Thanks again!

#5 - 03/24/2017 02:27 PM - fixeria

- Status changed from New to Closed

#6 - 03/24/2017 02:48 PM - laforge

- Status changed from Closed to In Progress

- % Done changed from 0 to 90

let's keep this open as a reminder until somebody has submitted a related patch that can be merged to the baseband-devel mailing list.

#7 - 07/10/2017 10:24 PM - laforge

would be great if somebody could submit a related patch...

Files

1.png	240 KB	02/20/2017	bbc250
2.png	290 KB	02/20/2017	bbc250
untitled.png	197 KB	03/09/2017	bbc250