OsmoTRX - Bug #4055

osmo-trx-lms: segfault on start with lime mini/usb

06/11/2019 03:55 PM - roh

Status:	Resolved	**Start date:**	06/11/2019
Priority:	Normal	**Due date:**	
Assignee:	pespin	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

setup is debian stable, packages from nightly freshly updated.
hardware is limesdr mini v1.2 - internal clock
i tried a limesdr usb too, but the result is the same

```
root@test123:/etc/osmocom# gdb --args /usr/bin/osmo-trx-lms -C /etc/osmocom/osmo-trx-lms.cfg
GNU gdb (Debian 7.12-6) 7.12.0.20161007-git
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 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.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from /usr/bin/osmo-trx-lms...Reading symbols from /usr/lib/debug/.build-id/e4/3c22
501c8dce35452481683c82f3c6608fac28.debug...done.
done.
(gdb) r
Starting program: /usr/bin/osmo-trx-lms -C /etc/osmocom/osmo-trx-lms.cfg
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Info: SSE3 support compiled in and supported by CPU
Info: SSE4.1 support compiled in and supported by CPU
Tue Jun 11 17:36:06 2019 DLGLOBAL <0004> telnet_interface.c:104 Available via telnet 127.0.0.1 423
7
Tue Jun 11 17:36:06 2019 DLCTRL <000b> control_if.c:911 CTRL at 127.0.0.1 4236
Tue Jun 11 17:36:06 2019 DMAIN <0000> osmo-trx.cpp:478 [tid=140737353853760] Config Settings
   Log Level............... 0
   Device args.............
   TRX Base Port........... 5700
   TRX Address............. 127.0.0.1
   GSM BTS Address......... 127.0.0.1
   Channels................ 1
   Tx Samples-per-Symbol... 4
   Rx Samples-per-Symbol... 4
   EDGE support............ 0
   Extended RACH support... 0
   Reference............... 0
   C0 Filler Table......... 1
   Multi-Carrier........... 0
   Tuning offset........... 0
   RSSI to dBm offset...... 0
   Swap channels........... 0
   Tx Antennas............. 'BAND1'
   Rx Antennas............. 'LNAW'
```

```
Tue Jun 11 17:36:06 2019 DMAIN <0000> osmo-trx.cpp:434 [tid=140737353853760] Setting SCHED_RR prio
rity 18
Tue Jun 11 17:36:06 2019 DDEV <0002> LMSDevice.cpp:52 [tid=140737353853760] creating LMS device...
Tue Jun 11 17:36:06 2019 DDEV <0002> LMSDevice.cpp:139 [tid=140737353853760] Opening LMS device..
[New Thread 0x7ffff425a700 (LWP 757)]
[New Thread 0x7ffff3a59700 (LWP 758)]
[New Thread 0x7ffff3258700 (LWP 759)]
Tue Jun 11 17:36:06 2019 DDEV <0002> LMSDevice.cpp:145 [tid=140737353853760] Devices found: 1
Tue Jun 11 17:36:06 2019 DDEV <0002> LMSDevice.cpp:155 [tid=140737353853760] Device [0]: LimeSDR M
ini, media=USB 2.0, module=FT601, addr=24607:1027, serial=1D3B7AA1A9F5CC
Tue Jun 11 17:36:06 2019 DDEV <0002> LMSDevice.cpp:164 [tid=140737353853760] Using device[0]
Tue Jun 11 17:36:06 2019 DLMS <0003> LMSDevice.cpp:92 [tid=140737353853760] Reference clock 40.00
MHz
Tue Jun 11 17:36:06 2019 DDEV <0002> LMSDevice.cpp:190 [tid=140737353853760] Init LMS device
Tue Jun 11 17:36:06 2019 DDEV <0002> LMSDevice.cpp:97 [tid=140737353853760] Sample Rate: Min=10000
0 Max=3.072e+07 Step=0
Tue Jun 11 17:36:06 2019 DDEV <0002> LMSDevice.cpp:226 [tid=140737353853760] Setting sample rate t
o 1.08333e+06 4
Tue Jun 11 17:36:06 2019 DDEV <0002> LMSDevice.cpp:232 [tid=140737353853760] Sample Rate: Host=1.0
8333e+06 RF=3.46667e+07
Tue Jun 11 17:36:06 2019 DMAIN <0000> LMSDevice.cpp:209 [tid=140737353853760] Antennas configured
successfully
[New Thread 0x7ffff7ff7700 (LWP 760)]
Tue Jun 11 17:36:06 2019 DMAIN <0000> Threads.cpp:116 [tid=140737354102528] Thread 140737354102528
 (task 760) set name: CtrlService0
Tue Jun 11 17:36:06 2019 DMAIN <0000> osmo-trx.cpp:526 [tid=140737353853760] -- Transceiver active
 with 1 channel(s)
Tue Jun 11 17:36:08 2019 DTRXCTRL <0001> Transceiver.cpp:717 [tid=140737354102528][chan=0] command
 is 'POWERON'
Tue Jun 11 17:36:08 2019 DMAIN <0000> Transceiver.cpp:244 [tid=140737354102528] Starting the trans
ceiver
Tue Jun 11 17:36:08 2019 DMAIN <0000> radioInterface.cpp:177 [tid=140737354102528] Starting radio
device
Tue Jun 11 17:36:08 2019 DDEV <0002> LMSDevice.cpp:260 [tid=140737354102528] starting LMS...
Tue Jun 11 17:36:08 2019 DDEV <0002> LMSDevice.cpp:409 [tid=140737354102528][chan=0] Setting TX ga
in to 66 dB
Tue Jun 11 17:36:08 2019 DDEV <0002> LMSDevice.cpp:424 [tid=140737354102528][chan=0] Setting RX ga
in to 36.5 dB
Tue Jun 11 17:36:08 2019 DDEV <0002> LMSDevice.cpp:360 [tid=140737354102528][chan=0] Setting filte
rs
Tue Jun 11 17:36:08 2019 DDEV <0002> LMSDevice.cpp:97 [tid=140737354102528] LPFBWRange Rx: Min=1.4
001e+06 Max=1.3e+08 Step=0
Tue Jun 11 17:36:08 2019 DDEV <0002> LMSDevice.cpp:97 [tid=140737354102528] LPFBWRange Tx: Min=1.4
001e+06 Max=1.3e+08 Step=0
Tue Jun 11 17:36:08 2019 DDEV <0002> LMSDevice.cpp:371 [tid=140737354102528][chan=0] LPFBW: Rx=1.4
001e+06 Tx=5.2e+06
Tue Jun 11 17:36:08 2019 DDEV <0002> LMSDevice.cpp:373 [tid=140737354102528][chan=0] Setting LPFBW

Thread 5 "CtrlService0" received signal SIGSEGV, Segmentation fault.
[Switching to Thread 0x7ffff7ff7700 (LWP 760)]
0x00007ffff5e1dd4e in _IO_vfprintf_internal (s=s@entry=0x7ffff7ff00f0, format=format@entry=0x7ffff
5f40580 <format> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n", ap=ap@entry=0x7ffff7ff0258) at vfprintf.c:126
7
1267    vfprintf.c: No such file or directory.
(gdb) bt
#0  0x00007ffff5e1dd4e in _IO_vfprintf_internal (s=s@entry=0x7ffff7ff00f0, format=format@entry=0x7
ffff5f40580 <format> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n", ap=ap@entry=0x7ffff7ff0258) at vfprintf.c
:1267
#1  0x00007ffff5e46e89 in _IO_vsnprintf (string=0x7ffff61729c0 <result> "", maxlen=<optimized out>
, format=0x7ffff5f40580 <format> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n", args=args@entry=0x7ffff7ff025
8) at vsnprintf.c:114
#2  0x00007ffff5e262c2 in __snprintf (s=s@entry=0x7ffff61729c0 <result> "", maxlen=maxlen@entry=11
4, format=format@entry=0x7ffff5f40580 <format> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n") at snprintf.c:3
3
#3  0x00007ffff5e7ee81 in asctime_internal (tp=<optimized out>, buf=buf@entry=0x7ffff61729c0 <resu
lt> "", buflen=buflen@entry=114) at asctime.c:56
#4  0x00007ffff5e7ef11 in __GI_asctime (tp=<optimized out>) at asctime.c:87
```

```
#5  0x00007ffff5e7ef85 in ctime (t=t@entry=0x7ffff7ff03d0) at ctime.c:27
#6  0x00007ffff6cee528 in _output (target=target@entry=0x5555557d65d0, subsys=subsys@entry=3, leve
l=level@entry=5, file=file@entry=0x555555592e39 "LMSDevice.cpp", line=line@entry=92, cont=cont@ent
ry=0, format=0x555555595e00 "%s\n",
    ap=0x7ffff7ff14a0) at logging.c:365
#7  0x00007ffff6cee84d in osmo_vlogp (subsys=<optimized out>, level=5, file=0x555555592e39 "LMSDev
ice.cpp", line=92, cont=0, format=0x555555595e00 "%s\n", ap=0x7ffff7ff1510) at logging.c:544
#8  0x00007ffff6cee9b7 in logp2 (subsys=<optimized out>, level=<optimized out>, file=<optimized ou
t>, line=<optimized out>, cont=cont@entry=0, format=format@entry=0x555555595e00 "%s\n") at logging
.c:577
#9  0x000055555558ee27 in Log::~Log (this=0x7ffff7ff17d0, __in_chrg=<optimized out>) at Logger.cpp
:55
#10 0x000055555555fbee in lms_log_callback (lvl=<optimized out>, msg=0x7ffff7ff19b0 "Rx LPF min ba
ndwidth is 4MHz when TIA gain is set to -12 dB") at LMSDevice.cpp:92
#11 0x00007ffff6a3d59a in lime::log (level=level@entry=lime::LOG_LEVEL_WARNING, format=format@entr
y=0x7fffe8000a50 "Rx LPF min bandwidth is 4MHz when TIA gain is set to -12 dB", argList=argList@en
try=0x7ffff7ff29e0) at ./src/Logger.cpp:76
#12 0x00007ffff6a4c711 in lime::warning (format=format@entry=0x7fffe8000a50 "Rx LPF min bandwidth
is 4MHz when TIA gain is set to -12 dB") at ./src/Logger.h:98
#13 0x00007ffff6a4c9ca in lime::LMS7002M::Log (this=0x55555585da50, text=0x7fffe8000a50 "Rx LPF mi
n bandwidth is 4MHz when TIA gain is set to -12 dB", type=<optimized out>) at ./src/lms7002m/LMS70
02M.cpp:59
#14 0x00007ffff6a4cbf4 in lime::LMS7002M::Log (this=0x55555585da50, type=lime::LMS7002M::LOG_WARNI
NG, format=<optimized out>, argList=argList@entry=0x7ffff7ff2b50) at ./src/lms7002m/LMS7002M.cpp:9
2
#15 0x00007ffff6a60e6f in lime::LMS7002M::Log (this=this@entry=0x55555585da50, type=type@entry=lim
e::LMS7002M::LOG_WARNING, format=format@entry=0x7ffff6ab5bd8 "Rx LPF min bandwidth is 4MHz when TI
A gain is set to -12 dB")
    at ./src/lms7002m/LMS7002M.h:488
#16 0x00007ffff6a6078d in lime::LMS7002M::TuneRxFilter (this=this@entry=0x55555585da50, rx_lpf_fre
q_RF=4000000) at ./src/lms7002m/LMS7002M_filtersCalibration.cpp:87
#17 0x00007ffff6a7eb55 in lime::LMS7_Device::SetLPF (this=<optimized out>, tx=<optimized out>, cha
n=chan@entry=0, en=en@entry=true, bandwidth=<optimized out>, bandwidth@entry=6.9533491739302031e-3
10) at ./src/API/lms7_device.cpp:756
#18 0x00007ffff6a78c3a in LMS_SetLPFBW (device=<optimized out>, dir_tx=dir_tx@entry=false, chan=ch
an@entry=0, bandwidth=6.9533491739302031e-310, bandwidth@entry=1400100) at ./src/API/lms7_api.cpp:
395
#19 0x0000555555563bc5 in LMSDevice::do_filters (this=this@entry=0x55555585ab00, chan=chan@entry=0
) at LMSDevice.cpp:374
#20 0x0000555555563f0d in LMSDevice::start (this=0x55555585ab00) at LMSDevice.cpp:278
#21 0x000055555556e34b in RadioInterface::start (this=0x55555585df50) at radioInterface.cpp:183
#22 0x000055555557414b in Transceiver::start (this=this@entry=0x55555585e1e0) at Transceiver.cpp:2
51
#23 0x0000555555578fdd in Transceiver::driveControl (this=this@entry=0x55555585e1e0, chan=chan@ent
ry=0) at Transceiver.cpp:723
#24 0x0000555555579cb3 in ControlServiceLoopAdapter (chan=<optimized out>) at Transceiver.cpp:1098
#25 0x00007ffff7bc34a4 in start_thread (arg=0x7ffff7ff7700) at pthread_create.c:456
#26 0x00007ffff5ebfd0f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:97

root@test123:/etc/osmocom# osmo-trx-lms --version
Info: SSE3 support compiled in and supported by CPU
Info: SSE4.1 support compiled in and supported by CPU
OsmoTRX version 1.0.0.44-bde5

Copyright (C) 2007-2014 Free Software Foundation, Inc.
Copyright (C) 2013 Thomas Tsou <tom@tsou.cc>
Copyright (C) 2015 Ettus Research LLC
Copyright (C) 2017-2018 by sysmocom s.f.m.c. GmbH <info@sysmocom.de>
License AGPLv3+: GNU AGPL version 3 or later <http://gnu.org/licenses/agpl-3.0.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

root@test123:/etc/osmocom# LimeUtil --make
Make device
  Device name: LimeSDR-Mini
  Expansion name: UNSUPPORTED
  Firmware version: 6
```

```
  Hardware version: 2
  Protocol version: 1
  Gateware version: 1
  Gateware revision: 30
  Gateware target: LimeSDR-Mini
  Serial number: 0x1d3b7aa1a9f5cc
  Free connection... OK

root@test123:/etc/osmocom# LimeUtil --make
Make device
  Device name: LimeSDR-USB
  Expansion name: UNSUPPORTED
  Firmware version: 4
  Hardware version: 4
  Protocol version: 1
  Gateware version: 2
  Gateware revision: 21
  Gateware target: LimeSDR-USB
  Serial number: 0x9060b00472227
  Free connection... OK
```

Related issues:

Related to OsmoTRX - Support #4059: osmo-trx-lms: segfault on start LimeSDR-USB	**Resolved**	**06/12/2019**

History

#1 - 06/11/2019 04:15 PM - laforge

- Assignee set to pespin

#2 - 06/11/2019 04:29 PM - pespin

I need output for all threads:

Use in gdb: "thread apply all bt"

Also please provide your osmo-trx.cfg file as well as parameters passed to the process, and would be nice having osmo-bts-trx/osmo-bsc .cfg.

#3 - 06/11/2019 04:32 PM - pespin

Also please provide libosmocore + LimeSuite version you are using

#4 - 06/12/2019 11:32 AM - fixeria

- Related to Support #4059: osmo-trx-lms: segfault on start LimeSDR-USB added

#5 - 06/12/2019 02:02 PM - roh

- File osmo-trx-lms.cfg added

- File osmo-bsc.cfg added

versions:

```
osmo-trx-lms   OsmoTRX version 1.0.0.45-6a30
libosmocore    1.1.0.50.186f
liblimesuite19.04-1
```

backtrace:

```
root@test123:~# gdb --args /usr/bin/osmo-trx-lms -C /etc/osmocom/osmo-trx-lms.cfg
GNU gdb (Debian 7.12-6) 7.12.0.20161007-git
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 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.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
```

```
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from /usr/bin/osmo-trx-lms...Reading symbols from /usr/lib/debug/.build-id/25/272b0086b574fedd
e7438e7d05cff7603c5b43.debug...done.
done.
(gdb) r
Starting program: /usr/bin/osmo-trx-lms -C /etc/osmocom/osmo-trx-lms.cfg
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Info: SSE3 support compiled in and supported by CPU
Info: SSE4.1 support compiled in and supported by CPU
Wed Jun 12 15:54:36 2019 DLGLOBAL <0004> telnet_interface.c:104 Available via telnet 127.0.0.1 4237
Wed Jun 12 15:54:36 2019 DLCTRL <000b> control_if.c:911 CTRL at 127.0.0.1 4236
Wed Jun 12 15:54:36 2019 DMAIN <0000> osmo-trx.cpp:478 [tid=140737353853760] Config Settings
   Log Level............... 0
   Device args.............
   TRX Base Port........... 5700
   TRX Address............. 127.0.0.1
   GSM BTS Address......... 127.0.0.1
   Channels................ 1
   Tx Samples-per-Symbol... 4
   Rx Samples-per-Symbol... 4
   EDGE support............ 0
   Extended RACH support... 0
   Reference............... 0
   C0 Filler Table......... 1
   Multi-Carrier........... 0
   Tuning offset........... 0
   RSSI to dBm offset...... 0
   Swap channels........... 0
   Tx Antennas............. 'BAND1'
   Rx Antennas............. 'LNAW'

Wed Jun 12 15:54:36 2019 DMAIN <0000> osmo-trx.cpp:434 [tid=140737353853760] Setting SCHED_RR priority 18
Wed Jun 12 15:54:36 2019 DDEV <0002> LMSDevice.cpp:52 [tid=140737353853760] creating LMS device...
Wed Jun 12 15:54:36 2019 DDEV <0002> LMSDevice.cpp:139 [tid=140737353853760] Opening LMS device..
[New Thread 0x7ffff425a700 (LWP 510)]
[New Thread 0x7ffff3a59700 (LWP 511)]
[New Thread 0x7ffff3258700 (LWP 512)]
Wed Jun 12 15:54:36 2019 DDEV <0002> LMSDevice.cpp:145 [tid=140737353853760] Devices found: 1
Wed Jun 12 15:54:36 2019 DDEV <0002> LMSDevice.cpp:155 [tid=140737353853760] Device [0]: LimeSDR-USB, media=US
B 2.0, module=FX3, addr=1d50:6108, serial=0009060B00472227
Wed Jun 12 15:54:36 2019 DDEV <0002> LMSDevice.cpp:164 [tid=140737353853760] Using device[0]
Wed Jun 12 15:54:37 2019 DLMS <0003> LMSDevice.cpp:92 [tid=140737353853760] Reference clock 30.72 MHz
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:190 [tid=140737353853760] Init LMS device
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:203 [tid=140737353853760] Setting Internal clock reference
Wed Jun 12 15:54:37 2019 DLMS <0003> LMSDevice.cpp:92 [tid=140737353853760] Disabling external reference clock
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:97 [tid=140737353853760] Sample Rate: Min=100000 Max=6.144e
+07 Step=0
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:226 [tid=140737353853760] Setting sample rate to 1.08333e+0
6 4
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:232 [tid=140737353853760] Sample Rate: Host=1.08333e+06 RF=
3.46667e+07
Wed Jun 12 15:54:37 2019 DMAIN <0000> LMSDevice.cpp:209 [tid=140737353853760] Antennas configured successfully
[New Thread 0x7ffff7ff7700 (LWP 513)]
Wed Jun 12 15:54:37 2019 DMAIN <0000> Threads.cpp:116 [tid=140737354102528] Thread 140737354102528 (task 513)
set name: CtrlService0
Wed Jun 12 15:54:37 2019 DMAIN <0000> osmo-trx.cpp:526 [tid=140737353853760] -- Transceiver active with 1 chan
nel(s)
Wed Jun 12 15:54:37 2019 DTRXCTRL <0001> Transceiver.cpp:717 [tid=140737354102528][chan=0] command is 'POWEROF
F'
Wed Jun 12 15:54:37 2019 DTRXCTRL <0001> Transceiver.cpp:848 [tid=140737354102528][chan=0] response is 'RSP PO
WEROFF 0'
Wed Jun 12 15:54:37 2019 DTRXCTRL <0001> Transceiver.cpp:717 [tid=140737354102528][chan=0] command is 'RXTUNE
1782000'
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:763 [tid=140737354102528][chan=0] Setting Rx Freq to 1.782e
+09 Hz
Wed Jun 12 15:54:37 2019 DTRXCTRL <0001> Transceiver.cpp:848 [tid=140737354102528][chan=0] response is 'RSP RX
TUNE 0 1782000'
Wed Jun 12 15:54:37 2019 DTRXCTRL <0001> Transceiver.cpp:717 [tid=140737354102528][chan=0] command is 'TXTUNE
```

```
1877000'
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:751 [tid=140737354102528][chan=0] Setting Tx Freq to 1.877e
+09 Hz
Wed Jun 12 15:54:37 2019 DTRXCTRL <0001> Transceiver.cpp:848 [tid=140737354102528][chan=0] response is 'RSP TX
TUNE 0 1877000'
Wed Jun 12 15:54:37 2019 DTRXCTRL <0001> Transceiver.cpp:717 [tid=140737354102528][chan=0] command is 'SETTSC
7'
Wed Jun 12 15:54:37 2019 DTRXCTRL <0001> Transceiver.cpp:819 [tid=140737354102528] Changing TSC from 0 to 7
Wed Jun 12 15:54:37 2019 DTRXCTRL <0001> Transceiver.cpp:848 [tid=140737354102528][chan=0] response is 'RSP SE
TTSC 0 7'
Wed Jun 12 15:54:37 2019 DTRXCTRL <0001> Transceiver.cpp:717 [tid=140737354102528][chan=0] command is 'POWERON
'
Wed Jun 12 15:54:37 2019 DMAIN <0000> Transceiver.cpp:244 [tid=140737354102528] Starting the transceiver
Wed Jun 12 15:54:37 2019 DMAIN <0000> radioInterface.cpp:177 [tid=140737354102528] Starting radio device
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:260 [tid=140737354102528] starting LMS...
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:409 [tid=140737354102528][chan=0] Setting TX gain to 73 dB
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:424 [tid=140737354102528][chan=0] Setting RX gain to 36.5 d
B
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:360 [tid=140737354102528][chan=0] Setting filters
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:97 [tid=140737354102528] LPFBWRange Rx: Min=1.4001e+06 Max=
1.3e+08 Step=0
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:97 [tid=140737354102528] LPFBWRange Tx: Min=1.4001e+06 Max=
1.3e+08 Step=0
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:371 [tid=140737354102528][chan=0] LPFBW: Rx=1.4001e+06 Tx=5
.2e+06
Wed Jun 12 15:54:37 2019 DDEV <0002> LMSDevice.cpp:373 [tid=140737354102528][chan=0] Setting LPFBW

Thread 5 "CtrlService0" received signal SIGSEGV, Segmentation fault.
[Switching to Thread 0x7ffff7ff7700 (LWP 513)]
0x00007ffff5e1dd4e in _IO_vfprintf_internal (s=s@entry=0x7ffff7ff00f0, format=format@entry=0x7ffff5f40580 <for
mat> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n", ap=ap@entry=0x7ffff7ff0258) at vfprintf.c:1267
1267    vfprintf.c: No such file or directory.
(gdb) thread apply all bt

Thread 5 (Thread 0x7ffff7ff7700 (LWP 513)):
#0  0x00007ffff5e1dd4e in _IO_vfprintf_internal (s=s@entry=0x7ffff7ff00f0, format=format@entry=0x7ffff5f40580
<format> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n", ap=ap@entry=0x7ffff7ff0258) at vfprintf.c:1267
#1  0x00007ffff5e46e89 in _IO_vsnprintf (string=0x7ffff61729c0 <result> "", maxlen=<optimized out>, format=0x7
ffff5f40580 <format> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n", args=args@entry=0x7ffff7ff0258) at vsnprintf.c:114
#2  0x00007ffff5e262c2 in __snprintf (s=s@entry=0x7ffff61729c0 <result> "", maxlen=maxlen@entry=114, format=fo
rmat@entry=0x7ffff5f40580 <format> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n") at snprintf.c:33
#3  0x00007ffff5e7ee81 in asctime_internal (tp=<optimized out>, buf=buf@entry=0x7ffff61729c0 <result> "", bufl
en=buflen@entry=114) at asctime.c:56
#4  0x00007ffff5e7ef11 in __GI_asctime (tp=<optimized out>) at asctime.c:87
#5  0x00007ffff5e7ef85 in ctime (t=t@entry=0x7ffff7ff03d0) at ctime.c:27
#6  0x00007ffff6cee528 in _output (target=target@entry=0x5555557d85d0, subsys=subsys@entry=3, level=level@entr
y=5, file=file@entry=0x555555594919 "LMSDevice.cpp", line=line@entry=92, cont=cont@entry=0, format=0x555555597
8e0 "%s\n",
    ap=0x7ffff7ff14a0) at logging.c:365
#7  0x00007ffff6cee84d in osmo_vlogp (subsys=<optimized out>, level=5, file=0x555555594919 "LMSDevice.cpp", li
ne=92, cont=0, format=0x5555555978e0 "%s\n", ap=0x7ffff7ff1510) at logging.c:544
#8  0x00007ffff6cee9b7 in logp2 (subsys=<optimized out>, level=<optimized out>, file=<optimized out>, line=<op
timized out>, cont=cont@entry=0, format=format@entry=0x5555555978e0 "%s\n") at logging.c:577
#9  0x0000555555558f0f7 in Log::~Log (this=0x7ffff7ff17d0, __in_chrg=<optimized out>) at Logger.cpp:55
#10 0x0000555555555febe in lms_log_callback (lvl=<optimized out>, msg=0x7ffff7ff19b0 "Rx LPF min bandwidth is 4
MHz when TIA gain is set to -12 dB") at LMSDevice.cpp:92
#11 0x00007ffff6a3d59a in lime::log (level=level@entry=lime::LOG_LEVEL_WARNING, format=format@entry=0x7fffe800
09c0 "Rx LPF min bandwidth is 4MHz when TIA gain is set to -12 dB", argList=argList@entry=0x7ffff7ff29e0) at .
/src/Logger.cpp:76
#12 0x00007ffff6a4c711 in lime::warning (format=format@entry=0x7fffe80009c0 "Rx LPF min bandwidth is 4MHz when
 TIA gain is set to -12 dB") at ./src/Logger.h:98
#13 0x00007ffff6a4c9ca in lime::LMS7002M::Log (this=0x5555558667e0, text=0x7fffe80009c0 "Rx LPF min bandwidth
is 4MHz when TIA gain is set to -12 dB", type=<optimized out>) at ./src/lms7002m/LMS7002M.cpp:59
#14 0x00007ffff6a4cbf4 in lime::LMS7002M::Log (this=0x5555558667e0, type=lime::LMS7002M::LOG_WARNING, format=<
optimized out>, argList=argList@entry=0x7ffff7ff2b50) at ./src/lms7002m/LMS7002M.cpp:92
#15 0x00007ffff6a60e6f in lime::LMS7002M::Log (this=this@entry=0x5555558667e0, type=type@entry=lime::LMS7002M:
:LOG_WARNING, format=format@entry=0x7ffff6ab5bd8 "Rx LPF min bandwidth is 4MHz when TIA gain is set to -12 dB"
)
    at ./src/lms7002m/LMS7002M.h:488
#16 0x00007ffff6a6078d in lime::LMS7002M::TuneRxFilter (this=this@entry=0x5555558667e0, rx_lpf_freq_RF=4000000
) at ./src/lms7002m/LMS7002M_filtersCalibration.cpp:87
#17 0x00007ffff6a7eb55 in lime::LMS7_Device::SetLPF (this=<optimized out>, tx=<optimized out>, chan=chan@entry
=0, en=en@entry=true, bandwidth=<optimized out>, bandwidth@entry=6.9533491739302031e-310) at ./src/API/lms7_de
vice.cpp:756
#18 0x00007ffff6a78c3a in LMS_SetLPFBW (device=<optimized out>, dir_tx=dir_tx@entry=false, chan=chan@entry=0,
```

```
bandwidth=6.9533491739302031e-310, bandwidth@entry=1400100) at ./src/API/lms7_api.cpp:395
#19 0x0000555555563e95 in LMSDevice::do_filters (this=this@entry=0x55555585faf0, chan=chan@entry=0) at LMSDevi
ce.cpp:374
#20 0x00005555555641dd in LMSDevice::start (this=0x55555585faf0) at LMSDevice.cpp:278
#21 0x000055555556e61b in RadioInterface::start (this=0x555555866d10) at radioInterface.cpp:183
#22 0x000055555557441b in Transceiver::start (this=this@entry=0x555555866fa0) at Transceiver.cpp:251
#23 0x00005555555792ad in Transceiver::driveControl (this=this@entry=0x555555866fa0, chan=chan@entry=0) at Tra
nsceiver.cpp:723
#24 0x0000555555579f83 in ControlServiceLoopAdapter (chan=<optimized out>) at Transceiver.cpp:1098
#25 0x00007ffff7bc34a4 in start_thread (arg=0x7ffff7ff7700) at pthread_create.c:456
#26 0x00007ffff5ebfd0f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:97

Thread 4 (Thread 0x7ffff3258700 (LWP 512)):
#0  0x00007ffff5eb68bd in poll () at ../sysdeps/unix/syscall-template.S:84
#1  0x00007ffff562a69d in ?? () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#2  0x00007ffff562b5f0 in libusb_handle_events_timeout_completed () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#3  0x00007ffff6aa2e5e in lime::ConnectionFT601Entry::handle_libusb_events (this=0x7ffff6cd92e0 <__loadConnect
ionFT601Entry()::FTDIEntry>) at ./src/ConnectionFTDI/ConnectionFT601Entry.cpp:19
#4  0x00007ffff674ae6f in ?? () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#5  0x00007ffff7bc34a4 in start_thread (arg=0x7ffff3258700) at pthread_create.c:456
#6  0x00007ffff5ebfd0f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:97

Thread 3 (Thread 0x7ffff3a59700 (LWP 511)):
#0  0x00007ffff5eb68bd in poll () at ../sysdeps/unix/syscall-template.S:84
#1  0x00007ffff562a69d in ?? () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#2  0x00007ffff562b5f0 in libusb_handle_events_timeout_completed () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#3  0x00007ffff6a9898e in lime::ConnectionFX3Entry::handle_libusb_events (this=0x7ffff6cd9200 <__loadConnectio
nFX3Entry()::FX3Entry>) at ./src/ConnectionFX3/ConnectionFX3Entry.cpp:20
#4  0x00007ffff674ae6f in ?? () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#5  0x00007ffff7bc34a4 in start_thread (arg=0x7ffff3a59700) at pthread_create.c:456
#6  0x00007ffff5ebfd0f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:97

Thread 2 (Thread 0x7ffff425a700 (LWP 510)):
#0  0x00007ffff5eb68bd in poll () at ../sysdeps/unix/syscall-template.S:84
#1  0x00007ffff5630bd1 in ?? () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#2  0x00007ffff7bc34a4 in start_thread (arg=0x7ffff425a700) at pthread_create.c:456
#3  0x00007ffff5ebfd0f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:97

Thread 1 (Thread 0x7ffff7fbab40 (LWP 506)):
#0  0x00007ffff5eb8603 in select () at ../sysdeps/unix/syscall-template.S:84
#1  0x00007ffff6ce562a in osmo_select_main (polling=0) at select.c:255
#2  0x0000555555555c7bf in main (argc=<optimized out>, argv=<optimized out>) at osmo-trx.cpp:637
(gdb) q
```

#6 - 06/12/2019 02:24 PM - pespin

- Status changed from New to Feedback

Please try again with this libosmocore patch applied:
https://gerrit.osmocom.org/c/libosmocore/+/14429 logging: Use reentrant ctime_r instead of ctime

#7 - 06/12/2019 03:59 PM - roh

i patched and rebuilt this multiple times to be sure the patch is applied... sadly no cake yet.

```
root@test123:~/src/packages# gdb --args /usr/bin/osmo-trx-lms -C /etc/osmocom/osmo-trx-lms.cfg
GNU gdb (Debian 7.12-6) 7.12.0.20161007-git
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 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.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from /usr/bin/osmo-trx-lms...Reading symbols from /usr/lib/debug/.build-id/25/272b0086b574fedd
e7438e7d05cff7603c5b43.debug...done.
done.
```

```
(gdb) r
Starting program: /usr/bin/osmo-trx-lms -C /etc/osmocom/osmo-trx-lms.cfg
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Info: SSE3 support compiled in and supported by CPU
Info: SSE4.1 support compiled in and supported by CPU
Wed Jun 12 17:55:33 2019 DLGLOBAL <0004> telnet_interface.c:104 Available via telnet 127.0.0.1 4237
Wed Jun 12 17:55:33 2019 DLCTRL <000b> control_if.c:911 CTRL at 127.0.0.1 4236
Wed Jun 12 17:55:33 2019 DMAIN <0000> osmo-trx.cpp:478 [tid=140737353849664] Config Settings
   Log Level............... 0
   Device args.............
   TRX Base Port........... 5700
   TRX Address............. 127.0.0.1
   GSM BTS Address......... 127.0.0.1
   Channels................ 1
   Tx Samples-per-Symbol... 4
   Rx Samples-per-Symbol... 4
   EDGE support............ 0
   Extended RACH support... 0
   Reference............... 0
   C0 Filler Table......... 1
   Multi-Carrier........... 0
   Tuning offset........... 0
   RSSI to dBm offset...... 0
   Swap channels........... 0
   Tx Antennas............. 'BAND1'
   Rx Antennas............. 'LNAW'

Wed Jun 12 17:55:33 2019 DMAIN <0000> osmo-trx.cpp:434 [tid=140737353849664] Setting SCHED_RR priority 18
Wed Jun 12 17:55:33 2019 DDEV <0002> LMSDevice.cpp:52 [tid=140737353849664] creating LMS device...
Wed Jun 12 17:55:33 2019 DDEV <0002> LMSDevice.cpp:139 [tid=140737353849664] Opening LMS device..
[New Thread 0x7ffff425a700 (LWP 22476)]
[New Thread 0x7ffff3a59700 (LWP 22477)]
[New Thread 0x7ffff3258700 (LWP 22478)]
Wed Jun 12 17:55:33 2019 DDEV <0002> LMSDevice.cpp:145 [tid=140737353849664] Devices found: 1
Wed Jun 12 17:55:33 2019 DDEV <0002> LMSDevice.cpp:155 [tid=140737353849664] Device [0]: LimeSDR-USB, media=US
B 2.0, module=FX3, addr=1d50:6108, serial=0009060B00472227
Wed Jun 12 17:55:33 2019 DDEV <0002> LMSDevice.cpp:164 [tid=140737353849664] Using device[0]
Wed Jun 12 17:55:33 2019 DLMS <0003> LMSDevice.cpp:92 [tid=140737353849664] Reference clock 30.72 MHz
Wed Jun 12 17:55:33 2019 DDEV <0002> LMSDevice.cpp:190 [tid=140737353849664] Init LMS device
Wed Jun 12 17:55:34 2019 DDEV <0002> LMSDevice.cpp:203 [tid=140737353849664] Setting Internal clock reference
Wed Jun 12 17:55:34 2019 DLMS <0003> LMSDevice.cpp:92 [tid=140737353849664] Disabling external reference clock
Wed Jun 12 17:55:34 2019 DDEV <0002> LMSDevice.cpp:97 [tid=140737353849664] Sample Rate: Min=100000 Max=6.144e
+07 Step=0
Wed Jun 12 17:55:34 2019 DDEV <0002> LMSDevice.cpp:226 [tid=140737353849664] Setting sample rate to 1.08333e+0
6 4
Wed Jun 12 17:55:34 2019 DDEV <0002> LMSDevice.cpp:232 [tid=140737353849664] Sample Rate: Host=1.08333e+06 RF=
3.46667e+07
Wed Jun 12 17:55:34 2019 DMAIN <0000> LMSDevice.cpp:209 [tid=140737353849664] Antennas configured successfully
[New Thread 0x7ffff7ff7700 (LWP 22479)]
Wed Jun 12 17:55:34 2019 DMAIN <0000> Threads.cpp:116 [tid=140737354102528] Thread 140737354102528 (task 22479
) set name: CtrlService0
Wed Jun 12 17:55:34 2019 DMAIN <0000> osmo-trx.cpp:526 [tid=140737353849664] -- Transceiver active with 1 chan
nel(s)
Wed Jun 12 17:55:34 2019 DTRXCTRL <0001> Transceiver.cpp:717 [tid=140737354102528][chan=0] command is 'POWERON
'
Wed Jun 12 17:55:34 2019 DMAIN <0000> Transceiver.cpp:244 [tid=140737354102528] Starting the transceiver
Wed Jun 12 17:55:34 2019 DMAIN <0000> radioInterface.cpp:177 [tid=140737354102528] Starting radio device
Wed Jun 12 17:55:34 2019 DDEV <0002> LMSDevice.cpp:260 [tid=140737354102528] starting LMS...
Wed Jun 12 17:55:34 2019 DDEV <0002> LMSDevice.cpp:409 [tid=140737354102528][chan=0] Setting TX gain to 73 dB
Wed Jun 12 17:55:34 2019 DDEV <0002> LMSDevice.cpp:424 [tid=140737354102528][chan=0] Setting RX gain to 36.5 d
B
Wed Jun 12 17:55:34 2019 DDEV <0002> LMSDevice.cpp:360 [tid=140737354102528][chan=0] Setting filters
Wed Jun 12 17:55:34 2019 DDEV <0002> LMSDevice.cpp:97 [tid=140737354102528] LPFBWRange Rx: Min=1.4001e+06 Max=
1.3e+08 Step=0
Wed Jun 12 17:55:34 2019 DDEV <0002> LMSDevice.cpp:97 [tid=140737354102528] LPFBWRange Tx: Min=1.4001e+06 Max=
1.3e+08 Step=0
Wed Jun 12 17:55:34 2019 DDEV <0002> LMSDevice.cpp:371 [tid=140737354102528][chan=0] LPFBW: Rx=1.4001e+06 Tx=5
.2e+06
Wed Jun 12 17:55:34 2019 DDEV <0002> LMSDevice.cpp:373 [tid=140737354102528][chan=0] Setting LPFBW

Thread 5 "CtrlService0" received signal SIGSEGV, Segmentation fault.
[Switching to Thread 0x7ffff7ff7700 (LWP 22479)]
0x00007ffff5e1dd4e in _IO_vfprintf_internal (s=s@entry=0x7ffff7ff0090, format=format@entry=0x7ffff5f40580 <for
mat> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n", ap=ap@entry=0x7ffff7ff01f8) at vfprintf.c:1267
```

```
1267    vfprintf.c: No such file or directory.
(gdb) thread apply all bt

Thread 5 (Thread 0x7ffff7ff7700 (LWP 22479)):
#0  0x00007ffff5e1dd4e in _IO_vfprintf_internal (s=s@entry=0x7ffff7ff0090, format=format@entry=0x7ffff5f40580
<format> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n", ap=ap@entry=0x7ffff7ff01f8) at vfprintf.c:1267
#1  0x00007ffff5e46e89 in _IO_vsnprintf (string=0x7ffff7ff03f0 "", maxlen=<optimized out>, format=0x7ffff5f405
80 <format> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n", args=args@entry=0x7ffff7ff01f8) at vsnprintf.c:114
#2  0x00007ffff5e262c2 in __snprintf (s=s@entry=0x7ffff7ff03f0 "", maxlen=maxlen@entry=26, format=format@entry
=0x7ffff5f40580 <format> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n") at snprintf.c:33
#3  0x00007ffff5e7ee81 in asctime_internal (tp=<optimized out>, buf=buf@entry=0x7ffff7ff03f0 "", buflen=buflen
@entry=26) at asctime.c:56
#4  0x00007ffff5e7eefa in __asctime_r (tp=<optimized out>, buf=buf@entry=0x7ffff7ff03f0 "") at asctime.c:77
#5  0x00007ffff5e7efab in ctime_r (t=t@entry=0x7ffff7ff03b0, buf=buf@entry=0x7ffff7ff03f0 "") at ctime_r.c:28
#6  0x00007ffff6cee4c9 in _output (target=target@entry=0x5555557d85d0, subsys=subsys@entry=3, level=level@entr
y=5, file=file@entry=0x555555594919 "LMSDevice.cpp", line=line@entry=92, cont=cont@entry=0, format=0x555555597
8e0 "%s\n",
    ap=0x7ffff7ff14a0) at logging.c:366
#7  0x00007ffff6cee82d in osmo_vlogp (subsys=<optimized out>, level=5, file=0x555555594919 "LMSDevice.cpp", li
ne=92, cont=0, format=0x5555555978e0 "%s\n", ap=0x7ffff7ff1510) at logging.c:547
#8  0x00007ffff6cee997 in logp2 (subsys=<optimized out>, level=<optimized out>, file=<optimized out>, line=<op
timized out>, cont=cont@entry=0, format=format@entry=0x5555555978e0 "%s\n") at logging.c:580
#9  0x0000555555558f0f7 in Log::~Log (this=0x7ffff7ff17d0, __in_chrg=<optimized out>) at Logger.cpp:55
#10 0x0000555555555febe in lms_log_callback (lvl=<optimized out>, msg=0x7ffff7ff19b0 "Rx LPF min bandwidth is 4
MHz when TIA gain is set to -12 dB") at LMSDevice.cpp:92
#11 0x00007ffff6a3d59a in lime::log (level=level@entry=lime::LOG_LEVEL_WARNING, format=format@entry=0x7fffe800
0ac0 "Rx LPF min bandwidth is 4MHz when TIA gain is set to -12 dB", argList=argList@entry=0x7ffff7ff29e0) at .
/src/Logger.cpp:76
#12 0x00007ffff6a4c711 in lime::warning (format=format@entry=0x7fffe8000ac0 "Rx LPF min bandwidth is 4MHz when
 TIA gain is set to -12 dB") at ./src/Logger.h:98
#13 0x00007ffff6a4c9ca in lime::LMS7002M::Log (this=0x5555558667f0, text=0x7fffe8000ac0 "Rx LPF min bandwidth
is 4MHz when TIA gain is set to -12 dB", type=<optimized out>) at ./src/lms7002m/LMS7002M.cpp:59
#14 0x00007ffff6a4cbf4 in lime::LMS7002M::Log (this=0x5555558667f0, type=lime::LMS7002M::LOG_WARNING, format=<
optimized out>, argList=argList@entry=0x7ffff7ff2b50) at ./src/lms7002m/LMS7002M.cpp:92
#15 0x00007ffff6a60e6f in lime::LMS7002M::Log (this=this@entry=0x5555558667f0, type=type@entry=lime::LMS7002M:
:LOG_WARNING, format=format@entry=0x7ffff6ab5bd8 "Rx LPF min bandwidth is 4MHz when TIA gain is set to -12 dB"
)
    at ./src/lms7002m/LMS7002M.h:488
#16 0x00007ffff6a6078d in lime::LMS7002M::TuneRxFilter (this=this@entry=0x5555558667f0, rx_lpf_freq_RF=4000000
) at ./src/lms7002m/LMS7002M_filtersCalibration.cpp:87
#17 0x00007ffff6a7eb55 in lime::LMS7_Device::SetLPF (this=<optimized out>, tx=<optimized out>, chan=chan@entry
=0, en=en@entry=true, bandwidth=<optimized out>, bandwidth@entry=6.9533491739302031e-310) at ./src/API/lms7_de
vice.cpp:756
#18 0x00007ffff6a78c3a in LMS_SetLPFBW (device=<optimized out>, dir_tx=dir_tx@entry=false, chan=chan@entry=0,
bandwidth=6.9533491739302031e-310, bandwidth@entry=1400100) at ./src/API/lms7_api.cpp:395
#19 0x0000555555563e95 in LMSDevice::do_filters (this=this@entry=0x55555585fb00, chan=chan@entry=0) at LMSDevi
ce.cpp:374
#20 0x00005555555641dd in LMSDevice::start (this=0x55555585fb00) at LMSDevice.cpp:278
#21 0x0000555555556e61b in RadioInterface::start (this=0x555555866d20) at radioInterface.cpp:183
#22 0x000055555557441b in Transceiver::start (this=this@entry=0x555555866fb0) at Transceiver.cpp:251
#23 0x00005555555792ad in Transceiver::driveControl (this=this@entry=0x555555866fb0, chan=chan@entry=0) at Tra
nsceiver.cpp:723
#24 0x0000555555579f83 in ControlServiceLoopAdapter (chan=<optimized out>) at Transceiver.cpp:1098
#25 0x00007ffff7bc34a4 in start_thread (arg=0x7ffff7ff7700) at pthread_create.c:456
#26 0x00007ffff5ebfd0f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:97

Thread 4 (Thread 0x7ffff3258700 (LWP 22478)):
#0  0x00007ffff5eb68bd in poll () at ../sysdeps/unix/syscall-template.S:84
#1  0x00007ffff562a69d in ?? () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#2  0x00007ffff562b5f0 in libusb_handle_events_timeout_completed () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#3  0x00007ffff6aa2e5e in lime::ConnectionFT601Entry::handle_libusb_events (this=0x7ffff6cd92e0 <__loadConnect
ionFT601Entry()::FTDIEntry>) at ./src/ConnectionFTDI/ConnectionFT601Entry.cpp:19
#4  0x00007ffff674ae6f in ?? () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#5  0x00007ffff7bc34a4 in start_thread (arg=0x7ffff3258700) at pthread_create.c:456
#6  0x00007ffff5ebfd0f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:97

Thread 3 (Thread 0x7ffff3a59700 (LWP 22477)):
#0  0x00007ffff5eb68bd in poll () at ../sysdeps/unix/syscall-template.S:84
#1  0x00007ffff562a69d in ?? () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#2  0x00007ffff562b5f0 in libusb_handle_events_timeout_completed () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#3  0x00007ffff6a9898e in lime::ConnectionFX3Entry::handle_libusb_events (this=0x7ffff6cd9200 <__loadConnectio
nFX3Entry()::FX3Entry>) at ./src/ConnectionFX3/ConnectionFX3Entry.cpp:20
#4  0x00007ffff674ae6f in ?? () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#5  0x00007ffff7bc34a4 in start_thread (arg=0x7ffff3a59700) at pthread_create.c:456
#6  0x00007ffff5ebfd0f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:97
```

```
Thread 2 (Thread 0x7ffff425a700 (LWP 22476)):
#0  0x00007ffff5eb68bd in poll () at ../sysdeps/unix/syscall-template.S:84
#1  0x00007ffff5630bd1 in ?? () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#2  0x00007ffff7bc34a4 in start_thread (arg=0x7ffff425a700) at pthread_create.c:456
#3  0x00007ffff5ebfd0f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:97

Thread 1 (Thread 0x7ffff7fb9b40 (LWP 22471)):
#0  0x00007ffff5eb8603 in select () at ../sysdeps/unix/syscall-template.S:84
#1  0x00007ffff6ce562a in osmo_select_main (polling=0) at select.c:255
#2  0x000055555555c7bf in main (argc=<optimized out>, argv=<optimized out>) at osmo-trx.cpp:637
(gdb)
```

... also having some weird timestamps on the package-binary results is confusing. i guess this is for reproducible reasons?

```
root@test123:~/src/packages# ls -al /usr/lib/x86_64-linux-gnu/libosmocore.*
-rw-r--r-- 1 root root 306900 May  7 18:36 /usr/lib/x86_64-linux-gnu/libosmocore.a
-rw-r--r-- 1 root root    974 May  7 18:36 /usr/lib/x86_64-linux-gnu/libosmocore.la
lrwxrwxrwx 1 root root     21 May  7 18:36 /usr/lib/x86_64-linux-gnu/libosmocore.so -> libosmocore.so.12.1.0
lrwxrwxrwx 1 root root     21 May  7 18:36 /usr/lib/x86_64-linux-gnu/libosmocore.so.12 -> libosmocore.so.12.1.
0
-rw-r--r-- 1 root root 174264 May  7 18:36 /usr/lib/x86_64-linux-gnu/libosmocore.so.12.1.0
```

#8 - 06/12/2019 05:46 PM - roh

2nd patch (from https://gerrit.osmocom.org/c/libosmocore/+/14432) i have tried:
sadly still no cigar.

```
root@test123:~/src/packages# gdb --args /usr/bin/osmo-trx-lms -C /etc/osmocom/osmo-trx-lms.cfg
GNU gdb (Debian 7.12-6) 7.12.0.20161007-git
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 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.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from /usr/bin/osmo-trx-lms...Reading symbols from /usr/lib/debug/.build-id/25/272b0086b574fedd
e7438e7d05cff7603c5b43.debug...done.
done.
(gdb) r
Starting program: /usr/bin/osmo-trx-lms -C /etc/osmocom/osmo-trx-lms.cfg
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Info: SSE3 support compiled in and supported by CPU
Info: SSE4.1 support compiled in and supported by CPU
Wed Jun 12 19:34:05 2019 DLGLOBAL <0004> telnet_interface.c:104 Available via telnet 127.0.0.1 4237
Wed Jun 12 19:34:05 2019 DLCTRL <000b> control_if.c:911 CTRL at 127.0.0.1 4236
Wed Jun 12 19:34:05 2019 DMAIN <0000> osmo-trx.cpp:478 [tid=140737353849664] Config Settings
   Log Level............... 0
   Device args.............
   TRX Base Port........... 5700
   TRX Address............. 127.0.0.1
   GSM BTS Address......... 127.0.0.1
   Channels................ 1
   Tx Samples-per-Symbol... 4
   Rx Samples-per-Symbol... 4
   EDGE support............ 0
   Extended RACH support... 0
   Reference............... 0
   C0 Filler Table......... 1
   Multi-Carrier........... 0
   Tuning offset........... 0
   RSSI to dBm offset...... 0
   Swap channels........... 0
   Tx Antennas............. 'BAND1'
   Rx Antennas............. 'LNAW'
```

```
Wed Jun 12 19:34:05 2019 DMAIN <0000> osmo-trx.cpp:434 [tid=140737353849664] Setting SCHED_RR priority 18
Wed Jun 12 19:34:05 2019 DDEV <0002> LMSDevice.cpp:52 [tid=140737353849664] creating LMS device...
Wed Jun 12 19:34:05 2019 DDEV <0002> LMSDevice.cpp:139 [tid=140737353849664] Opening LMS device..
[New Thread 0x7ffff425a700 (LWP 22642)]
[New Thread 0x7ffff3a59700 (LWP 22643)]
[New Thread 0x7ffff3258700 (LWP 22644)]
Wed Jun 12 19:34:05 2019 DDEV <0002> LMSDevice.cpp:145 [tid=140737353849664] Devices found: 1
Wed Jun 12 19:34:05 2019 DDEV <0002> LMSDevice.cpp:155 [tid=140737353849664] Device [0]: LimeSDR-USB, media=US
B 2.0, module=FX3, addr=1d50:6108, serial=0009060B00472227
Wed Jun 12 19:34:05 2019 DDEV <0002> LMSDevice.cpp:164 [tid=140737353849664] Using device[0]
Wed Jun 12 19:34:05 2019 DLMS <0003> LMSDevice.cpp:92 [tid=140737353849664] Reference clock 30.72 MHz
Wed Jun 12 19:34:05 2019 DDEV <0002> LMSDevice.cpp:190 [tid=140737353849664] Init LMS device
Wed Jun 12 19:34:05 2019 DDEV <0002> LMSDevice.cpp:203 [tid=140737353849664] Setting Internal clock reference
Wed Jun 12 19:34:05 2019 DLMS <0003> LMSDevice.cpp:92 [tid=140737353849664] Disabling external reference clock
Wed Jun 12 19:34:06 2019 DDEV <0002> LMSDevice.cpp:97 [tid=140737353849664] Sample Rate: Min=100000 Max=6.144e
+07 Step=0
Wed Jun 12 19:34:06 2019 DDEV <0002> LMSDevice.cpp:226 [tid=140737353849664] Setting sample rate to 1.08333e+0
6 4
Wed Jun 12 19:34:06 2019 DDEV <0002> LMSDevice.cpp:232 [tid=140737353849664] Sample Rate: Host=1.08333e+06 RF=
3.46667e+07
Wed Jun 12 19:34:06 2019 DMAIN <0000> LMSDevice.cpp:209 [tid=140737353849664] Antennas configured successfully
[New Thread 0x7ffff7ff7700 (LWP 22645)]
Wed Jun 12 19:34:06 2019 DMAIN <0000> Threads.cpp:116 [tid=140737354102528] Thread 140737354102528 (task 22645
) set name: CtrlService0
Wed Jun 12 19:34:06 2019 DMAIN <0000> osmo-trx.cpp:526 [tid=140737353849664] -- Transceiver active with 1 chan
nel(s)
Wed Jun 12 19:34:06 2019 DTRXCTRL <0001> Transceiver.cpp:717 [tid=140737354102528][chan=0] command is 'POWERON
'
Wed Jun 12 19:34:06 2019 DMAIN <0000> Transceiver.cpp:244 [tid=140737354102528] Starting the transceiver
Wed Jun 12 19:34:06 2019 DMAIN <0000> radioInterface.cpp:177 [tid=140737354102528] Starting radio device
Wed Jun 12 19:34:06 2019 DDEV <0002> LMSDevice.cpp:260 [tid=140737354102528] starting LMS...
Wed Jun 12 19:34:06 2019 DDEV <0002> LMSDevice.cpp:409 [tid=140737354102528][chan=0] Setting TX gain to 73 dB
Wed Jun 12 19:34:06 2019 DDEV <0002> LMSDevice.cpp:424 [tid=140737354102528][chan=0] Setting RX gain to 36.5 d
B
Wed Jun 12 19:34:07 2019 DDEV <0002> LMSDevice.cpp:360 [tid=140737354102528][chan=0] Setting filters
Wed Jun 12 19:34:07 2019 DDEV <0002> LMSDevice.cpp:97 [tid=140737354102528] LPFBWRange Rx: Min=1.4001e+06 Max=
1.3e+08 Step=0
Wed Jun 12 19:34:07 2019 DDEV <0002> LMSDevice.cpp:97 [tid=140737354102528] LPFBWRange Tx: Min=1.4001e+06 Max=
1.3e+08 Step=0
Wed Jun 12 19:34:07 2019 DDEV <0002> LMSDevice.cpp:371 [tid=140737354102528][chan=0] LPFBW: Rx=1.4001e+06 Tx=5
.2e+06
Wed Jun 12 19:34:07 2019 DDEV <0002> LMSDevice.cpp:373 [tid=140737354102528][chan=0] Setting LPFBW

Thread 5 "CtrlService0" received signal SIGSEGV, Segmentation fault.
[Switching to Thread 0x7ffff7ff7700 (LWP 22645)]
0x00007ffff5e1dd4e in _IO_vfprintf_internal (s=s@entry=0x7ffff7ff0090, format=format@entry=0x7ffff5f40580 <for
mat> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n", ap=ap@entry=0x7ffff7ff01f8) at vfprintf.c:1267
1267    vfprintf.c: No such file or directory.
(gdb) frame 6
#6  0x00007ffff6cee4ab in _output (target=target@entry=0x5555557d85d0, subsys=subsys@entry=3, level=level@entr
y=5, file=file@entry=0x555555594919 "LMSDevice.cpp", line=line@entry=92, cont=cont@entry=0, format=0x555555597
8e0 "%s\n",
    ap=0x7ffff7ff14a0) at logging.c:367
367    logging.c: No such file or directory.
(gdb) thread apply all bt

Thread 5 (Thread 0x7ffff7ff7700 (LWP 22645)):
#0  0x00007ffff5e1dd4e in _IO_vfprintf_internal (s=s@entry=0x7ffff7ff0090, format=format@entry=0x7ffff5f40580
<format> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n", ap=ap@entry=0x7ffff7ff01f8) at vfprintf.c:1267
#1  0x00007ffff5e46e89 in _IO_vsnprintf (string=0x7ffff7ff03f0 "", maxlen=<optimized out>, format=0x7ffff5f405
80 <format> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n", args=args@entry=0x7ffff7ff01f8) at vsnprintf.c:114
#2  0x00007ffff5e262c2 in __snprintf (s=s@entry=0x7ffff7ff03f0 "", maxlen=maxlen@entry=26, format=format@entry
=0x7ffff5f40580 <format> "%.3s %.3s%3d %.2d:%.2d:%.2d %d\n") at snprintf.c:33
#3  0x00007ffff5e7ee81 in asctime_internal (tp=<optimized out>, buf=buf@entry=0x7ffff7ff03f0 "", buflen=buflen
@entry=26) at asctime.c:56
#4  0x00007ffff5e7eefa in __asctime_r (tp=<optimized out>, buf=buf@entry=0x7ffff7ff03f0 "") at asctime.c:77
#5  0x00007ffff5e7efab in ctime_r (t=t@entry=0x7ffff7ff03b0, buf=buf@entry=0x7ffff7ff03f0 "") at ctime_r.c:28
#6  0x00007ffff6cee4ab in _output (target=target@entry=0x5555557d85d0, subsys=subsys@entry=3, level=level@entr
y=5, file=file@entry=0x555555594919 "LMSDevice.cpp", line=line@entry=92, cont=cont@entry=0, format=0x555555597
8e0 "%s\n",
    ap=0x7ffff7ff14a0) at logging.c:367
#7  0x00007ffff6cee83d in osmo_vlogp (subsys=<optimized out>, level=5, file=0x555555594919 "LMSDevice.cpp", li
ne=92, cont=0, format=0x5555555978e0 "%s\n", ap=0x7ffff7ff1510) at logging.c:548
#8  0x00007ffff6cee9a7 in logp2 (subsys=<optimized out>, level=<optimized out>, file=<optimized out>, line=<op
```

```
timized out>, cont=cont@entry=0, format=format@entry=0x5555555978e0 "%s\n") at logging.c:581
#9  0x000055555558f0f7 in Log::~Log (this=0x7ffff7ff17d0, __in_chrg=<optimized out>) at Logger.cpp:55
#10 0x000055555555febe in lms_log_callback (lvl=<optimized out>, msg=0x7ffff7ff19b0 "Rx LPF min bandwidth is 4
MHz when TIA gain is set to -12 dB") at LMSDevice.cpp:92
#11 0x00007ffff6a3d59a in lime::log (level=level@entry=lime::LOG_LEVEL_WARNING, format=format@entry=0x7fffe800
0ac0 "Rx LPF min bandwidth is 4MHz when TIA gain is set to -12 dB", argList=argList@entry=0x7ffff7ff29e0) at .
/src/Logger.cpp:76
#12 0x00007ffff6a4c711 in lime::warning (format=format@entry=0x7fffe8000ac0 "Rx LPF min bandwidth is 4MHz when
 TIA gain is set to -12 dB") at ./src/Logger.h:98
#13 0x00007ffff6a4c9ca in lime::LMS7002M::Log (this=0x5555558667f0, text=0x7fffe8000ac0 "Rx LPF min bandwidth
is 4MHz when TIA gain is set to -12 dB", type=<optimized out>) at ./src/lms7002m/LMS7002M.cpp:59
#14 0x00007ffff6a4cbf4 in lime::LMS7002M::Log (this=0x5555558667f0, type=lime::LMS7002M::LOG_WARNING, format=<
optimized out>, argList=argList@entry=0x7ffff7ff2b50) at ./src/lms7002m/LMS7002M.cpp:92
#15 0x00007ffff6a60e6f in lime::LMS7002M::Log (this=this@entry=0x5555558667f0, type=type@entry=lime::LMS7002M:
:LOG_WARNING, format=format@entry=0x7ffff6ab5bd8 "Rx LPF min bandwidth is 4MHz when TIA gain is set to -12 dB"
)
    at ./src/lms7002m/LMS7002M.h:488
#16 0x00007ffff6a6078d in lime::LMS7002M::TuneRxFilter (this=this@entry=0x5555558667f0, rx_lpf_freq_RF=4000000
) at ./src/lms7002m/LMS7002M_filtersCalibration.cpp:87
#17 0x00007ffff6a7eb55 in lime::LMS7_Device::SetLPF (this=<optimized out>, tx=<optimized out>, chan=chan@entry
=0, en=en@entry=true, bandwidth=<optimized out>, bandwidth@entry=6.9533491739302031e-310) at ./src/API/lms7_de
vice.cpp:756
#18 0x00007ffff6a78c3a in LMS_SetLPFBW (device=<optimized out>, dir_tx=dir_tx@entry=false, chan=chan@entry=0,
bandwidth=6.9533491739302031e-310, bandwidth@entry=1400100) at ./src/API/lms7_api.cpp:395
#19 0x0000555555563e95 in LMSDevice::do_filters (this=this@entry=0x55555585fb00, chan=chan@entry=0) at LMSDevi
ce.cpp:374
#20 0x00005555555641dd in LMSDevice::start (this=0x55555585fb00) at LMSDevice.cpp:278
#21 0x000055555556e61b in RadioInterface::start (this=0x555555866d20) at radioInterface.cpp:183
#22 0x000055555557441b in Transceiver::start (this=this@entry=0x555555866fb0) at Transceiver.cpp:251
#23 0x00005555555792ad in Transceiver::driveControl (this=this@entry=0x555555866fb0, chan=chan@entry=0) at Tra
nsceiver.cpp:723
#24 0x0000555555579f83 in ControlServiceLoopAdapter (chan=<optimized out>) at Transceiver.cpp:1098
#25 0x00007ffff7bc34a4 in start_thread (arg=0x7ffff7ff7700) at pthread_create.c:456
#26 0x00007ffff5ebfd0f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:97

Thread 4 (Thread 0x7ffff3258700 (LWP 22644)):
#0  0x00007ffff5eb68bd in poll () at ../sysdeps/unix/syscall-template.S:84
#1  0x00007ffff562a69d in ?? () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#2  0x00007ffff562b5f0 in libusb_handle_events_timeout_completed () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#3  0x00007ffff6aa2e5e in lime::ConnectionFT601Entry::handle_libusb_events (this=0x7ffff6cd92e0 <__loadConnect
ionFT601Entry()::FTDIEntry>) at ./src/ConnectionFTDI/ConnectionFT601Entry.cpp:19
#4  0x00007ffff674ae6f in ?? () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#5  0x00007ffff7bc34a4 in start_thread (arg=0x7ffff3258700) at pthread_create.c:456
#6  0x00007ffff5ebfd0f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:97

Thread 3 (Thread 0x7ffff3a59700 (LWP 22643)):
#0  0x00007ffff5eb68bd in poll () at ../sysdeps/unix/syscall-template.S:84
#1  0x00007ffff562a69d in ?? () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#2  0x00007ffff562b5f0 in libusb_handle_events_timeout_completed () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#3  0x00007ffff6a9898e in lime::ConnectionFX3Entry::handle_libusb_events (this=0x7ffff6cd9200 <__loadConnectio
nFX3Entry()::FX3Entry>) at ./src/ConnectionFX3/ConnectionFX3Entry.cpp:20
#4  0x00007ffff674ae6f in ?? () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#5  0x00007ffff7bc34a4 in start_thread (arg=0x7ffff3a59700) at pthread_create.c:456
#6  0x00007ffff5ebfd0f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:97

Thread 2 (Thread 0x7ffff425a700 (LWP 22642)):
#0  0x00007ffff5eb68bd in poll () at ../sysdeps/unix/syscall-template.S:84
#1  0x00007ffff5630bd1 in ?? () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
#2  0x00007ffff7bc34a4 in start_thread (arg=0x7ffff425a700) at pthread_create.c:456
#3  0x00007ffff5ebfd0f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:97

Thread 1 (Thread 0x7ffff7fb9b40 (LWP 22638)):
#0  0x00007ffff5eb8603 in select () at ../sysdeps/unix/syscall-template.S:84
#1  0x00007ffff6ce562a in osmo_select_main (polling=0) at select.c:255
#2  0x000055555555c7bf in main (argc=<optimized out>, argv=<optimized out>) at osmo-trx.cpp:637
(gdb)
```

#9 - 06/14/2019 02:07 PM - Hoernchen

I've just tried to use my lime mini, and ran into this as well, I can reproduce the issue every time, the segfault happens upon stepping into _output in the function prologue, and judging by the parameters printed by gdb the stack appears to be corrupted...

```
Fri Jun 14 17:07:59 2019 DDEV <0002> LMSDevice.cpp:226 [tid=140737353849792] Setting sample rate to 1.08333e+0
```

```
6 4
Fri Jun 14 17:07:59 2019 DDEV <0002> LMSDevice.cpp:232 [tid=140737353849792] Sample Rate: Host=1.08333e+06 RF=
3.46667e+07
Fri Jun 14 17:07:59 2019 DMAIN <0000> LMSDevice.cpp:209 [tid=140737353849792] Antennas configured successfully
sigProcLib.cpp:975:21: runtime error: division by zero
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior sigProcLib.cpp:975:21 in
[New Thread 0x7ffff7e11700 (LWP 31850)]
Fri Jun 14 17:07:59 2019 DMAIN <0000> Threads.cpp:116 [tid=140737352111872] Thread 140737352111872 (task 31850
) set name: CtrlService0
Fri Jun 14 17:07:59 2019 DMAIN <0000> osmo-trx.cpp:526 [tid=140737353849792] -- Transceiver active with 1 chan
nel(s)

Thread 5 "CtrlService0" received signal SIGSEGV, Segmentation fault.
[Switching to Thread 0x7ffff7e11700 (LWP 31850)]
0x00007ffff6836044 in _output (target=0x60d000000172, subsys=24784, level=371, file=0x0, line=24864, cont=160,

    format=0x612000000108 "\003\v", ap=0x3) at logging.c:331
331    {
(gdb) thread apply all bt full

Thread 5 (Thread 0x7ffff7e11700 (LWP 31850)):
#0  0x00007ffff6836044 in _output (target=0x60d000000172, subsys=24784, level=371, file=0x0, line=24864, cont=
160,
    format=0x612000000108 "\003\v", ap=0x3) at logging.c:331
        buf = '\000' <repeats 824 times>...
        ret = 24864
        len = 160
        offset = 24864
        rem = 264
        c_subsys = 0x0
#1  0x00007ffff6834fbd in osmo_vlogp (subsys=1, level=3, file=0x6a7778 "Transceiver.cpp", line=717, cont=0, fo
rmat=0x6b7980 <.str> "%s\n",
    ap=0x7ffff7e0b980) at logging.c:548
        bp = {{gp_offset = 48, fp_offset = 48, overflow_arg_area = 0x7ffff7e0bc10, reg_save_area = 0x7ffff7e0b
ad0}}
        tar = 0x6120000000a0
#2  0x00007ffff683a244 in logp2 (subsys=1, level=3, file=0x6a7778 "Transceiver.cpp", line=717, cont=0, format=
0x6b7980 <.str> "%s\n")
    at logging.c:581
        ap = {{gp_offset = 48, fp_offset = 48, overflow_arg_area = 0x7ffff7e0bc10, reg_save_area = 0x7ffff7e0b
ad0}}
#3  0x000000000065b68a in Log::~Log (this=<optimized out>) at Logger.cpp:55
        mlen = <optimized out>
        fmt = 0x6b7980 <.str> "%s\n"
        old_state = <optimized out>
        neednl = <optimized out>
        lock = {mMutex = @0x12b4ec0}
#4  0x00000000005a9a4b in Transceiver::driveControl (this=0x619000009180, chan=0) at Transceiver.cpp:717
        buffer = "CMD POWERON", '\000' <repeats 89 times>
        response = '\000' <repeats 100 times>
        params = 0x0
        command = 0x7ffff7e0be64 "POWERON"
        msgLen = 12
#5  0x0000000000059bbb0 in ControlServiceLoopAdapter (chan=0x6020000327f0) at Transceiver.cpp:1098
        thread_name = "CtrlService0\000\177\000"
        trx = 0x619000009180
        num = 0
#6  0x00007ffff7bbd6db in start_thread (arg=0x7ffff7e11700) at pthread_create.c:463
        pd = 0x7ffff7e11700
        now = <optimized out>
        unwind_buf = {cancel_jmp_buf = {{jmp_buf = {140737352111872, -7001150341729343638, 140737352096576, 0,
 140737488338464,
                106034152608168, 7001132705674831722, 7001133332878206826}, mask_was_saved = 0}}, priv = {pad
= {0x0, 0x0, 0x0, 0x0},
            data = {prev = 0x0, cleanup = 0x0, canceltype = 0}}}
        not_first_call = <optimized out>
#7  0x00007ffff54ec88f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:95
No locals.

Thread 4 (Thread 0x7fffef6fd700 (LWP 31847)):
#0  0x00007ffff54dfbf9 in __GI___poll (fds=0x60300000a900, nfds=3, timeout=250) at ../sysdeps/unix/sysv/linux/
poll.c:29
        resultvar = 18446744073709551100
        sc_cancel_oldtype = 0
        sc_ret = <optimized out>
```

```
#1  0x0000000000046e7d8 in poll ()
No symbol table info available.
#2  0x00007ffff3dd71cd in ?? () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
No symbol table info available.
#3  0x00007ffff3dd8130 in libusb_handle_events_timeout_completed () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
No symbol table info available.
#4  0x00007ffff659bee6 in lime::ConnectionFT601Entry::handle_libusb_events() () from /usr/local/lib/libLimeSui
te.so.19.04-1
No symbol table info available.
#5  0x00007ffff623b66f in ?? () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
No symbol table info available.
#6  0x00007ffff7bbd6db in start_thread (arg=0x7fffef6fd700) at pthread_create.c:463
        pd = 0x7fffef6fd700
        now = <optimized out>
        unwind_buf = {cancel_jmp_buf = {{jmp_buf = {140737210472192, -7001150341729343638, 140737210456896, 0,
 140737488330912,
                140737488328688, 7001184290379540330, 7001133332878206826}, mask_was_saved = 0}}, priv = {pad
= {0x0, 0x0, 0x0, 0x0},
            data = {prev = 0x0, cleanup = 0x0, canceltype = 0}}}
        not_first_call = <optimized out>
#7  0x00007ffff54ec88f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:95
No locals.

Thread 3 (Thread 0x7fffefefe700 (LWP 31846)):
#0  0x00007ffff54dfbf9 in __GI___poll (fds=0x60200000c010, nfds=2, timeout=250) at ../sysdeps/unix/sysv/linux/
poll.c:29
        resultvar = 18446744073709551100
        sc_cancel_oldtype = 0
        sc_ret = <optimized out>
#1  0x0000000000046e7d8 in poll ()
---Type <return> to continue, or q <return> to quit---
No symbol table info available.
#2  0x00007ffff3dd71cd in ?? () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
No symbol table info available.
#3  0x00007ffff3dd8130 in libusb_handle_events_timeout_completed () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
No symbol table info available.
#4  0x00007ffff658fd26 in lime::ConnectionFX3Entry::handle_libusb_events() () from /usr/local/lib/libLimeSuite
.so.19.04-1
No symbol table info available.
#5  0x00007ffff623b66f in ?? () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
No symbol table info available.
#6  0x00007ffff7bbd6db in start_thread (arg=0x7fffefefe700) at pthread_create.c:463
        pd = 0x7fffefefe700
        now = <optimized out>
        unwind_buf = {cancel_jmp_buf = {{jmp_buf = {140737218864896, -7001150341729343638, 140737218849600, 0,
 140737488330912,
                140737488328688, 7001185390428039018, 7001133332878206826}, mask_was_saved = 0}}, priv = {pad
= {0x0, 0x0, 0x0, 0x0},
            data = {prev = 0x0, cleanup = 0x0, canceltype = 0}}}
        not_first_call = <optimized out>
#7  0x00007ffff54ec88f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:95
No locals.

Thread 2 (Thread 0x7ffff06ff700 (LWP 31845)):
#0  0x00007ffff54dfbf9 in __GI___poll (fds=0x7ffff06fba40, nfds=2, timeout=-1) at ../sysdeps/unix/sysv/linux/p
oll.c:29
        resultvar = 18446744073709551100
        sc_cancel_oldtype = 0
        sc_ret = <optimized out>
#1  0x0000000000046e7d8 in poll ()
No symbol table info available.
#2  0x00007ffff3ddd6ff in ?? () from /lib/x86_64-linux-gnu/libusb-1.0.so.0
No symbol table info available.
#3  0x00007ffff7bbd6db in start_thread (arg=0x7ffff06ff700) at pthread_create.c:463
        pd = 0x7ffff06ff700
        now = <optimized out>
        unwind_buf = {cancel_jmp_buf = {{jmp_buf = {140737227257600, -7001150341729343638, 140737227242304, 0,
 140737488330576,
                140737488328352, 7001138111964915562, 7001133332878206826}, mask_was_saved = 0}}, priv = {pad
= {0x0, 0x0, 0x0, 0x0},
            data = {prev = 0x0, cleanup = 0x0, canceltype = 0}}}
        not_first_call = <optimized out>
#4  0x00007ffff54ec88f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:95
No locals.
```

```
Thread 1 (Thread 0x7ffff7fb9bc0 (LWP 31841)):
#0  0x00007ffff54e203f in __GI___select (nfds=7, readfds=0x7fffffffd5a0, writefds=0x7fffffffd640, exceptfds=0x
7fffffffd6e0,
    timeout=0x7ffff6acb220 <nearest>) at ../sysdeps/unix/sysv/linux/select.c:41
        resultvar = 18446744073709551102
        sc_cancel_oldtype = 0
        sc_ret = <optimized out>
#1  0x00007ffff6813218 in osmo_select_main (polling=0) at select.c:255
        rc = 0
        readset = {__fds_bits = {120, 0 <repeats 15 times>}}
        writeset = {__fds_bits = {0 <repeats 16 times>}}
        exceptset = {__fds_bits = {0 <repeats 16 times>}}
        no_time = {tv_sec = 0, tv_usec = 0}
#2  0x000000000050844a in main (argc=3, argv=0x7fffffffe128) at osmo-trx.cpp:637
        rc = 0
(gdb)
```

#10 - 06/14/2019 03:53 PM - pespin

Running with ASan:

```
Fri Jun 14 17:49:55 2019 DLMS <0003> LMSDevice.cpp:92 [tid=140106084933056] RemoteControl Listening on port: 5
000
Fri Jun 14 17:49:55 2019 DLMS <0003> LMSDevice.cpp:92 [tid=140106084933056] Reference clock 40.00 MHz
Fri Jun 14 17:49:55 2019 DDEV <0002> LMSDevice.cpp:190 [tid=140106084933056] Init LMS device
Fri Jun 14 17:49:56 2019 DDEV <0002> LMSDevice.cpp:97 [tid=140106084933056] Sample Rate: Min=100000 Max=3.072e
+07 Step=1.97626e-323
Fri Jun 14 17:49:56 2019 DDEV <0002> LMSDevice.cpp:226 [tid=140106084933056] Setting sample rate to 1.08333e+0
6 4
Fri Jun 14 17:49:56 2019 DDEV <0002> LMSDevice.cpp:232 [tid=140106084933056] Sample Rate: Host=1.08333e+06 RF=
3.46667e+07
Fri Jun 14 17:49:56 2019 DMAIN <0000> LMSDevice.cpp:209 [tid=140106084933056] Antennas configured successfully
Fri Jun 14 17:49:56 2019 DMAIN <0000> Threads.cpp:116 [tid=140106045757184] Thread 140106045757184 (task 3683)
 set name: CtrlService0
Fri Jun 14 17:49:56 2019 DMAIN <0000> osmo-trx.cpp:526 [tid=140106084933056] -- Transceiver active with 1 chan
nel(s)
Fri Jun 14 17:50:07 2019 DTRXCTRL <0001> Transceiver.cpp:717 [tid=140106045757184][chan=0] command is 'POWEROF
F'
Fri Jun 14 17:50:07 2019 DTRXCTRL <0001> Transceiver.cpp:848 [tid=140106045757184][chan=0] response is 'RSP PO
WEROFF 0'
Fri Jun 14 17:50:07 2019 DTRXCTRL <0001> Transceiver.cpp:717 [tid=140106045757184][chan=0] command is 'POWEROF
F'
Fri Jun 14 17:50:07 2019 DTRXCTRL <0001> Transceiver.cpp:848 [tid=140106045757184][chan=0] response is 'RSP PO
WEROFF 0'
Fri Jun 14 17:50:07 2019 DTRXCTRL <0001> Transceiver.cpp:717 [tid=140106045757184][chan=0] command is 'RXTUNE
1781800'
Fri Jun 14 17:50:07 2019 DDEV <0002> LMSDevice.cpp:763 [tid=140106045757184][chan=0] Setting Rx Freq to 1.7818
e+09 Hz
AddressSanitizer:DEADLYSIGNAL
=================================================================
==3656==ERROR: AddressSanitizer: stack-overflow on address 0x7f6cfb161f88 (pc 0x7f6cfece4011 bp 0x00000000001a
 sp 0x7f6cfb161f00 T5)
    #0 0x7f6cfece4010 in __vsnprintf_internal (/usr/lib/libc.so.6+0x79010)
    #1 0x7f6cfecbe1f5 in __GI___snprintf (/usr/lib/libc.so.6+0x531f5)
    #2 0x7f6cfed21040 in asctime_internal (/usr/lib/libc.so.6+0xb6040)
    #3 0x7f6cfed211be in ctime_r (/usr/lib/libc.so.6+0xb61be)
    #4 0x7f6d0016e7ab in __interceptor_ctime_r /build/gcc/src/gcc/libsanitizer/sanitizer_common/sanitizer_comm
on_interceptors.inc:1244
    #5 0x7f6cff331fd7 in _output /home/pespin/dev/sysmocom/git/libosmocore/src/logging.c:367
    #6 0x7f6cff33446a in osmo_vlogp /home/pespin/dev/sysmocom/git/libosmocore/src/logging.c:548
    #7 0x7f6cff3348a4 in logp2 /home/pespin/dev/sysmocom/git/libosmocore/src/logging.c:581
    #8 0x563b8b6961b9 in Log::~Log() /home/pespin/dev/sysmocom/git/osmo-trx/CommonLibs/Logger.cpp:55
    #9 0x563b8b65dd74 in lms_log_callback /home/pespin/dev/sysmocom/git/osmo-trx/Transceiver52M/device/lms/LMS
Device.cpp:92
    #10 0x7f6cff1529e3 in lime::log(lime::LogLevel, char const*, __va_list_tag*) (/usr/lib/libLimeSuite.so.19.
04-1+0x309e3)
    #11 0x7f6cff199731  (/usr/lib/libLimeSuite.so.19.04-1+0x77731)
    #12 0x7f6cff19988d  (/usr/lib/libLimeSuite.so.19.04-1+0x7788d)
    #13 0x7f6cff199ebd  (/usr/lib/libLimeSuite.so.19.04-1+0x77ebd)
    #14 0x563b8b663a82 in LMSDevice::setRxFreq(double, unsigned long) /home/pespin/dev/sysmocom/git/osmo-trx/T
ransceiver52M/device/lms/LMSDevice.cpp:765
    #15 0x563b8b668e35 in RadioInterface::tuneRx(double, unsigned long) /home/pespin/dev/sysmocom/git/osmo-trx
/Transceiver52M/radioInterface.cpp:153
    #16 0x563b8b6759d1 in Transceiver::driveControl(unsigned long) /home/pespin/dev/sysmocom/git/osmo-trx/Tran
```

```
sceiver52M/Transceiver.cpp:795
    #17 0x563b8b677813 in ControlServiceLoopAdapter(TransceiverChannel*) /home/pespin/dev/sysmocom/git/osmo-tr
x/Transceiver52M/Transceiver.cpp:1098
    #18 0x7f6d000eaa91 in start_thread (/usr/lib/libpthread.so.0+0x7a91)
    #19 0x7f6cfed65cd2 in __clone (/usr/lib/libc.so.6+0xfacd2)

SUMMARY: AddressSanitizer: stack-overflow (/usr/lib/libc.so.6+0x79010) in __vsnprintf_internal
Thread T5 (CtrlService0) created by T0 here:
    #0 0x7f6d001566d5 in __interceptor_pthread_create /build/gcc/src/gcc/libsanitizer/asan/asan_interceptors.c
c:202
    #1 0x563b8b69579d in Thread::start(void* (*)(void*), void*) /home/pespin/dev/sysmocom/git/osmo-trx/CommonL
ibs/Threads.cpp:140

==3656==ABORTING
```

#11 - 06/17/2019 12:46 PM - pespin

- Status changed from Feedback to Resolved

- % Done changed from 0 to 100

Fixed by https://gerrit.osmocom.org/c/osmo-trx/+/14488

Default stack size is now defined by OS, so it's configurable and default linux size should be bigger and enough.

Files

osmo-trx-lms.cfg	361 Bytes	06/12/2019	roh
osmo-bsc.cfg	3.41 KB	06/12/2019	roh