OsmoBTS - Bug #2316

osmo-bts aborts on sysmoBTS

06/01/2017 06:28 PM - neels

Status:	Closed	**Start date:**	06/01/2017
Priority:	High	**Due date:**	
Assignee:	neels	**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

The osmo-gsm-tester reports SIGABRT during startup of osmo-bts on the sysmoBTS.
The cause is not yet clear. It may be due to a recent commit, possibly also due to a failure in setup on the osmo-gsm-tester.
Details follow.

Related issues:

Related to OsmoBSC - Bug #1614: better identification of BTS model / capabili...	**Stalled**	**02/23/2016**

History

#1 - 06/01/2017 06:35 PM - neels

http://jenkins.osmocom.org/jenkins/view/osmo-gsm-tester/job/osmo-gsm-tester_run/295/console

```
| 19700702025820467 DLCTRL <0017> control_if.c:787 CTRL at 127.0.0.1 4238
| [0;m19700702025820468 DLGLOBAL <0010> telnet_interface.c:95 telnet at 127.0.0.1 4241
| [0;m19700702025820470 DLINP <0012> input/ipaccess.c:885 enabling ipaccess BTS mode, OML connecting to 10.42.
42.2:3002
| [0;m19700702025820471 DABIS <000d> abis.c:207 Input Signal 4 received
| [0;m19700702025820472 DL1C <0006> phy_link.c:58 PHY link state change shutdown -> connecting
| [0;m19700702025820472 DL1C <0006> l1_if.c:1631 sysmoBTSv2 L1IF compiled against API headers v5.1.0
| [0;m19700702025821645 DL1C <0006> l1_if.c:1619 Read clock calibration(-71) from EEPROM.
| [0;m19700702025821670 DL1C <0006> l1_if.c:184 Tx SYS prim LAYER1-RESET.req
| [0;m19700702025821670 DL1C <0006> l1_if.c:1840 Assuming 1002 for sysmoBTS Model number 65535
| [0;msh: line 1: 27295 Aborted
```

No core file was found.

Running manually with gdb:

```
(gdb) run
Starting program: /osmo-gsm-tester/osmo-bts-sysmo/bin/osmo-bts-sysmo -c /osmo-gsm-tester/osmo-bts-sysmo.cfg -r
 1 -i 10.42.42.2
warning: File "/lib/libthread_db-1.0.so" auto-loading has been declined by your `auto-load safe-path' set to "
$debugdir:$datadir/auto-load".
To enable execution of this file add
    add-auto-load-safe-path /lib/libthread_db-1.0.so
line to your configuration file "/home/root/.gdbinit".
To completely disable this security protection add
    set auto-load safe-path /
line to your configuration file "/home/root/.gdbinit".
For more information about this security protection see the
"Auto-loading safe path" section in the GDB manual.  E.g., run from the shell:
    info "(gdb)Auto-loading safe path"
warning: Unable to find libthread_db matching inferior's thread library, thread debugging will not be availabl
e.
((*))
  |
 / \ OsmoBTS
19700702031733079 DLCTRL <0017> control_if.c:787 CTRL at 127.0.0.1 4238
19700702031733080 DLGLOBAL <0010> telnet_interface.c:95 telnet at 127.0.0.1 4241
19700702031733082 DLINP <0012> input/ipaccess.c:885 enabling ipaccess BTS mode, OML connecting to 10.42.42.2:3
002
19700702031733083 DABIS <000d> abis.c:207 Input Signal 4 received
19700702031733084 DL1C <0006> phy_link.c:58 PHY link state change shutdown -> connecting
19700702031733084 DL1C <0006> l1_if.c:1631 sysmoBTSv2 L1IF compiled against API headers v5.1.0
```

```
19700702031734257 DL1C <0006> l1_if.c:1619 Read clock calibration(-71) from EEPROM.
19700702031734282 DL1C <0006> l1_if.c:184 Tx SYS prim LAYER1-RESET.req
19700702031734283 DL1C <0006> l1_if.c:1840 Assuming 1002 for sysmoBTS Model number 65535

Program received signal SIGABRT, Aborted.
0x45237208 in raise () from /lib/libc.so.6
(gdb) bt
#0  0x45237208 in raise () from /lib/libc.so.6
#1  0x4523ad8c in abort () from /lib/libc.so.6
#2  0x00000020 in ?? ()
#3  0x00000020 in ?? ()
Backtrace stopped: previous frame identical to this frame (corrupt stack?)
(gdb)
```

The osmo-gsm-tester build job does re-build all osmo* dependencies and the SDK matches the sysmobts firmware. Nevertheless, we could update the sysmoBTS firmware and the SDK used to build the binaries...

#2 - 06/01/2017 07:59 PM - neels

updated rootfs image and SDK show no change, still SIGABRT.
used:

sysmocom-nitb-image-sysmobts-v2-20170530010059.rootfs.ubi
poky-eglibc-i686-meta-toolchain-osmo-armv5te-toolchain-osmo-1.5.4-20170530010059.sh

#3 - 06/02/2017 02:19 PM - neels

Test failures continue.

In the mean time I spent some time on enhancing the osmo-gsm-tester build scripts to be able to more easily bisect by issuing specific git hashes to build. https://gerrit.osmocom.org/2828

#4 - 06/02/2017 03:08 PM - neels

A build with libosmocore b6c8dda5e34df6b74183ad24cf66c98601065e56 and osmo-bts 72993079edf3fa3285c4c50ef92bd6517b933d36 succeeded, so this is definitely a regression. Now need to pinpoint which exactly is the cause.

#5 - 06/02/2017 03:34 PM - neels

intermediate status: running with libosmocore master HEAD and osmo-bts 3f97e4b1fcdc788345ab7740bd4fb8a3d73f5526 also worked. looking further...

#6 - 06/02/2017 03:58 PM - neels

The failure appears to have been introduced by:

```
commit 9eeb0b1a136fc8c24a86cb4d832c264674c10db0
Refs: 0.4.0-462-g9eeb0b1
Author:     Max <msuraev@sysmocom.de>
AuthorDate: Mon May 29 16:23:02 2017 +0200
Commit:     Harald Welte <laforge@gnumonks.org>
CommitDate: Mon May 29 21:13:45 2017 +0000

    Add version to phy_instance

    Change-Id: I5b2352b8d15e9b0d8616fcd526b4902d247e4693
    Related: OS#1614
```

The sysmobts artifact was built by http://jenkins.osmocom.org/jenkins/view/osmo-gsm-tester/job/osmo-gsm-tester_build-osmo-bts-sysmo/78/ and tested by http://jenkins.osmocom.org/jenkins/view/osmo-gsm-tester/job/osmo-gsm-tester_run/326/

Testing the preceding osmo-bts commit succeeded in http://jenkins.osmocom.org/jenkins/view/osmo-gsm-tester/job/osmo-gsm-tester_run/325/

#7 - 06/02/2017 04:10 PM - neels

- Assignee changed from neels to msuraev

#8 - 06/02/2017 04:32 PM - msuraev

Reproduced on sysmobts:
<0017> control_if.c:787 CTRL at 127.0.0.1 4238
<0010> telnet_interface.c:95 telnet at 127.0.0.1 4241
<0012> input/ipaccess.c:885 enabling ipaccess BTS mode, OML connecting to 127.0.0.1:3002
<0006> phy_link.c:58 PHY link state change shutdown -> connecting
<0006> l1_if.c:1631 sysmoBTSv2 L1IF compiled against API headers v5.1.0
<0006> l1_if.c:1619 Read clock calibration(-52) from EEPROM.
<0006> l1_if.c:184 Tx SYS prim LAYER1-RESET.req
<0006> l1_if.c:1840 Assuming 1002 for sysmoBTS Model number 65535
Aborted

The model number looks completely out of place, backtrace doesn't look meaningful - seems like a stack corruption? Will have a look.

#9 - 06/02/2017 07:07 PM - neels

- Related to Bug #1614: better identification of BTS model / capabilities to BSC added

#10 - 06/02/2017 08:07 PM - neels

in osmo-bts-sysmo/l1_if.c, you use talloc_asprintf to write to the char version[MAX_VERSION_LENGTH]; talloc_asprintf() however is intended to work on string buffers allocated by talloc, and attempts to reallocate the version[] array.

#11 - 06/02/2017 08:22 PM - neels

In this patch, you pass pinst as data to app_info_sys_compl_cb(), but this cb never uses the data pointer?

#12 - 06/02/2017 08:52 PM - neels

- Status changed from New to Resolved

- Assignee changed from msuraev to neels

I have reverted 9eeb0b1a136fc8c24a86cb4d832c264674c10db0 in d36b3a84638d6db940387f0e18c98855202f554d.
Explanation in http://git.osmocom.org/osmo-bts/commit/?id=d36b3a84638d6db940387f0e18c98855202f554d

This fixes the issue for sysmoBTS, but leaves the patch reverted (related to #1614).

#13 - 08/08/2017 07:06 PM - laforge

- Status changed from Resolved to Closed