OsmoBTS - Bug #3746

Sending RTP stream with unconfigured AMR mode crashes OS

01/04/2019 06:23 PM - keith

Status:	Closed	**Start date:**	01/04/2019
Priority:	Normal	**Due date:**	
Assignee:	sysmocom	**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

If I send an RTP stream with an unconfigured AMR mode to the osmo-bts on my sysmoBTS 1002, the unit crashes and resets.

------------[cut here]------------
WARNING: CPU: 0 PID: -821874208 at
/home/yoctopyrobuild/system-images/build.sysmobts/tmp/work-shared/sysmobts-v2/kernel-source/kernel/sched/core.c:3151
preempt_count_add+0xec/0x134
DEBUG_LOCKS_WARN_ON((preempt_count() < 0))Modules linked in:
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430
Unhandled fault: page domain fault (0x01b) at 0x4711e430

end of output of serial terminal

Related issues:

Related to OsmoBSC - Bug #4002: AMR defaults to bandwidth-efficient mode	**In Progress**	**05/15/2019**

History

#1 - 05/08/2019 06:06 PM - laforge

- Status changed from New to Feedback

- Assignee set to sysmocom

keith, can you please elaborate on how to reproduce this? Thanks! Do you mean you're sending an AMR mode in RTP which is not part of the active set of AMR modes as permitted for the given logical channel?

#2 - 05/08/2019 06:53 PM - pespin

May be related to the known bug where sysmobts kernel crashes when receiving AMR octet-aligned (or the other one, whichever is not supported by superfemto fw).

#3 - 05/15/2019 02:48 PM - pespin

Possibly related to OS#4002, SYS#4063.

Fix for SYS#4063: https://gerrit.osmocom.org/#/c/osmo-bts/+/6351/

#4 - 05/15/2019 02:48 PM - pespin

- Related to Bug #4002: AMR defaults to bandwidth-efficient mode added

#5 - 05/16/2019 11:34 AM - keith

laforge wrote:

> Do you mean you're sending an AMR mode in RTP which is not part of the active set of AMR modes as permitted for the given logical channel?

Yes, that's what i remember observing, however, you're right, I can't reproduce it now, and neither can I reproduce it by sending BE mode AMR to the bts. - That would make sense, given that https://gerrit.osmocom.org/#/c/osmo-bts/+/6351/ has been merged for a while now.

As I have been running so many versions of osmo-bts on different hardware over the last 4 months, and I neglected to include info here on which version, I would just go ahead and close this ticket.

I suspect what I refer to was happening with a rather old osmo-bts but I wouldn't really see the point in going back now to verify if it was actually an AMR mode or BE as pespin says.

I do have a memory of having seen "AMR CMI X not part of AMR MR set" before this crash, but I didn't log it here so let's just close this.

thanks!

k

#6 - 06/19/2019 08:32 AM - laforge

- Status changed from Feedback to Closed