

osmo-sip-connector - Bug #3518

Rapid SETUP followed DISC results in lingering B-leg

09/04/2018 03:34 PM - keith

Status:	New	Start date:	09/04/2018
Priority:	Normal	Due date:	
Assignee:	keith	% Done:	0%
Category:			
Target version:			
Resolution:			
Description			
This is 100% reproducible at the moment.			
First log output is from correct behaviour, (slightly longer before pressing END on UE)			
Second log output shows some clue of what's happening..			
A race condition?			
<pre>Tue Sep 4 17:30:22 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_SETUP_IND Tue Sep 4 17:30:22 2018 DMNCC <0001> mncc.c:466 Created call(5018) with MNCC leg(2147483734) IMSI (262423203000396) Tue Sep 4 17:30:22 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_RTP_CREATE Tue Sep 4 17:30:22 2018 DMNCC <0001> mncc.c:391 RTP cnt leg(2147483734) ip(172.16.0.15), port(165 36) pt(98) ptm(771) Tue Sep 4 17:30:22 2018 DMNCC <0001> mncc.c:81 Got response(0x204), stopping timer on leg(2147483 734) Tue Sep 4 17:30:22 2018 DSIP <0000> sip.c:223 SIP event(7) status(0) phrase(INVITE sent) 0x1476e5 0 Tue Sep 4 17:30:22 2018 DSIP <0000> sip.c:290 nua_callback() did nothing with event(7), status(0) Tue Sep 4 17:30:22 2018 DSIP <0000> sip.c:223 SIP event(1) status(100) phrase(Trying) (nil) Tue Sep 4 17:30:22 2018 DSIP <0000> sip.c:89 Incoming call handle(0x147fb10) Tue Sep 4 17:30:22 2018 DSIP <0000> sip.c:223 SIP event(7) status(100) phrase(Trying) 0x1487b30 Tue Sep 4 17:30:22 2018 DSIP <0000> sip.c:290 nua_callback() did nothing with event(7), status(10 0) Tue Sep 4 17:30:23 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_DISC_IND Tue Sep 4 17:30:23 2018 DMNCC <0001> mncc.c:511 Rcvd MNCC_DISC_IND, Cause: NORM_CALL_CLEAR Tue Sep 4 17:30:23 2018 DMNCC <0001> mncc.c:513 leg(2147483734) was disconnected. Releasing Tue Sep 4 17:30:23 2018 DSIP <0000> sip.c:332 sip_release_call(): Release with MNCC cause(NORM_CA LL_CLEAR) Tue Sep 4 17:30:23 2018 DSIP <0000> sip.c:304 cause2status(): Mapping cause(NORM_CALL_CLEAR) to s tatus(200) Tue Sep 4 17:30:23 2018 DSIP <0000> sip.c:338 Canceling leg(0x1476e50) in int state Tue Sep 4 17:30:23 2018 DSIP <0000> :0 nta_outgoing_tcancel: trying to cancel cancelled request Tue Sep 4 17:30:23 2018 DSIP <0000> sip.c:223 SIP event(2) status(200) phrase(OK) 0x1487b30 Tue Sep 4 17:30:23 2018 DSIP <0000> sip.c:280 Canceled on leg(0x1487b30) Tue Sep 4 17:30:23 2018 DMNCC <0001> mncc.c:253 Releasing call in initial-state leg(5019) Tue Sep 4 17:30:23 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_REL_CNF Tue Sep 4 17:30:23 2018 DMNCC <0001> mncc.c:81 Got response(0x112), stopping timer on leg(5019) Tue Sep 4 17:30:23 2018 DMNCC <0001> mncc.c:560 leg(5019) was cnf released. Tue Sep 4 17:30:23 2018 DAPP <0002> call.c:88 call(5019) released. Tue Sep 4 17:30:23 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_REL_CNF Tue Sep 4 17:30:23 2018 DMNCC <0001> mncc.c:81 Got response(0x112), stopping timer on leg(2147483 734) Tue Sep 4 17:30:23 2018 DMNCC <0001> mncc.c:560 leg(2147483734) was cnf released. Tue Sep 4 17:30:23 2018 DAPP <0002> call.c:88 call(5018) released. Tue Sep 4 17:30:27 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_SETUP_IND Tue Sep 4 17:30:27 2018 DMNCC <0001> mncc.c:466 Created call(5020) with MNCC leg(2147483735) IMSI (262423203000396) Tue Sep 4 17:30:27 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_DISC_IND</pre>			

```

Tue Sep 4 17:30:27 2018 DMNCC <0001> mncc.c:511 Rcvd MNCC_DISC_IND, Cause: NORM_CALL_CLEAR
Tue Sep 4 17:30:27 2018 DMNCC <0001> mncc.c:513 leg(2147483735) was disconnected. Releasing
Tue Sep 4 17:30:27 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_RTP_CREATE
Tue Sep 4 17:30:27 2018 DMNCC <0001> mncc.c:391 RTP cnt leg(2147483735) ip(172.16.0.15), port(165
38) pt(98) ptm(771)
Tue Sep 4 17:30:27 2018 DMNCC <0001> mncc.c:75 Wanted rsp(274) but got(516) for leg(2147483735)
Tue Sep 4 17:30:27 2018 DSIP <0000> sip.c:223 SIP event(7) status(0) phrase(INVITE sent) 0x148b95
0
Tue Sep 4 17:30:27 2018 DSIP <0000> sip.c:290 nua_callback() did nothing with event(7), status(0)
Tue Sep 4 17:30:27 2018 DSIP <0000> sip.c:223 SIP event(1) status(100) phrase(Trying) (nil)
Tue Sep 4 17:30:27 2018 DSIP <0000> sip.c:89 Incoming call handle(0x1489690)
Tue Sep 4 17:30:27 2018 DSIP <0000> sip.c:223 SIP event(7) status(100) phrase(Trying) 0x148e950
Tue Sep 4 17:30:27 2018 DSIP <0000> sip.c:290 nua_callback() did nothing with event(7), status(10
0)
Tue Sep 4 17:30:27 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_REL_CNF
Tue Sep 4 17:30:27 2018 DMNCC <0001> mncc.c:81 Got response(0x112), stopping timer on leg(2147483
735)
Tue Sep 4 17:30:27 2018 DMNCC <0001> mncc.c:560 leg(2147483735) was cnf released.
Tue Sep 4 17:30:27 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_CALL_CONF_IND
Tue Sep 4 17:30:27 2018 DMNCC <0001> mncc.c:609 leg(5021) confirmend. creating RTP socket.
Tue Sep 4 17:30:28 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_RTP_CREATE
Tue Sep 4 17:30:28 2018 DMNCC <0001> mncc.c:391 RTP cnt leg(5021) ip(172.16.0.15), port(16540) pt
(3) ptm(768)
Tue Sep 4 17:30:28 2018 DMNCC <0001> mncc.c:81 Got response(0x204), stopping timer on leg(5021)
Tue Sep 4 17:30:28 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_ALERT_IND
Tue Sep 4 17:30:28 2018 DMNCC <0001> mncc.c:626 leg(5021) is alerting.
Tue Sep 4 17:30:28 2018 DSIP <0000> sip.c:223 SIP event(7) status(180) phrase(Ringing) 0x148e950
Tue Sep 4 17:30:28 2018 DSIP <0000> sip.c:290 nua_callback() did nothing with event(7), status(18
0)
Tue Sep 4 17:30:28 2018 DSIP <0000> sip.c:223 SIP event(31) status(183) phrase(Session Progress)
0x148b950
Tue Sep 4 17:30:28 2018 DSIP <0000> sip.c:223 SIP event(7) status(183) phrase(Session Progress) 0
x148b950
Tue Sep 4 17:30:28 2018 DSIP <0000> sip.c:290 nua_callback() did nothing with event(7), status(18
3)
Tue Sep 4 17:30:30 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_DISC_IND
Tue Sep 4 17:30:30 2018 DMNCC <0001> mncc.c:511 Rcvd MNCC_DISC_IND, Cause: USER_BUSY
Tue Sep 4 17:30:30 2018 DMNCC <0001> mncc.c:513 leg(5021) was disconnected. Releasing
Tue Sep 4 17:30:30 2018 DSIP <0000> sip.c:332 sip_release_call(): Release with MNCC cause(USER_BU
SY)
Tue Sep 4 17:30:30 2018 DSIP <0000> sip.c:304 cause2status(): Mapping cause(USER_BUSY) to status(
486)
Tue Sep 4 17:30:30 2018 DSIP <0000> sip.c:343 Canceling leg(0x148e950) in cnfd state
Tue Sep 4 17:30:30 2018 DMNCC <0001> mncc.c:845 MNCC rcvd message type: MNCC_REL_CNF
Tue Sep 4 17:30:30 2018 DMNCC <0001> mncc.c:81 Got response(0x112), stopping timer on leg(5021)
Tue Sep 4 17:30:30 2018 DMNCC <0001> mncc.c:560 leg(5021) was cnf released.
Tue Sep 4 17:30:30 2018 DAPP <0002> call.c:88 call(5021) released.
Tue Sep 4 17:30:37 2018 DSIP <0000> sip.c:223 SIP event(31) status(486) phrase(Busy Here) 0x148b9
50
Tue Sep 4 17:30:37 2018 DSIP <0000> sip.c:242 leg(0x148b950) unknown SIP status(486), releasing.
Tue Sep 4 17:30:37 2018 DAPP <0002> call.c:88 call(5020) released.

```

History

#1 - 09/04/2018 05:39 PM - fixeria

It would be great to have some protocol traces (*.pcap) and some logs of the other MNCC side (i.e. OsmoMSC or OpenBSC) attached.

#2 - 09/06/2018 07:28 AM - keith

Hi Vadim!

Yes. traces, of course would be useful.

[EDIT: On seconds thoughts, possibly not so useful, at least not for anyone familiar with what's happening on the other side of the MNCC socket (nitb/msc)]

Unfortunately, I have to divert attention to something else right now, but rather than let the noted issue leak out of my (grey-matter) memory I made this note of the problem.

Seeing as how (as I said), it is 100% reproducible, maybe somebody else might get around to adding said trace. ;-)

That said, I have a sneaky feeling that the problem is *probably* visible even with static analysis.

#3 - 10/02/2018 11:25 AM - keith

Static Analysis:

It appears we are getting MNCC_RTP_CREATE after MNCC_DISC_IND (this was observed with osmo-nitb)

On receipt of MNCC_RTP_CREATE, check_rtp_create() calls stop_cmd_timer() which complains and returns, and then we go ahead with continue_call() anyway, ultimately resulting in the setup of the B-leg, even though the A leg is gone.

So we need to check someplace for the continuing validity of the A-leg.

Also this would appear to reveal a bug on the MSC side, in that somehow we are getting this MNCC_RTP_CREATE from the MNCC socket (in this case, I repeat, osmo-nitb) **after** we got the MNCC_DISC_IND.

Note to self: Maybe that's because we didn't send back some response to MNCC_DISC_IND yet?

#4 - 10/02/2018 03:37 PM - laforge

#7 - 12/06/2018 10:49 AM - keith

Adding link to possible workaround patch here:

<https://gerrit.osmocom.org/#/c/osmo-sip-connector/+11194/>