libosmo-sccp + libosmo-sigtran - Bug #2333

osmo_sock_init2() called from osmo_sccp_simple_client() may never return

06/20/2017 08:22 PM - neels

Status:	Resolved	**Start date:**	06/20/2017
Priority:	Normal	**Due date:**	
Assignee:	dexter	**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

I am trying to get the OsmoHNBGW to work with the new SIGTRAN. The configuration there is certainly still wrong, but I am hitting a peculiar situation where instead of erroring out, osmo_sccp_simple_client() never returns.

First off, the OsmoHNBGW successfully creates a link to CS; then, when setting up the PS link, osmo_sccp_simple_client() never returns.
Both should connect to osmo-stp at 127.0.0.1, the root reason why PS fails is that it still attempts to connect to 127.0.0.2 where no process is listening. The point is that it osmo_ss7 should not idle indefinitely when no connection can be established.

Details follow.

Related issues:

Related to OsmoMSC - Feature #2289: implement AoverIP (OsmoMSC side)	**Closed**	**05/24/2017**

History

#1 - 06/20/2017 08:29 PM - neels

I added some 'XXX' printf()s because I was puzzled by CS vs. PS behavior. I expect to see an identical sequence of XXX messages for both CS and PS, but see that the hngbw_cnlink_init() never returns for PS:

```
Starting program: /usr/local/bin/osmo-hnbgw
20170620222237783 DLGLOBAL <0004> ../../../src/vty/telnet_interface.c:101 telnet at 127.0.0.1 2323
XXXXXXXXXX hello cs
XXXXXXXXXX yes CS
20170620222237783 DRUA <0002> ../../src/hnbgw_cn.c:402 New hnbgw_cnlink 0x6974b0 (gw 0x6481c0): 127.0.0.1 2905
 CS
20170620222237783 DMAIN <0000> ../../src/hnbgw_cn.c:403 adsfasdfad
XXXXXXXXXX osmo_sccp_simple_client CS
20170620222237783 DLSS7 <0010> ../../src/osmo_ss7.c:338 1: Creating SS7 Instance
20170620222237783 DLSS7 <0010> ../../src/osmo_ss7.c:624 1: Creating Route Table system
20170620222237783 DLSS7 <0010> ../../src/osmo_ss7.c:833 1: Creating AS as-clnt-CS
20170620222237783 DLSS7 <0010> ../../src/fsm.c:228 XUA_AS(as-clnt-CS)[0x697a20]{AS_DOWN}: Allocated
20170620222237783 DLSS7 <0010> ../../src/osmo_ss7.c:865 1: Adding ASP asp-clnt-CS to AS as-clnt-CS
20170620222237783 DLSS7 <0010> ../../src/fsm.c:228 xua_default_lm(asp-clnt-CS)[0x698d40]{IDLE}: Allocated
20170620222237783 DLSS7 <0010> ../../src/osmo_ss7.c:1101 1: Restarting ASP asp-clnt-CS
20170620222237783 DLSS7 <0010> ../../src/fsm.c:228 XUA_ASP(asp-clnt-CS)[0x699210]{ASP_DOWN}: Allocated
20170620222237783 DLSS7 <0010> ../../src/osmo_ss7.c:419 registering user=SCCP for SI 3 with priv 0x699520
XXXXXXXXXX osmo_sccp_simple_client done CS
XXXXXXXXX cnlink->sccp = 0x6974b0->0x699520
20170620222237783 DLSCCP <0011> ../../src/sccp_user.c:81 Binding user 'OsmoHNBGW-CS' to SSN=142 PC=0 (pc_valid
=0)
XXXXXXXXXX done cs
XXXXXXXXXX hello ps
XXXXXXXXXX yes PS
20170620222237783 DRUA <0002> ../../src/hnbgw_cn.c:402 New hnbgw_cnlink 0x699730 (gw 0x6481c0): 127.0.0.2 2905
 PS
20170620222237783 DMAIN <0000> ../../src/hnbgw_cn.c:403 adsfasdfad
XXXXXXXXXX osmo_sccp_simple_client PS
20170620222237783 DLSS7 <0010> ../../src/osmo_ss7.c:833 1: Creating AS as-clnt-PS
20170620222237783 DLSS7 <0010> ../../src/fsm.c:228 XUA_AS(as-clnt-PS)[0x699ba0]{AS_DOWN}: Allocated
20170620222237783 DLSS7 <0010> ../../src/osmo_ss7.c:865 1: Adding ASP asp-clnt-PS to AS as-clnt-PS
20170620222237783 DLSS7 <0010> ../../src/fsm.c:228 xua_default_lm(asp-clnt-PS)[0x69a210]{IDLE}: Allocated
20170620222237783 DLSS7 <0010> ../../src/osmo_ss7.c:1101 1: Restarting ASP asp-clnt-PS
...nothing happens. hitting ctrl-C:
```

```
^C
Program received signal SIGINT, Interrupt.
0x00007ffff636f350 in __connect_nocancel ()
    at ../sysdeps/unix/syscall-template.S:81
81    ../sysdeps/unix/syscall-template.S: No such file or directory.
(gdb) bt
#0  0x00007ffff636f350 in __connect_nocancel ()
    at ../sysdeps/unix/syscall-template.S:81
#1  0x00007ffff775e05f in osmo_sock_init2 (family=family@entry=2,
    type=type@entry=1, proto=<optimized out>, local_host=<optimized out>,
    local_port=<optimized out>, remote_host=0x699950 "127.0.0.2",
    remote_port=2905, flags=3) at ../../src/socket.c:207
#2  0x00007ffff69d17a5 in osmo_stream_cli_open2 (cli=0x69a4c0, reconnect=1)
    at ../../src/stream.c:425
#3  0x00007ffff6df09bf in osmo_ss7_asp_restart (asp=0x699fe0)
    at ../../src/osmo_ss7.c:1131
#4  0x00007ffff6dec2c6 in osmo_sccp_simple_client (ctx=<optimized out>,
    name=<optimized out>, pc=<optimized out>, prot=OSMO_SS7_ASP_PROT_M3UA,
    local_port=0, local_ip=0x423132 "127.0.0.5", remote_port=2905,
    remote_ip=0x6483a0 "127.0.0.2") at ../../src/sccp_user.c:281
#5  0x000000000040ed9d in hnbgw_cnlink_init (gw=0x6481c0,
    host=0x699190 "\002", port=16, is_ps=1) at ../../src/hnbgw_cn.c:406
#6  0x0000000000403b0d in main (argc=1, argv=0x7fffffffe728)
    at ../../src/hnbgw.c:514
(gdb)
```

#2 - 06/20/2017 08:33 PM - neels

If I set CS to 127.0.0.2 as well, CS also halts in the same way. So it's not about creating a second link, only about using an address where "nothing is happening".

#3 - 07/19/2017 04:27 PM - laforge

- Assignee set to dexter

#4 - 07/24/2017 07:25 PM - dexter

Does it still hang with our current simple client implementation? Looks like it has some problems with the restarting of the ASP. Maybe we should reproduce it on my machine, then I can have a look at it.

#5 - 07/25/2017 08:02 AM - dexter

- Related to Feature #2289: implement AoverIP (OsmoMSC side) added

#6 - 07/25/2017 09:49 AM - neels

reproduction is simple: try to connect to osmo-stp at invalid or not-running address, should be the same from any osmo-{bsc,msc,hnbgw}

#7 - 10/02/2017 12:15 PM - neels

- Subject changed from osmo_sccp_simple_client() may never return to osmo_sock_init2() called from osmo_sccp_simple_client() may never return

I hit the same problem again now, during VTY tests.

I have an osmo-msc config of

```
network
 network country code 1
 mobile network code 1
 short name OsmoMSC
 long name OsmoMSC
 auth policy closed
 location updating reject cause 13
 encryption a5 0
 rrlp mode none
 mm info 1
cs7 instance 0
 point-code 0.23.1
 asp asp-clnt-OsmoMSC-A-Iu 2905 0 m3ua
  ! where to reach the STP:
  remote-ip 10.23.24.1
! local-ip 10.23.24.1
msc
 cs7-instance-a 0
 cs7-instance-iu 0
 mgcpgw remote-ip 10.23.24.1
 assign-tmsi
```

Note the 10.23.24.1 remote-ip under asp. With this, osmo-msc starts but hangs, connecting telnet to the VTY starts, but never returns with a prompt. (the mgcpgw remote-ip has no effect on startup success or failure)

If I change the asp's remote-ip to 127.0.0.1, osmo-msc starts, the VTY works, and osmo-msc attempts to re-connect to STP regularly.
127.0.0.9 also works.
192.168.0.3 works (my current IP address)
192.168.0.1 does not work (the local DSL modem's router)
10.9.1.120 does not work (via VPN tunnel to my office computer)
Could it be related to whether SCTP can be routed to that IP address???

Most confusing to me is why the same VTY test always worked, only today I am hitting the hangs again.

Notably, no STP is running anywhere.

It also appears that we are not seeing jenkins failures because the osmo_sock_init2() hangs for a very long time, but then returns and the test completes. It's just that the runs take very long now due to the hang: https://jenkins.osmocom.org/jenkins/job/osmo-msc/28/

#8 - 10/02/2017 01:26 PM - neels

The long wait happens during

```
rc = connect(sfd, rp->ai_addr, rp->ai_addrlen);
```

in libosmocore osmo_sock_init2().

#9 - 10/02/2017 02:10 PM - neels

the timeout is usually about 5 min. 30 seconds per osmo_sock_init2().

When I add OSMO_SOCK_F_NONBLOCK to the osmo_sock_init2() call, connect() doesn't block.
IIUC though we then need to select() to determine whether we are connected or not.

It is a patch in libosmo-netif:

```
diff --git a/src/stream.c b/src/stream.c
index a80d842..3b82626 100644
--- a/src/stream.c
+++ b/src/stream.c
@@ -424,7 +424,7 @@ int osmo_stream_cli_open2(struct osmo_stream_cli *cli, int reconnect)
     ret = osmo_sock_init2(AF_INET, SOCK_STREAM, cli->proto,
                   cli->local_addr, cli->local_port,
                   cli->addr, cli->port,
-                  OSMO_SOCK_F_CONNECT|OSMO_SOCK_F_BIND);
+                  OSMO_SOCK_F_CONNECT|OSMO_SOCK_F_BIND|OSMO_SOCK_F_NONBLOCK);
     if (ret < 0) {
         if (reconnect && errno == ECONNREFUSED)
             osmo_stream_cli_reconnect(cli);
```

To summarize: when I pick a local IP address 127.0.0.1 where no OsmoSTP is running, this exits immediately with connection failue.
When I pick a random other IP address, connect() takes >5 minutes to determine that it cannot connect.
When I add NONBLOCK, this wait does not happen, but I am not proficient enough on sockets to know what I may have broken by doing that.

We pass reconnect=1 in osmo_ss7.c to osmo_stream_cli_open2(), which makes me assume we want to retry connecting like the GSUP client does:

```
20171002155853313 DLGSUP <002b> ../../../../src/osmo-msc/src/libcommon/gsup_client.c:134 GSUP link to 127.0.0.
1:4222 DOWN
20171002155903319 DLGSUP <002b> ../../../../src/osmo-msc/src/libcommon/gsup_client.c:76 GSUP connecting to 127
.0.0.1:4222
20171002155903319 DLGSUP <002b> ../../../../src/osmo-msc/src/libcommon/gsup_client.c:134 GSUP link to 127.0.0.
1:4222 DOWN
20171002155913324 DLGSUP <002b> ../../../../src/osmo-msc/src/libcommon/gsup_client.c:76 GSUP connecting to 127
.0.0.1:4222
20171002155913324 DLGSUP <002b> ../../../../src/osmo-msc/src/libcommon/gsup_client.c:134 GSUP link to 127.0.0.
1:4222 DOWN
20171002155923329 DLGSUP <002b> ../../../../src/osmo-msc/src/libcommon/gsup_client.c:76 GSUP connecting to 127
.0.0.1:4222
```

That one uses osmo_sock_init() and passes NONBLOCK to it ... but also has a timer calling gsup_client_connect().

Should we make osmo_ss7 act the same way?

#10 - 10/02/2017 03:37 PM - laforge

On Mon, Oct 02, 2017 at 01:26:50PM +0000, neels [REDMINE] wrote:

> The long wait happens during
>
> ```
> rc = connect(sfd, rp->ai_addr, rp->ai_addrlen);
> ```

seems like 'sfd' is not marked non-blocking before calling connect() somehow.

#11 - 07/09/2018 08:19 AM - dexter

- Status changed from New to Resolved

This seems to be resolved by #3383