OsmoNITB - Feature #1712

Feature # 1595 (Closed): Addition of an Iu-CS interface

3G Voice

05/14/2016 12:08 AM - neels

Status:	Closed	**Start date:**	05/14/2016
Priority:	Urgent	**Due date:**	
Assignee:	Osmocom CNI Developers	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

Related issues:

Related to OsmoMSC - Bug #2265: OsmoMSC must DLCX after a voice call is done	**Closed**	**05/16/2017**
Related to OsmoMSC - Bug #2279: osmo-mgcp-gw: Fix: cleanup of transaction IDs...	**Closed**	**05/22/2017**
Related to OpenBSC - Feature #1845: Full BSC/MSC split in NITB/MSC	**Closed**	**11/18/2016**
Related to OsmoMSC - Feature #2260: "next generation" osmo-bsc_mgcp	**Resolved**	**05/16/2017**
Related to OsmoHNBGW - Feature #2264: make sure osmo-hnbgw re-connects dynami...	**Closed**	**05/16/2017**
Related to OsmoMSC - Feature #2281: allow multiple MGCP-GW per MSC	**Rejected**	**05/22/2017**

History

#1 - 08/09/2016 12:15 PM - laforge

- Assignee set to neels

- Priority changed from Normal to Urgent

#2 - 08/09/2016 02:56 PM - neels

- Status changed from New to In Progress

starting to find my way around 3G voice support:

- Our libmsc must not access lchans and so forth directly, but issue assignment requests to establish calls -- firstly within osmo-nitb as a function call. For 3G, this will junction to a RAB Assignment, for 2G ultimately to a BSSMAP Assignment Request on the to-be-done A-interface.
- Similarly to osmo-bsc standalone operation, we will operate an osmo-bsc-mgcp proxy to relay RTP streams.
- libmsc must manage RTP ports, probably by configuring osmo-bsc-mgcp to connect to e.g. a freeswitch port, or back to itself in case of a local call.

Starting to find my way around the details of this task...

#3 - 08/15/2016 07:44 PM - neels

status: not really started yet, am first getting the sysmocom/iups and sysmocom/cscn branches synced to openbsc master and verifying that things still work.

#4 - 08/30/2016 12:07 PM - neels

- Related to Feature #1576: consider using hLayer2 as a pointer storage added

#5 - 08/30/2016 12:08 PM - neels

- Related to deleted (Feature #1576: consider using hLayer2 as a pointer storage)

#6 - 08/30/2016 12:08 PM - neels

- Related to Feature #1594: Split of BSC part from CoreNITB part added

#7 - 09/13/2016 03:49 PM - neels

- % Done changed from 0 to 20

General status update: I'm moving forward slowly, some problems are
sorted out, others are being solved.

I'm testing with both the ip.access nano3G and the femto-X we
have in the office.

In summary:

- RAB Assignment seems to work on femto-X, still fails on nano3G.
- Paging for a voice call seems to work on femto-X, still fails on nano3G
  (nano3G reboots as soon as it receives a Paging for voice, though
  it should be identical to a paging for SMS; difference not pinpointed yet.)
- next up:
  - after successful Paging on femto-X, continue with a RAB Assignment.
  - after successful RAB Assignment on femto-X, continue with RTP stream setup.
  - try to get the nano3G to work the same way as the femto-X already does.
    (we'd like to publish 3G traces preferably by using the nano3G.)
- In other news:
  - SMS state machine apparently needs improvement for 3G
  - Found a cleanup bug on IuRelease that needs fixing

Details...

The first step towards voice on 3G is to have a successful RAB assignment.
The signalling up to that point is mostly working (except partial Paging failure
on the nano3G).

I start up an osmo-bsc_mgcp (which is thus becoming a misnomer, since it is
now talking to an RNC and not a BSC. It should possibly be called 'osmo-mgcpgw'
or something similar instead).

I am so far patching up hacks to understand and probe how things work,
in the openbsc:neels/cscn and neels/cscn_ghost_call branches.
My first step is to obtain a pcap trace with an RTP connection.

The hacks:

- Configured an mgcp queue to send commands to the MGCP GW from osmo-cscn,
  the mgcp config is blindly placed in struct gsm_network so far.
- hardcoded mgcp gw IP address in:
  - RAB Assignment TransportLayerAddress IE
  - MGCP queue from osmo-cscn to MGCP GW
- hardcoded mgcp CRCX message.
- mncc_builtin.c hack to try and establish only one half of a call

There are several "frontiers" to move forward:

SMS

SMS delivery employs Paging like for voice calls, so this serves as
a nice comparison for Paging.

(SMS probably belongs in a separate issue)

Both femto cells:
I notice that Paging only succeeds when the phone has Iu-Released.
When SMS'ing to self, there is one unsuccessful Paging:
A Paging is sent, but since the UE is still Iu-attached from sending
the SMS just a second ago, there is no Paging Response.
When the UE releases a few seconds later, the next Paging attempt
succeeds, and with the Paging Response received, the SMS is delivered.

Thus for Iu, Paging should apparently be skipped when a UE connection
context is already established. We should simply send signalling
and not rely on a Paging Response to continue in the state machine.

nano3G:
SMS seem to be partly unreliable on the nano3G in that SMS to another UE aren't always delivered, and I see in the CSCN log:

```
20160913144048249 <0022> gsm0411_smc.c:467 SMC(0) message MNSMS-REL-REQ received in state WAIT_CP_ACK
20160913144048249 <0022> gsm0411_smc.c:332 SMC(0) cannot release yet current state: WAIT_CP_ACK
```

femto-X:
On the femto-X, Paging works well, but I notice that only one SMS is delivered per InitialUE message, i.e. UE is paged, replies, one SMS is delivered, nothing happens until Iu-Release in a few seconds, then UE is paged again, next SMS is delivered... and so on. Technically, the CSCN could pump any number of SMS per successful Paging.

So it seems the state machine concerning SMS on 3G signalling is not yet accurate.

Voice Call

Calling self or an unknown extension is usually thwarted by signalling (CC Release) before any part of the call is established. Thus I have two ways of testing:

One is a hack that doesn't care about the second half of the call and allows to establish an RTP stream to the first half without interfering; I call it a "ghost call".

The other is actually having two phones, which involves Paging.

Calling a second phone

First off, since we have a hardcoded Ki for 3G auth, I set up a second SIM card with the same Ki and picked a Samsung Galaxy SII from the cupboard. This allows me to have two UE subscribed at the same time.

nano3G:
When trying to call one UE from the other UE, the nano3G doesn't like the Paging. Though the SMS Paging seems to work fine, the Paging for a voice call for some reason makes the nano3G reboot immediately. It does print some logs, but so far I haven't understood the cause, since the Paging should be similar to SMS:

```
Sep 13 12:06:17.702 [UEContext-15] RANAP CommonId from CSDomain
Sep 13 12:06:17.702 [UEContext-15] HNB-GW> RANAP CommonId, CSDomain
Sep 13 12:06:17.702 [UEContext-15] RANAP CommonId provided IMSI 901990000000038
Sep 13 12:06:17.818 [UEContext-15] URSL> UplinkDirectTransfer
Sep 13 12:06:17.818 [UEContext-15] URSL Uplink DirectTransfer from UE, CSDomain, NAS len 30
Sep 13 12:06:17.823 [UEContext-15] RUA DirectTransferInd, domain 0, RANAP length 19
Sep 13 12:06:17.824 [UEContext-15] HNB-GW> RANAP DirectTransfer CSDomain
Sep 13 12:06:17.828 [3GAP-3] C3GAP::Send uRSL msg id 7
Sep 13 12:06:18.023 [UEContext-15] RUA DirectTransferInd, domain 0, RANAP length 76
Sep 13 12:06:18.026 [UEContext-15] RANAP RAB Assignment from CSDomain
Sep 13 12:06:18.026 [UEContext-15] HNB-GW> RANAP RABAssignmentRequest, CSDomain
Sep 13 12:06:18.035 [3GAP-3] C3GAP::Send uRSL msg id 13
Sep 13 12:06:18.046 [RANAP ConnectionlessInd] RANAP Paging provided IMSI 262778026147135
Sep 13 12:06:18.046 [RANAP] Paging 262778026147135
Sep 13 12:06:18.050 [3GAP-3] C3GAP::Send uRSL msg id 20
Sep 13 12:06:18.060 [UEContext-15] URSL> UserPlaneCfgRequest
Sep 13 12:06:18.062 [3GAP-3] C3GAP::Send uRSL msg id 22
Sep 13 12:06:18.119 ERR: [CInterface] Recv from 127.0.0.1 failed, closing.
Sep 13 12:06:18.119 [3GAP-3] Connection from id 'LOCAL' failed
Sep 13 12:06:18.120 [3GAP-3] Stream from id 'LOCAL' failed
Sep 13 12:06:18.120 [URSLManager-4] Sending HNBDeregister to HNB-GW
Sep 13 12:06:18.122 [3GAP-3] C3GAP::Send uRSL msg id 9
Sep 13 12:06:18.123 [UEContext-15] UE context destroyed.  SRNTI 166754, ACUEId 9, IuH CtxtId 2342
Sep 13 12:06:18.123 [UEContext-15] Destroyed UEContext-15, Remaining URSLManager-4 UEContext-8 MIBCnx-1 3GAP-3
 IuhClient-12 SysAgent-2
Sep 13 12:06:18.123 [IuhClient-12] Iuh Connection close request
Sep 13 12:06:18.123 [IuhClient-12] Dropping connection with 10.9.1.120, socket 20
Sep 13 12:06:19.124 [URSLManager-4] Iuh disconnected
Sep 13 12:06:19.125 [IuhClient-12] SCTP stats file read: Shutdowns 1 to 2; Aborts 0 to 0
Sep 13 12:06:19.125 [SysAgent-2] SctpAssociationClosures incremented by 1
```

```
Sep 13 12:06:19.126 [IuhClient-12] Destroyed IuhClient-12, Remaining URSLManager-4 UEContext-8 MIBCnx-1 3GAP-3
 SysAgent-2
Sep 13 12:06:19.126 [3GAP-3] URSL unavailable, previously closed
Sep 13 12:06:19.126 [MIBCnx-1] Update localHnbGwConnectionStatus in MIB: 0
Sep 13 12:06:19.128 [MIBCnx-1] Update hnbGwConnectionState in MIB: 0
Sep 13 12:06:19.128 [URSLManager-4] Going to clear the DNS Info
Sep 13 12:06:19.129 [UEContext-8] REL_IND from Manager
Sep 13 12:06:19.130 [UEContext-8] UE context destroyed.  SRNTI 166754, ACUEId 3, IuH CtxtId 2342
Sep 13 12:06:19.130 ERR: [UEContext-8] UE Deregister was pending but not sent
Sep 13 12:06:19.130 [UEContext-8] Destroyed UEContext-8, Remaining URSLManager-4 MIBCnx-1 3GAP-3 SysAgent-2
Sep 13 12:06:19.130 [URSLManager-4] Destroyed URSLManager-4, Remaining MIBCnx-1 3GAP-3 SysAgent-2
Sep 13 12:06:19.131 [3GAP-3] Connection with 3GAP at 127.0.0.1 dropped
Sep 13 12:06:20.131 [3GAP-3] Destroyed 3GAP-3, Remaining MIBCnx-1 SysAgent-2
Sep 13 12:06:30.210 ERR: [CInterface] Recv from 127.0.0.1 failed, closing.
Sep 13 12:06:30.210 [MIBCnx-1] Connection from id '' failed
Connection to 10.9.1.168 closed by remote host.
Connection to 10.9.1.168 closed.
```

femto-X:
Paging successfully completes for a voice call (without code modifications).

After a successful Paging, the 3G code doesn't yet lead into a RAB Assignment, this is the next thing I want to get to work.

Ghost call

When hacking the mncc_builtin.c to establish only the first half of a call, the CSCN sends a RAB Assignment with the IPv4 address and port of my osmo-bsc_mgcp gateway.

I needed a patch in osmo-iuh to enable the port part of a TransportLayerInformation IE sent in a RAB-Assignment (was #if 0'd to be port 1 always).

I also send a CRCX message to the mgcp gw to enable the RTP port.

nano3G:
Firstly, this needed a patching for the nano3G to send the 32bit address format in the RAB Assignment.
I see connections made to an RTP port of the MGCP GW.
The MGCP GW posts some seemingly neglectable error ("Failed to send dummy packet").
After a timeout of some seconds, the RAB Activation is nacked by the nano3G, with an Outcome message indicating cause "misc - unspecified failure".
The dummy packet error seems to be irrelevant though (see below).

MGCP GW logs on the nano3G:

```
20160913172326216 <000b> mgcp_main.c:237 VTY at 127.0.0.1 4243
20160913172326216 <000b> mgcp_main.c:291 Configured for MGCP.
20160913172521369 <000b> mgcp_protocol.c:662 Configuring RTP endpoint: local port 0
20160913172521369 <000b> mgcp_protocol.c:662 Configuring RTP endpoint: local port 0
20160913172521369 <000b> mgcp_protocol.c:872 Creating endpoint on: 0x1 CI: 1 port: 16002/4002
20160913172521369 <000b> mgcp_network.c:120 Failed to send dummy RTP packet: Invalid argument on: 0x1 to 0.0.0
.0:0
20160913172521369 <000b> mgcp_protocol.c:160 Generated response: code: 200 for '200 1234 OK
I: 1

v=0
o=- 1 23 IN IP4 10.9.1.120
s=-
c=IN IP4 10.9.1.120
t=0 0
m=audio 16002 RTP/AVP 98
a=rtpmap:98 AMR/8000
a=ptime:20
'
20160913172521625 <000b> mgcp_network.c:752 Found BTS for endpoint: 0x1 on port: 1024/0 of 10.9.1.168
20160913172521625 <000b> mgcp_network.c:442 Initializing stream on 0x1 SSRC: 683016449 timestamp: 0 pkt-durati
on: 160, from 10.9.1.168:1024 in 1
```

nano3G trace log after the RAB Assignment failure:

```
Sep 13 15:25:21.253 [UEContext-9] RANAP CommonId from CSDomain
```

```
Sep 13 15:25:21.253 [UEContext-9] HNB-GW> RANAP CommonId, CSDomain
Sep 13 15:25:21.254 [UEContext-9] RANAP CommonId provided IMSI 901990000000038
Sep 13 15:25:21.369 [UEContext-9] URSL> UplinkDirectTransfer
Sep 13 15:25:21.369 [UEContext-9] URSL Uplink DirectTransfer from UE, CSDomain, NAS len 30
Sep 13 15:25:21.372 [UEContext-9] RUA DirectTransferInd, domain 0, RANAP length 19
Sep 13 15:25:21.373 [UEContext-9] HNB-GW> RANAP DirectTransfer CSDomain
Sep 13 15:25:21.377 [3GAP-3] C3GAP::Send uRSL msg id 7
Sep 13 15:25:21.572 [UEContext-9] RUA DirectTransferInd, domain 0, RANAP length 76
Sep 13 15:25:21.574 [UEContext-9] RANAP RAB Assignment from CSDomain
Sep 13 15:25:21.574 [UEContext-9] HNB-GW> RANAP RABAssignmentRequest, CSDomain
Sep 13 15:25:21.583 [3GAP-3] C3GAP::Send uRSL msg id 13
Sep 13 15:25:21.603 [UEContext-9] URSL> UserPlaneCfgRequest
Sep 13 15:25:21.605 [3GAP-3] C3GAP::Send uRSL msg id 22
Sep 13 15:25:29.732 [SCTP] Setting SCTP heartbeat to 5
Sep 13 15:25:33.645 [UEContext-9] URSL RABAssignmentResponse from UE, CSDomain, Assignment failed, RANAP cause
 115
Sep 13 15:25:33.645 [UEContext-9] URSL RABAssignmentResponse from UE, CSDomain, Assignment failed, RANAP cause
 115
Sep 13 15:25:51.519 [UEContext-9] URSL> UplinkDirectTransfer
Sep 13 15:25:51.519 [UEContext-9] URSL Uplink DirectTransfer from UE, CSDomain, NAS len 5
Sep 13 15:25:51.522 [UEContext-9] RUA DirectTransferInd, domain 0, RANAP length 23
Sep 13 15:25:51.523 [UEContext-9] HNB-GW> RANAP DirectTransfer CSDomain
Sep 13 15:25:51.527 [3GAP-3] C3GAP::Send uRSL msg id 7
Sep 13 15:25:51.708 [UEContext-9] URSL> UplinkDirectTransfer
Sep 13 15:25:51.708 [UEContext-9] URSL Uplink DirectTransfer from UE, CSDomain, NAS len 2
Sep 13 15:26:01.679 [UEContext-9] URSL IuReleaseRequest
Sep 13 15:26:01.680 [UEContext-9] URSL IuReleaseReq from UE, CSDomain, Iap Cause 1
Sep 13 15:26:01.682 [UEContext-9] RUA DirectTransferInd, domain 0, RANAP length 13
Sep 13 15:26:01.683 [UEContext-9] RANAP IuReleaseCommand
Sep 13 15:26:01.683 [UEContext-9] HNB-GW> RANAP IuRelease, CSDomain
Sep 13 15:26:01.683 [UEContext-9] Sending RUADisconnect to HNB-GW for CSDomain Context 0x926
Sep 13 15:26:01.684 [UEContext-9] Sending RUADisconnect to HNB-GW for CSDomain Context 0x926
Sep 13 15:26:01.691 [3GAP-3] C3GAP::Send uRSL msg id 9
Sep 13 15:26:01.833 [UEContext-9] UEContextRelease from UE
```

femto-X:
The connection to the MGCP GW seems to be successful here,
and femto-X replies with a successful RAB Assignment outcome immediately.

MGCP GW log for femto-X:

```
20160913165947123 <000b> mgcp_main.c:237 VTY at 127.0.0.1 4243
20160913165947123 <000b> mgcp_main.c:291 Configured for MGCP.
20160913170100378 <000b> mgcp_protocol.c:662 Configuring RTP endpoint: local port 0
20160913170100378 <000b> mgcp_protocol.c:662 Configuring RTP endpoint: local port 0
20160913170100378 <000b> mgcp_protocol.c:872 Creating endpoint on: 0x1 CI: 1 port: 16002/4002
20160913170100378 <000b> mgcp_network.c:120 Failed to send dummy RTP packet: Invalid argument on: 0x1 to 0.0.0
.0:0
20160913170100378 <000b> mgcp_protocol.c:160 Generated response: code: 200 for '200 1234 OK
I: 1

v=0
o=- 1 23 IN IP4 10.9.1.120
s=-
c=IN IP4 10.9.1.120
t=0 0
m=audio 16002 RTP/AVP 98
a=rtpmap:98 AMR/8000
a=ptime:20
'
20160913170101767 <000b> mgcp_network.c:752 Found BTS for endpoint: 0x1 on port: 8000/0 of 10.9.1.11
20160913170101767 <000b> mgcp_network.c:442 Initializing stream on 0x1 SSRC: 1002855813 timestamp: 0 pkt-durat
ion: 160, from 10.9.1.11:8000 in 1
20160913170101768 <000b> mgcp_network.c:376 RTP seqno made a very large jump on 0x1 delta: 10112
20160913170101768 <000b> mgcp_network.c:185 The input timestamp delta is 0 on 0x1 SSRC: 1002855813 timestamp:
 8037710 from 10.9.1.11:8000 in 1
20160913170101768 <000b> mgcp_network.c:185 The output timestamp delta is 0 on 0x1 SSRC: 1002855813 timestamp:
 8037710 from 10.9.1.11:8000 in 1
```

clean up failure

As a side note:

femto-X: When I fail to encode the RTP port (osmo-iuh patch missing),

I see no rejection of the RAB Assignment, but simply an Iu Release.
This leads the CSCN into a segfault since some timer is not cleaned up:

```
20160913161416014 <0000> ranap_decoder.c:4055 Decoding message RANAP_Iu_ReleaseCompleteIEs (ranap_decoder.c:40
55)
20160913161416014 <0019> iu.c:460 handle_co(dir=2, proc=1)
20160913161416014 <001b> cscn_main.c:461 got IuCS event 2: IU_EVENT_IU_RELEASE
20160913161416014 <001b> iucs.c:87 Looking for IuCS subscriber: link_id 0x6e2fc0, conn_id 1
20160913161416014 <001b> iucs.c:50   0: 901990000000038 Iu link 0x6e2fc0, conn_id 1
20160913161416014 <001b> iucs.c:75 subscribers registered: 1
20160913161416014 <001b> iucs.c:96 Found IuCS subscriber for link_id 0x6e2fc0, conn_id 1
20160913161416014 <001b> iucs_ranap.c:102 IuCS release for 901990000000038
20160913161416014 <0006> mncc_builtin.c:369 (call 80000001) Received message MNCC_REL_IND
20160913161416014 <0006> mncc_builtin.c:272 (call 80000001) Releasing remote with cause 47
20160913161416014 <0006> mncc_builtin.c:52 (call 80000001) Call removed.
20160913161416014 <0006> gsm_04_08.c:3390 receive message MNCC_REL_REQ
20160913161416014 <0001> gsm_04_08.c:3605 (ti 08 sub 40014) Received 'MNCC_REL_REQ' from MNCC in state 3 (MO_C
ALL_PROC)
20160913161416014 <0001> gsm_04_08.c:1942 starting timer T308 with 10 seconds
20160913161416014 <0001> gsm_04_08.c:1398 new state MO_CALL_PROC -> RELEASE_REQ
20160913161416014 <0019> iu.c:398 Transmitting L3 Message as RANAP DT (SUA link 0x6e2fc0 conn_id 1)
<RANAP_IE>
    <id>16</id>
    <criticality><ignore/></criticality>
    <value>06 83 2D 08 02 81 AF</value>
</RANAP_IE>
<RANAP_IE>
    <id>59</id>
    <criticality><ignore/></criticality>
    <value>00</value>
</RANAP_IE>
20160913161416014 <001a> sua.c:591 Received SCCP User Primitive (N-DATArequest)
20160913161416014 <001a> sua.c:245 sua_link_send(01 00 08 08 00 00 00 34 00 06 00 08 00 00 00 00 01 05 00 08 0
0 00 03 e8 01 0b 00 1b 00 14 00 13 00 00 02 00 10 40 07 06 83 2d 08 02 81 af 00 3b 40 01 00 00 )
20160913161416014 <0001> gsm_04_08.c:1398 new state RELEASE_REQ -> NULL
20160913161416014 <001a> sua.c:339 (1) state chg ACTIVE->IDLE
20160913161416014 <001e> stream.c:561 connected read/write
20160913161416014 <001e> stream.c:526 sending data
20160913161416014 <001e> stream.c:561 connected read/write
20160913161416014 <001e> stream.c:526 sending data
20160913161416210 <001e> stream.c:561 connected read/write
20160913161416210 <001e> stream.c:509 message received
20160913161416210 <001a> sua.c:1274 sua_srv_conn_cb(): sctp_recvmsg() returned 12
NOTIFICATION 32777 flags=0x0
===> SCTP_SENDER_DRY_EVENT

Program received signal SIGSEGV, Segmentation fault.
rb_insert_color (node=node@entry=0x641098,
    root=root@entry=0x7ffff777d010 <timer_root>) at rbtree.c:80
80            if (parent == gparent->rb_left)
(gdb) bt
#0  rb_insert_color (node=node@entry=0x641098,
    root=root@entry=0x7ffff777d010 <timer_root>) at rbtree.c:80
#1  0x00007ffff756d0ce in __add_timer (timer=0x641098) at timer.c:65
#2  osmo_timer_add (timer=timer@entry=0x641098) at timer.c:76
#3  0x00007ffff756d128 in osmo_timer_schedule (timer=0x641098, seconds=10,
    microseconds=0) at timer.c:98
#4  0x00007ffff756d39c in osmo_timers_update () at timer.c:244
#5  0x00007ffff756d8a9 in osmo_select_main (polling=0) at select.c:188
#6  0x0000000000405ab4 in main (argc=1, argv=0x6dfc40) at cscn_main.c:651
(gdb)
```

Though this only happens when the RTP port is not encoded correctly, we should
make sure to properly clean up upon an Iu Release.
This should not be a lot of effort.

#8 - 09/16/2016 01:32 PM - neels

- % Done changed from 20 to 30

Breaking news: first successful osmocom-3G phone-to-phone voice call!

With the femto-X and using the neels/cscn branch, the first complete
voice call with working audio streams in both directions worked out
some minutes ago.

Most of the things like IP addresses and port numbers are still pretty hardcoded / hacked and some things are incomplete, but now the road is clear and I can work on making things nice.

The voice call is using the osmo-bsc_mgcp as MGCP-GW to relay the RTP stream from the femto cell back to the femto cell. That means we should be able to connect any RTP src/dst fairly easily.

The ip.access nano3G is still unchanged, i.e. reboots upon Paging, I hope to be able to get it to work the same way as the femto-X does soon.

Anyway, we should be able to publish a pcap with RTP now/soon.

#9 - 09/19/2016 12:27 AM - neels

Noticed one possible cause for failures on the nano3G:

Background: on the nano3G upon a HNBAP UE Register, a UE may try to register with a TMSI even though it is seen for the first time.
We'd prefer/expect an IMSI. In order to help with development, we have a hack that just accepts UE Registration with a TMSI. We so far don't use any recorded state in the HNBGW anyway.

However, the UE Register Accept contains a context ID that the HNBGW tells the femto cell about. With a TMSI registration, we actually just always return context ID 2342 as part of the hack.

It appears the nano3G uses this context ID, and may fall over the fact that it is the same for any UE registering by TMSI.

So far, incrementing the hacked context ID for each UE hasn't magically solved any problems though, except a nicer log on the nano3G.

With or without duplicate context IDs, I can no longer reproduce the nano3G reboots upon paging for voice. It seems some or other bad value in our messages doesn't always cause the same kind of failure.

Still searching for the bad value/values that stop the nano3G show.

#10 - 09/19/2016 01:04 AM - neels

neels wrote:

> So far, incrementing the hacked context ID for each UE hasn't magically solved any problems though, except a nicer log on the nano3G.

I can confirm that when the phones register by IMSI, Paging works on the nano3G.

I manually attempt to register the phones on a real network (and get rejected) to clear the TMSI. Then, when the phones go through our normal hnbgw code to register with a context ID that is valid, the Paging is replied upon.

The paged phone goes on to authenticate and a CC Setup + Call Confirmed is sent. Next would be the RAB Assignment.

However, the RAB Assignment still fails the same way as with the ghost call test, only twice, once for each phone; cause 115 (unspecified-failure):

```
Sep 19 00:40:03.868 [UEContext-11] RANAP RAB Assignment from CSDomain
Sep 19 00:40:03.868 [UEContext-11] HNB-GW> RANAP RABAssignmentRequest, CSDomain
Sep 19 00:40:03.882 [3GAP-3] C3GAP::Send uRSL msg id 13
[...]
Sep 19 00:40:06.476 [UEContext-12] RANAP RAB Assignment from CSDomain
Sep 19 00:40:06.477 [UEContext-12] HNB-GW> RANAP RABAssignmentRequest, CSDomain
Sep 19 00:40:06.488 [3GAP-3] C3GAP::Send uRSL msg id 13
Sep 19 00:40:06.500 [UEContext-12] URSL> UserPlaneCfgRequest
Sep 19 00:40:06.501 [3GAP-3] C3GAP::Send uRSL msg id 22
Sep 19 00:40:15.945 [UEContext-11] URSL RABAssignmentResponse from UE, CSDomain, Assignment failed, RANAP caus
e 115
Sep 19 00:40:15.946 [UEContext-11] URSL RABAssignmentResponse from UE, CSDomain, Assignment failed, RANAP caus
```

```
e 115
Sep 19 00:40:18.530 [UEContext-12] URSL RABAssignmentResponse from UE, CSDomain, Assignment failed, RANAP caus
e 115
Sep 19 00:40:18.530 [UEContext-12] URSL RABAssignmentResponse from UE, CSDomain, Assignment failed, RANAP caus
e 115
```

Some seconds pass between RAB Assignment request and response, and as with the ghost call test, I see some requests on the MGCPGW:

```
20160919023622051 <000b> mgcp_main.c:237 VTY at 127.0.0.1 4243
20160919023622051 <000b> mgcp_main.c:291 Configured for MGCP.
20160919024008710 <000b> mgcp_protocol.c:662 Configuring RTP endpoint: local port 0
20160919024008710 <000b> mgcp_protocol.c:662 Configuring RTP endpoint: local port 0
20160919024008710 <000b> mgcp_protocol.c:872 Creating endpoint on: 0x3 CI: 1 port: 16006/4006
20160919024008710 <000b> mgcp_network.c:120 Failed to send dummy RTP packet: Invalid argument on: 0x3 to 0.0.0
.0:0
20160919024008710 <000b> mgcp_protocol.c:160 Generated response: code: 200 for '200 423 OK
I: 1

v=0
o=- 1 23 IN IP4 192.168.0.132
s=-
c=IN IP4 192.168.0.132
t=0 0
m=audio 16006 RTP/AVP 98
a=rtpmap:98 AMR/8000
a=ptime:20
'
20160919024008974 <000b> mgcp_network.c:752 Found BTS for endpoint: 0x3 on port: 1024/0 of 192.168.0.124
20160919024008974 <000b> mgcp_network.c:442 Initializing stream on 0x3 SSRC: 683016465 timestamp: 0 pkt-durati
on: 160, from 192.168.0.124:1024 in 1
20160919024011520 <000b> mgcp_protocol.c:662 Configuring RTP endpoint: local port 0
20160919024011520 <000b> mgcp_protocol.c:662 Configuring RTP endpoint: local port 0
20160919024011520 <000b> mgcp_protocol.c:872 Creating endpoint on: 0x4 CI: 2 port: 16008/4008
20160919024011520 <000b> mgcp_network.c:120 Failed to send dummy RTP packet: Invalid argument on: 0x4 to 0.0.0
.0:0
20160919024011520 <000b> mgcp_protocol.c:160 Generated response: code: 200 for '200 424 OK
I: 2

v=0
o=- 2 23 IN IP4 192.168.0.132
s=-
c=IN IP4 192.168.0.132
t=0 0
m=audio 16008 RTP/AVP 98
a=rtpmap:98 AMR/8000
a=ptime:20
'
20160919024011563 <000b> mgcp_network.c:752 Found BTS for endpoint: 0x4 on port: 1026/0 of 192.168.0.124
20160919024011563 <000b> mgcp_network.c:442 Initializing stream on 0x4 SSRC: 683016450 timestamp: 0 pkt-durati
on: 160, from 192.168.0.124:1026 in 1
```

#11 - 09/19/2016 01:14 AM - neels

Things to do:

- Transform the HNBGW HNBAP TMSI hack into a proper procedure that registers a context ID for the new subscriber.
- Find out why the nano3G is discovered by the MGCPGW with IP address and port but still the nano3G concludes that the RAB Assignment was unsuccessful.

```
Found BTS for endpoint: 0x4 on port: 1026/0 of 192.168.0.124
```

#12 - 10/10/2016 07:26 PM - neels

- % Done changed from 30 to 50

The HNBAP UE Register with TMSI now registers a proper context ID on osmo-hnbgw, which helps testing the nano3G.

MGCP for 3G voice is still in the process of being made configurable.
Not tested with calls across cells, only two phones on the same cell.

#13 - 10/18/2016 06:26 PM - neels

- % Done changed from 50 to 60

Added proper parsing of the MGCP responses from the MGCP GW.
The audio port number is no longer hardcoded but taken from the CRCX response.
IuCS now parses the MGCP GW responses and can evaluate error codes.

Whether any action is needed in case of error codes still needs to be tested.
Arguably the call establishment gsm_trans will simply timeout in the usual fashion.

#14 - 11/03/2016 01:47 PM - neels

Still, the biggest show stopper here is that the nano3G persistently refuses to accept
RAB Assignments for IuCS.

The log message actually states that the RAB is rejected by the UE, which might
be an unintentional implication: if I send the wrong IP address format in the RAB
assignment, the nano3G also logs the identical error message. Note "from UE":

```
Oct 20 16:41:03.313 [UEContext-38] URSL RABAssignmentResponse from UE, CSDomain, Assignment failed, RANAP caus
e 115
```

Attempts to use a Quectel EC20 to analyse the UE side so far failed because our
nano3G uses the US 1900 band, which the EC20 so far does not recognise.
(The same EC20 successfully produces GSMTAP for the Euro-band sysmocell 5000)

Clarify: is this a Euro-band EC20? Should we buy a quad-band EC20?
Is there an AT command to switch bands?

A PDF for the Quectel M10 mentions AT commands to switch bands:
AT+QBAND=? / AT+QBAND=PCS_MODE
but our EC20 just replies 'ERROR' to those.

The EC20 however is branded as an LTE module that is backwards compatible
with UMTS, so possibly the command set is different. We should get hold
of an actual EC20 command set manual.

(Other commands like AT+COPS=..., AT+CUSD=..., ATA and ATH however work
as expected)

Once the nano3G works we might attempt routing calls between two separate 3G cells.

#15 - 11/03/2016 10:07 PM - neels

neels wrote:

> Clarify: is this a Euro-band EC20? Should we buy a quad-band EC20?
> Is there an AT command to switch bands?

There is an AT command to switch bands. It is **not** AT+QBAND, but

```
AT+QCFG="band"[,<bandval>,<ltebandval>,<tdsbandval>[,<effect>]]
```

e.g.

```
AT+QCFG="band",0000006c,0,0,0
```

and needs a power cycle to take effect.
The effect is verified:

```
AT+QCFG="band"
+QCFG: "band",0x6c,0x800d5,0x0
```

Using this, I tried to switch the band, or also enable all bands at the same time
(0xff), but so far the EC20 does not see the nano3G cell (i.e. AT+COPS=? doesn't show it).

#16 - 11/04/2016 12:26 AM - neels

Opened the case, the label says
"EC20 / E QA" and smaller: "EC20EA-256-STD / EC20EQAR02AA01E2G"

So I assume its an EC20-E model, i.e. a quad-band
according to http://www.quectel.com/product/prodetail.aspx?id=84
which means that it **should** work.

Tried to find further hints in the AT commands manual.
Tried to AT+COPS=? numerous times in case it misses it sporadically.
So, I have not yet found out why the EC20 doesn't see the nano3G cell.

#17 - 11/04/2016 12:32 AM - neels

Also took another look at the RAB assignment message itself.
The "convenience" here is that the nano3G plainly reboots when it doesn't like a RAB Assignment.

So whichever tiny parameter I tweaked so far to see whether it makes a difference caused the
nano3G to reboot right away.

The fact that the nano3G does not reboot and already sends RTP packets to the IP address
and port set in the RAB Assignment message makes me assume that our RAB Assignment Request
is actually exactly the way it should be.

Right after the RAB Assignment, we echo the same RTP packets back that we receive from the
nano3G (works well with the SysmoCell 5000). I tried modifying select parameters there:
ssrc id, sequence number, timestamp, to see whether they caused some collision. No effect.

So despite all efforts, so far the nano3G remains stubbornly voiceless.

#18 - 11/04/2016 12:49 AM - neels

also made sure that the rab ids between CS and PS don't cause collision (of course not)

also tried to not echo back RTPC, only RTP. No difference.
The RAB Assignment unsuccessful outcome always follows after six RTP packets,
for both of the UEs involved in the call.

BTW, the called=MT UE does not ring / indicate an incoming call yet, nevertheless
we do receive RTP packets both from the MO and the MT sides. I'd like to assume
that the nano3G thus does all of the RTP up to then, but that is handwavy at best.

Thought experiment: are any of the SDU sizes or other parameters such that the nano3G
would feed them to the UE, but the UE would reject them? In that case the very same
two UEs should not be able to call each other using the sysmocell 5000 and same params.

#19 - 11/09/2016 04:22 PM - neels

There has been success with UE-GSMTAP on the nano3G:

They key point is that the EC20-E does not support UMTS 1900 aka B2.
However, it does support B5, i.e. UMTS 850.

UMTS: B1/B5/B8
https://en.wikipedia.org/wiki/UMTS_frequency_bands

Setting the nano3G onto a B5 frequency worked out:
picking DL-ARFCN 4400 resulted in the cell becoming visible to the EC20.

Hence we have nano3G GSMTAP of the RAB-Assignment procedure.
The RAB-Assignment however does not go through to the UE...

#20 - 11/24/2016 04:39 PM - neels

- Status changed from In Progress to Stalled

Still no progress on nano3G RAB.

Directing my attention to #1711 / #1592 now -- the 3G capable VLR.

#21 - 01/24/2017 10:58 AM - neels

- Status changed from Stalled to In Progress

- % Done changed from 60 to 70

We've finally found out how to get the nano3G to accept a CS RAB Assignment!

When we send a RAB Assignment request to the nano3G, it sends a first RTP packet to the specified port.
We then echo the same RTP packet back, but we need to **overwrite** the first two payload bytes with 'e400'.

The RAB Assignment message itself seems to be fairly irrelevant.

We've also found out that the nano3G indeed accepts X.213 NSAP for transportLayerAddress,
but it needs to be 160 bits long: i.e. the X.213 header '350001' followed by the 32bit
encoded IPv4 address, followed by zero bits to fill up 160. Before, we sent only 56 bits.

So far there is no obvious explanation of the 'e400' bytes in the RTP payload.
It makes no sense whatsoever when looking at AMR or other RTP payload specs.
All we know is that the nano3G rejects RAB Assignments without them.

In summary:

- 3G Voice is working with the sysmocell5000, with two UEs on the same cell.
- 3G Voice is probably going to work with the nano3G, now that we have a RAB Assignment.
  Pending: a test of an actual voice call with two UE subscribed at the same nano3G.
- It's possible that the nano3G uses a proprietary RTP payload, find out whether
  a nano3G stream forwarded to a sysmocell5000 works.
- forwarding voice streams between separate 3G cells is not tested yet.
- forwarding voice streams to SIP is not implemented nor tested yet.

#22 - 01/24/2017 03:09 PM - neels

The first RTP payload that the nano3G sends is always

```
e000df99160051673c012700008200000017100001 00
```

which we echo back with 'e4' written over the start.
This looks nonstandard / ip.access specific.
However, when looking at the sysmocell5000, we also get an 'e0' in the first RTP frame payload:

```
e000dcf9...
```

This is a completely different femto cell stack sending the same weird e0 byte,
so there seems to be something about this e0 that we don't know yet.

#23 - 02/02/2017 03:09 PM - neels

The solution to the nano3G RTP payload is that IuCS actually uses IuUP, UP encapsulated in RTP.
See 3GPP TS 25.414, and 25.415 6.6.2.

With the SysmoCell5000, echoing its own Initialization back to itself results in an ACK
being sent, which we can also echo back to itself, so mere echoing works there.

The nano3G seems to not reply with an ACK when it receives an IuUP Initialization frame.
Thus it is not possible to merely echo its own RTP packets back to itself; instead, the
first RTP frame received from the nano3G (that is an IuUP Initialization) can be changed
to an ACK Initialization by writing 0xe4 to the first payload byte. Sending this back to
the nano3G then results in successful RAB Assignment.

#24 - 02/20/2017 01:47 PM - neels

Still missing/untested for 3G voice is forwarding RTP streams between several cells and/or a 3rd party media gateway.

#25 - 02/20/2017 02:00 PM - neels

Actually, also missing is to have a ring tone while dialling.

We're also currently echoing RTP back during call establishment, switching from echo to forward once both legs of a call are established. It works, but maybe that's not the proper way to do it. But changing this is low priority, might depend on a media gw.

#26 - 02/24/2017 02:48 PM - neels

On the sysmocom/iu branch, OsmoCSCN has been renamed to OsmoMSC.
I'm also sweeping osmocom.org to apply the rename.

#27 - 03/02/2017 05:42 PM - neels

While rebasing onto VLR, I see that we haven't yet implemented sending cipher mode cmd over Iu.
Will be swift to add with the VLR code in place, and it does work on 2G, just noting it.

#28 - 03/04/2017 04:16 AM - neels

neels wrote:

> While rebasing onto VLR, I see that we haven't yet implemented sending cipher mode cmd over Iu.

We do SecurityModeControl; need to clarify whether that is "the same" as Ciphering or in addition.
I knew it once but forgot...

#29 - 05/15/2017 01:56 PM - neels

- Status changed from In Progress to Stalled

- Assignee changed from neels to Osmocom CNI Developers

neels wrote:

> We do SecurityModeControl; need to clarify whether that is "the same" as Ciphering or in addition.

Yes, that's sufficient.

Generally, we still need to resolve directing RTP between multiple hNodeBs, which will also relate to recent AoIP developments. We are focusing on AoIP now; I'm not working on 3G at present, we'll mark back to in-progress when someone is actually working on it.

#30 - 05/24/2017 12:27 PM - neels

- Related to Bug #2265: OsmoMSC must DLCX after a voice call is done added

#31 - 05/24/2017 12:27 PM - neels

- Related to Bug #2279: osmo-mgcp-gw: Fix: cleanup of transaction IDs aka port numbers to be used by the MGCP gw added

#32 - 05/24/2017 01:39 PM - neels

- Related to Feature #1845: Full BSC/MSC split in NITB/MSC added

#33 - 05/24/2017 01:39 PM - neels

- Related to deleted (Feature #1594: Split of BSC part from CoreNITB part)

#34 - 05/24/2017 01:41 PM - neels

- Related to Feature #2260: "next generation" osmo-bsc_mgcp added

#35 - 05/24/2017 01:57 PM - neels

- Status changed from Stalled to In Progress

#36 - 05/24/2017 01:58 PM - neels

- Related to Feature #2264: make sure osmo-hnbgw re-connects dynamically added

#37 - 05/24/2017 02:10 PM - neels

- Related to Feature #2281: allow multiple MGCP-GW per MSC added

#38 - 05/30/2017 12:57 PM - neels

- % Done changed from 0 to 70

(for some reason the % Done value was reset to 0)

#39 - 07/17/2017 10:54 AM - neels

loosely related: dexter has fixed the MNCC connector functionality on the 3G+AoIP branch, hence possibly allowing to route calls between 3G and SIP. Needs to be tested, obviously. One question there is whether/which external PBX support IuUP, the special within-RTP encapsulation used in 3G.

#40 - 10/09/2017 02:56 PM - neels

- Status changed from In Progress to Resolved

- % Done changed from 70 to 100

We have open issues with 3G voice about IuUP and the nano3G needing the IuUP Initialization Ack message and routing of calls between 2G and 3G,
but it makes decreasing sense to keep this issue open.

Let's see IuCS as initially implemented, especially since it now is merged on osmo-msc master, available and working.

For ongoing development, see #1937, #2459, https://osmocom.org/projects/osmomsc , https://osmocom.org/projects/osmo-mgw ...

#41 - 10/11/2017 02:48 AM - laforge

- Status changed from Resolved to Closed