Université Cheikh Anta DIOP De Dakar

ECOLE SUPERIEURE POLYTECHNIQUE

Département Génie informatique

DIC2 SYSTÈMES RÉSEAUX ET TÉLÉCOMMUNICATIONS

(DIC2 SRT)

Compte Rendu Rapport OSMOCOM

Préparé par: **Pr:I. DIOUM**

Alioune BALDE

Mouhamadou Lamine DIOUM

Abbas Lamine GUEYE

RESUMÉ

Table des matières

I) installation et configuration des différents entités nécessaire au bon fonctionnement d’ OSMOCOM

nous avons joint à travers notre git un script permettant d’installer ces différents entités qui sont:

- **HLR**
- **BSC**
- **MSC**
- **BTS**
- **MGW**
- **...**

Nous avons à travers le hlr créer un abonné en lui donnant un imei, un imsi et son MSISDN

```
OsmoHLR# subscriber imsi 608010000000002 update imei 35761300444848
% Updated subscriber IMSI='608010000000002' to IMEI='35761300444848'
OsmoHLR# subscriber imei 35761300444848 sh
    ID: 1
    IMSI: 608010000000002
    MSISDN: 763232572
    IMEI: 357613004448485
    2G auth: COMP128v3
             KI=beefedcafefaceacedaddeddecadefee
    3G auth: MILENAGE
             K=deaf0ff1ced0d0dabbedd1ced1cef00d
             OPC=cededeffacedacefacedbadfadedbeef
             IND-bitlen=5
OsmoHLR#
```

Maintenant on adapte les autres fichiers de configurations des entités en fonction de ces informations (ca sera le cas pour le mobile.cgf afin qu'on puisse utilisé le mobile d' OSMOCOM comme MS et lui attribué les informations de l'abonné),

II) DÉMARRAGE DES ENTITÉS ET TEST D'APPEL

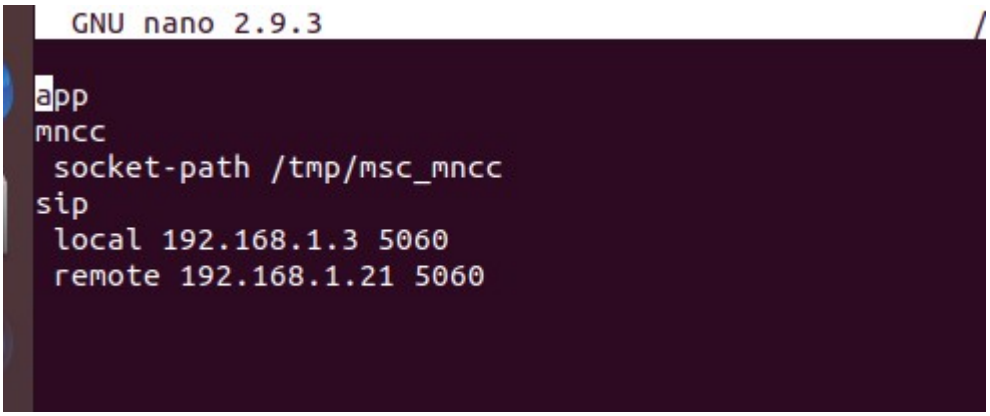
Dans notre git, on a aussi ecrit un script (StartOmoServ.sh) permettant de demarrer les entités dans un ordre bien précis afin de pouvoir simuler le mobile.
Une fois lancée, tous les entités seront allumées et on va pouvoir utiliser le mobile d' OSMOCOM.

L'image suivante montre que le mobile est bien connecté et prêt à être utiliser.

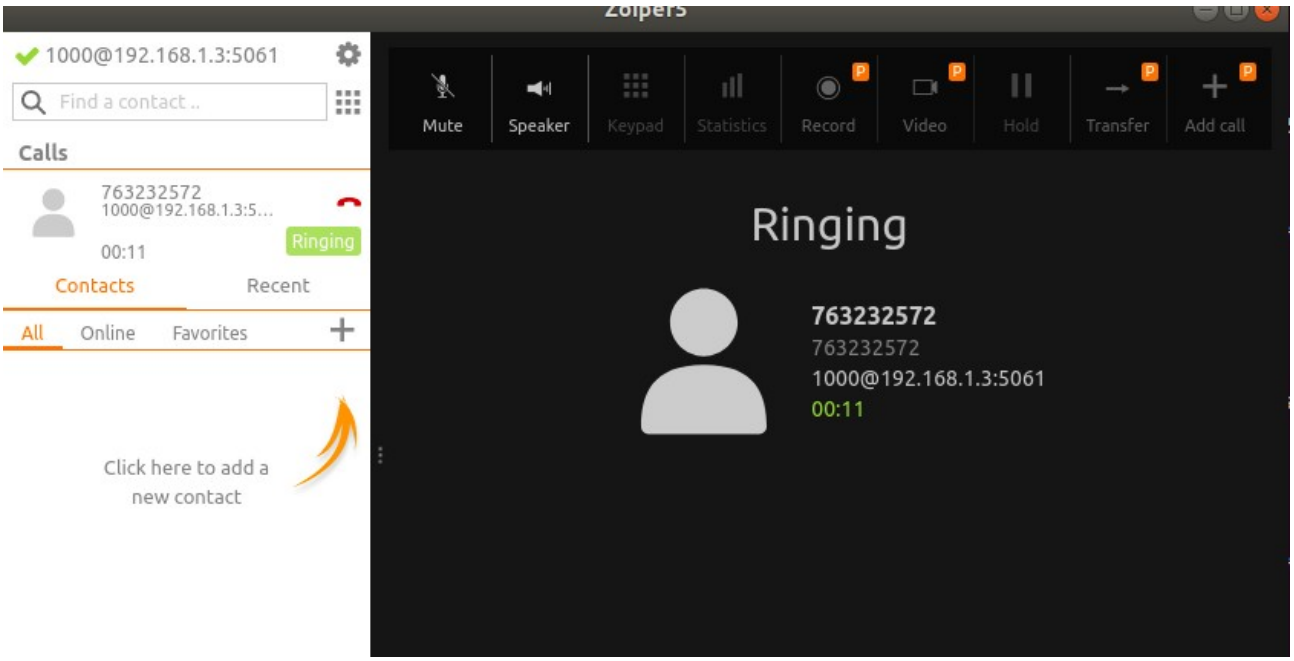
```
alioune@zandaz:~/osmo/src/osmocom-bb/src/host/layer23/src/mobile$ telnet 127.0.0.1 4247
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Welcome to the OsmocomBB VTY interface

OsmocomBB> en
OsmocomBB# sh ms 1
% Ambiguous command.
OsmocomBB# sh
show       shutdown
OsmocomBB# sho
OsmocomBB# show m
OsmocomBB# show ms 1
OsmocomBB# show ms 1
MS '1' is up, service is normal
  IMEI: 357613004448485
     IMEISV: 3576130044484850
     IMEI generation: fixed
  automatic network selection state: A2 on PLMN
                                     MCC=608 MNC=01 (Senegal, Orange (telecommunications))
  cell selection state: C3 camped normally
                        ARFCN=871(DCS) MCC=608 MNC=01 LAC=0x0001 CELLID=0x1b39
                        (Senegal, Orange (telecommunications))
  radio resource layer state: idle
  mobility management layer state: MM idle, normal service
OsmocomBB#
```

Pour rappel on peut connecter **OSMOCOM et SIP** et passer des appels.

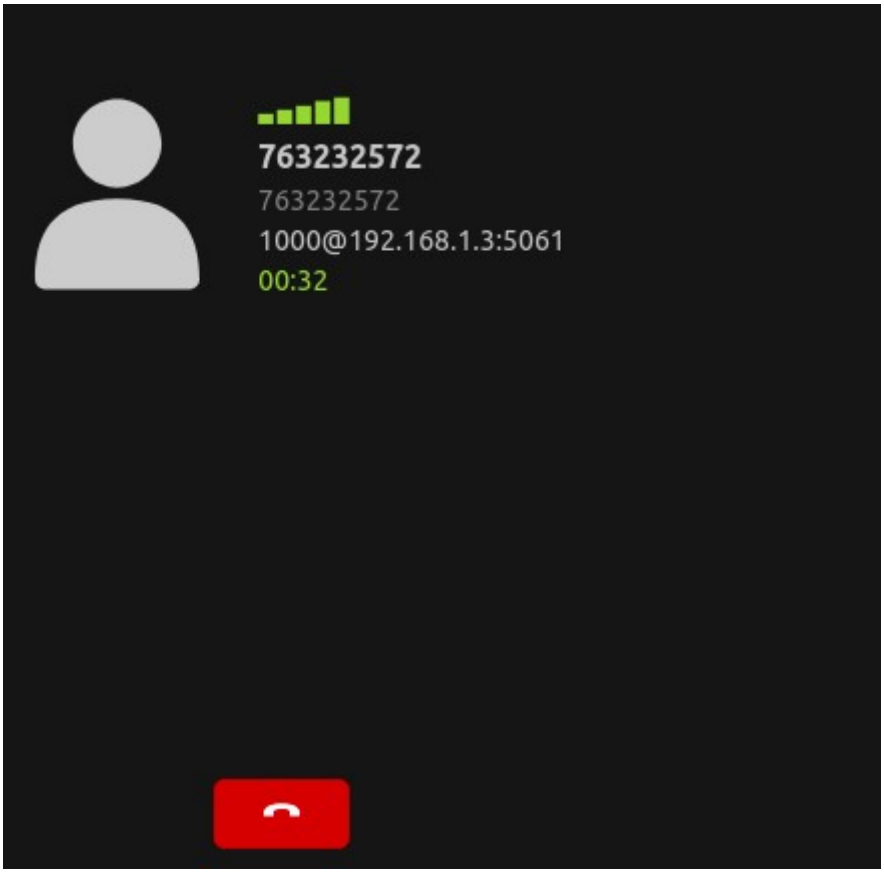
Dans ce cas il nous faut configurer osmo-sip-connector en y renseignant le serveur ASTERISK, son port d'écoute et l'adresse de notre serveur OSMOCOM aussi comme le montre l'image suivante :



Donc arriver ici on peut faire les test d'appel de OSMOCOM vers SIP et de SIP vers OSMOCOM



```
OsmocomBB#
% (MS 1)
% Incoming call (from 1000)

OsmocomBB# call 1
emergency  answer     hangup     hold       retrieve   dtmf
OsmocomBB# call 1 answer
OsmocomBB#
% (MS 1)
% Call is connected

OsmocomBB# cal
OsmocomBB# call 1 hangup
OsmocomBB#
% (MS 1)
% Call has been released

% (MS 1)
% On Network, normal service: Senegal, Orange (telecommunications)
```



III) CAPTURE DES PAQUETS AVEC WIRESHARK DE L'ETABLISSEMENT À LA COMMUNICATION

Si on lance wireshark avant le demarrage des entités on remarque qu'il a une communication entre les differents entités
dans la capture suivante nous voyons le protocole BSSAP qui est est utilisé pour transférer les informations de gestion de la mobilité et de gestion de session entre le **BSS et le MSC**

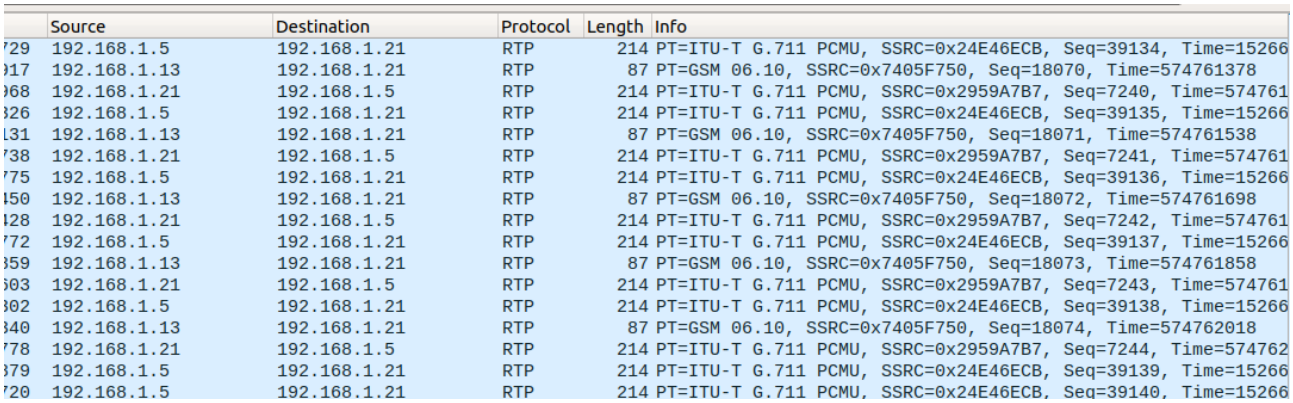
113	53.849983977	127.0.0.1	127.0.0.1	M3UA (…	96	SACK ASPAC_ACK
114	53.850005366	127.0.0.1	127.0.0.1	M3UA (…	88	NTFY
115	53.850011662	127.0.0.1	127.0.0.1	SCTP	64	SACK
116	54.051616247	127.0.0.1	127.0.0.1	SCTP	64	SACK
117	55.806506045	b6:b0:24:00:ef:97		ARP	44	Who has 192.168.1.21? Tell 192.168.1.4
118	55.806932771	IntelCor_68:82:79		ARP	62	192.168.1.21 is at 58:a0:23:68:82:79
119	56.431678606	127.0.0.1	192.168.1.3	SCTP	100	HEARTBEAT
120	56.431708642	127.0.0.1	127.0.0.1	SCTP	100	HEARTBEAT_ACK
121	56.850546622	187	185	BSSAP	120	UDT (BSSMAP) Reset
122	56.850723597	187	185	BSSAP	120	UDT (BSSMAP) Reset
123	56.851018689	185	187	BSSAP	132	SACK UDT (BSSMAP) Reset Acknowledge
124	56.851166018	185	187	BSSAP	132	SACK UDT (BSSMAP) Reset Acknowledge
125	57.051602617	127.0.0.1	127.0.0.1	SCTP	64	SACK
126	57.051617179	127.0.0.1	127.0.0.1	SCTP	64	SACK
127	61.228562175	127.0.0.1	127.0.0.1	TCP	76	36299 → 3002 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PER
128	61.228572422	127.0.0.1	127.0.0.1	TCP	76	3002 → 36299 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=654
129	61.228579013	127.0.0.1	127.0.0.1	TCP	68	36299 → 3002 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=109268
130	61.228712762	127.0.0.1	127.0.0.1	IPA	88	IPA IDENTITY REQUEST

le protocole IPA (permet d'utiliser le *GSM* sur le protocol IP)

L'OML opération et maintenance de lien entre le BSC et le BTS

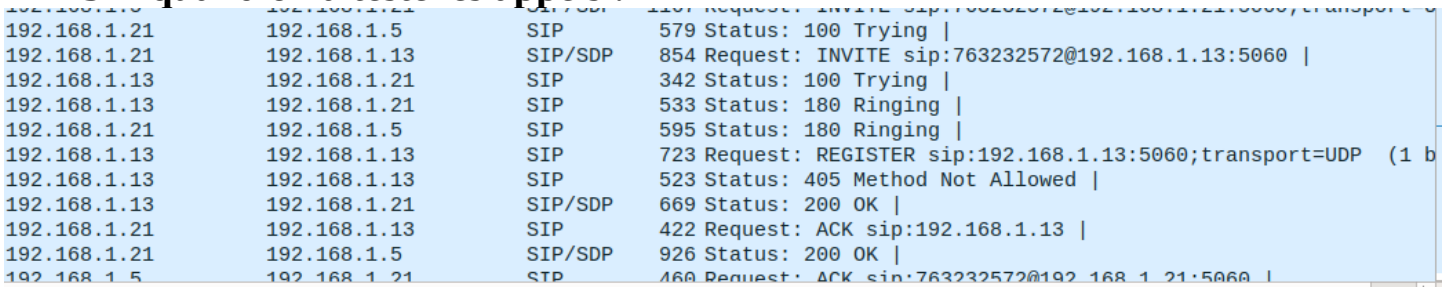
128	61.228572422	127.0.0.1	127.0.0.1	TCP	76	3002 → 36299 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=654
129	61.228579013	127.0.0.1	127.0.0.1	TCP	68	36299 → 3002 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=109268
130	61.228712762	127.0.0.1	127.0.0.1	IPA	88	IPA IDENTITY REQUEST
131	61.228719790	127.0.0.1	127.0.0.1	TCP	68	36299 → 3002 [ACK] Seq=1 Ack=21 Win=65536 Len=0 TSval=10926
132	61.229271784	127.0.0.1	127.0.0.1	UDP	57	5801 → 5701 Len=13
133	61.229555472	127.0.0.1	127.0.0.1	UDP	59	5701 → 5801 Len=15
134	61.229589581	127.0.0.1	127.0.0.1	IPA	176	IPA IDENTITY RESPONSE
135	61.229593712	127.0.0.1	127.0.0.1	TCP	68	3002 → 36299 [ACK] Seq=21 Ack=109 Win=65536 Len=0 TSval=109
136	61.229605986	127.0.0.1	127.0.0.1	IPA	72	IPA IDENTITY ACK
137	61.229609340	127.0.0.1	127.0.0.1	TCP	68	3002 → 36299 [ACK] Seq=21 Ack=113 Win=65536 Len=0 TSval=109
138	61.229651936	127.0.0.1	127.0.0.1	IPA	72	IPA IDENTITY ACK
139	61.229655472	127.0.0.1	127.0.0.1	TCP	68	36299 → 3002 [ACK] Seq=113 Ack=25 Win=65536 Len=0 TSval=109
140	61.229705498	127.0.0.1	127.0.0.1	OML	80	OML BTS Site Manager(ff,ff,ff) Software Activated Report
141	61.229708919	127.0.0.1	127.0.0.1	TCP	68	3002 → 36299 [ACK] Seq=25 Ack=125 Win=65536 Len=0 TSval=109
142	61.229731440	127.0.0.1	127.0.0.1	UDP	57	5801 → 5701 Len=13
143	61.229743712	127.0.0.1	127.0.0.1	OML	88	OML BTS Site Manager(ff,ff,ff) State Changed Event Report D
144	61.229746359	127.0.0.1	127.0.0.1	TCP	68	3002 → 36299 [ACK] Seq=25 Ack=145 Win=65536 Len=0 TSval=109

le protocole RTP aussi pour le REAL-TIME



	Source	Destination	Protocol	Length	Info
729	192.168.1.5	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x24E46ECB, Seq=39134, Time=15266
917	192.168.1.13	192.168.1.21	RTP	87	PT=GSM 06.10, SSRC=0x7405F750, Seq=18070, Time=574761378
968	192.168.1.21	192.168.1.5	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2959A7B7, Seq=7240, Time=574761
826	192.168.1.5	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x24E46ECB, Seq=39135, Time=15266
131	192.168.1.13	192.168.1.21	RTP	87	PT=GSM 06.10, SSRC=0x7405F750, Seq=18071, Time=574761538
738	192.168.1.21	192.168.1.5	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2959A7B7, Seq=7241, Time=574761
775	192.168.1.5	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x24E46ECB, Seq=39136, Time=15266
450	192.168.1.13	192.168.1.21	RTP	87	PT=GSM 06.10, SSRC=0x7405F750, Seq=18072, Time=574761698
428	192.168.1.21	192.168.1.5	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2959A7B7, Seq=7242, Time=574761
772	192.168.1.5	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x24E46ECB, Seq=39137, Time=15266
859	192.168.1.13	192.168.1.21	RTP	87	PT=GSM 06.10, SSRC=0x7405F750, Seq=18073, Time=574761858
503	192.168.1.21	192.168.1.5	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2959A7B7, Seq=7243, Time=574761
802	192.168.1.5	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x24E46ECB, Seq=39138, Time=15266
840	192.168.1.13	192.168.1.21	RTP	87	PT=GSM 06.10, SSRC=0x7405F750, Seq=18074, Time=574762018
778	192.168.1.21	192.168.1.5	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2959A7B7, Seq=7244, Time=574762
879	192.168.1.5	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x24E46ECB, Seq=39139, Time=15266
720	192.168.1.5	192.168.1.21	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x24E46ECB, Seq=39140, Time=15266

SIP quand on a testé les appels :



192.168.1.21	192.168.1.5	SIP	579	Status: 100 Trying |
192.168.1.21	192.168.1.13	SIP/SDP	854	Request: INVITE sip:763232572@192.168.1.13:5060 |
192.168.1.13	192.168.1.21	SIP	342	Status: 100 Trying |
192.168.1.13	192.168.1.21	SIP	533	Status: 180 Ringing |
192.168.1.21	192.168.1.5	SIP	595	Status: 180 Ringing |
192.168.1.13	192.168.1.13	SIP	723	Request: REGISTER sip:192.168.1.13:5060;transport=UDP (1 b
192.168.1.13	192.168.1.13	SIP	523	Status: 405 Method Not Allowed |
192.168.1.13	192.168.1.21	SIP/SDP	669	Status: 200 OK |
192.168.1.21	192.168.1.13	SIP	422	Request: ACK sip:192.168.1.13 |
192.168.1.21	192.168.1.5	SIP/SDP	926	Status: 200 OK |
192.168.1.5	192.168.1.21	SIP	460	Request: ACK sip:763232572@192.168.1.21:5060 |

On joint ainsi dans le git le fichier wireshark. Il y’en a d’autres et on peut voir aussi comment ils sont definis leur tailles et autres.