

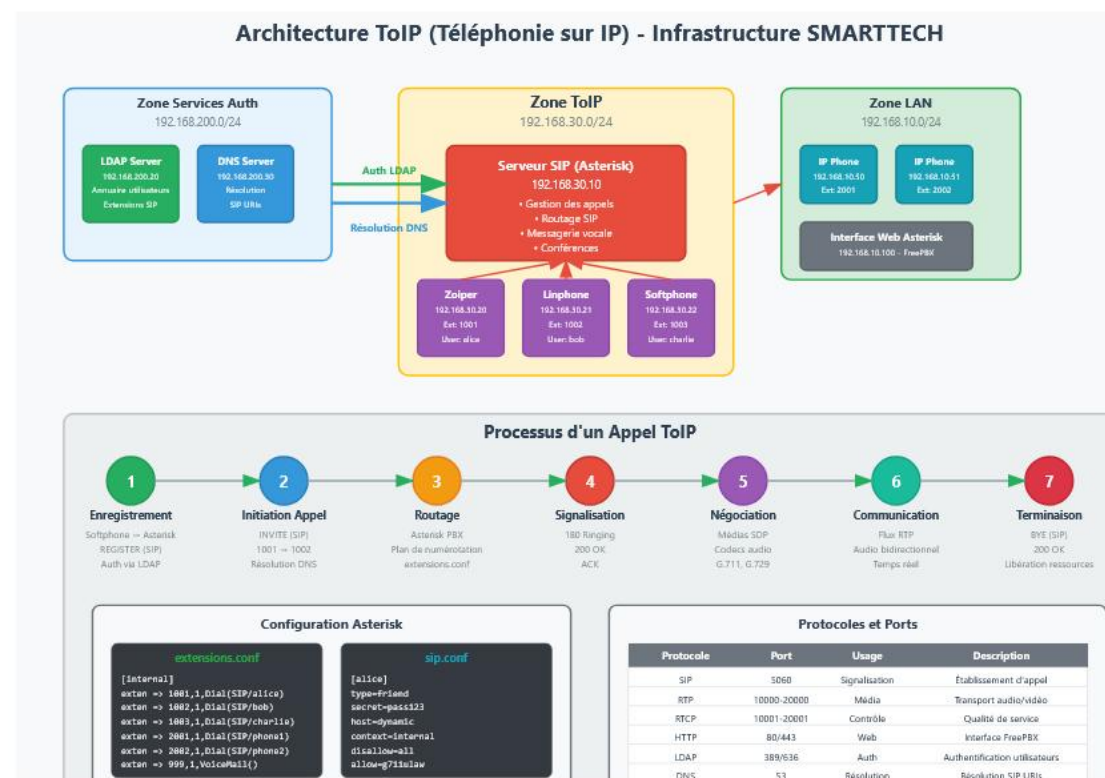
TOIP :

INTRODUCTION :

La téléphonie sur IP (ToIP) a été mise en place afin de permettre une communication interne efficace et moderne.

Elle repose sur un serveur SIP (Asterisk) connecté à l'annuaire LDAP pour l'authentification des utilisateurs.

Les softphones des employés utilisent des comptes LDAP et sont organisés dans une unité dédiée, ce qui facilite la gestion centralisée.



On utilise **ldapadd** pour ajouter une nouvelle entrée dans l'annuaire LDAP (ici dc=local), à partir d'un fichier LDIF contenant les objets nécessaires à la ToIP (ex : ou=people). L'opération est effectuée avec le compte administrateur cn=admin,dc=tp,dc=local.

```
phone1@phone:~$ ldapadd -x -D "cn=admin,dc=tp,dc=local" -W -H ldap://localhost
f ou_people.ldif
Enter LDAP Password:
adding new entry "ou=people,dc=tp,dc=local"
```

On utilise **slappasswd** pour générer un mot de passe chiffré au format SSHA. Ce hash sera utilisé dans les fichiers LDIF pour définir le mot de passe d'un utilisateur LDAP de façon sécurisée.

```
phone1@phone:~$ sudo slappasswd
New password:
Re-enter new password:
{SSHA}yju0iHi3/bo5D4Qf+Aseui3b0Nha16U
```

On crée un fichier **asterisk_user.ldif** pour ajouter un utilisateur LDAP dédié à Asterisk (le serveur SIP). Ce fichier contiendra les attributs nécessaires comme **uid**, **cn**, **sn**, **userPassword**, etc.

```
phone1@phone:~$ sudo nano asterisk_user.ldif
```

Ce fichier définit un utilisateur LDAP nommé **asterisk**, avec les classes d'objet **inetOrgPerson** et **posixAccount**. Il possède un UID/GID, un répertoire personnel, un shell, et un mot de passe chiffré. Cet utilisateur sera utilisé pour authentifier le service Asterisk.

```
dn: uid=asterisk,ou=people,dc=tp,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
cn: Asterisk
sn: test
uid: asterisk
uidNumber: 10003
gidNumber: 10003
homeDirectory: /home/asterisk
loginShell: /bin/bash
userPassword: {SSHA}yju0iHi3/bo5D4Qf+Aseui3b0Nha16U
```

On ajoute l'utilisateur **asterisk** à l'annuaire LDAP en utilisant la commande **ldapadd** avec le fichier **asterisk_user.ldif**. L'opération s'effectue avec le compte administrateur LDAP et confirme que l'entrée a bien été ajoutée.

```
phone1@phone:~$ ldapadd -x -D "cn=admin,dc=tp,dc=local" -W -f asterisk_user.ldif
Enter LDAP Password:
adding new entry "uid=asterisk,ou=people,dc=tp,dc=local"
```

On crée un fichier **asterisk.ldap-schema** pour définir le schéma LDAP personnalisé utilisé par Asterisk (attributs spécifiques au SIP). Puis *cn crée un fichier asterisk.ldif pour convertir ou inclure le schéma Asterisk dans le serveur LDAP.*

On copie le schéma LDAP personnalisé dans le dossier **/etc/ldap/schema/** afin qu'il soit reconnu par le serveur LDAP. Et on redémarre le service **slapd** pour appliquer les modifications et prendre en compte le nouveau schéma.

```
phone1@phone:~$ sudo nano asterisk.ldap-schema
phone1@phone:~$ sudo nano asterisk.ldif
phone1@phone:~$ sudo cp asterisk.ldap-schema /etc/ldap/schema/
phone1@phone:~$ sudo service slapd restart
```

On utilise **slapcat** pour exporter la configuration LDAP (base 0) dans un fichier **config-full.ldif**. Cela permet d'intégrer un nouveau schéma comme celui d'Asterisk.

```
sudo slapcat -n 0 -F /etc/ldap/slapd.d -l /tmp/config-full.ldif
```

On ouvre le fichier **/tmp/config-full.ldif** pour y ajouter manuellement la déclaration du schéma Asterisk. Cela permet au serveur LDAP de reconnaître les attributs spécifiques à la ToIP.

```
dn: olcDatabase={0}config,cn=config
objectClass: olcDatabaseConfig
olcDatabase: {0}config
olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth manage by * break
olcRootDN: cn=admin,cn=config
olcRootPW: {SSHA}QzgLD440QeP+AUwjtzaP87jul+ju+js7
```

Cette section configure l'accès à la base **cn=config** de LDAP. Elle définit les droits d'administration, l'utilisateur root (**olcRootDN**) et son mot de passe chiffré (**olcRootPW**). Cela permet de gérer dynamiquement la configuration, y compris l'ajout de nouveaux schémas comme celui d'Asterisk.

On arrête le service **slapd** pour modifier sa configuration sans conflit. Puis on sauvegarde l'ancienne configuration dynamique (**slapd.d**) en la renommant. Ensuite on crée un nouveau répertoire vide pour reconstruire la configuration. Enfin *On donne les droits du répertoire à l'utilisateur **openldap** pour que le service puisse y accéder.*

```
$ sudo systemctl stop slapd
$ sudo mv /etc/ldap/slapd.d /etc/ldap/slapd.d.bak
$ sudo mkdir /etc/ldap/slapd.d
$ sudo chown openldap:openldap /etc/ldap/slapd.d
```

*On importe le fichier **config-full.ldif** dans le nouveau répertoire de configuration **slapd.d** avec **slapadd**.*

```
phone1@phone:~$ sudo slapadd -n0 -F /etc/ldap/slapd.d -l /tmp/config-full.ldif
Closing DB...
```

On redémarre le service **slapd** maintenant .

```
sudo systemctl start slapd
```

On ajoute le schéma **Asterisk** dans la configuration via **ldapadd** avec le fichier **asterisk.ldif**

```
phone1@phone:~$ ldapadd -x -D "cn=admin,cn=config" -W -H ldapi:/// -f asterisk.ldif
Enter LDAP Password:
adding new entry "cn=asterisk,cn=schema,cn=config"
```

On crée une unité organisationnelle **ou=pjsip** dans LDAP à l'aide du fichier **ou_pjsip.ldif**. Cette **OU** servira à organiser les comptes SIP utilisés par Asterisk pour la ToIP.

```
GNU nano 7.2 ou_pjsip.ldif
dn: ou=pjsip,dc=tp,dc=local
objectClass: organizationalUnit
ou: pjsip
```

On ajoute dans LDAP deux comptes SIP (**cn=101** et **cn=102**) sous l'unité **ou=pjsip**. Ces comptes représenteront les postes téléphoniques ou softphones gérés par le serveur Asterisk.

```
phone1@phone:~$ ldapadd -x -D "cn=admin,dc=tp,dc=local" -W -H ldapi:/// -f peers.ldif
Enter LDAP Password:
adding new entry "cn=101,ou=pjsip,dc=tp,dc=local"

adding new entry "cn=102,ou=pjsip,dc=tp,dc=local"
```

On édite le fichier `/etc/asterisk/res_ldap.conf`

```
phone1@phone:~$ sudo nano /etc/asterisk/res_ldap.conf
```

- ◇ Ce fichier **res_ldap.conf** permet à Asterisk de se connecter au serveur LDAP situé à l'adresse **192.168.200.50** via le port 389 et le protocole LDAPv3. Il utilise le DN de liaison **ou=people,dc=tp,dc=local** avec le mot de passe *Passer123* pour s'authentifier.

- ◇ La configuration associe des identifiants LDAP à des objets SIP d'Asterisk : **ps_aors**, **ps_auths** et **ps_endpoints**. Ces sections définissent les paramètres des utilisateurs SIP comme les identifiants, le transport, le contexte d'appel, le mot de passe, et les codecs autorisés.

- ◇ Cela permet à **Asterisk** d'extraire dynamiquement les informations des comptes SIP depuis l'annuaire LDAP, simplifiant ainsi la gestion centralisée des utilisateurs téléphoniques.

```

[_general]
;
; Specify one of either host and port OR url. URL is preferred, as you can
; use more options.
;host=192.168.1.1 ; LDAP host
;port=389
;url=ldap://ldap3.mydomain.com:3890
;protocol=3 ; Version of the LDAP protocol to use; default is 3.
;basedn=dc=example,dc=tld ; Base DN
;user=cn=asterisk,dc=example,dc=tld ; Bind DN
;pass=MyPassword ; Bind password

host=192.168.200.50
port=389
protocol=3
basedn=ou=pjsip,dc=tp,dc=local
user=uid=asterisk,ou=people,dc=tp,dc=local
pass=Passer123

[ps_aors]
id=AstAorId
max_contacts=AstAorMaxContacts

```

```

[ps_auths]
id=AstAuthId
auth_type=AstAuthType
username=AstAuthUsername
password=AstAuthPassword

[ps_endpoints]
id=AstEndpointId
transport=AstEndpointTransport
aors=AstEndpointAors
auth=AstEndpointAuth
context=AstEndpointContext
disallow=AstEndpointDisallow
allow=AstEndpointAllow
direct_media=AstEndpointDirectMedia

```

On édite le fichier **extconfig.conf** pour indiquer à Asterisk d'utiliser LDAP comme source externe pour les informations de configuration.

```

phone1@phone:~$ sudo nano /etc/asterisk/extconfig.conf

```

On renseigne les modules SIP dans le fichier extconfig.conf pour que Asterisk utilise LDAP comme backend pour les **objets ps_endpoints, ps_auths et ps_aors**.

```

[settings]

ps_endpoints => ldap,"ou=pjsip,dc=tp,dc=local",ps_endpoints
ps_auths => ldap,"ou=pjsip,dc=tp,dc=local",ps_auths
ps_aors => ldap,"ou=pjsip,dc=tp,dc=local",ps_aors

```

On édite le fichier sorcery.conf pour activer l'utilisation de LDAP comme backend pour les modules SIP d'Asterisk.

```
$ sudo nano /etc/asterisk/sorcery.conf
```

On configure les sections **Sorcery** pour que les modules SIP d'Asterisk utilisent les données en temps réel stockées dans LDAP via les objets **ps_endpoints**, **ps_auths** et **ps_aors**.

```
[test_sorcery_section]
test=memory

[test_sorcery_cache]
test/cache=test
test=memory

[res_pjsip]
endpoint=realtime,ps_endpoints
auth=realtime,ps_auths
aor=realtime,ps_aors
```

On redémarre et lance l'interface en ligne de commande d'Asterisk pour vérifier et tester la configuration en temps réel.

```
phone1@phone:~$ systemctl restart asterisk
phone1@phone:~$ sudo rasterisk
```

On redémarre Asterisk directement depuis son interface CLI pour appliquer immédiatement toutes les modifications sans quitter l'interface.

```
phone*CLI> core restart now
phone*CLI>
Disconnected from Asterisk server
Asterisk cleanly ending (0).
Executing last minute cleanups
phone1@phone:~$ sudo rasterisk
```

On vérifie le statut de la connexion LDAP en temps réel depuis l'interface **Asterisk CLI**.

Cette commande confirme qu'Asterisk est bien connecté à l'annuaire LDAP, avec la base DN et l'utilisateur configurés, ce qui valide l'intégration LDAP pour la ToIP.

```
phone*CLI> realtime show ldap status
Connected to 'ldap://192.168.200.50:389', baseDN ou=pjsip,dc=tp,dc=local with username uid=asterisk,ou=people,dc=tp,dc=local for 26 seconds
phone*CLI>
```

On affiche la liste des **endpoints SIP** configurés dans Asterisk via LDAP.

Cette commande permet de vérifier que les comptes SIP (comme le 101) sont bien reconnus et actifs, prêts à recevoir ou passer des appels.


```

phone*CLI> pjsip show endpoints

Endpoint: <Endpoint/CID.....> <State.....> <
Channels.>
  I/OAuth: <AuthId/UserName.....>
.....>
  Aor: <Aor.....> <MaxContact>
  Contact: <Aor/ContactUri.....> <Hash....> <Status> <
RTT(ms)..>
  Transport: <TransportId.....> <Type> <cos> <tos> <BindAddress.....>
.....>
  Identify: <Identify/Endpoint.....>
.....>
  Match: <criteria.....>
  Channel: <ChannelId.....> <State.....> <
Time.....>
  Exten: <DialedExten.....> CLCID: <ConnectedLineCID.....>
=====
=====

Endpoint: 101                                     Unavailable 0

```

```

Endpoint: 101                                     Unavailable 0
of inf
  InAuth: 101/101
  Aor: 101                                     1
  Transport: transport-udp                     udp      0      0 0.0.0.0:5060

Endpoint: 102                                     Unavailable 0
of inf
  InAuth: 102/102
  Aor: 102                                     1
  Transport: transport-udp                     udp      0      0 0.0.0.0:5060

Objects found: 2

```

On édite le fichier de dialplan pour définir les extensions SIP 101 et 102. Chaque extension déclenche un appel vers le poste SIP correspondant via Dial(PJSIP/...).

On active l'enregistrement automatique de l'appel avec **MixMonitor** pour sauvegarder les fichiers audio, puis on termine l'appel avec **Hangup()**.

```

[testing]
;exten => 101,1,Dial(PJSIP/101)
;exten => 102,1,Dial(PJSIP/102)
exten => 101,1,Set(CALLFILENAME=${STRFTIME(${EPOCH},,%Y%m%d-%H%M%S)}-${CALLERID})
exten => 101,n,MixMonitor(/var/spool/asterisk/recordings/${CALLFILENAME}.wav)
exten => 101,n,Dial(PJSIP/101)
exten => 101,n,Hangup()

exten => 102,1,Set(CALLFILENAME=${STRFTIME(${EPOCH},,%Y%m%d-%H%M%S)}-${CALLERID})
exten => 102,n,MixMonitor(/var/spool/asterisk/recordings/${CALLFILENAME}.wav)
exten => 102,n,Dial(PJSIP/102)
exten => 102,n,Hangup()

```

On configure un softphone avec le **compte SIP 101**, le **mot de passe, aziz** comme **display name**, et le **domaine 192.168.30.10**. Le protocole UDP est utilisé pour le transport SIP.

Cela permet au softphone de se connecter et de s'authentifier sur le serveur Asterisk.

< @ Third-party SIP account

Username*

101

Password*

...

Domain*

192.168.30.10

Display name

aziz

Transport

UDP

Connection

On configure un second softphone avec le **compte SIP 102**, son **mot de passe, maguette** comme **display name**, et le **domaine 192.168.30.10**.

<

Third-party SIP account

Username*

102

Password*

...

Domain*

192.168.30.10

Display name

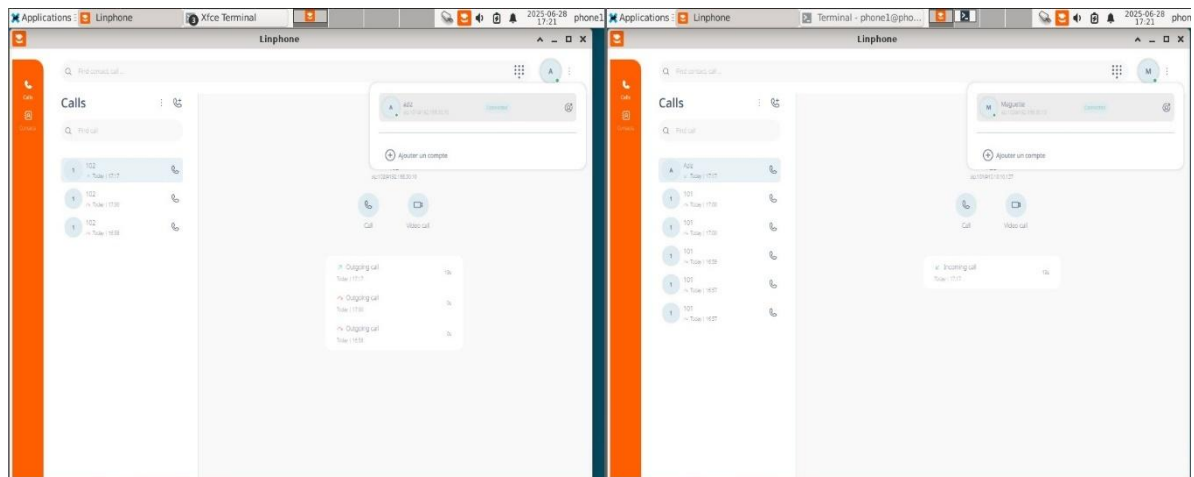
Maguette

Transport

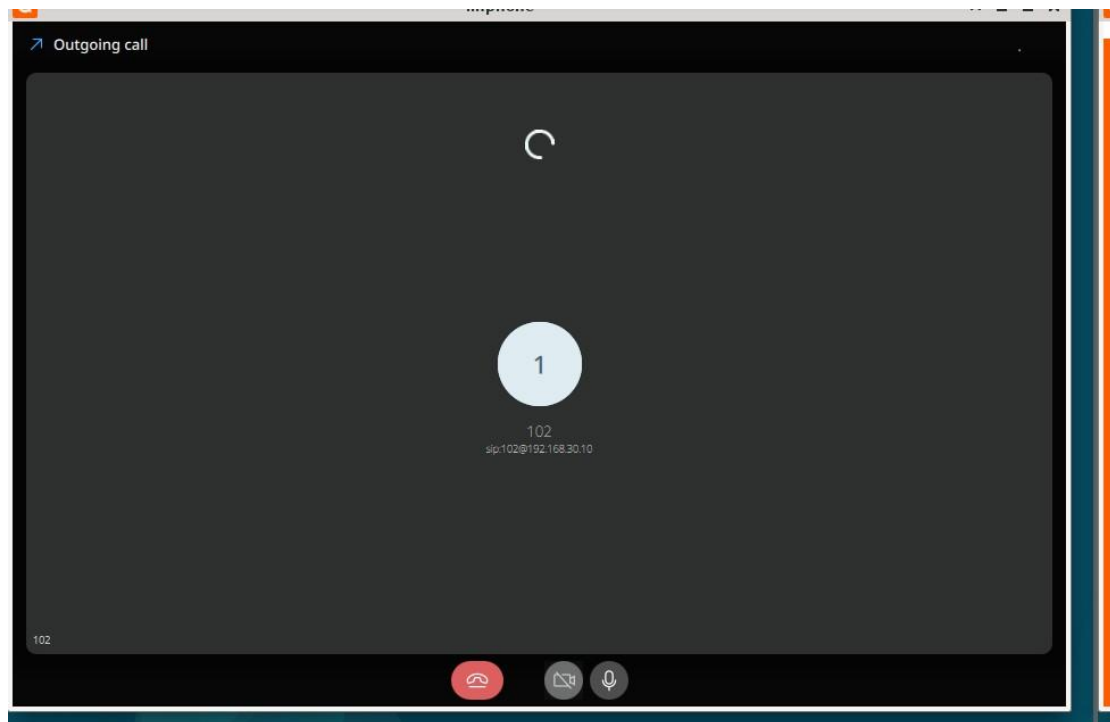
UDP

Connection

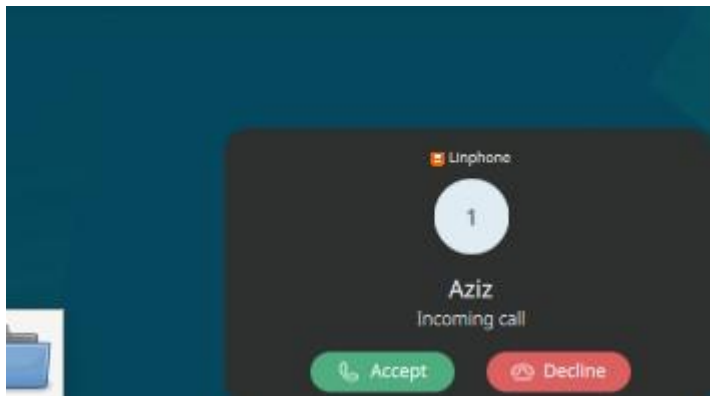
On voit ici deux interfaces qui affichent l'historique des appels des deux softphones Aziz et Maguette qui ont déjà tenté de se joindre avec les dates d'appels et l'heure d'appels .



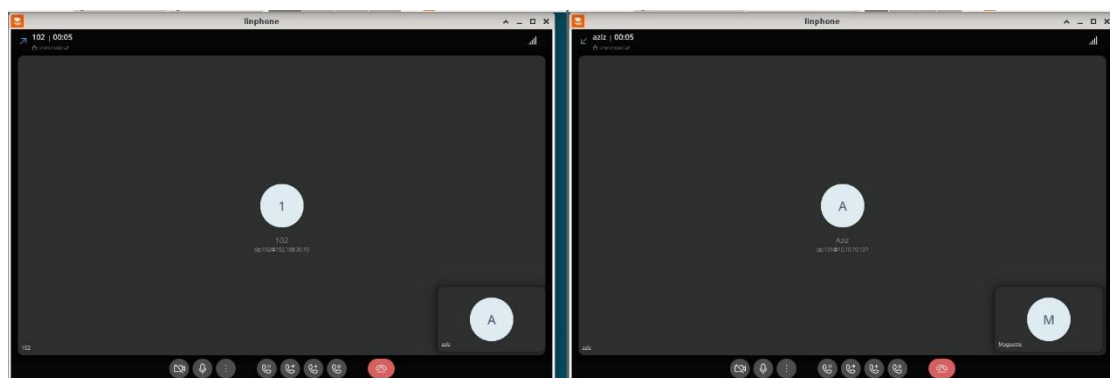
Le softphones (101) aziz essaye de joindre le softphones(102) Maguette .



On remarque que ca sonne au niveau du softphone 102 Maguette .



Ces deux interfaces montrent que l'appel a démarré dans les deux softphones après que Maguette a accepté l'appel d'Aziz .



On observe **les logs de l'appel** entre les extensions SIP. Asterisk démarre l'enregistrement avec MixMonitor dès que l'appel débute.

L'extension 102 a été jointe via le dialplan, puis l'appel s'est terminé normalement.
L'enregistrement est ensuite fermé et sauvegardé.
Cela confirme que le système ToIP fonctionne correctement avec enregistrement actif.

```
== Setting global variable 'CONSOLE' to 'Console/dsp'  
== Setting global variable 'TRUNK' to 'DAHDI/G2'  
== Setting global variable 'TRUNKMSD' to '1'  
== Begin MixMonitor Recording PJSIP/101-00000002  
== Spawn extension (testing, 102, 3) exited non-zero on 'PJSIP/101-00000002'  
== MixMonitor close filestream (mixed)  
== End MixMonitor Recording PJSIP/101-00000002
```

On vérifie que les enregistrements des appels ont bien été sauvegardés dans le dossier `/var/spool/asterisk/recordings/`.

```
phone1@Serveur-ToIP-Asterisk:~$ ls -l /var/spool/asterisk/recordings/  
total 1668  
-rw-r--r-- 1 root root 695404 Jun 28 17:53 20250628-175229-101-102.wav  
-rw-r--r-- 1 root root 1009004 Jun 28 17:59 20250628-175838-101-102.wav  
phone1@Serveur-ToIP-Asterisk:~$
```

On crée un nouveau fichier de mise à jour de schéma LDAP dans FreeIPA pour ajouter l'attribut personnalisé `astSIPHA1`, utilisé par Asterisk.

On copie le schéma LDAP personnalisé dans le dossier `/etc/ldap/schema/` afin qu'il soit reconnu par le serveur LDAP. Et on redémarre le service **slapd** pour appliquer les modifications et prendre en compte le nouveau schéma

```
phone1@phone:~$ sudo nano asterisk.ldap-schema  
phone1@phone:~$ sudo nano asterisk.ldif  
phone1@phone:~$ sudo cp asterisk.ldap-schema /etc/ldap/schema/  
phone1@phone:~$ sudo service slapd restart
```

On applique ensuite le nouveau schéma à l'annuaire avec `ipa-ldap-updater`. Cela permet à FreeIPA de reconnaître l'attribut `astSIPHA1` utilisé pour l'authentification SIP.

```
[user1@ipa ~]$ sudo tee /usr/share/ipa/updates/99-astSIPHA1.ldif > /dev/null <<  
'EOF'  
dn: cn=schema  
changetype: modify  
add: attributeTypes  
attributeTypes: ( 1.3.6.1.4.1.99999.1.1.1 NAME 'astSIPHA1' DESC 'HA1 SIP' EQUALI  
TY caseExactMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )  
EOF  
[user1@ipa ~]$ sudo ipa-ldap-updater --schema-file /usr/share/ipa/updates/99-ast  
SIPHA1.ldif  
Update complete  
The ipa-ldap-updater command was successful  
[user1@ipa ~]$
```

CONCLUSION :

La mise en œuvre de la ToIP a permis d'intégrer la téléphonie au sein de l'infrastructure réseau tout en s'appuyant sur l'annuaire LDAP.
Les appels entre postes fonctionnent correctement, avec enregistrement automatique

des communications pour un meilleur suivi.

Cette solution offre une flexibilité de gestion, une réduction des coûts et une sécurité accrue grâce à l'unification des identités.