IUT de La Rochelle

Université La Rochelle

- TP projet -
Serveur ToIP Asterisk

par [redacted] & Édouard Lumet

LA ROCHELLE

iut réseaux & télécoms

Sommaire

Introduction

Ce TP projet s'est étendu sur plusieurs séances. L'objectif final est de disposer d'un réseau téléphonique IP avec un serveur de téléphonie IP appelé serveur ToIP, de téléphones (hardphones) IP et de logiciels de téléphonie IP (softphones). Pour cela, nous devons mettre en place sur un réseau IP différents éléments :

- un serveur ToIP Asterisk sur Linux,
- un serveur DHCP et FTP sur Linux,
- un serveur mail Postfix/Dovecot sur Linux,
- un gestionnaire de base de données MySQL sur Linux,
- deux hardphones (6757i et GXV3140),
- un softphone (Jitsi sur la machine sur laquelle on travaille).

Les quatre serveurs seront sur des VMs Ubuntu Server séparées. On utilisera alors VirtualBox sur notre station de travail Windows.

Le plan d'adressage est le suivant :

Machine	Adresse IPv4	Masque	Gateway	DNS
Asterisk-Server	192.168.11.101	255.255.255.0	192.168.11.254	192.168.1.1 10.2.40.230
DHCP-FTP-Server	192.168.11.111	255.255.255.0	192.168.11.254	192.168.1.1 10.2.40.230
Mail-Server	192.168.11.121	255.255.255.0	192.168.11.254	192.168.1.1 10.2.40.230
MySQL-Server	192.168.11.131	255.255.255.0	192.168.11.254	192.168.1.1 10.2.40.230
			Extension	
Softphone Jitsi	192.168.11.201	255.255.255.0	3103	
Hardphone 6757i	192.168.11.211	255.255.255.0	3101	
Hardphone GXV3140	192.168.11.221	255.255.255.0	3102	

Nous devrons aussi mettre en place le « provisioning » des postes (déploiement automatique) avec un service FTP, un service DHCP pour l'attribution des adresses des postes, un service de messagerie électronique pour l'envoi des messages vocaux par email, un lien trunk-SIP pour se connecter à un autre serveur ToIP, un gestionnaire de base de données pour y conserver les configurations Asterisk, etc.

1. Configuration des paramètres réseau

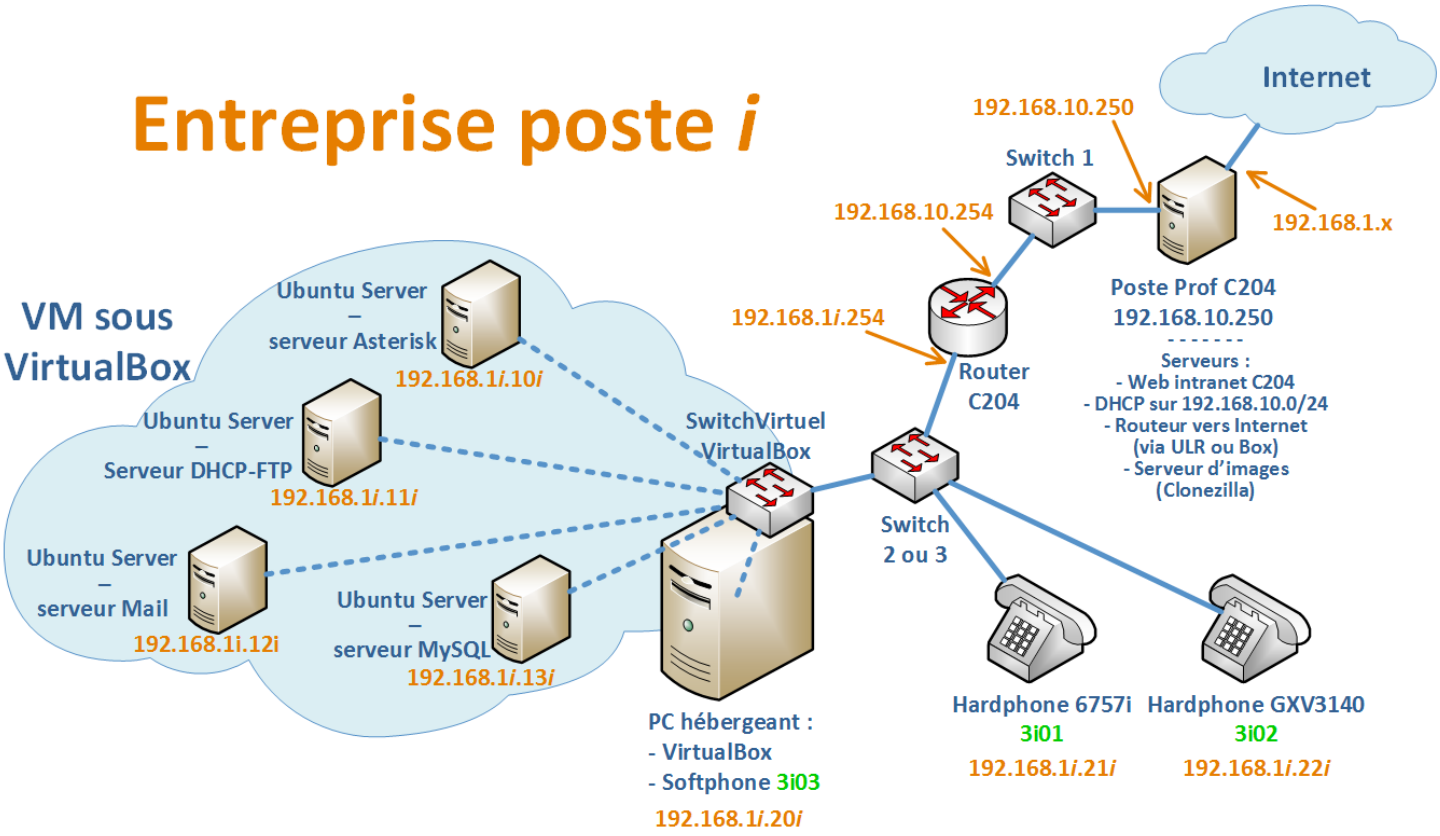
Étant au poste 1, nous avons connecté notre PC au switch 2. Nous disposons des ports 1 à 6 sur ce switch et du sous-réseau 192.168.11.0/24.

Notre machine a donc pour adresse 192.168.11.201/24 et pour passerelle 192.168.11.254.

2. VMs utilisées pour le projet

2.1. Schéma logique du réseau d'entreprise

Le schéma logique tel que décrit dans l'introduction est le suivant :



2.2. Plate-forme de virtualisation VirtualBox

VirtualBox est l'hyperviseur qui nous permettra d'utiliser des machines virtuelles (VMs) pour héberger les serveurs dont nous avons besoin. Nous les configurons en mode « accès par pont » (« bridge ») ce qui a pour effet de créer une connexion direct entre la carte virtuelle et la carte physique.

3. Configuration du serveur ToIP Asterisk

3.1. Configuration des paramètres réseau

- Le couple login/mdp de la VM Asterisk-Server est user/rtrt.
- On effectue une configuration réseau permanente en modifiant le fichier */etc/network/interfaces*.
- La vérification de l'application des paramètres réseau s'effectue principalement à l'aide de deux commandes : **ifconfig eth0** et **route -n** afin de vérifier l'adressage et la gateway (route par défaut).

3.2. Installation du serveur Asterisk

Après avoir mis à jour la liste des paquets et installer les dépendances nécessaires, on télécharge l'archive Asterisk.

Une fois l'archive extraite, on peut lancer la compilation (utilitaire make).

3.3. Démarrage du serveur Asterisk

Le démarrage du serveur Asterisk se fait à l'aide de la commande **asterisk -vvvvc**. Si le serveur est déjà en cours d'exécution, il suffit d'exécuter **asterisk -vvvvr** pour récupérer l'interface en ligne de commande (CLI) d'Asterisk.

Deux commandes sont intéressantes dans Asterisk : **reload** et **sip show peers**. Elles permettent respectivement de recharger la configuration Asterisk et de visualiser les machines liées à Asterisk via SIP (clients ou autres serveurs ToIP). Ctrl-C nous permet de quitter le CLI et d'arrêter Asterisk.

L'installation d'un serveur SSH (*openssh-server*) nous permettra de nous connecter à la VM Asterisk-Server via SSH à l'aide de TeraTerm et ainsi de disposer de plusieurs terminaux de notre serveur.

Des modifications préliminaires sont nécessaires pour préparer l'installation des téléphones IP. Dans le fichier */etc/asterisk/extensions.conf* on indique dans le contexte *[default]* que notre plan de numérotation est *[plan-num-prive]*. C'est dans le premier contexte que Asterisk cherche les correspondances pour les numéros composés. Il faut alors définir dans ce même fichier notre contexte *[plan-num-prive]*. C'est ici que nous ajouterons nos extensions 3101, 3102, etc.

4. Mise en service de clients ToIP

4.1. Mise en service du hardphone Aastra 6757i

Une fois alimenté, on effectue un redémarrage en configuration usine du téléphone. On désactive ensuite le DHCP. L'adresse est alors de type 169.154.x.x, ce qui correspond à une adresse déterminée par le téléphone lui-même puisqu'il n'a aucune configuration réseau.

En saisissant l'adresse IP du téléphone dans le navigateur web, on accède à l'interface web de celui-ci. On peut alors effectuer sa configuration réseau statique selon le plan d'adressage. Il faut bien évidemment avoir modifié l'adresse IP de notre PC au préalable afin d'être dans le même réseau que le téléphone.

Dans cette même interface, on peut configurer le nom du poste et, point essentiel, l'adresse et le port du serveur registrar, notre serveur ToIP.

La déclaration du poste se fait dans le fichier */etc/asterisk/sip.conf* de la VM Asterisk-Server. On crée alors un contexte portant le nom du poste soit *poste3101* pour ce premier hardphone. Un secret partagé permet de bénéficier d'une authentification sécurisée du poste auprès du serveur Asterisk (ici : 'rtrt'). Le contexte 'plan-num-prive' (créé dans la partie 3.3) que l'on déclare dans la définition du poste est le plan de numérotation suivi par ce poste.

Une fois ces configurations effectuées, on peut recharger la configuration d'Asterisk (**reload**) puis redémarrer le téléphone. La commande **sip show peers** nous montre alors que le poste 'poste3101' est associé au serveur Asterisk. En composant le 3999 sur le téléphone, on entend un message de bienvenue « Bonjour, bienvenue aux R&T de La Rochelle… ».

La ligne de code ajoutée est un scénario associé à une extension. On ajoute le numéro (ou extension) 3101 dans le plan de numérotation est on indique au serveur Asterisk ce qu'il doit faire. Ici, on indique qu'**en premier lieu** le serveur doit faire **sonner** le poste **SIP poste3101** pendant une **durée de 10 secondes**. Après avoir rechargé Asterisk, la commande **console dial 3101** permet d'effectuer un appel au 3101 depuis le serveur et par conséquent de vérifier que la configuration est correcte.

4.2. Mise en service du visiophone GXV3140

Ce visiophone sait également gérer le protcole SIP, il est donc compatible avec notre serveur Asterisk. En plus d'un téléphone classique, il faudra aussi nous intéresser, ultérieurement, aux codecs vidéo en plus des codecs audio si nous souhaitons exploiter les capacités vidéo de ce poste. Nous lui affecterons le n° d'abonné « 3i02 ».

Nous alimentons et connectons le GXV3140 à un port du switch appartenant à votre VLAN. Puis il faut aller dans « Menu > Settings > Maintenance > Upgrade » pour effectuer un reset usine (« Full Reset »).

Une fois redémarré, affecter les paramètres réseau dans « Menu > Settings > Network > Connection » :

- configuration IPv4 statique (non DHCP)

- @ IP : 192.168.11.221 ; masque : 255.255.255.0 ; passerelle : 192.168.11.254.

Nous redémarrons le téléphone (« Reboot » dans « Menu > Settings > Maintenance > Upgrade »), puis accédons depuis un navigateur au portail web embarqué dans le GXV3140 ; utiliser les identifiants « admin / admin ».

Dans les onglets « Account1 » et « Account3 », désactiver les comptes 1 et 3 (ne pas oublier de sauver...)

Dans l'onglet « Account2 », configurer le profil 2 comme ceci :

-Account Name : poste3102

-SIP Server : 192.168.11.101

-SIP User ID : poste3102

-Authenticate ID : poste3102

-Authenticate Password : rtrt

-Voice Mail UserID : (rien)

-Name : Poste de l'abonné 3102

-User ID is phone number : (non coché)

Effectuons maintenant côté serveur une configuration similaire à celle effectuée pour le téléphone précédent :

```
[poste3102]
type=friend
secret=rtrt
host=dynamic
context=default
disallow=all
allow=alaw
allow=ulaw
allow=gsm
dtmfmode=rfc2833
canreinvite=yes
language=fr
insecure = invite ; permet d<92>autoriser les ré-invitations entre terminaux
```

Nous avons ensuite redémarré Asterisk afin que les modifications faites soient prises en compte, puis nous avons redémarré le GXV3140.

On vérifie ensuite que l'ajout du téléphone a été pris en compte par le serveur Asterisk.

Nous composons le « 3999 » sur le téléphone et nous entendons un message similaire à celui que nous avions entendu dans la partie 4.1.

Il ne reste qu'à configurer le plan de numérotation du serveur afin de définir le n° d'abonné 3102 au GXV3140 :

```
exten => 3102,1,NoOp()
same => n,Dial(SIP/poste3102,10,tTxX)
same => n,GotoIf($["${DIALSTATUS}" = "BUSY"]?busy:unavail)
same => n(unavail),VoiceMail(3102@default,u)
same => n,Hangup()
same => n(busy),VoiceMail(3102@default,b)
same => n,Hangup()
```

Puis on recharge Asterisk et on teste le plan de numérotation depuis la console en utilisant la commande **console dial 3102**. On peut joindre correctement le GXV3140. Nous pouvons également tester que la communication fonctionne entre les postes d'abonnés 3101 et 3102.

4.3. Mise en service du softphone

Il est aussi possible de connecter sur le réseau téléphonique privé des téléphones logiciels, appelés softphones. Nous allons donc installer un softphone sur votre PC physique. Différents softphones existent, notamment X-Lite ou encore Jitsi. Ce dernier a l'avantage de permettre les communications vidéo, alors que X-Lite ne le propose pas dans sa version gratuite. Nous allons ainsi choisir d'installer le softphone gratuit Jitsi, projet communautaire LGPL de jitsi.org :

Pour cela il faut télécharger le logiciel Jitsi sur le site de Jitsi (jitsi.org) et l'installer sur votre PC physique (sous OS Windows 8.1). Pour configurer correctement Jitsi avec le n° d'abonné 3103 :

fermer la fenêtre « S'identifier », et dans la fenêtre principale, aller dans « Fichier > Ajouter un nouveau compte » et choisir le protocole Réseau « SIP » ; cliquer sur « Avancé », et remplir les champs suivants :

-Identifiant SIP : poste3i03

-Mot de passe : rtrt

-Nom affiché : poste 3103

-Registrar : 192.168.11.101

-Port : 5060

-Nom d'autorisation : poste3103

Déclarons maintenant le softphone sur le serveur :

Il faut explicitement les changements à réaliser dans « sip.conf » afin d'inscrire le softphone sur votre réseau téléphonique privé ; (« dtmfmode » configuré en « rfc2833 »).

Puis on redémarre Asterisk et le softphone. Afin de vérifier que l'ajout du softphone a été pris en compte par le serveur Asterisk. Ensuite, nous branchons un casque, et nous composons le « 3999 » sur le softphone. Nous pouvons entendre un message de bienvenue.

Nous configurons le plan de numérotation pour lui affecter le n° d'abonné 3103 :

Il faut modifier le fichier */etc/asterisk/extensions.conf* pour affecter le n° d'abonné 3103 à ce poste.

Nous rechargeons Asterisk puis nous testons le plan de numérotation depuis la console en utilisant la commande **console dial 3103**.

Puis nous testons dans les 2 sens les appels entre les abonnés 3101, 3102 et 3103 pour vérifier que le fonctionnement soit correct, ce qui est le cas.

5. Serveur de temps NTP

Afin de synchroniser l'horloge des téléphones, nous allons installer un serveur de temps sur la VM exécutant Asterisk.

Un serveur NTP est un serveur de temps (Network Time Protocol). Installer un serveur de temps NTP en réseau permet d'avoir une machine, et surtout un serveur, toujours à l'heure. Si un serveur reste allumé sans rebooter pendant des mois ou des années il va finir par être décalé avec l'heure réelle.

Sur la VM hébergeant Asterisk, nous allons mettre à jour la liste des paquets et installer NTP en utilisant les commandes : **apt-get update** et **apt-get install ntp**.

Puis nous avons ouvert le fichier */etc/ntp.conf* permettant de configurer le serveur NTP, et modifier la liste des serveurs de temps afin que ceux servant de référence soient :

-server 0.fr.pool.ntp.org

-server 1.fr.pool.ntp.org

-server 2.fr.pool.ntp.org

-server 3.fr.pool.ntp.org

Puis on va mettre en commentaire « server ntp.ubuntu.com » pour que cette configuration ne soit plus prise en compte.

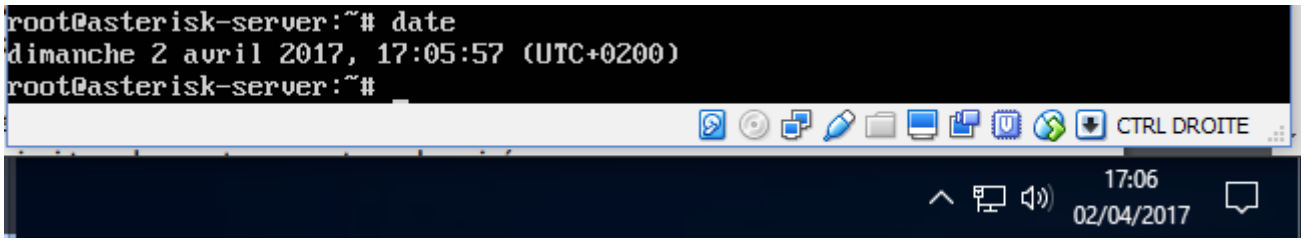
Nous avons limité également l'accès au serveur NTP (port 123) uniquement aux clients NTP de votre LAN avec la commande suivante :

« restrict 192.168.11.0 mask 255.255.255.0 »

Puis pour diagnostiquer le bon état de notre serveur, nous avons interrogé les serveurs qui ont servi de source de temps, et leur niveau dans la strate des serveurs permettant la définition au plus juste du temps :

```
root@asterisk-server:~# ntpq -p
No association ID's returned
```

Puis on vérifie la date :



On peut observer que tout est normal.

Nous allons configurer nos hardphones pour se servir du serveur NTP de votre VM comme référence de temps ; ainsi tous les postes seront synchronisés :

Pour le 6757i : appuyer sur la clé, puis > 2-Préférences > 6-Time and Date : > 4-Time : Zone : Bruxelles => appuyer sur Done > 5-Time Server 1 : adresse_IP_asterisk_server => Done

Sortir des menus : le temps doit maintenant être correctement affiché sur le poste.

Pour le GXV3140 : > Menu > Settings > Time : NTP server : 192.168.11.101 / Time Zone : GMT+01 => appuyer sur Save et sortir. L'heure doit être affichée correctement sur l'écran.

6. Observations des trames générées

6.1. Enregistrement d'un poste IP sur le serveur

6.2. Initialisation et fermeture d'une communication

6.3. Transport de la voix pendant une communication

6.4. Écoute de conversations

6.5. Sécurisation des flux

7. Déploiement automatique des postes

Nous allons voir comment améliorer le déploiement des hardphones IP car la configuration manuelle poste par poste deviendrait ingérable dès que le nombre de postes devient important. Pour gagner du temps, nous allons nous intéresser uniquement au déploiement des postes 6757i ; le déploiement d'un autre type de postes (les GXV3140 par exemple) se ferait selon un processus identique, il n'y a donc aucun intérêt à le faire deux fois.

Le déploiement automatique (auto-provisioning) de postes se base sur l'utilisation de :

- un serveur DHCP pour fournir automatiquement les paramètres IP aux téléphones et l'adresse du serveur FTP ou TFTP qu'ils devront utiliser

- un serveur FTP ou TFTP pour que les postes IP viennent chercher leur firmware (éventuellement, en cas de mise à jour du firmware des postes déployés), et leur fichier de configuration contenant les paramètres propres à chaque téléphone. Ici en l'occurrence, nous aurons besoin d'un serveur FTP pour les postes 6757i.

7.1. VM hébergeant les services DHCP et FTP

Nous allons nous intéresser maintenant à une 2ème VM, la VM « M4205-DHCP-FTP-Server » qui devra héberger les serveurs DHCP et FTP.

Npus démarrons la VM DHCP-FTP-Server, et l'on s'identifie avec « user/rtrt », puis on modifie le nom de la machine contenu dans le fichier */etc/hostname* en « M4205-DHCP-FTPServer.postei.c204.rtlr ». Puis on redémarre notre VM avec **shutdown -r now**.

Ensuite comme pour la VM Asterisk-Server, on configure la carte réseau eth0 de la VM da façon permanente en allant dans *etc/network/interfaces* et en mettant « 192.168.11.111 » comme adresse IP.

7.2. Consultation des docs techniques Aastra

Pour la réalisation de ce déploiement automatique, la consultation des documents constructeurs des postes IP est fondamentale. En l'occurrence ici, le document « AMT_PTD_TR_0014_7_1_FR.pdf » disponible sur l'extranet d'Aastra (et dans les annexes du serveur Intranet de la salle) donne des indications sur le déploiement des postes 6757i.

7.3. Installation et configuration du serveur DHCP

Nous allons installer sur la VM « DHCP-FTP-Server » le serveur « isc-dhcp-server ».

Pour cela nous faisons un **sudo apt update** pour mettre à jour la liste des paquets puis nous installons le serveur en utilisant la commande suivante : **apt get install isc-dhcp-server**.

Puis nous commençons la configuration du serveur DHCP en sélectionnant l'interface sur laquelle le serveur devra écouter et distribuer des adresses IP :

on indique dans le fichier */etc/default/isc-dhcp-server* sur l'interface d'écoute soit : « INTERFACES="eth0" »

La configuration du service DHCP se fait dans le fichier dans */etc/dhcp/dhcpd.conf*, en utilisant notamment des options (paramètres) définis tels que dans le tableau présenté ici : http://www.ipamworldwide.com/ipam/isc-dhcpv4-options.html .

La configuration DHCP peut être très différente selon les besoins. Différents comportements peuvent être souhaités :

- dans certaines installations, on ne souhaite adresser aucune @ IP à des inconnus, et seules les cartes réseau d'@ MAC connues et déclarées se verront attribuer une @ IP qui peut être réservée (fixe) ; la config ci-dessous en est un exemple :

```
subnet 192.168.18.0 netmask 255.255.255.0 {
        default-lease-time 21600;
        max-lease-time 21600;
        # option 3 :
        option routers                  192.168.18.254;
        # option 1 :
        option subnet-mask              255.255.255.0;
        # option 28 :
        option broadcast-address        192.168.18.255;
        # option 6 :
        option domain-name-servers      192.168.1.1, 10.1.30.24;
        # option 42 :
        option ntp-servers              192.168.18.108;
        # option 66 :
        option tftp-server-name         "192.168.18.118";

        host 6757i-bureauB101 {
                hardware ethernet A1:B1:C1:D1:E1:F1;
                fixed-address 192.168.18.50;
        }
        host 6757i- bureauB102 {
                hardware ethernet A2:B2:C2:D2:E2:F2;
                fixed-address 192.168.18.51;
        }
        ...
}
```

-dans d'autres installations, on préférera ne pas figer les @IP sur les @MAC des postes si on estime que la tâche de suivi des @MAC est trop « lourde » ; on peut alors se baser sur l'utilisation d'un paramètre émis par les équipements lors d'une demande d'attribution d'adresse : le « vendor-class-identifier » ; dans ce cas, un pool d'adresses IP est réservé pour tous les équipements de même « vendor-classidentifier », et dans ce cas, pas besoin de gérer le suivi des @ MAC des téléphones. La config ci-dessous en est un exemple :

```
class "hardphonesIPAastra" {
        match if substring (option vendor-class-identifier, 0, 8) = "AastraIP" ;
}

subnet 192.168.18.0 netmask 255.255.255.0 {
        default-lease-time 21600;
        max-lease-time 21600;
        # option 3 :
        option routers                  192.168.18.254;
        # option 1 :
        option subnet-mask              255.255.255.0;
        # option 28 :
        option broadcast-address        192.168.18.255;
        # option 6 :
        option domain-name-servers      192.168.1.1, 10.1.30.24;
        # option 42 :
        option ntp-servers              192.168.18.108;
        # option 66 :
        option tftp-server-name         "192.168.18.118";

        pool {
                allow members of "hardphonesIPAastra";
                range 192.168.18.50 192.168.18.99;
        }
}
```

Puis en nous inspirant de l'exemple précédent, nous avons ajouté un bloc pour notre sous-réseau dans */etc/dhcp/dhcpd.conf* en respectant les consignes suivantes :

-o délivrance d'une @ IP uniquement aux équipements 6757i, membres d'une classe « 6757i », qui effectue une discrimination sur le « vendor-classidentifier » complet défini pour les 6757i (voir les extraits des docs constructeurs données pages précédentes, où le 'x' sera à remplacer par un '7'). Pool d'adresses disponibles : 192.168.11.211 à 192.168.11.219

```
class "6757i" {
        match if substring (option vendor-class-identifier, 0, 16) = "AastraIPPh
one57i";
}
#
option space Connexio-57i;
option Connexio-57i.cfg-server-address code 2 = string;
#
subnet 192.168.11.0 netmask 255.255.255.0 {
        default-lease-time 21600;
        max-lease-time 21600;
        option routers 192.168.11.254;
        option subnet-mask 255.255.255.0;
        option broadcast-address 192.168.11.255;
        option domain-name-servers 192.168.1.1;
        option ntp-servers 192.168.11.101;
        option tftp-server-name "192.168.11.111";
```

```
# range 192.168.11.211 192.168.11.219;
        pool {
                allow members of "6757i";
                range 192.168.11.211 192.168.11.219;
                if substring(option vendor-class-identifier,0,16) = "AastraIPPho
ne57i" {
                        option server.vendor-option-space Connexio-57i;
                        option Connexio-57i.cfg-server-address "ftp://posteip:Aa
stra6757i@192.168.11.111";
                }
        }
}
~
```

Puis nous avons la possibilité, de vérifier la syntaxe de notre fichier de configuration avec la commande suivante, et le cas échéant, corriger nos erreurs avec la commande **dhcp -t**.

Mais dans notre cas, comme indiqué dans les docs Aastra, les postes Aastra 6757i ne sont pas conçus pour utiliser un serveur TFTP, mais un serveur FTP ; l'option 66 classiquement utilisée n'est donc pas suffisante, il faut alors rajouter une option non standardisée, pour renseigner un champ propre au concepteur du téléphone. Pour cela, nous allons utiliser l'option « 43 » :

Aastra utilise FTP et non pas TFTP puisque FTP utilise TCP, ce qui augmente la fiabilité. L'option 43 est l'option spécifique vendeur, elle permet d'indiquer le serveur fournissant la configuration. En cas de TFTP, on emploie l'option 66 en indiquant seulement l'adresse IP. Ici, il faut indiquer le protocole, le nom d'utilisateur, le mot de passe et l'adresse du serveur.

On redémarre notre serveur DHCP avec la commande **service isc-dhcp-server restart**.

Tout semble maintenant opérationnel côté serveur DHCP. Les postes 6757i vont recevoir les informations nécessaires pour savoir comment se connecter à leur serveur FTP.

7.4. Configuration du serveur FTP

Nous allons utiliser le serveur FTP Pure-ftp. Tout d'abord nous allons installer le paquet **sudo apt install pure-ftpd** sur la VM DHCP-FTP-Server.

Nous allons créé l'utilisateur/groupe système avec lequel le serveur FTP sera lancé :

- **groupadd ftpgroup**

- **useradd -g ftpgroup -d /dev/null -s /usr/sbin/nologin ftpuser**

L'ensemble des fichiers de configuration de Pure-ftpd se trouve dans le répertoire */etc/pureftpd/*.

Nous avons ensuite activé l'authentification liée à Pure-FTP (création d'un lien symbolique pour activer l'authentification des utilisateurs virtuels) :

ln -s /etc/pure-ftpd/conf/PureDB /etc/pure-ftpd/auth/

Puis nous créons un dossier pour l'utilisateur virtuel « posteip », l'affecter à l'utilisateur/groupe du serveur FTP (pour ne pas le laisser en root/root), puis lui créer un compte avec le même mot de passe que celui déclaré sur le serveur DHCP :

- **mkdir -p /home/ftp/posteip**

- **chown -R ftpuser:ftpgroup /home/ftp/posteip**

- **pure-pw useradd posteip -u ftpuser -g ftpgroup -d /home/ftp/posteip**

La dernière commande renseigne le fichier */etc/pure-ftpd/pureftpd.passwd* avec le nouvel utilisateur de Pure-ftp ; vous pouvez d'ailleurs consulter son contenu avec la commande **cat**. Enfin il faut transformer ce fichier dans un format sécurisé et lisible par le serveur FTP */etc/pure-ftpd/pureftpd.pdb*.

Puis nous régénérons les fichiers des utilisateurs : **pure-pw mkdb**.

NB : cette commande est à exécuter après chaque modification ou rajout d'utilisateur afin de régénérer le fichier des utilisateurs.

Ensuite nous allons redémarrer notre serveur FTP pour que la configuration soit prise en compte **service pure-ftpd restart**.

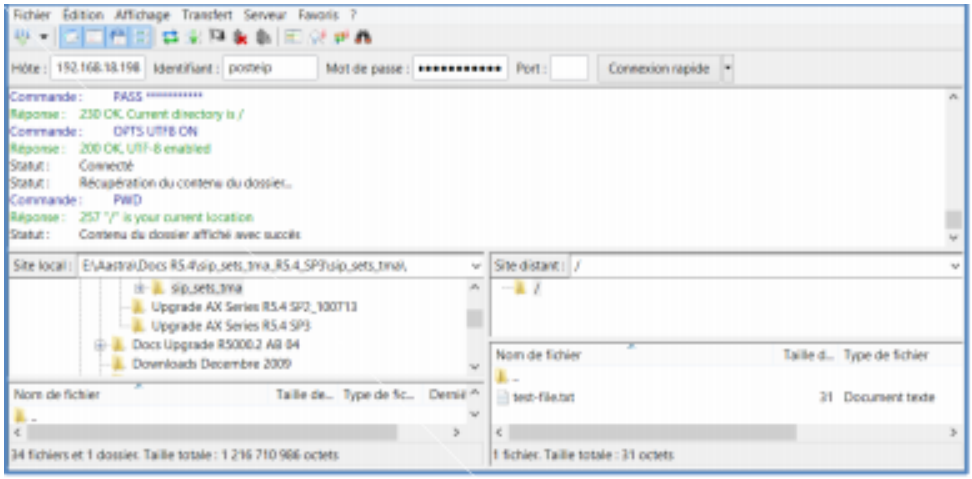
On vérifie la liste des utilisateurs ayant un compte sur ce serveur FTP : **pure-pw list** :

```
root@M4205-DHCP-FTP-Server:~# pure-pw list
posteip                 /home/ftp/posteip/./
```

Avant de tester si tout ce que nous venons de faire va fonctionner avec les téléphones, testons une connexion sur le serveur depuis le client Filezilla installé sur le PC physique.

Nous allons créer un fichier texte et le placer dans le dossier FTP de l'utilisateur « posteip ».

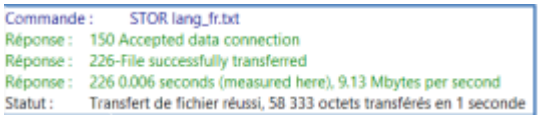
Puis nous allons tenter une connexion avec Filezilla depuis le PC physique avec les identifiants « posteip » / « Aastra6757i » :



La connexion fonctionne et on peut voir les fichiers. On peut également les télécharger.

Puis nous testons également l'envoi d'un fichier depuis votre PC vers le serveur FTP pour vérifier que le transfert est possible (et donc que le droit en écriture est correctement configuré, même si cela n'est pas nécessaire pour notre configuration).

Maintenant que nos 2 serveurs fonctionnent, il ne reste plus qu'à nous intéresser aux fichiers nécessaires pour le provisioning (déploiement) des postes 6757i :



7.5. Préparation des fichiers de provisioning

Les postes 6757i vont venir consulter le serveur FTP pour rechercher notamment :

- la présence firmware, pour le cas échéant se mettre à jour automatiquement,

- la présence d'un fichier de configuration contenant des paramètres globaux ou personnalisés par adresse MAC,

- la présence de fichiers sons, en langue française par exemple, personnalisés ou non.

Les formats des fichiers utilisés par les 6757i pour le provisioning sont les suivants :

- firmware : « 57i.st »,

- fichier de configuration global des postes : « aastra.cfg »,

- fichier de configuration spécifique à un poste : « @MAC.cfg » (ex:00085D3A2451.cfg)

- fichiers pack langue: lang__.txt ou lang_.txt (ex: lang_fr_ca.txt ou lang_de.txt)

Puis on récupère ces fichiers sur l'intranet de la C204 (dans les documents Annexes) ; consulter leur contenu.

On place déjà les 2 fichiers que nous n'avons pas besoin de modifier « 57i.st » et « lang_fr.txt » sur le serveur FTP.

Puis on a ouvert le fichier « aastra.cfg » et nous avons effectué les ajouts ou modifications suivants les les paramètres du serveur ToIP soient automatiquement renseignés lors du provisioning pour n'importe quel poste 6757i :

time server1: 192.168.11.101

sip line1 proxy ip: 192.168.11.101

sip line1 proxy port : 5060

sip line1 registrar ip: 192.168.11.101

sip line1 registrar port : 5060

Le fichier précédent est un fichier standard, qui sera exploité par les hardphones 6757i qui n'auront aucun fichier de configuration personnalisé.

Mais nous allons aussi créer maintenant un fichier personnalisé pour notre poste 6757i afin qu'il soit téléchargé lors du démarrage, et qui renseignera les paramètres personnels que le poste doit prendre. Nous allons ainsi directement préciser à chaque poste, en se basant sur leur @MAC, leur paramètres globaux ainsi que leur identité propre (nom d'abonné, n° d'abonné, nom à afficher, password...) :

Puis nous avons ouvert le fichier « MAC_57i.cfg » et nous l'avons sauvegardé sous le nom de l'@ MAC de votre 6757i (lettres en majuscules !), avec l'extension « .cfg » (ex : « A1B2C3D4E5F6.cfg ») ; y effectuer ensuite les ajouts ou modifications suivants :

time server1 : 192.168.11.101

sip line1 proxy ip : 192.168.11.101

sip line1 proxy port : 5060

sip line1 registrar ip : 192.168.11.101

sip line1 registrar port : 5060

sip screen name: "poste 3i01"

sip user name: poste3i01

sip line1 user name: poste3i01

sip line1 auth name: poste3i01

sip line1 password: rtrt

sip line1 screen name 2: " "

#sip line2 user name:

#sip line2 screen name: " "

topsoftkey5 value: http://192.168.1i.10i/annuaire/i5xi.php

Ainsi, les hardphones IP téléchargeront préférentiellement :

- soit leur fichier spécifique portant le nom de leur @ MAC

- soit le fichier généraliste « aastra.cfg », dans le cas où aucun fichier ne portant leur @ MAC n'est présent sur le serveur FTP.

Puis nous plaçons sur le serveur FTP vos 2 fichiers modifiés *aastra.cfg* et *notre@MAC.cfg*.

7.6. Test du provisoning du 6757i

8. Mise en place d'appels visio

9. Fonctionnalités et services sous Asterisk

9.1. Renvoi d'appels sur non-réponse

Comme nous l'avons vu au début du TP, lorsque nous déclarons des extensions dans le fichier */etc/asterisk/extensions.conf* on précise pour le scénario un numéro d'ordre. Ce numéro sert à définir plusieurs actions à effectuer dans un ordre défini lorsque l'on compose un numéro.

On peut alors définir un renvoi d'appel vers un autre poste en guise de seconde action. Si on ajoute un autre renvoi d'appel vers le numéro originel comme troisième action, on crée alors une boucle jusqu'à ce que l'un des deux réponde.

9.2. Groupement d'abonnés

Un groupement d'abonnés correspond à une extension nous permettant d'appeler un groupe de postes. L'extension 3110 est un groupement formé des abonnés 3101 et 3102 :

```
exten => 3110,1,Dial(SIP/poste3101&SIP/poste3102)
```

Les deux postes sonnent alors simultanément.

~~9.3. Services accessibles depuis des touches programmées sur les postes IP~~

9.4. Services par composition de suffixes

9.4.1. Transfert d'appel

Le transfert d'appel est une fonctionnalité couramment utilisée permettant de transférer un appel vers un autre poste abonné. Pour activer cette fonctionnalité, il suffit d'ajouter 'tT' après le délai d'attente dans le scénario.

Dans le fichier */etc/asterisk/features.conf*, le paramètre *transferdigittimeout* est le timer correspondant à la durée maximale entre chaque numéro composé lorsque l'on compose un numéro lors du transfert par exemple.

~~9.4.2. Interception d'appel~~

~~9.4.3. Enregistrement de conversation~~

~~9.4.4. Mise en attente d'appels (parcage), musique d'attente~~

~~9.5. Mise en place de conférences~~

~~9.6. Distribution automatique des appels~~

9.7. Messagerie vocale, messagerie unifiée

9.7.1. Messagerie vocale classique

Le fichier de configuration */etc/asterisk/voicemail.conf* permet de paramétrer la messagerie vocale. Il faut y déclarer une boite vocale par poste en indiquant un mot de passe et optionnellement un prénom, nom, une adresse mail et diverses options.

Il faut ensuite modifier le plan de numérotation en ajoutant dans le scénario de chaque extension la redirection vers la boite vocale en cas de non réponse par exemple.

On distingue alors deux cas : "busy" et "unavailable". "busy" signifie "occupé", le poste appelé est alors déjà en ligne. "unavailable" signifie "non disponible", le poste appelé est alors déconnecté ou hors réseau.

Pour que chaque abonné puisse consulter sa messagerie, il faut créer une extension que l'abonné appellera et renverra alors vers la messagerie. En appelant cette extension, on accède alors à la messagerie et il nous est demandé de saisir notre numéro puis notre mot de passe.

La messagerie unifiée est une fonctionnalité de messagerie vocale qui intègre l'envoi d'une notification de l'arrivée d'un nouveau message vocal par email. Il est également possible de recevoir ledit message en pièce jointe.

9.7.2. Configuration de la VM dédiée à la messagerie

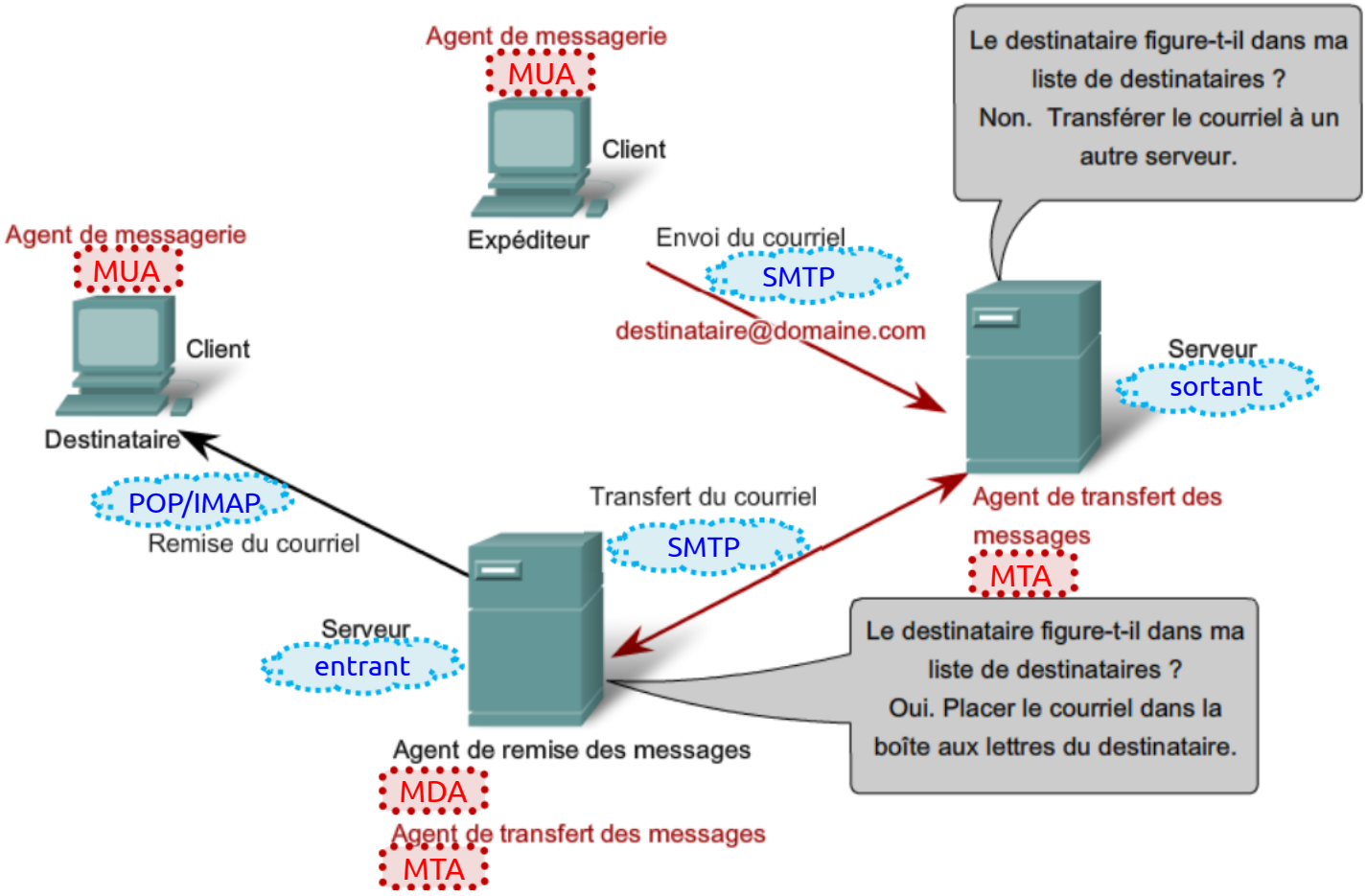
MUA signifie Mail User Agent. C'est l'élément qui permet de consulter et de rédiger de nouveaux messages. C'est un logiciel type Thunderbird par exemple.

MTA signifie Mail Transfer Agent. C'est le serveur qui transfère les mails lors de l'envoi notamment, vers son MTA.

MDA signifie Mail Delivery Agent. C’est le serveur qui délivre les mails au MUA, soit le serveur de réception.

Le protocole SMTP (Simple Mail Transfer Protocol) est celui utilisé pour l’envoi de mails entre le MUA et le MTA mais également entre deux MTA. Le numéro de port réservé est 25 ou 465 (sécurisé).

Concernant la livraison d’emails, il existe les protcoles POP (Post-Office Protocol) et IMAP (Internet Message Access Protocol). Les numéros de ports réservés sont respectivement 110 et 143 ou 995 et 993 (sécurisé).



9.7.3. *Installation basique de Postfix*

Pour l'envoi de mails, Postfix utilise le protocole SMTP.

On crée un domaine *poste1.c204.rtlr* qui sera notre nom de courrier. Sur la VM Asterisk-Server, on ajoute alors dans le fichier */etc/hosts* le nom de la machine ainsi que son adresse IP.

10. Connexion externe – Trunk SIP

SIP est de loin le plus populaire des protocoles VoIP. C'est un protocole peer-to-peer, et il n'y a pas vraiment de spécificités formelles pour réaliser un trunk en SIP ; si on connecte un seul téléphone à son serveur ou si on réalise une connexion entre deux serveurs, les connexions SIP seront similaires. Les trunks SIP sont réalisés dans 2 cas principalement :

- besoin d'interconnecter les serveurs ToIP de 2 sites distants d'une même entreprise (maison mère et succursale)

- connecter son réseau privé au serveur de son fournisseur d'accès au réseau téléphonique public (SIP provider). Nous allons réaliser les 2 possibilités.

10.1. Interconnexion de 2 serveurs SIP privés

Nous allons réaliser un trunk entre votre serveur Asterisk et celui d'un autre binôme, afin de réaliser un pseudo-réseau unique, où il sera possible d'appeler un poste du site distant en composant simplement les 4 chiffres internes du n° de poste visé. Puis dans */etc/asterisk/sip.conf*, il faut modifier pour les 3 postes le champ context en « default » au lieu de « plan-num-prive ».

Puis il faut former des binômes avec un autre groupe. La mise en place du trunk SIP va reposer ici sur une configuration symétrique de la liaison sur les 2 serveurs Asterisk. Dans les instructions suivantes, les paramètres j et k feront référence aux numéros de binômes qui réaliseront le trunk ; vous devrez les remplacer par les n°de binômes (1 à 6) correspondants. Sur notre VM Asterisk-Server, dans */etc/asterisk/sip.conf*, on crée le profil SIP suivant :

```
[serverj]
; Specify the SIP account type as 'peer'. This means that incoming
; calls will be matched on IP address and port number. So, when Asterisk
; receives a call from 192.168.1k.10k and the standard SIP port of 5060,
; it will match this entry in sip.conf. It will then request authentication
; and expect the password to match the 'secret' specified here.
type = peer
; This is the IP address for the remote box (serverk). This option can also
; be provided a hostname.
host = 192.168.17.107
; When we send calls to this SIP peer and must provide authentication,
; we use 'serverj' as our default username.
defaultuser = serverj
; This is the shared secret with serverk. It will be used as the password
; when either receiving a call from serverk, or sending a call to serverk.
secret = rtrt
; When receiving a call from serverk, match it against extensions
; in the 'plan-num-prive' context of extensions.conf.
context = plan-num-prive
; Start by clearing out the list of allowed codecs.
disallow = all
; Allow the alaw and gsm codecs
allow = gsm
allow = alaw
```

Nous vérifions ensuite avec la c la commande « sip show peers » que le lien SIP avec le serveur distant est bien déclaré.

Il nous reste à configurer le plan de numérotation pour tenir compte du fait qu'il faille rediriger les appels pour les n° d'abonnements distants vers le trunk SIP :

10.2. Connexion à un fournisseur SIP

Lorsqu'on s'inscrit à un fournisseur SIP (SIP provider), on dispose alors d'un service d'envoi et de réception d'appels téléphoniques publics.

La configuration peut légèrement différer en fonction du fournisseur SIP qui, logiquement, fournit les paramètres nécessaires et parfois des exemples de configuration d'Asterisk pour nous aider à se connecter plus facilement.

Afin de pouvoir recevoir des appels, le provider aura probablement besoin que notre serveur s'enregistre auprès de l'un de ses serveurs.

Nous allons aujourd'hui avoir recours à un abonnement chez le prestataire SIP « RTLR TELECOM » très économique , aux caractéristiques suivantes :

-@ IP serveur : 192.168.10.251

-login / mot de passe : postei / passwordi

-service « plutôt restreint », limité aux n° suivants :

N° poste de travail	n° internes	n° publics (entête + SDA)
1	31xx	05 46 01 31 xx
2	32xx	05 46 02 32 xx
3	33xx	05 46 03 33 xx
4	34xx	05 46 04 34 xx
5	35xx	05 46 05 35 xx
6	36xx	05 46 06 36 xx
7	37xx	05 46 07 37 xx

Pour que notre serveur puisse se connecter au provider SIP, il nous faut ajouter une ligne d'enregistrement :

dans la section [general] de */etc/asterisk/sip.conf* la ligne suivante :

register =>poste7:rtrt@192.168.10.251

Les systèmes à contrôle centralisé ont une architecture de tableau noir tandis que ceux à contrôle distribué ont une architecture multi-agents.

Les systèmes du premier type sont moins concernés par les problèmes de communication que par les problèmes de contrôle, tandis que cela s'inverse pour les systèmes du second type. Une ré-invitation permet de changer dynamiquement les paramètres d'une session.

Puis on rajoute à nos profils [poste3101], [poste3102], ... le paramètre suivant :

insecure = invite ; permet d'autoriser les ré-invitations entre terminaux ; finaux (NB : le paramètre « canreinvite » est normalement déjà à « yes »)

Puis on crée également dans « sip.conf » un profil de type « peer » pour votre provider :

```
[mon-provider-sip]

type = peer host = 192.168.10.251

defaultuser = poste1

secret = password1

insecure = invite

context = appels-entrants

dtmfmode = rfc2833

disallow = all

allow = alaw

allow = gsm

deny = 0.0.0.0/0

permit = 192.168.10.251/32
```

Puis on exécute la commande « sip show registry » pour consulter si l'enregistrement auprès du provider SIP s'est bien déroulé.

Maintenant que le compte a été défini, il reste à configurer dans */etc/asterisk/extensions.conf* le plan de numérotation pour nous permettre d'envoyer des appels via le provider SIP, ici sans avoir besoin de composer le 0 pour indiquer qu'on souhaite sortir du réseau privé :

```
[default]

include => plan-num-prive

include => appels-sortants

[appels-sortants]

exten => _0ZXXXXXXXX,1,Dial(SIP/${EXTEN}@mon-provider-sip)

[appels-entrants]

exten => _3iXX,1,Ringing(1) ; Attendre une seconde en faisant retentir

la ; sonnerie du telephone de l'apellant

same => n,Answer() ; Répond à l'appel

same => n,Goto(plan-num-prive,${EXTEN},1)
```

Et lorsqu'un poste s'enregistre, le message suivant apparait sur la console du serveur de « RTLR Telecom » ; et quand on exécute **sip show peers** sur le serveur opérateur, on voit (avant de configurer le plan de num dans */etc/asterisk/extensions.conf*).

Dans « extensions.conf » :

```
...
[default]
include => routage-appels
...
[routage-appels]
exten => _05460131XX,1,Dial(SIP/${EXTEN:-4:4}@poste1) ; on ne transmet
        same => n,Hangup()          ; que les 4 derniers chiffres composés
exten => _05460232XX,1,Dial(SIP/${EXTEN:-4:4}@poste2)
        same => n,Hangup()
...
```

Rq : La variable ${EXTEN} a la syntaxe ${EXTEN:x:y}, où x désigne la position du début et y le nombre de chiffres retenus. Par exemple, pour le n° composé « 94169671111 », cela donne :

- ${EXTEN:1:3} commence 1 chiffre après le début et garde 3 chiffres, soit 416
- ${EXTEN:4:7} commence 4 chiffre après le début et garde 7 chiffres, soit 9671111
- ${EXTEN:-4:4} commence 4 chiffres avant la fin et garde 4 chiffres, soit 1111
- ${EXTEN:2:-4} commence 2 chiffres après le début et exclut les 4 derniers, soit 16967
- ${EXTEN:-6:-4} commence 6 chiffres avant la fin et exclut les 4 derniers, soit 67
- ${EXTEN:1} commence 2 chiffres après le début et garde tout le reste : 4169671111 (si le nombre de chiffres à retourner est vide, la fonction retourne l'ensemble des chiffres restants).

11. Intégration dans une base de données

La limitation actuelle de notre système est qu'au moindre changement d'un profil d'abonné SIP par exemple, il faut redémarrer certains modules d'Asterisk afin que les modifications effectuées dans les fichiers de configuration soient prises en compte. Une solution afin que l'on puisse modifier certaines données en « temps réel » est de stocker les données nécessaires au fonctionnement d'Asterisk dans une base de données.

Paramétrer Asterisk afin qu'il exploite les informations stockées dans une base de données est l'un des aspects fondamentaux de la construction d'un grand système fiable et performant, déployable en cluster ou distribué.

La puissance d'une base de données permet de :

- utiliser et modifier dynamiquement les données des abonnés et des plans de numérotation, sans dépendre uniquement de quelques fichiers clés (sip.conf, extensions.conf, ...)

- intégrer facilement des outils de gestion des données par interfaces web

- partager les informations entre le serveur ToIP Asterisk et d'autres outils ou services réseaux.

Nous allons donc chercher dans cette partie à stocker la configuration des postes SIP et le plan de numérotation (informations actuellement rentrées dans les fichiers « sip.conf » et « extensions.conf ») dans une base de données. Il existe différents types de bases de données, nous allons utiliser ici une base de données MySQL.

L'architecture temps réel d'Asterisk (Asterisk Realtime Architecture) permet de stocker tous les paramètres, normalement stockés dans les fichiers de configuration Asterisk, dans une base de données. Il existe deux types de temps réel: statique et dynamique :

-méthode statique : elle est similaire à la méthode traditionnelle de lecture d'un fichier de configuration (l'information est chargée uniquement en cas de déclenchement d'un « reload » depuis la CLI), excepté le fait que les données sont lues sur la base de données et non plus dans les fichiers de configuration ; avec ce mode statique, apporter des changements aux données nécessite un rechargement, tout comme si on avait changé un fichier de configuration

-méthode dynamique : Asterisk charge et met à jour l'information telle qu'elle est utilisée par le système en direct ; ceci est couramment utilisé pour par exemple les profils SIP et les boîtes vocales car il n'y a pas besoin de recharger Asterisk lorsque des modifications ont été apportées à ces données.

Le type de temps réel est configuré dans le fichier */etc/asterisk/extconfig.conf*. Ce fichier indique à Asterisk les informations qu'il faut charger depuis la base de données et où le trouver. Cela permet par exemple de charger une partie des paramètres et données depuis la base de données où ils sont stockés, et les autres paramètres ou données à partir des fichiers de configuration standard.

11.1. Création d'une VM pour la base de données

Nous aurions pu installer une base de données sur la même VM à côté du serveur ToIP Asterisk, mais ici, afin de bien dissocier les rôles de chaque machine, nous allons exploiter une 3ème VM, « M4205-MySQL-Server », qui hébergera la base de données MySQL.

Comme pour le server Asterisk, configurer la carte réseau eth0 de la VM MySQL-Server de façon permanente, avec les paramètres IP adéquats (soit l'adresse IP : 192.168.11.131).

11.2. Installation de la base de données MySQL

Nous installons ensuite le paquet « mysql-server », et choisir « rtrt » comme mot de passe pour le compte administrateur « root » de MySQL.

Avec la base de données MySQL active maintenant, nous allons commencer par sécuriser notre installation. Nous allons exécuter un script permettant d'entrer un nouveau mot de passe pour l'utilisateur root, avec quelques options supplémentaires :

Puis nous exécutons le script en donnant les bon droits au fichier :

/usr/bin/mysql_secure_installation

L'exécution de ce script assez simple, choisir de supprimer l'utilisateur « anonymous », maintenir l'autorisation d'accès distant (pas exclusivement depuis « localhost ») ; pour les autres choix, sélectionner les valeurs par défaut.

Puis on se connecte à l'ILC de la base MySQL avec la commande **mysql -u root -p**

Le prompt de la console MySQL doit s'afficher : mysql > On crée ensuite un utilisateur « asterisk » (mot de passe « rtrtsql ») avec la commande suivante, où le % indique que l'utilisateur « asterisk » peut se connecter depuis n'importe quel hôte :

mysql> create user 'asterisk'@'%' identified by 'rtrtsql' ;

On crée une base de données « asteriskdb », que nous exploiterons avec Asterisk :

mysql> create database asteriskdb ;

Puis nous visualisons si la base de données a bien été créée :

mysql> show databases ;

Maintenant qu'ont été créés d'une part un utilisateur « asterisk » et d'autre part une base de données « asteriskdb », autoriser cet utilisateur à accéder à la base de données : **mysql> grant all privileges on asteriskdb.* to 'asterisk'@'%'**

Enfin on sort de la console MySQL et vérifier que vous pouvez correctement vous loguer sur la base de données « asteriskdb » en tant qu'utilisateur « asterisk » : **mysql> exit**

root@asterisk-server:# mysql -u asterisk -p asteriskdb

Et nous quittons la console MySQL.

Il nous faut maintenant vérifier que la VM Asterisk-Server pourra accéder à la base de données « asteriskdb ». Pour cela, effectuons les vérifications suivantes :

-un nmap en indiquant l'adresse IP de notre VM MySQL depuis une autre machine doit révéler que le port 3306 est ouvert,

-de même avec la commande **lsof -i -P** exécutée cette fois-ci sur la VM elle-même.

Puis notre dernier test : depuis la VM Asterisk-Server, nous tentons de nous connecter sur la base de données distante.

Pour cela il nous faut installer sur Asterisk-Server le client « mysql-client-core-5.6 », puis nous tentons la connexion sur la base « asteriskdb» :

mysql -u asterisk -p asteriskdb -h 192.168.11.131

Nous nous apercevons que la connexion ne fonctionne pas.

Pour cela sur MySQL-Server, nous modifions la ligne suivante dans */etc/mysql/my.cnf* :

« bind-address = 127.0.0.1 »

en « bind-address = 0.0.0.0 »

En redémarrant nous avons pu observer que le port d'écoute avait changé.

Nous retentons la connexion, celle-ci fonctionne cette fois-ci. Et nous fermons la connexion.

C'est tout pour le moment concernant la config du serveur MySQL.

11.3. Installation d'ODBC sur Asterisk-Server

11.4. Enregistrement des postes SIP dans la base de données

11.5. Enregistrement du plan de numérotation dans la base de données

11.6. Exportation des boites vocales dans la base de données

12. Listing des appels – Taxation

Conclusion

Ce très long et fastidieux TP, nous à permis de découvrir le monde IP de la téléphonie qui devrait être installé dans les entreprises. Nous avons pu voir comment installer Asterisk en maîtrisant chacune des étapes de configuration. La mise en service des hardphones IP et des softphones, ainsi que l'analyse des trames générées par le serveur et les postes. Nous avons pu essayer de développer notre démarche logique afin de géolocaliser un problème lorsqu'il survient, l'identifier et essayer de le résoudre. Nous avons été également capable d'installer des serveurs DHCP et TFTP pour la mise à jour et la configuration automatiques des postes. De plus, nous avons pu installer une solution de messagerie unifiée, de mettre en service une base de données pour le stockage des données.

Cette vaste configuration, nous permet de comprendre la complexité et l'ingéniosité de la structure IP de la téléphonie dans les entreprises, ainsi que la stupéfaction à laquelle nous devons faire lorsque nous devons identifier un problème et le résoudre dans cette structure.