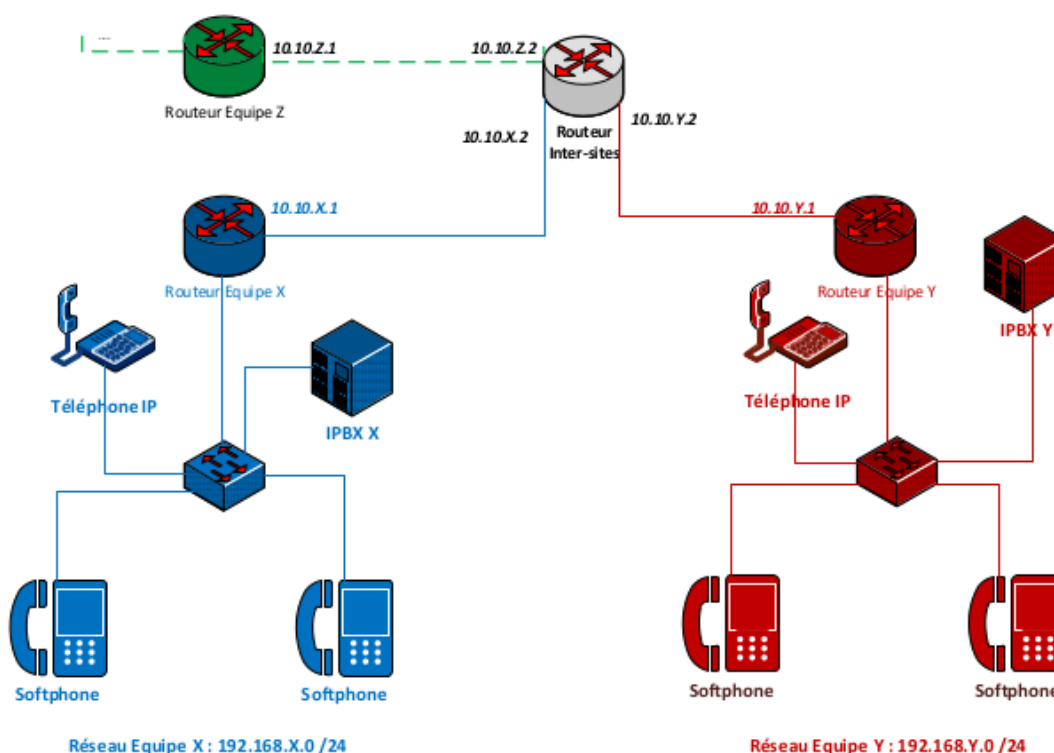


# Mise en place et sécurisation d'une infrastructure de téléphonie IP avec Asterisk

## Activité 6 – Mise en place d'un plan d'appel inter-sites avec utilisation d'un trunk IAX.

La plate-forme de test à mettre en œuvre est la suivante :



### Adressage et numérotation

CONTEXTES	RÉSEAU IP	N° DE TÉLÉPHONE sur 4 chiffres	N° DE MESSAGERIE	SERVEUR ASTERISK
Finance	192.168.X.0/24	Commencent par X1 Exemple 1101, 1102 etc. pour l'équipe n°1	X199	192.168.X.200/24
Compta		Commencent par X2. Exemple : 1201, 1202, etc. pour l'équipe n° 1	X299	

Le plan d'adressage et de numérotation ci-dessus illustre deux contextes (finance et compta) qui veulent communiquer au sein d'un même site (un seul serveur Asterisk). Dans la numérotation mise en place, X représente un numéro de groupe de travail d'étudiants (équipe) pouvant aller de 1 à 8. Les captures d'écrans réalisées sont associées à l'équipe n°1.

Par exemple, 1101 représente le numéro du premier téléphone de l'équipe 1 appartenant au contexte *finance*. 1202 représente le numéro d'un deuxième téléphone de l'équipe 1 associé au contexte *compta*.

**Vous disposez d'un document illustrant les différentes étapes à suivre.**

## Travail à faire

À l'aide du dossier documentaire fourni, vous devez réaliser l'ensemble des travaux. Vous prendrez soin de rédiger une documentation au fur et à mesure de votre avancement. Lors de chaque étape, vous devez indiquer les commandes utilisées vous permettant de tester vos configurations. Vos captures d'écran ne devront prendre en compte que la zone d'affichage nécessaire à vos démonstrations.

Dans cette activité, la communication se fera entre deux softphones Ekiga installés sur des machines Linux ou Windows. Dans les captures d'écrans du dossier documentaire, X vaut 1 et Y vaut 2.

### Travail à faire 1 : préparation des machines et routage

**Q1.1.** Commencer par préparer les machines qui serviront pour les softphones des équipes X et Y. Pour cela, suivre les étapes suivantes :

Concernant l'équipe X ;

- Démarrer une première machine de type Linux ou Windows et configurer l'adressage IP suivant : 192.168.X.11/24, passerelle 192.168.X.254. Installer le softphone Ekiga ainsi que Wireshark. Cette machine servira pour le softphone de l'équipe X.

Concernant l'équipe Y :

- Démarrer une seconde machine sur le modèle de la première et configurer l'adressage IP suivant : 192.168.Y.12/24, passerelle 192.168.Y.254. Installer le softphone Ekiga ainsi que Wireshark. Cette machine servira pour le softphone de l'équipe Y.

Pour le moment, ne pas configurer de comptes sur ces softphones.

**Q1.2.** A l'aide de la commande ping, vérifier que les deux machines précédentes peuvent se joindre. En cas de soucis, vérifier notamment la configuration des routeurs des équipes ainsi que du routeur inter-sites.

**Q1.3.** Utiliser la commande traceroute afin de vérifier le chemin suivi par un softphone pour parvenir au second softphone.

### Travail à faire 2 : préparation du serveur IPBX de chaque équipe

Dans cette partie, chaque équipe doit disposer d'un serveur IPBX Asterisk sur le modèle de celui déjà utilisé dans les activités précédentes. Deux utilisateurs doivent être configurés pour chaque équipe.

**Q2.1.** Démarrer le serveur IPBX de votre équipe et commencer par modifier les fichiers **users.conf** et **voicemail.conf** afin de disposer des deux utilisateurs suivants :

ÉQUIPES	CONTEXTES	UTILISATEURS	NUMÉROS	N° MESSAGERIE
X	finance	Utilisateur1	X101	X199
	compta	Utilisateur2	X201	X299
Y	finance	Utilisateur3	Y101	Y199
	compta	Utilisateur4	Y201	Y299

Redémarrer le serveur IPBX de votre équipe et utiliser la commande de console **sip show users** afin de vérifier la présence de vos utilisateurs.

**Q2.2.** A l'aide du dossier documentaire, créer la configuration du fichier **iax.conf** sur le serveur IPBX de chaque équipe. Sur chaque serveur, choisir un login et un mot de passe d'authentification IAX et le communiquer à l'autre équipe.

Redémarrer les serveurs IPBX et vérifier que la liaison IAX est opérationnelle en utilisant la commande de console **iax2 show peers**.

Remarque : après le redémarrage des serveurs, il faut attendre un petit moment pour que les deux serveurs se détectent.

**Q2.3.** A l'aide du dossier documentaire, modifier la configuration du fichier **extensions.conf** afin de permettre la communication IAX entre les téléphones des deux équipes. Pour ce qui est du fichier **sip.conf**, il doit être similaire à celui utilisé dans les activités 1 à 4 avec des communications non chiffrées.

### Travail à faire 3 : appels et captures de trames

**Q3.1.** Tester différents appels pour vérifier que tous les utilisateurs peuvent se contacter.

**Q3.2.** Lors d'un appel inter-site, capturer les trames en positionnant **Wireshark** sur le softphone de chaque équipe. Reporter sur votre documentation des extraits de captures associés aux différentes étapes de la communication : signalisation, échange et fermeture.

**Q3.3.** Lors d'un appel inter-sites, capturer les trames en positionnant **Tshark** sur le serveur IPBX de chaque équipe. Les serveurs IPBX étant sans environnement graphique de bureau, suivre les étapes suivantes :

- installer le logiciel Tshark sur chaque serveur IPBX : **apt-get install tshark** ;
- créer sur chaque serveur IPBX un fichier nommé *capture* avec la commande **touch capture** ;
- lancer la commande suivante : **tshark -w capture**. Cette commande lance une capture de trames et redirige la capture vers le fichier nommé *capture* ;
- tester un appel vers le site distant ;
- arrêter la capture en utilisant la combinaison des touches CTRL+C ;
- exporter votre fichier de capture sur une machine graphique disposant de Wireshark ;
- lancer Wireshark et ouvrir le fichier de capture associé à votre équipe ;
- filtrer les trames associées au protocole **IAX2** et reporter une capture d'écran sur votre documentation.

## Dossier documentaire

### Document 1 – Configuration d'un trunk IAX

#### D1.1 – Présentation

Dans le cas d'un réseau comportant plusieurs serveurs Asterisk, il est nécessaire de permettre aux postes rattachés à un serveur de pouvoir communiquer avec les postes rattachés à un autre serveur. Cette liaison entre serveurs Asterisk peut s'effectuer en utilisant le protocole IAX (Inter eXchange Asterisk) avec une méthode qui connecte les serveurs via leur adresse IP. Les exemples des paragraphes suivants concernent la configuration de l'IPBX de l'équipe 1 (X=1) pour la liaison avec l'IPBX de l'équipe 2 (Y=2).

#### D1.2 - Le fichier iax.conf

**Pensez à conserver une sauvegarde du fichier iax.conf d'origine.**

☐ Authentification auprès du serveur distant

Il faut ajouter une première ligne qui permet au serveur IPBX de s'authentifier auprès du serveur Asterisk de l'autre site.

```
[general]
register => asterisk-equipe-X:1234@192.168.Y.200
```

Dans cette ligne, notre serveur s'annonce avec le login **asterisk-equipe-X** et le mot de passe **1234**. L'adresse IP indiquée est celle du serveur IPBX distant.

☐ Vérification d'une demande d'authentification du serveur distant

Ensuite, il faut ajouter un bloc qui permet au serveur IPBX distant de s'authentifier sur notre serveur.

```
[asterisk-equipe-Y]
type = friend                ;voir explication dans l'activité 1.
host = dynamic                ;ip fixe (static) ou dynamique pour le serveur distant.
trunk = yes
secret = 1234
context = liaison-serveur-y  ;contexte associé à la gestion des appels distants.
qualify = yes                 ;permet de monitorer la connexion vers le serveur.
```

Dans cet exemple, le serveur distant de l'équipe Y devra s'annoncer avec le login **asterisk-equipe-Y** et le mot de passe **1234**. Le contexte dans lequel seront acheminés les appels s'intitule **liaison-serveur-Y**.

Le fichier *iax.conf* du serveur Asterisk du site distant doit être configuré de la même manière en adaptant les valeurs des paramètres ainsi que l'adresse IP du serveur à joindre.

En cas de difficulté, penser à passer en mode débogage :

```
*CLI > iax2 set debug on
```

### D1.3 - Le fichier extensions.conf

Dans ce fichier, il faut commencer par ajouter une ligne permettant à chaque contexte de joindre le serveur distant. Par exemple, sur le fichier du serveur de l'équipe x (voir les lignes en gras) :

```
[general]
...
[finance]
....
exten => _2XXX,1,Goto(liaison-serveur-Y,${EXTEN},1)

[compta]
...
exten => _2XXX,1,Goto(liaison-serveur-Y,${EXTEN},1)
```

Ensuite, il faut définir le contexte qui permet de router les appels.

```
[general]
...
[finance]
....
[compta]
...
[liaison-serveur-Y]
;routing des appels sortants vers le site distant
exten => _2XXX,1,Dial(IAX2/asterisk-equipe-Y/${EXTEN})

;routing des appels distants entrants vers les contextes internes finance et compta
exten => _11XX,1,Goto(finance,${EXTEN},1)
exten => _12XX,1,Goto(compta,${EXTEN},1)
```

Le fichier extensions.conf du serveur Asterisk du site distant doit être configuré de la même manière en adaptant les valeurs des paramètres.

### D1.4 - Trace des échanges

Lors d'un appel, la console Asterisk du site distant trace la demande d'authentification.

Pour un appel émis par le site de l'équipe X=1.

```
Connected to Asterisk 11.13.1~dfsg-2+b1 currently running on asterisk-equipe-y (pid = 1376)
-- Accepting AUTHENTICATED call from 192.168.1.200:
--   > requested format = ulaw,
--   > requested prefs = (),
--   > actual format = ulaw,
--   > host prefs = (),
--   > priority = mine
-- Executing [2101@liaison-serveur-x:1] Goto("IAX2/asterisk-equipe-x-5221", "finance,2101,1") in new stack
-- Goto (finance,2101,1)
-- Executing [2101@finance:1] Dial("IAX2/asterisk-equipe-x-5221", "SIP/2101,20") in new stack
== Using SIP RTP CoS mark 5
-- Called SIP/2101
-- SIP/2101-00000002 is ringing
-- SIP/2101-00000002 answered IAX2/asterisk-equipe-x-5221
  > 0x7f7e7801f780 -- Probation passed - setting RTP source address to 192.168.2.12:5064
```

Pour un appel émis par le site de l'équipe Y=2.

```
Connected to Asterisk 11.13.1~dfsg-2+b1 currently running on asterisk-equipe-x (
pid = 1292)
-- Accepting AUTHENTICATED call from 192.168.2.200:
--      > requested format = ulaw,
--      > requested prefs = (),
--      > actual format = ulaw,
--      > host prefs = (),
--      > priority = mine
-- Executing [1101@liaison-serveur-y:1] Goto("IAX2/asterisk-equipe-y-5891",
"finance,1101,1") in new stack
-- Goto (finance,1101,1)
-- Executing [1101@finance:1] Dial("IAX2/asterisk-equipe-y-5891", "SIP/1101,
20") in new stack
== Using SIP RTP CoS mark 5
-- Called SIP/1101
-- SIP/1101-00000005 is ringing
-- SIP/1101-00000005 answered IAX2/asterisk-equipe-y-5891
-- > 0x7f7268008830 -- Probation passed - setting RTP source address to 192.
168.1.11:5078
```