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

Propriétés	Description
Intitulé long	Mise en place et sécurisation d'une infrastructure de téléphonie IP avec Asterisk
Intitulé court	Téléphonie IP avec Asterisk
Formation concernée	BTS SIO
Matières	SISR3 : Exploitation des services.
Présentation	Ce Côté Labo a pour objectif de mettre en place une maquette complète de ToIP autour du serveur IPBX Asterisk. Au delà de la présentation des fonctionnalités de base offertes par le logiciel, les travaux menés permettent d'illustrer un aspect lié à la sécurité d'une infrastructure TOIP, à savoir la prévention des écoutes clandestines (attaque de type eavesdropping) et de mettre en place un trunk SIP. Il s'inscrit dans le contexte GSB et est découpé en plusieurs activités : • **activité 1** : installation, prise en main d'Asterisk et une première découverte des fonctionnalités ; • **activité 2** : découverte des principales fonctionnalités ; • **activité 3** : utilisation de téléphones IP ; • **activité 4** : mise en place d'une écoute clandestine ; • **activité 5** : mise en place de contre-mesures avec chiffrement ; • **activité 6** : mise en place d'un plan d'appel inter-sites avec utilisation d'un trunk IAX.
Notions du programme	**Activités supports de l'acquisition des compétences** **D2.1 - Exploitation des services** • A2.1.2 Évaluation et maintien de la qualité de service **D3.1 - Conception d'une solution d'infrastructure** • A3.1.1 Proposition d'une solution d'infrastructure • A3.1.3 Prise en compte du niveau de sécurité nécessaire à une infrastructure **D3.2 – Installation d'une solution d'infrastructure** **D3.3 - Administration et supervision d'une infrastructure** • A3.3.1 Administration sur site ou à distance des éléments d'un réseau, de serveurs, de services et d'équipements terminaux **Savoir-faire** • Caractériser les éléments nécessaires à la qualité et à la sécurité d'un service • Installer et configurer les éléments nécessaires à la qualité et à la continuité du service • Administrer et sécuriser un service • Contrôler et améliorer les performances d'un service • Valider et documenter la qualité et la sécurité d'un service **Savoirs associés** • Qualité et sécurité des services, méthodes, technologies, techniques, normes et standards associés
Pré-requis	Commandes de base d'administration d'un système Linux
Outils	Un serveur physique ou une machine virtuelle (Vmware, VirtualBox…), Asterisk 11.13.1, Debian Jessie, téléphones IP compatibles SIP, un commutateur PoE, une machine cliente sous Linux pour réaliser l'attaque. Site officiel : http://www.asterisk.org
Mots-clés	ToIP, Asterisk, MITM, ARP Poisonning, chiffrement TLS, softphone.

Durée	12h
Auteur.e(s)	Patrice DIGNAN, David DURON, Apollonie RAFFALLI, avec la relecture et les suggestions de Yann Barrot.
Version	V 1.0
Format	Découpage en plusieurs activités.
Date de publication	Décembre 2016

Présentation de la ToIP

La voix sur IP (VoIP pour Voice Over Internet Protocole) est une technologie qui permet de faire passer de la voix (paquets de données correspondant à des échantillons de voix numérisée) sur des réseaux IP. Cette technologie est notamment utilisée pour prendre en charge le service de téléphonie sur IP (ToIP pour Telephony over Internet Protocol).
La ToIP représente donc la VoIP en addition de toutes les fonctions (applications téléphoniques) réalisées par un autocommutateur téléphonique PABX (Private Automatic Branch Exchange) IP ou IPBX .

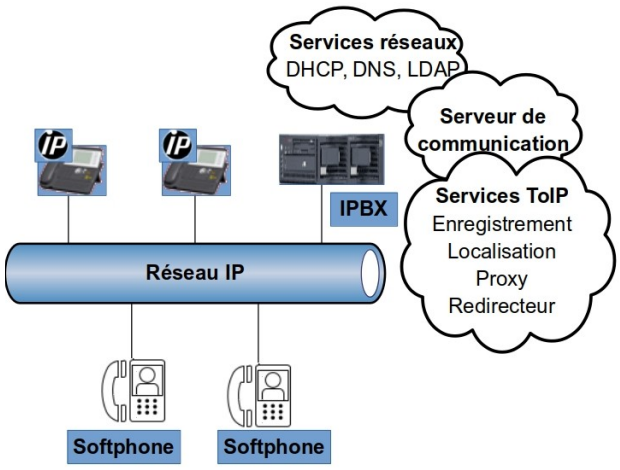
Pourquoi les organisations basculent-elles vers la ToIP ?

Avant 2002, la ToIP n'a pas connu d'évolutions significatives à cause de la complexité des premiers serveurs, le coût de la bande passante, un protocole H323 issu de la téléphonie traditionnelle pas toujours adapté et la faible implantation du haut débit dans les entreprises. Depuis 2002, on constate une évolution rapide qui s'est accentuée à partir de 2010 pour les raisons suivantes :

- **réduction des coûts** de communications nationales et internationales (offres de téléphones IP bon marché) et, bien sûr, celles concernant les réseaux IP inter-sites (WAN) ;
- **Ça « marche » de mieux en mieux** : haut débit, protocoles adaptés natifs du monde IP, meilleure maîtrise de la qualité et de la sécurité, etc. ;
- **meilleure mobilité** : les postes ne sont plus physiquement reliés à des lignes ==> la téléphonie sur IP permet à l'utilisateur de conserver son numéro dans ses déplacements et d'avoir plusieurs téléphones correspondants à un seul numéro.
- **mutualisation et convergence des outils de communication** : la téléphonie sur IP rassemble tous les matériels de l'entreprise (téléphone IP, visioconférence, fax, PC) sur un même réseau ==> Il est possible d'utiliser tous les types de médias (voix, image, écrit) quel que soit le terminal ou le réseau, cela permet aux entreprises d'offrir de nouveaux services.
- **réduction des consommations d'énergie** grâce à la centralisation des équipements et à la mutualisation des réseaux qui entraînent une réduction importante des équipements ;
- **Évolution d'une infrastructure obsolète** : Orange va progressivement abandonner l'infrastructure propre au réseau téléphonique commuté (RTC) à partir de 2021 ; à terme, il n'y aura donc plus de services téléphoniques analogiques et numériques.

Architecture physique simple de la ToIP

Une infrastructure ToIP est architecturée autour :



- **d'un IPBX** (PABX IP) qui est un autocommutateur associé à un serveur de communication intégrant de nombreux services (double appel, messagerie vocale, conférence, etc.). Il dispose aussi de services réseaux spécifiques à la ToIP. C'est le cœur du système : il enregistre et permet le paramétrage d'un nouveau terminal, il teste si l'appel est permis, il fait la résolution d'adresse et il redirige l'appel vers le bon "client" ;
- **de terminaux IP** (téléphones qui se connectent via un câble Ethernet à un commutateur) et de **softphones** (logiciels installés sur des ordinateurs) ;
- **d'un commutateur** en règle générale **PoE** (Power over Ethernet ou courant par l'Ethernet - norme 802.3af qui permet d'alimenter électriquement un périphérique via un câble Ethernet) : les téléphones IP doivent être alimentés en électricité et ne disposent généralement pas de câble électrique.

En ce qui concerne l'IPBX, plusieurs constructeurs sont présents sur le marché de la ToIP et proposent des solutions de PABX IP (généralement sous forme de "boitiers") comme Cisco ou Alcatel. La solution libre que nous étudierons dans ce côté labo s'appelle Asterisk.

Il est aussi possible d'utiliser des logiciels pour faire de la téléphonie depuis un ordinateur plutôt qu'un téléphone (softphone Ekiga, Zoiper…). Les communications nécessitent alors l'utilisation d'un microcasque ou de hauts-parleurs reliés à la carte son. Dans ce Côté Labo, nous travaillerons avec les softphones Ekiga et Blink ainsi qu'avec des téléphones IP CISCO SPA 303.

Présentation d'Asterisk

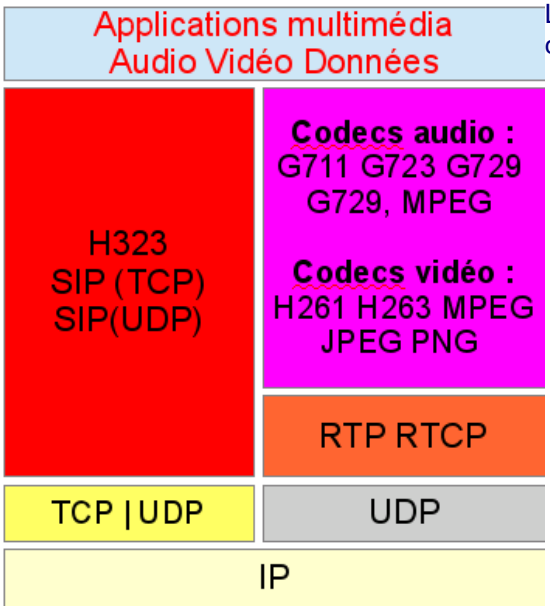
Asterisk est un logiciel open source qui permet de transformer un ordinateur en autocommutateur téléphonique privé (PABX). Il dispose de nombreuses fonctionnalités permettant de couvrir un grand nombre de besoins : messagerie vocale, transfert d'appels, files d'attentes, call parking, standard automatique, conférences, musiques d'attentes, groupement d'appels…

La ToIP sur Asterisk passe par la prise en charge de plusieurs protocoles dont les deux principaux sont SIP (Session Initiation Protocol) et IAX (Inter-Asterisk eXchange) qui permet la communication entre deux sites distants.

Il est possible de configurer Asterisk pour lui faire jouer le rôle de passerelle avec les réseaux publics ce qui offre la possibilité de le lier à la ligne téléphonique de son fournisseur de service afin de pouvoir passer des appels externes via un *trunk SIP*.

Services réseaux / ToIP et protocoles

Les protocoles classiques mis en œuvre



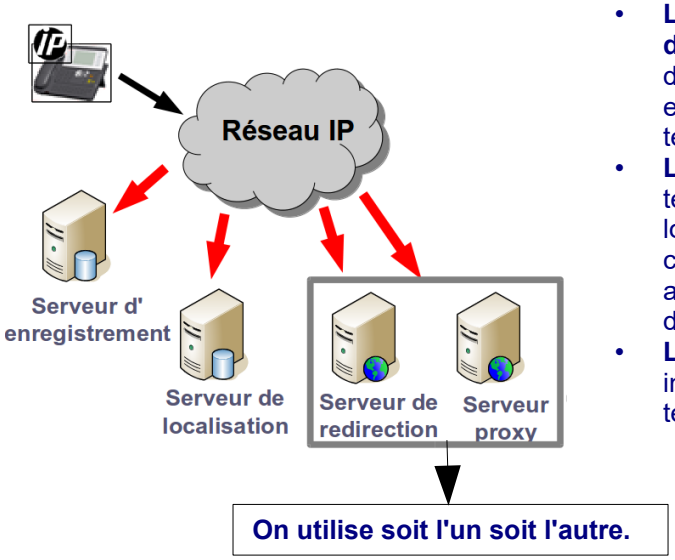
L'appel proprement dit nécessite ainsi une double connexion :

- **la première pour l'appel**, l'authentification et la mise en relation des hôtes : on utilise des protocoles de signalisation et de mise en relation des clients comme H323 et **SIP**. H323 est un protocole inventé en 1996 et natif du monde de la téléphonie, il cède de plus en plus de place au protocole **SIP (Session Initiation Protocol)** développé en 1997 et natif du monde de l'Internet standardisé par l'IETF (décrit par la RFC 3261 et complété par la RFC 3265), c'est le protocole de référence en matière de téléphonie. **Il est moins lourd à configurer et il est implémenté dans tous les matériels actuels** (téléphones IP, softphones, IPBX).
- **Numérisation, compression et transport des données** : on utilise de protocoles de transport des données multimédia (RTP, RTCP)

Les codecs audios et vidéos sont des algorithmes de codage et de décodage des données multimédia. Ils sont négociés dans la première phase et utilisés dans la seconde.

L'architecture SIP

Elle s'articule principalement autour de 5 entités :

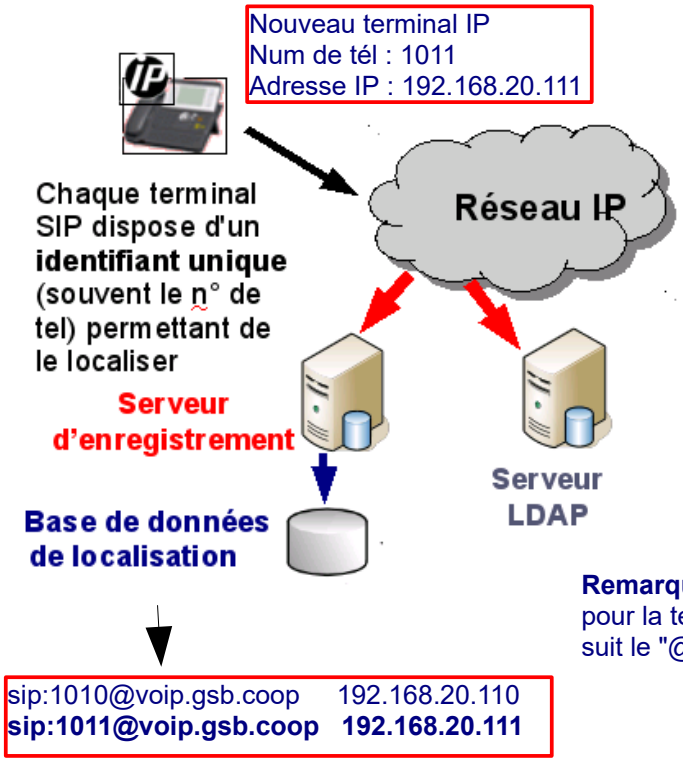


- **Les serveurs d'enregistrement et serveurs de localisation** permettent respectivement d'associer une adresse IP à un terminal et ensuite de le localiser à la demande d'un autre terminal.
- **Le serveur de redirection** est sollicité par le terminal pour contacter le serveur de localisation afin de déterminer la position courante d'un utilisateur : il renvoie la réponse au premier terminal qui dialogue ensuite directement avec le second.
- **Le serveur proxy** joue le même rôle mais initie lui-même la connexion auprès du second terminal et ainsi de suite.

Ces 4 serveurs sont généralement regroupés au sein du même outil (par exemple, le logiciel Asterisk).

Quelles sont les étapes nécessaires pour qu'une communication entre deux terminaux puissent s'établir ?

1. Enregistrement des terminaux : avant d'initier et de recevoir un appel, les terminaux doivent être enregistrés auprès de leur serveur d'enregistrement (*REGISTRAR*) afin de signaler leur emplacement courant, c'est-à-dire leur adresse IP. Cet enregistrement se fait automatiquement (via une requête *REGISTER*) du moment que l'on connecte le terminal à un commutateur lui-même connecté à un serveur d'enregistrement (IPBX).



Il est attribué à chaque terminal SIP* dotée d'une adresse IP (éventuellement fournie par un serveur DHCP) un numéro de téléphone unique dans le plan de numérotage de l'organisation : à ce numéro correspond en général (mais pas forcément) une entrée dans un annuaire LDAP (pour la présentation du nom de l'appelant ou pour la fonction d'appel par nom).

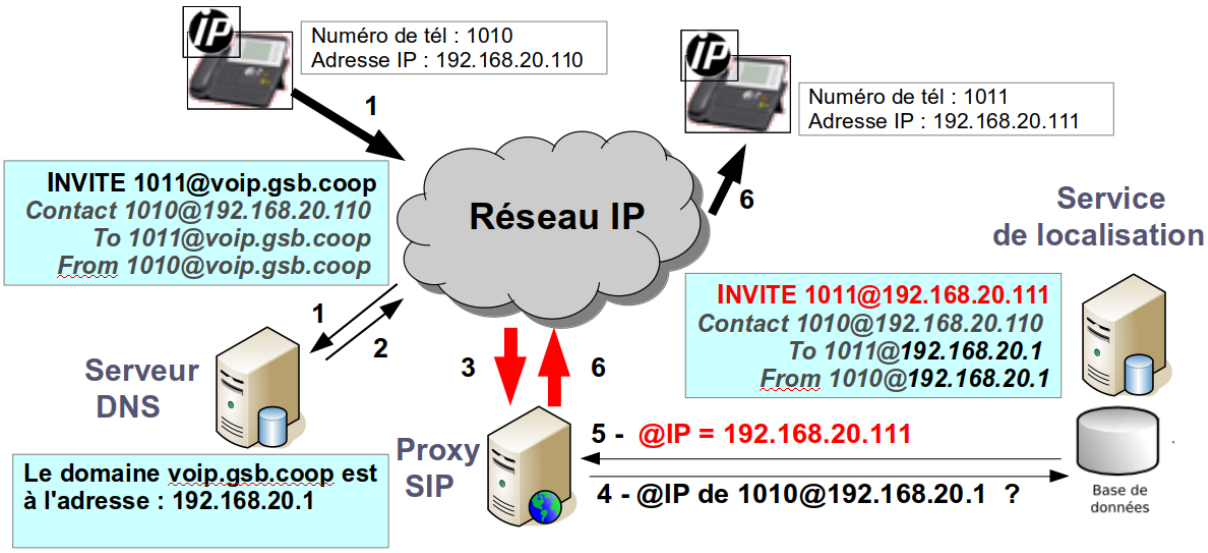
Le format d'une adresse SIP (ou URL SIP) respecte la RFC 3986 (nommée Uniform Resource Identifier : Generic Syntax). Cette adresse ressemble à une adresse mail et se présente généralement sous la forme : sip:identifiant@domaine (par exemple, 489@voip.gsb.coop)

Remarque : s'il n'y a pas de serveur DNS prévu pour la téléphonie, c'est l'adresse IP de l'IPBX qui suit le "@".

* On trouve dans les terminaux IP un agent SIP (*User Agents) :* il s'agit du dispositif logiciel qui gère le protocole SIP, c'est cet agent qui a en charge l'enregistrement du terminal IP auprès du *registrar.*

2. Mise en relation des terminaux via un proxy SIP

Un appel du terminal IP 1010 est lancé vers le terminal IP 1011. On suppose ici que le *User Agent* de l'appelant ne connaît pas la localisation (c'est à dire l'adresse IP) de l'appelé : le proxy SIP relaie sa requête "*INVITE*" vers un serveur de localisation.



Un **Proxy SIP** (implémenté dans l'IPBX) sert d'intermédiaire entre deux *User Agents* qui ne connaissent pas leurs emplacements respectifs (adresse IP). Le Proxy interroge la base de données de localisation dans laquelle il va trouver l'association *URI-AdresseIP* pour diriger les messages vers le destinataire.

Une fois que le proxy SIP a interrogé sa base de données (actions 3 et 4) et a réussi à localiser le terminal appelé c'est-à dire qu'il a réussi à récupérer son adresse IP (action 5), il achemine la demande d'initiation de session à la destination (action 6).

À noter que les services d'enregistrement et de localisation sont très souvent confondus. Ils sont, de toutes façons, regroupés dans le même outil.

3. Établissement de la communication

Une fois la session établie, les données (voix, vidéo, etc.) sont transmises au format numérique via le protocole RTP.
Le *flux RTP* contenant les données ne transitent pas par le serveur Proxy (sauf si configuration contraire) mais sont échangées directement entre les User Agents.

À noter que :

- la requête INVITE permet également la négociation sur le protocole à utiliser dans la deuxième phase et la façon de coder les informations à échanger comme le choix des codecs ;
- le protocole SIP utilise par défaut les ports 5060 en UDP et TCP ;
- les utilisateurs SIP peuvent aussi joindre des terminaux connectés à des réseaux de nature différente (RTC par exemple) via des passerelles assurant la conversion des signaux d'un réseau à un autre ;
- les messages utilisés par SIP sont similaires à ceux utilisés par le HTTP. Ils sont codés en ASCII et utilisent des codes proches de ceux du HTTP.

Contexte logistique et matériel

Le laboratoire Galaxy Swiss Bourdin (GSB) est issue de la fusion entre le géant américain Galaxy (spécialisé dans le secteur des maladies virales dont le SIDA et les hépatites) et le conglomérat européen Swiss Bourdin (travaillant sur des médicaments plus conventionnels), lui-même déjà union de trois petits laboratoires. En 2009, les deux géants pharmaceutiques ont uni leurs forces pour créer un leader de ce secteur industriel.
L'entité Galaxy Swiss Bourdin Europe a établi son siège administratif à Paris.
Le siège social de la multinationale est située à Philadelphie dans l'état de Pennsylvanie aux Etats-Unis.

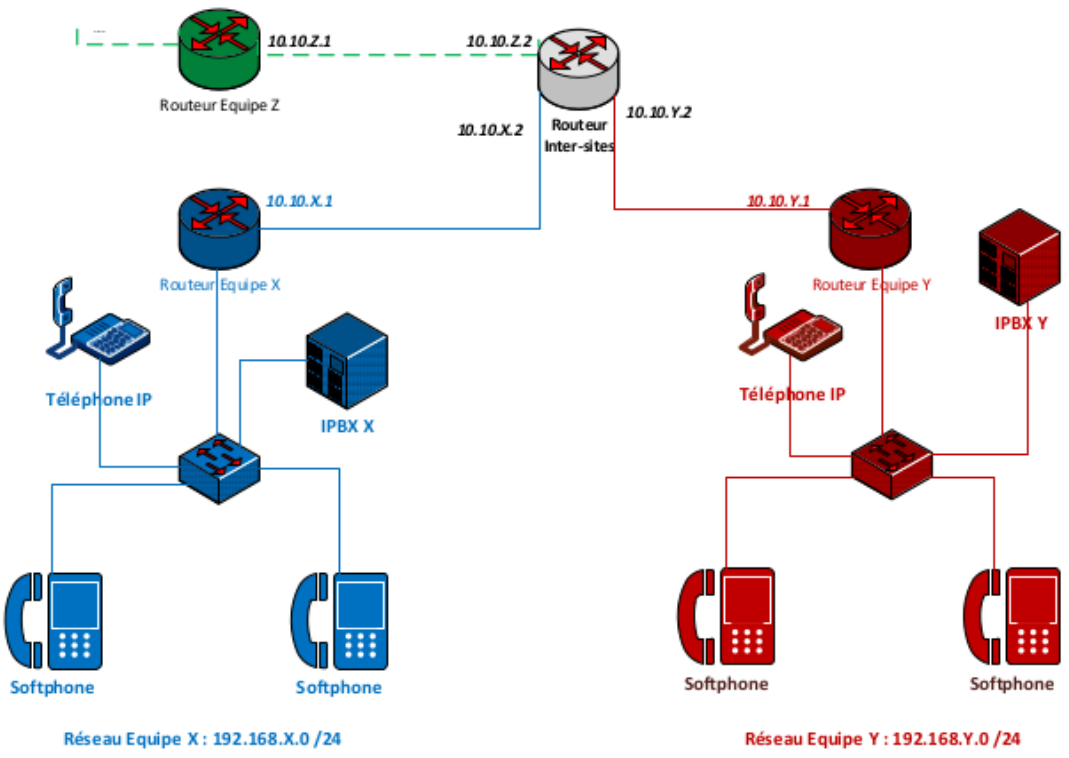
Chaque entité dispose d'un accès Numéris T2 qui leur coûte très cher en abonnement et en consommation. Les dirigeants désireraient réduire les coûts de communications nationales et internationales ainsi que les coûts des communications inter-sites.

Par ailleurs, la convivialité et les services actuels disponibles ne correspondent plus aux attentes des utilisateurs.

De plus, l'obsolescence de certains équipements laisse présager des difficultés de maintenance et d'évolutivité d'autant plus qu'Orange annonce officiellement son intention d'abandonner progressivement l'infrastructure propre au réseau téléphonique commuté (RTC) à compter de 2021, support des services de téléphonie traditionnelle analogique et numérique.

Il est donc envisagé la migration des systèmes téléphoniques existants vers la ToIP, migration qui doit être préparée et simulée dans un laboratoire.

Le schéma final de la plate-forme de test (avant intégration au réseau GSB) est le suivant :



Les activités proposées ont pour objectif de construire, étape par étape, cette plate-forme de test sans négliger d'une part les aspects liés à la sécurisation d'une infrastructure TOIP en prévenant les écoutes clandestines et d'autre part ceux liés à la qualité des communications :

L'activité 1 consiste à mettre en place une plate-forme physique minimaliste représentant un seul site (un commutateur, un serveur, 2 machines clientes) puis à installer Asterisk sur le serveur et un softphone sur chaque machine cliente. Il s'agira ensuite de procéder à une première configuration de l'outil Asterisk :

- mise en œuvre d'un plan d'appels entre les utilisateurs d'un même *contexte. Un contexte étant en ensemble* d'utilisateurs appartenant à un service comptabilité finance...) et qui ont des paramètres de configuration en commun. Dans un premier temps, nous ferons dialoguer des utilisateurs appartenant au contexte Finance puis la démarche sera reproduite pour le contexte Comptabilité.
- mise en place d'une messagerie vocale.

Cela sera aussi l'occasion d'approfondir le fonctionnement des protocoles SIP et RTP en jeu dans les échanges entre les deux softphones.

L'activité 2 a pour objectif de faire la liaison entre les deux contextes supports des tests (le contexte finance et le contexte compta) en créant un plan d'appels pour le second contexte et en permettant les appels entre les deux contextes.

L'activité 3 consiste à intégrer physiquement un téléphone IP en remplacement d'un softphone. Il s'agit ici du téléphone IP CISCO SPA 303 mais n'importe quel autre téléphone IP compatible avec le protocole SIP peut être intégré.

L'activité 4 consiste à mettre en place une écoute clandestine en simulant une attaque de type eavesdropping.

L'activité 5 a pour objectif de mettre en place des contre-mesures en chiffrant les communications via le protocole TLS.

L'activité 6 intègre la simulation du second site.

D'autres activités sont prévues notamment en ce qui concerne les problématiques liées à la qualité des communications.