TABLES DES MATIERES

ABREVIATIONS

EIB	European Industrial Bus
CPL	Courant Porteur en Ligne
DA	Discovery Agent
DHCP	Dynamic Host Configuration Protocol
HAVi	Home Audio Video interoperability
Hi-Fi	High-Fidelity
HomeRF	Home Radio Frequency
HTTP	Hyper Text Transfert Protocol
ID	IDentity
IP	Internet Protocol
IPBX	Internet Protocol PABX
IETF	Internet Engineering Task Force
KNX	Konnex
LAN	Local Area Network
LUS	LookUp Service
MC	Multipoint Control
MCU	Multipoint Control Unit
MP	Multipoint Processor
MGCP	Media Gateway Control Protocol

NAT	Network Address Translation
PABX	Private Automatic Branch eXchange
PC	Personal Computer
PDA	Personal Digital Assistant
PS	Proxy Server
QoS	Quality of Service
RAS	Registration Admission and Status
RF	Radio Fréquency
RFC	Request For Comments
RG	Registrar Server
RNIS	Réseau Numérique à Intégration de Services
RS	Redirect Service
RTC	Réseau Téléphonique Commuté
RTP	Real-time Transport Protocol
SA	Service Agent
SIP	Session Initiation Protocol
SDP	Session Description Protocol
SLP	Service Location Protocol
SMTP	Simple Mail Transport Protocol
SOHO	Small Office Home Office
SWAP	Shared Wireless Access Protocol

TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
ITU-T	Internationale Télécommunication Union - Télécommunication
URL	Uniform Resource Locator
UWB	Ultra Wide Band
VoIP	Voice over IP

INTRODUCTION GENERALE

Dans nos sociétés, l'homme veut maitriser l'environnement et la nature par la technique. Il veut plier la nature à ses désirs, plutôt que s'y adapter et, de ce point de vue, la technologie représente le pouvoir. Ce désir de domination s'étend à nos habitations: nous voulons des maisons de plus en plus à notre service, des maisons que nous pouvons maitriser, et c'est dans ce contexte que la domotique s'inscrit.

Le concept de domotique fait l'objet de nombreuses définitions. De la maison intelligente à la maison communicante, toutes les gradations sont possibles. De fait, la domotique concerne l'application à l'habitat de toutes les technologies dites nouvelles pouvant s'intégrer à ce contexte.

En outre, le monde entier est dorénavant relié au moyen de routes virtuelles qui constituent la toile mondiale. Presque tout le monde utilise des PC, des tablettes, des Smartphones et Internet, au travail et pendant son temps libre pour communiquer avec les autres, pour échanger des données et, parfois, pour se parler à l'aide des applications existantes.

Jusque vers le milieu des années 90, les organismes de normalisation ont tenté de transmettre les données de manière toujours plus efficace sur des réseaux conçus pour la téléphonie. Ainsi est née une nouvelle technologie qui consiste à faire basculer une partie du trafic issu des lignes téléphoniques conventionnelles sur le réseau Internet, c'est la Voice over IP *(VoIP)* ou la voix sur IP. La VoIP qui remporte actuellement un vif succès grâce à son coût très avantageux.

Notre thème de mémoire est axé sur la combinaison de ces deux technologies. Il s'intitule : « SMART LIFE AVEC VoIP ».

Pour ce faire, cet ouvrage est décomposé en quatre chapitres. Le premier chapitre aura comme rôle de présenter une vue d'ensemble sur la domotique. Le second chapitre sera consacré à la technologie VoIP. Le troisième chapitre détaillera l'étude conceptuelle du Smart Life avec VoIP. Et enfin, le dernier chapitre s'occupera des applications de notre plateforme domotique.

CHAPITRE 1: LA DOMOTIQUE

1.1 Introduction

Les progrès technologiques ont permis le développement des systèmes de transmission des commandes à distance et favorise l'éclosion d'une offre abondante de nouveaux services pour les occupants des logements. Ces services, regroupés sous le terme "domotique", concernent principalement le confort (commande à distance des équipements), la sécurité (protection contre les intrusions, détection des incendies), l'économie d'énergie (programmation, gestion de l'éclairage), la communication. Le fonctionnement de ces services est fondé sur les réseaux de communication internes au logement et sur leurs liaisons avec l'extérieur.

Dans ce chapitre, nous allons parler de ce nouveau domaine.

1.2 Généralités

La domotique rassemble les technologies de l'informatique, de l'électronique et des télécommunications permettant de superviser, d'automatiser, de programmer, de coordonner, les tâches de confort, de sécurité, de maintenance et plus généralement des services dans les domiciles [01].

1.2.1 Pourquoi la domotique ?

Une nouvelle fois, le consommateur ou l'usager est à l'origine de la domotique puisque cette dernière est une valeur ajoutée à son habitat, à sa qualité de vie.

Les motivations de l'usager pour la domotique sont multiple et nous pouvons plus particulièrement considérer les points suivants: communication, surveillance, sécurité, gestion de l'énergie, confort et commodité et commande à distance d'une maison [02].

1.2.1.1 Le confort

L'accroissement du niveau de confort des habitations a été le premier objectif de la domotique. En effet, il est possible de gérer et commander à distance des fonctions dans une maison, grâce à Internet ou via un Smartphone ou un ordinateur. Il est donc facile d'imaginer un nombre illimité

des fonctions qui pourraient faciliter le confort quotidien dans la maison: par exemple la cafetière s'allume et les volets s'ouvrent à 7h tous les matins; fermer à distance les fenêtres en cas de pluies.

1.2.1.2 La gestion de l'énergie

L'économie d'énergie justifie à elle-même l'investissement dans la gestion automatisée de l'habitat. Les deux éléments sur lesquels la domotique va influencer la dépense d'énergie sont :

- la distribution de chaleur dans les pièces ;
- la suppression de la consommation électrique inutile.

Un système de régulation domestique est automatique et capable de faire face à tout évènement lié au chauffage. Le réglage des températures est simple et visuel, chaque pièce peut bénéficier d'un réglage qui lui est propre (absence/présence, jour/nuit) et une commande à distance par téléphone est possible afin de mettre la maison sur "confort" ou bien "économie" lors de l'absence des habitants. De plus, le gaspillage d'énergie peut être limité avec des produits domestiques afin de ne pas avoir de lampe oubliée à la cave pendant plusieurs jours, un éclairage surdimensionné ou une lampe allumée en plein jour.

1.2.1.3 La sécurité

En cas de menace pour la sécurité de la maison, tout composant domotique est capable d'émettre un message sur l'installation qui sera repris et traité par un module spécialisé pour la surveillance. Ce module peut alors déclencher n'importe quel composant présent dans l'installation afin de simuler une présence (lumière qui s'allume ou musique) ou bien renforcer la sécurité (verrouillage de toutes les serrures, déclenchement des alarmes). Ces actions peuvent se faire selon un choix particulier, selon une durée ou un nombre de détections ou bien directement par téléphone ou par un ordinateur à distance.

1.2.1.4 La communication

Des nouveaux services comme les films ou l'information à la demande, le téléachat et la banque à domicile devraient être offerts aux utilisateurs. Toutes ces activités seront principalement organisées autour d'un téléviseur évolué, d'un téléphone mobile ou d'un PC.

1.2.2 Exemple des scénarios

- Le matin : Ouverture des fenêtres, enclenchement de la machine à café.
- Départ au travail : Contrôle des fenêtres ouvertes, extinction de toutes les lumières, enclenchement de la sécurité.
- La soirée : Diminution des lumières pour le Home Cinéma, contrôle des portes ouvertes (entrée, garage), fermeture des fenêtres.
- La nuit : Extinction de toutes les lumières des pièces non utilisées, enclenchement de la sécurité.
- Dans mon bureau : 30mn avant de rentrer ; allumage à distance du chauffe-eau, mise en marche du four avec un smartphone ou un ordinateur.

Tous ces scénarios peuvent être manipulés par un simple bouton, un PDA, un PC ou une télécommande.

La figure 1.01 présente les applications les plus courantes comme :

- Sécurité des biens et des personnes
- Gestion d'ambiance (sonore ou lumineuse)
- Régulation de chauffage ou de climatisation

La domotique met en œuvre des dispositifs qu'on peut appeler « appliances » qui sont une solution conjuguant hard et soft pour fournir une solution immédiatement opérationnelle. En général, il s'agit d'un ordinateur sommaire, tournant le plus souvent sous Lunix, chargé d'une application directement utilisable [03].

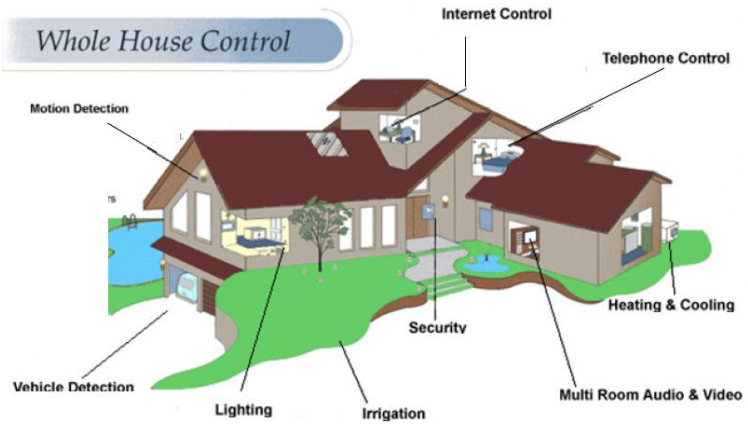

Figure 1.01 : *Applications domotiques*

1.2.3 Fonctions assurées par la domotique

La domotique assure plusieurs fonctions dans la vie quotidienne. Ces différentes fonctions sont données dans la figure ci-dessous:

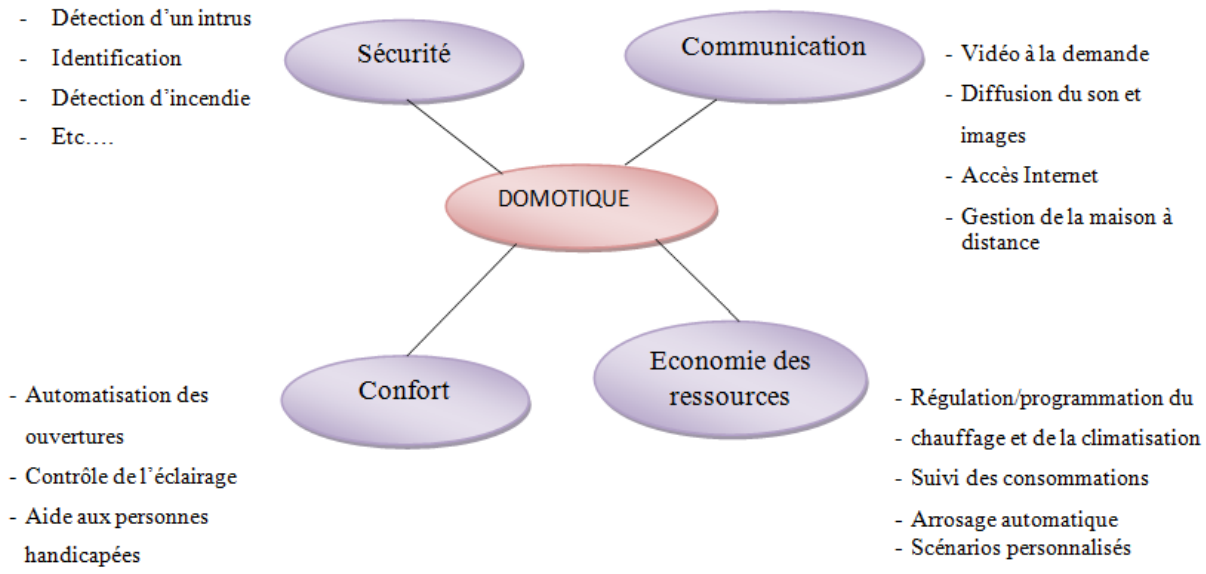

Figure 1.02 : *Fonctions assurées par la domotique*

1.2.4 But de la domotique

Le but de la domotique est de rendre les activités usuelles simples, d'améliorer notre protection et notre confort dans la vie quotidienne. La domotique automatise le pilotage de la maison afin de faciliter la vie quotidienne et de faire des économies d'énergie [04].

En effet, avec la domotique, on peut:

- contrôler à distance ou directement chez soi le comportement des appareils qui sont intégrés au système domotique ;
- automatiser les tâches répétitives du quotidien ;
- mieux gérer la consommation en électricité et donc faire des économies [05].

1.3 Principe de fonctionnement

Le principe de la domotique est de collecter, transmettre et traiter des informations afin de coordonner des actionneurs et des capteurs au sein d'un local.

Autrement dit, le principe de la domotique est de programmer et contrôler localement ou à distance le comportement d'appareils que l'on aura intégrés dans un réseau. Le réseau qui peut être câblé ou sans fil est destiné à recevoir et émettre des informations entre les unités de commande et les appareils commandés [06].

L'information circule dans les deux sens sur le réseau:

- une unité de commande envoie des informations aux récepteurs chargés de faire effectuer une tache précise à des appareils qui eux-mêmes envoient vers la ou les unités de commande des informations concernant leur état.

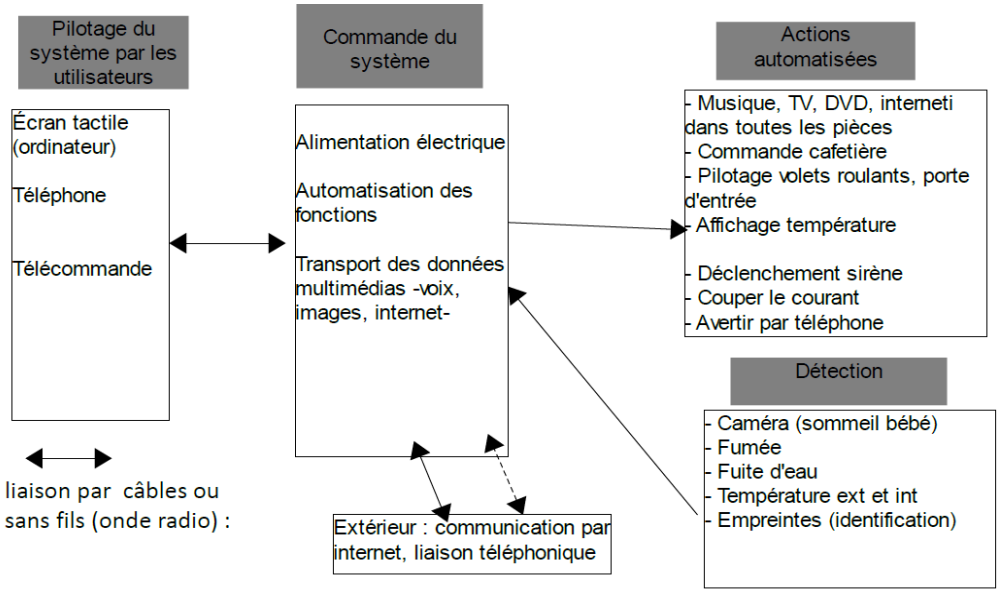

Figure 1.03 : *Fonctionnement de la domotique*

Les informations échangées entre les différents appareils sur un réseau domotique communiquent en respectant un langage appelé "protocole".

Certains réseaux domotiques nécessitent des interfaces appelées "passerelles" chargées de faire communiquer des appareils qui communiquent via des protocoles différents (ce sont en quelque sorte des traducteurs).

1.3.1 Les équipements domotiques

Pour le bon fonctionnement du système domotique, il est nécessaire d'avoir un ordinateur central. Ensuite des modules émetteurs, récepteurs et capteurs (ou détecteurs) qui permettront à l'ordinateur de gérer les tâches domestiques quotidiennes, de réagir à un stimulus imprévu, de vérifier le bon fonctionnement général du système [07].

1.3.1.1 L'ordinateur central

L'ordinateur central constitue le cerveau de l'installation domotique. Il est ainsi en mesure de contrôler la totalité des appareils domestiques reliés à l'installation, ou plutôt la totalité des modules reliés à l'installation. Ce sont ces modules, qui à leur tour, sont en relation directe avec les appareils domestiques.

1.3.1.2 Le récepteur

L'intérêt d'un système réside dans le fait que tous les appareils de la maison peuvent y être reliés. Ainsi, la mise en marche (ou l'arrêt) de chacun des appareils domestiques peut être commandée par l'ordinateur central. Pourtant, des équipements tels que les fours, le chauffe-eau ne sont pas vendus dans le commerce comme étant conçus spécifiquement pour telle ou telle installation domotique. C'est grâce à l'utilisation des modules récepteurs que cette performance soit possible. Ces derniers sont directement reliés au réseau électrique de la maison et se présente sous la forme d'une prise secteur légèrement plus encombrante que les prises courantes. Il suffit alors de brancher les appareils sur ces modules afin de permettre au PC central d'en prendre le contrôle.

1.3.1.3 L'émetteur

Le PC central communique avec les modules récepteurs par l'intermédiaire d'une interface directement reliée entre l'ordinateur et le réseau électrique de la maison, qui utilise un protocole domotique (X10, EIB/KNX). Or, contrairement à ce que l'on aurait pu penser jusqu'ici, il n'est pas nécessaire de laisser l'ordinateur allumé en permanence : l'installation domotique peut fonctionner même s'il est éteint. Ceci est possible grâce à l'utilisation de modules émetteurs.

Le principe est très simple : l'ordinateur central envoie, une seule fois, les commandes et l'heure à laquelle effectuer ces commandes au module émetteur. Ensuite, même si l'ordinateur est éteint, le

module émetteur continue d'envoyer les commandes aux différents modules récepteurs installés dans la maison.

1.3.1.4 Les capteurs et détecteurs

Les modules détecteurs/capteurs jouent un rôle important dans la partie « sécurité » d'une installation domotique.

Par exemple, l'existence de modules qui détectent le bris de verre ; en cas d'infraction, un signal d'alarme est donc rapidement déclenché.

Ces modules jouent le rôle de vigiles et envoient un signal à l'ordinateur central dès qu'ils ont repéré une action inhabituelle.

1.3.2 Les réseaux domotiques

La domotique est basée sur la mise en réseau des différents appareils électriques de la maison contrôlés par une "intelligence" centralisée. L'intelligence qui gère ces commandes est une centrale programmable, des modules embarqués (passerelles domestiques) ou bien une interface micro-informatique (écran tactile, serveur, etc.) [08].

Cette interconnexion d'équipements domestiques hétérogènes (ordinateurs, téléviseurs, assistants numériques personnels PDA, matériel Hi-Fi, appareils électroménagers.) dans le but de proposer des services à valeurs ajoutées aux utilisateurs qu'on appelle réseau domotique. L'accès peut se faire soit depuis l'intérieur du domicile (sur des médias filaires ou sans fils), soit depuis l'extérieur via l'Internet ou via un Smartphone ou un ordinateur.

Deux familles de réseaux coexistent, les réseaux de type traditionnel : exploitation du câblage électrique de la maison comme outil de transmission et les signaux électriques comme langage de transmission ; et les réseaux basés sur le modèle TCP/IP, de plus en plus en vogue.

1.3.2.1 Les réseaux domestiques traditionnels

Ces réseaux, avant-gardistes de la domotique, se servent de courants porteurs en ligne (CPL) prenant en charge le transfert d'informations numériques via les lignes électriques. Ce fonctionnement utilise un autre signal que celui émis par le courant électrique de 50 Hz, un signal

à plus haute fréquence mais consommant moins d'énergie qui vogue vers l'installation électrique. Ce même signal est ensuite reçu par tout récepteur adéquat, un CPL. Les courants porteurs en ligne haut débit sont réservés au transfert de données informatiques, au partage d'un accès à Internet, et les courants porteurs en ligne bas débit concernent davantage un système de domotique standard afin de mettre en réseau machines à laver, volets roulants, lave-vaisselle, chauffe-eau, radiateurs.

1.3.2.2 Les réseaux domotiques TCP/IP

Ces réseaux filaires sont de plus en plus utilisés dans le cadre de la domotique. Il s'agit de mettre en place un câblage universel VDI (voix-données-image) relié à des prises RJ45, lesquelles sont liées à un boîtier placé dans l'armoire électrique. Discrétion, facilité, pratique et efficacité, les prises RJ45 sont très « prisées ». Le principe : entrent en scène les récepteurs ayant pour tâche de transférer les ordres provenant de l'ordinateur central ou d'un module émetteur. Ces réseaux sont amenés à dominer le système domotisé étant donné les termes des normes en vigueur, très précises sur ce point.

1.4 Les technologies appliquées à la domotique

Dans cette partie, nous allons détailler les différentes technologies appliquées à la domotique telles que les technologies de support de transport et les technologies de découverte des services.

1.4.1 Matériels et technologies de support de transport

Les réseaux domotiques concernent les infrastructures de communication proposées traditionnellement pour le contrôle d'équipements d'habitation. Ils concernent aussi bien des technologies sans fils, radio ou infrarouge, ou encore des technologies filaires.

1.4.1.1 Les technologies filaires

a. X10

X10 est une technologie qui utilise le CPL (Courant Porteur en Ligne). Elle permet aux produits compatibles de dialoguer ensemble via les fils électriques du secteur de l'habitation. L'avantage est qu'il n'est pas nécessaire d'installer de nouveaux câbles de communication, on réutilise ceux déjà en place (les fils par lesquels arrive le courant électrique), et ceci sans dégradation. Le signal

de communication est superposé à la tension 110 Volts ou 220 Volts. Le protocole X10 régit la communication entre les commandes (télécommandes, boitiers de contrôle ou ordinateurs) et les différents équipements de la maison. Pour cela, on place entre les appareils à commander et les prises de courant des modules de communications.

La norme X10 utilise des transmetteurs spécifiques qui émettent un signal codé à travers le réseau électrique de la maison. Les récepteurs X10 branchés entre les appareils et les prises de courant détectent ce signal et agissent en fonction du message reçu. Le contrôle des messages est effectué grâce à un tableau de commande, une télécommande ou encore par un ordinateur, relié à un transmetteur qui relayera les ordres aux différents modules branchés sur le réseau électrique [9][10].

La technologie X10 possède les avantages suivants :

- Contrôle automatique des lumières extérieures ou des lampes de sécurité.
- Simulation de présence dans la maison en cas d'absence.
- Commande de toutes les lumières intérieures et extérieures avec les télécommandes RF
- Programmation des scénarios pour un système X10 avec lequel il est possible d'exécuter plusieurs commandes simultanément comme par exemple « Allumer toutes les lampes » ou « Scénario matin » suivant un mode de vie personnelle.
- Installation d'interrupteurs grâce aux interrupteurs sans fils dans n'importe quel endroit où il n'y a pas de câbles.
- Adaptation des maisons pour des personnes âgées ou des personnes handicapées d'une façon simple et flexibles. Grâce aux télécommandes sans fil ils peuvent commander tout en poussant sur un seul bouton.

La figure 1.04 représente les différents équipements dans une installation X10 [10].

Figure 1.04 : *Un système X10*

La domotique se trouve au carrefour de l'informatique, de l'électronique et du contrôle des maisons. Dans ce cadre, le protocole X10 se positionne comme une solution simple, économique et efficace. Cette technologie commence à se développer et, de plus, des solutions intéressantes sont proposées dans le commerce. Le X10 se positionne comme une technologie puissante et bon marché avec de grandes perspectives d'évolution de par sa facilité de mise en œuvre.

b. HAVi

Home Audio Video interoperability est le nom de l'organisation créée par Grunidg, Hitachi, Matsushita/ Panasonic, Philips, Sharp, Thomson multimédia et Toshiba pour développer des spécifications visant à faciliter la communication entre équipements grand public audiovisuels et multimédias dans la maison [11].

La spécification HAVi 1.0 définit un ensemble de modules logiciels (API et middleware) qui automatisent l'échange des messages entre équipements et la mise en commun de leurs ressources par le biais du bus série. Toute application tournant sur un produit HAVi est alors capable de détecter et d'utiliser une fonction offerte par un autre matériel connecté au réseau, et ce, quelle que soit leurs marques respectives.

c. CEBus

CEBus (Consumer Electronics Bus) est un standard de communication développé par l'EIA (Electronics Industry Association) et le CEMA (Consumer Electronics Manufacturers Association). Ce standard est ouvert et par conséquent tout le monde peut l'utiliser. La norme ne s'applique pas simplement à la transmission par courant porteur mais également à la transmission par câble coaxial, RF et infrarouge. L'inconvénient de CEBus est qu'il y a relativement peu de produits disponibles et le coût de ses produits est élevé [12].

d. EIB

Le standard EIB (European Industrial Bus) est normalisé ISO (International Standardisation Organisation). C'est un système ouvert ; il regroupe plus de 23 organisations nationales. Il couvre tous les besoins concernant l'habitat et le bâtiment en matière de confort, d'économie d'énergie et aussi de sécurité. Contrairement à une installation traditionnelle, dans une installation domotique EIB, seuls les éléments qui ont besoin d'énergie sont reliés au 220V. Tous les interrupteurs et autres capteurs présents ne sont reliés que par un seul câble EIB 29V [13].

La figure 1.05 montre le bus EIB.

Figure 1.05 : *Bus EIB*

Un système EIB se compose de deux éléments :

- les actionneurs qui sont les exécuteurs d'ordres.
  Par exemple : les lampes, stores, vannes, moteurs, prises de courant
- les capteurs qui sont les transmetteurs d'ordres
  Exemple : les interrupteurs, les écrans de commandes, les sondes.

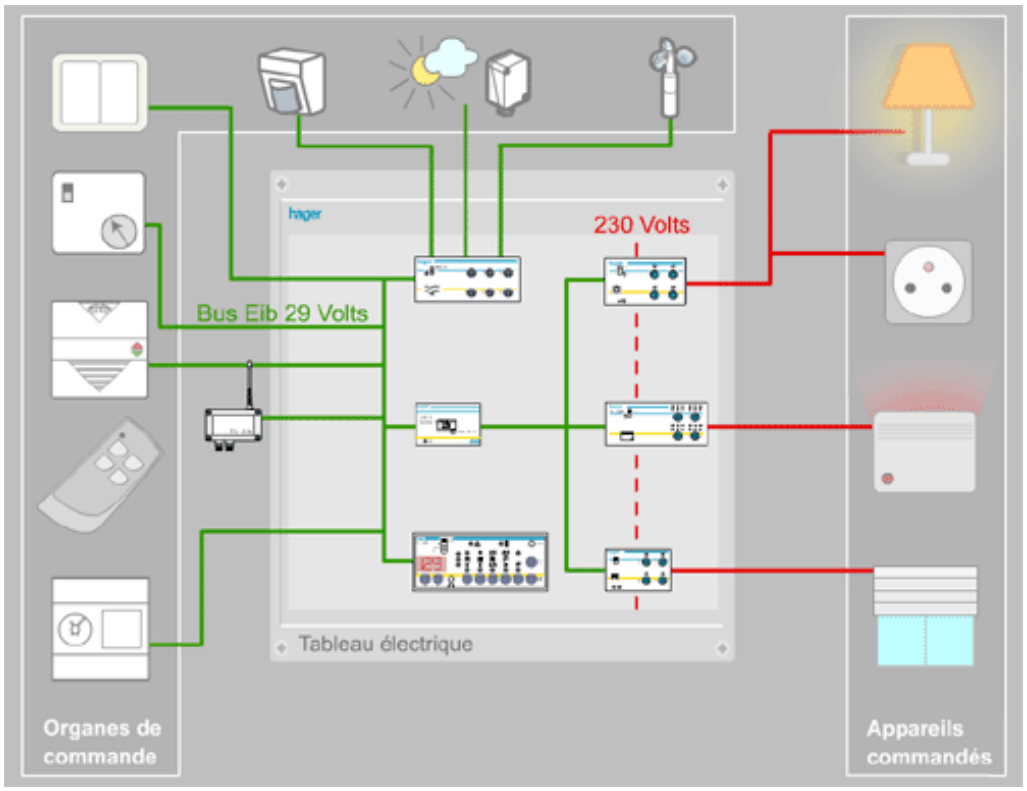

Figure 1.05 : *Une installation EIB*

1.4.1.2 Les technologies sans fil

a. *HomeRF*

HomeRF est une spécification de réseau sans fil (Shared Wireless Access Protocol-SWAP) permettant à des périphériques domestiques d'échanger des données entre eux. Elle a été mise au point par le HomeRF Working Group, un groupe de sociétés actives dans le réseau sans fil incluant Siemens, Motorola et plus de cent autres sociétés. Le groupe a été dissout en Janvier 2003 lorsque la norme Wi-Fi IEEE 802.11 est devenue disponible pour des usages domestiques et que Microsoft a choisi Bluetooth, concurrent direct de HomeRF, dans ses systèmes Windows, ce qui provoqua le déclin de cette spécification [14].

b. *Bluetooth*

Bluetooth, inventé par Ericsson et adapté par Toshiba, IBM et Nokia, est un système de transmission et de réception simultanée ou bien séparée aussi bien des données que de voix. La technologie Bluetooth a pour objectif principal de substituer le câblage entre équipements

électroniques, informatiques et téléphoniques par un lien radio universel (bande ISM à 2.4GHz) courte portée à faible consommation d'énergie. Les équipements en question peuvent être des terminaux téléphoniques, des matériaux électroniques, des PC et leurs périphériques.

Bluetooth, qui s'adapte à l'environnement domestique, permet ainsi de créer de petits réseaux d'équipements (téléphone, ordinateurs, PDA,…) sans avoir les contraintes d'infrastructures fixes des réseaux habituellement mise en œuvre. Les propriétés Bluetooth permettent de gérer un ensemble considérable de dispositifs dans le domicile tout en offrant la possibilité de plusieurs connexions simultanées, ce qui permet par exemple la gestion des alarmes et appels d'urgence pendant l'exécution d'une commande.

Malheureusement, le grand défaut de cette technologie est sa trop grande consommation d'énergie. Elle ne peut donc pas être utilisée par des capteurs qui sont alimentés par une batterie et qui, idéalement, devraient fonctionner durant plusieurs années.

c. *ZigBee*

ZigBee est une technologie radio basée sur le standard IEEE 802.15.4 et destinée en premier lieu au contrôle, à la surveillance et à la gestion des commandes à distance. Des applications peuvent par exemple être trouvées dans le domaine de la domotique tel que :

- Activation d'un éclairage à distance
- Surveillance d'un bâtiment
- Relevé d'informations transmises par des capteurs.

Cette technologie convient particulièrement au marché des bâtiments commerciaux. Le standard ZigBee offre d'une part des caractéristiques qui répondent aux besoins des réseaux domotiques et d'autre part il garantit des débits de données moindres mais consomme également nettement moins d'énergie que Bluetooth. En effet, un petit débit de données n'est pas handicapant pour un réseau de capteurs où les débits de transmission ne sont pas soutenus et conséquents.

En mettant l'accent sur la fiabilité, le faible coût, la longue durée de vie des piles et la facilité du déploiement, ZigBee prépare le terrain pour permettre à des capteurs intelligents d'offrir une efficacité accrue de l'énergie et un meilleur contrôle des systèmes d'éclairage, de chauffage, de climatisation et de sécurité dans les bureaux et dans leurs environs.

Malgré tout, la tendance actuelle des constructeurs est d'employer des technologies propriétaires qui ont pour avantage d'être spécifiquement optimisées pour une utilisation précise mais qui ont comme gros inconvénient de ne pas être compatibles entre elles.

De nouvelles technologies vont influencer considérablement l'avenir des réseaux domotiques. UWB (Ultra Wide Band) en est un très bon exemple. Cette technique de transmission permettra d'atteindre des niveaux de consommation extrêmement bas grâce à sa simplicité au niveau matériel. De plus, l'atténuation du signal engendré par des obstacles est moindre qu'avec les systèmes radio à bande étroite conventionnels.

Il existe une certification ZigBee qui garantit l'interopérabilité des solutions matérielles et logicielles venant de multiples fournisseurs. C'est la ZigBee alliance qui assure le développement et la promotion de la technologie ZigBee. Il constitue un groupe de certification pour la norme IEEE 802.15.4. L'Alliance ZigBee est une association d'entreprises qui collaborent dans la conception des produits de supervision et de contrôle réseau sans fil fiables, économiques et à faible consommation, fondés sur un standard ouvert mondial. L'Alliance ZigBee se compose des fournisseurs de technologies et des fabricants d'équipements dans le monde entier.

1.4.2 Les technologies de découverte de services

Les protocoles de découverte de services étudiés ici ont pour objectif de permettre à un équipement ou un logiciel de trouver les services du réseau domotique d'une manière automatique sans que la configuration manuelle soit nécessaire. Par exemple, les protocoles de découverte des services Jini, SLP, UPnP,… fournissent les mécanismes automatiques pour localiser les services offerts dans un réseau. Ces protocoles permettent aux serveurs de publier leurs services, et aux clients de découvrir ces services.

1.4.2.1 JINI

Jini est une technologie développée et distribuée par Sun Microsystems. Elle offre une infrastructure logicielle permettant à des objets Java (services) de se découvrir et de s'utiliser de façon spontanée.

Un réseau Jini est constitué des entités suivantes :

- Proxy : c'est un objet Java sérialisable qui assure la connexion aux services et les invocations des méthodes
- Service lookup (LUS) : les services enregistrent leurs Proxy auprès des LUS.
- Service : il prépare un Proxy d'accès au service, recherche un LUS et enregistre le service auprès du LUS.
- Client : interroge tous les LUS voisins pour obtenir la liste des Proxy, invoque les méthodes sur un Proxy.

Les concepts de base de Jini sont :

- La découverte : c'est un processus par lequel un client trouve un service lookup pour enregistrer ou demander des services.
- L'enregistrement d'un service (join) : lorsqu'un client reçoit le Proxy du lookup sur lequel il souhaite s'enregistrer, il le fait via la méthode « register() » de l'interface « Service Registrar », de cette façon, le service client a la capacité de transmettre au lookup son propre proxy.
- La recherche d'un service (lookup) : la recherche d'un service se déroule de la même façon que dans l'enregistrement, en invoquant la méthode « lookup() » sur le Proxy du LUS qu'on a reçu lors de la phase de découverte. La spécification de Jini n'impose aucun protocole pour la communication entre les services, bien que l'implémentation de SUN utilise RMI pour contacter le service lookup.

L'inconvénient de Jini est qu'elle a besoin d'un LUS, sorte d'annuaire centralisé et aussi elle est assez lourde à mettre en place.

1.4.2.2 SLP

SLP est un standard proposé par IETF (Internet Engeneering Task Force) pour découvrir spontanément les services dans les réseaux IP. Son architecture est similaire à celle du Jini.

Il définit trois types d'agents :

- Agent Utilisateur (User Agent : UA)
- Agent de service (Service Agent : SA)
- Agent Annuaire (Discovery Agent : DA)

Les UA découvrent les services qui sont offerts par les SA et qui sont enregistrés aux DA.

SLP peut aussi tolérer l'absence de DA, en permettant aux SA de diffuser en Multicast les requêtes de recherche de services. Grâce aux DA et l'utilisation soigneuse de messages Multicast, il peut être utilisé dans les réseaux de grande taille comme les réseaux d'entreprises.

1.4.2.3 UPnP

UPnP (Universal Plug and Play) est un nouveau standard de communication entre périphériques, pour les petites entreprises ou les réseaux résidentiels (SOHO : Small Office Home Office), développé par un consortium dont fait partie Intel et Microsoft.

Il a été développé dans l'optique d'être un standard convivial et flexible pour des réseaux Ad-hoc ou non gérés pour des résidences ou des petits bureaux, des endroits publics. UPnP est plus qu'une simple extension du standard de périphériques Plug and Play. Il permet aux différents périphériques d'un réseau de configurer automatiquement, d'offrir des services de façon dynamique et transparente.

UPnP est une solution qui comporte aussi quelques désavantages.

- Premièrement, une modification est nécessaire au sein des applications afin de permettre aux applications de communiquer avec les dispositifs UPnP.
- Deuxièmement, les périphériques tels que les pare-feu et les routeurs NAT doivent être remplacés par des dispositifs équivalents supportant UPnP.
- Finalement, UPnP peut créer une brèche dans un réseau. En effet, tous les programmes et les dispositifs UPnP peuvent ouvrir des trous d'épingle sans authentification.

En bref, un programme illicite pourrait ouvrir des portes sur un pare-feu ou un routeur NAT et rendre un réseau vulnérable. Cette solution ne peut donc pas être utilisée dans des réseaux d'entreprises.

1.5 Impact économique et social de la domotique

Lorsqu'on s'intéresse aux nouvelles technologies, une des questions principales qui se posent, est l'impact que les personnes peuvent avoir pour celles-ci. C'est pour cela que nous allons citer les intérêts que les gens aient en ayant une maison domotisée.

1.5.1 Impact économique

1.5.1.1 Le gain d'argent

La domotique permet également de faire des économies d'argent car si par exemple, on a oublié d'éteindre certains appareils (la lampe par exemple) et qu'on ne peut pas rentrer pour les éteindre, la consommation augmentera certainement. Mais avec la domotique, on peut les éteindre avec le smartphone ou la tablette et par conséquent la consommation diminuera.

1.5.1.2 Le gain de temps

Le second intérêt réside dans le gain de temps que procurent ces nouvelles technologies. La faculté de contrôler la maison permet de gagner du temps. Les temps perdus à cause des oublis sont souvent considérables. Cela peut causer des retards au bureau et entrainer des ennuis.

Il peut aussi arriver qu'un de vos enfants arrivent à la maison et qu'il ait oublié ses clés. Sans la domotique, il devrait vous joindre pour prendre les clés. Mais si la maison est équipée de domotique, il vous suffit tout simplement de faire un petit clic et la maison peut s'ouvrir.

1.5.2 Impact social

1.5.2.1 Le bien-être

Un premier intérêt qui peut être mis en avant en parlant de la domotique est la question du bien-être, ou autrement dit, plus de confort. Les individus seraient de plus en plus demandeurs de la domotique pour une raison simple, celle de se sentir au mieux dans leur maison.

1.5.2.2 Anticiper les oublis à distance

L'oublie est une chose typiquement humaine. Il peut arriver qu'on se rende quelque part et en cours de route, on constate qu'on n'a pas fermé le robinet du gaz. Normalement, on devra courir

pour le fermer afin d'éviter de brûler la maison. Mais avec la domotique, on peut effectuer l'opération à partir du Smartphone ou de la tablette.

1.5.2.3 Sécurité optimale

Au niveau de la sécurité également, la domotique peut jouer beaucoup. A distance, on peut connaitre en temps réel l'état de la maison. Si jamais il y a un incendie, on peut le constater tout de suite. De même pour les cas de braquage.

1.5.2.4 Préservation de l'écologie et de l'environnement

Qui dit économies dit aussi préservation de l'écologie et de l'environnement en général en ne consommant que si nécessaire et utile donc en polluant moins.

Pollution, gaz à effet de serre et autres catastrophes minent la Terre et les concertations mènent toutes vers la même conclusion : utiliser l'énergie en l'économisant et préserver l'écologie. Et la domotique arrive en tête des concepts permettant de relever le défi. Au-delà de toutes les notions de confort, de simplicité, de fonctionnalité et de liberté, la domotique est une technologie de pointe permettant même l'analyse de vos habitudes quotidiennes et vous permettant par la même occasion de mieux tempérer vos différentes consommations.

1.5.2.5 La dépendance

Avec la domotique, nous sommes à la fois libres et dépendants. Cette nouvelle technologie nous accorderait, certes, plus de liberté, cependant cette dernière serait de l'ordre de l'aliénation, car nous transférions nos capacités à une machine. En effet, nous ne serions plus qu'une simple extension de la machine, vivant avec un sentiment énorme de dépossession et étant dans une relation de dépendance envers les nouvelles technologies.

Ainsi, nous sommes dépendants des pannes. En effet, les technologies de la domotique sont des technologies plus compliquées, qui nous échappent, et qui nous rendent beaucoup plus dépendants. Nous sommes tributaires des spécialistes, contrairement à une maison rustique où sont les objets sont réparables par les habitants. Ces technologies nous subordonnent donc à d'autres personnes.

1.5.2.6 La surveillance, perte de liberté

Avec le développement des nouvelles technologies de la domotique, nous sommes de plus en plus surveillés dans nos sociétés. La domotique nous permet, d'une part, d'avoir plus de pouvoir et de contrôle sur les objets mais, d'un autre côté, nous sommes plus surveillés car on laisse des traces partout. En effet, la technique nous surveille puisqu'elle connaît les actions qui ont été accomplies.

Bref, la domination technologique dans nos maisons représente du danger potentiel comme la perte de liberté. Mais de nombreuses personnes sont désormais prêtes à sacrifier leur liberté au profit de la sécurité.

1.5.2.7 Perte de lien social physique et de la communication

La domotique représente un fort danger pour la sociabilité de l'homme. La solidarité est en voie de disparition dans notre société, car la facilité. E effet, l'usage de cette technologie devient prioritaire et favorise le « chacun pour soi ».

1.5.2.8 Perte de contrôle de la vie

Les utilisateurs de la domotique ne pensent plus à contrôler sa vie ; par exemple, ils ne vérifient plus si ses fenêtres sont déjà fermées. Ils programment simplement l'ouverture et la fermeture de ses fenêtres.

1.6 Conclusion

L'évolution de la technologie et du mode de vie permet aujourd'hui de prévoir des logements mieux adaptés, tant en nouvelle construction qu'en rénovation. On doit ces nouvelles possibilités principalement aux progrès réalisés en électronique et à la nouvelle conception des réseaux de communication tant à l'intérieur qu'à l'extérieur des habitations.

La domotique ouvre non seulement de nouvelles possibilités dans le domaine de l'automatisation de l'habitation, mais constitue aussi et surtout un moyen offert à l'individu de contrôler et de gérer son environnement. Grâce à cette nouvelle technologie, l'habitant sera à même de mieux gérer son milieu de travail et de vie sur le plan de la sécurité, du confort, des communications et des applications ménagères. Par contre, elle rend les hommes dépendant et réduit sa liberté, ainsi favorise le chacun pour soi.

CHAPITRE 2: LA VOIX SUR LE RESEAU IP (VoIP)

2.1 Introduction

La voix sur IP (Voice over IP) est une technologie de communication vocale en pleine émergence. Elle fait partie d'un tournant dans le monde de la communication. En effet, la convergence du triple play (voix, données et vidéo) fait partie des enjeux principaux des acteurs de la télécommunication aujourd'hui. Plus récemment l'Internet s'est étendu partiellement dans l'Intranet de chaque organisation, voyant le trafic total basé sur un transport réseau de paquets IP surpasser le trafic traditionnel du réseau voix (réseau à commutation de circuits). Il devenait clair que dans le sillage de cette avancée technologique, les opérateurs, entreprises ou organisations et fournisseurs devaient, pour bénéficier de l'avantage du transport unique IP, introduire de nouveaux services voix et vidéo. Ce fut en 1996 la naissance de la première version voix sur IP appelée H323. Issu de l'organisation de standardisation européenne UIT-T sur la base de la signalisation voix RNIS (Q931), ce standard a maintenant donné suite à de nombreuses évolutions, quelques nouveaux standards prenant d'autres orientations technologiques.

2.2 Présentation de la VoIP

2.2.1 Définition

VoIP signifie Voice over Internet Protocol ou Voix sur IP. Comme son nom l'indique, elle permet de transmettre des sons (en particulier la voix) dans des paquets IP circulant sur Internet. La VoIP peut utiliser du matériel d'accélération pour réaliser ce but et peut aussi être utilisée en environnement de PC.

2.2.2 Architecture

La VoIP étant une nouvelle technologie de communication, elle n'a pas encore de standard unique. En effet, chaque constructeur apporte ses normes et ses fonctionnalités à ses solutions. Les trois principaux protocoles sont H .323, SIP et MGCP/MEGACO. Il existe donc plusieurs approches pour offrir des services de téléphonie et de visiophonie sur des réseaux IP. Certaines placent l'intelligence dans le réseau alors que d'autres préfèrent une approche égale à égale avec l'intelligence repartie à la périphérie, chacune ayant ses avantages et ses inconvénients [19].

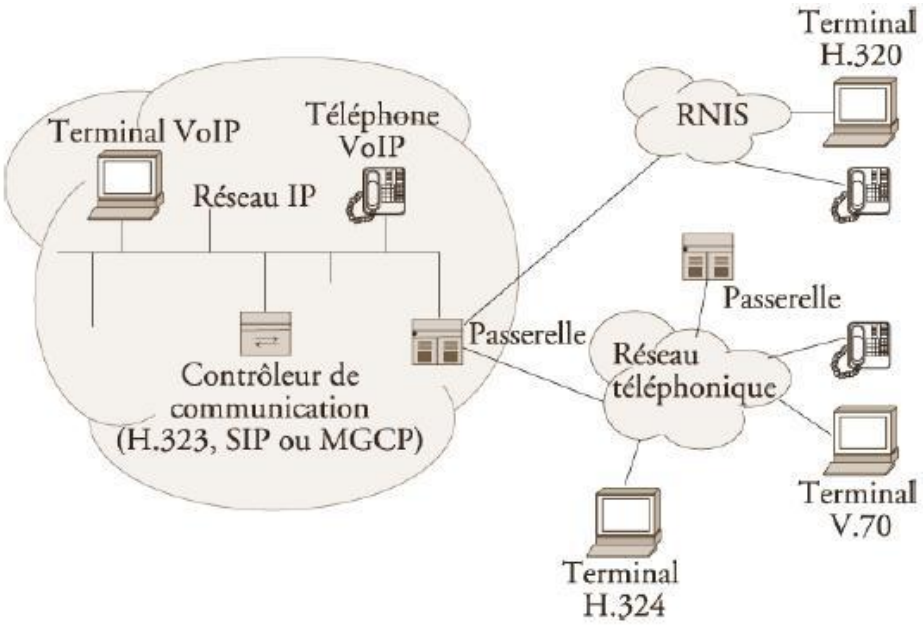

Figure 2.01 : *Topologie d'un réseau VoIP*

La figure 1.1 décrit de façon générale la topologie d'un réseau VoIP. Elle comprend toujours des terminaux, un serveur de communication et une passerelle vers les autres réseaux. Chaque norme a ensuite ses propres caractéristiques pour garantir une plus ou moins grande qualité de service. L'intelligence du réseau est aussi déportée soit sur les terminaux, soit sur les passerelles/contrôleur de commutation, appelées Gatekeeper. On retrouve les éléments communs suivants :

- Le routeur : permet d'aiguiller les données et le routage des paquets entre deux réseaux. Certains routeurs permettent de simuler un Gatekeeper grâce à l'ajout des cartes spécialisées supportant les protocoles VoIP.
- La passerelle : permet d'interfacer le réseau commuté et le réseau IP.
- Le PABX : est le commutateur du réseau téléphonique classique. Il permet de faire le lien entre la passerelle ou le routeur, et le réseau téléphonique commuté (RTC). Toutefois, si tout le réseau devient IP, ce matériel devient obsolète.
- Les Terminaux : sont généralement de type logiciel (software phone) ou matériel (hardphone), le softphone est installé dans le PC de l'utilisateur. L'interface audio peut être un microphone et des haut-parleurs branchés sur la carte son, même si un casque est recommandé. Pour une meilleure clarté, un téléphone USB ou Bluetooth peut être utilisé.

Pour transmettre les paquets, on utilise RTP, standardisé en 1996. Il est un protocole adapté aux applications présentant des propriétés temps réel. Il permet ainsi de reconstituer la base de temps des flux (horodatage des paquets : possibilité de resynchronisation des flux par le récepteur), de détecter les pertes de paquets et en informer la source, et d'identifier le contenu des données pour leurs associer un transport sécurisé.

En revanche, ce n'est pas "la solution" qui permettrait d'obtenir des transmissions temps réel sur IP. En effet, il ne procure pas de réservation de ressources sur le réseau, de fiabilisation des échanges (pas de retransmission automatique, pas de régulation automatique du débit) et de garantie dans le délai de livraison (seules les couches de niveau inférieur le peuvent) et dans la continuité du flux temps réel. Bien qu'autonome, RTP peut être complété par RTCP. Ce dernier apporte un retour d'informations sur la transmission et sur les éléments destinataires. Ce protocole de contrôle permet de renvoyer à la source des informations sur les récepteurs et ainsi lui permettre, par exemple, d'adapter un type de codage ou encore de modifier le débit des données.

2.2.3 Gateway et gatekeeper

La passerelle est un des éléments clefs d'un réseau VoIP. Les passerelles ou gateways en téléphonie IP sont des ordinateurs qui fournissent une interface où se fait la convergence entre les réseaux téléphoniques commutés (RTC) et les réseaux basés sur la commutation de paquets TCP/IP. C'est une partie essentielle de l'architecture du réseau de téléphonie IP. Le gatekeeper est l'élément qui fournit de l'intelligence à la passerelle. Comme nous l'avons déjà fait remarquer, nous pouvons séparer les parties matérielles et logicielles d'une passerelle. Le gatekeeper est le compagnon logiciel du gateway.

Un gateway permet aux terminaux d'opérer en environnements hétérogènes. Ces environnements peuvent être très différents, utilisant diverses technologies telles que le Numéris, la téléphonie commutée ou la téléphonie IP. Les gateways doivent aussi être compatibles avec les terminaux téléphoniques analogiques. Le gateway fournit la possibilité d'établir une connexion entre un terminal analogique et un terminal multimédia (un PC en général). Beaucoup de sociétés fournissent des passerelles mais cela ne signifie pas qu'elles fournissent le même service. Les gateways (partie physique) et les gatekeepers (partie logicielle) font l'objet de deux sections séparées pour bien cerner la différence. Certaines sociétés vendent un produit " gateway ", mais en

réalité, elles incorporent un autre gateway du marché avec leur gatekeeper pour proposer une solution commerciale [20].

Un gatekeeper fournit deux services principaux : la gestion des permissions et la résolution d'adresses. Le gatekeeper est aussi responsable de la sécurité. Quand un client veut émettre un appel, il doit le faire au travers du gatekeeper. C'est alors que celui-ci fournit une résolution d'adresse du client de destination. Dans le cas où il y a plusieurs gateways sur le réseau, il peut rediriger l'appel vers un autre couple gateway/gatekeeper qui essaiera à son tour de router l'appel. Pendant la résolution d'adresse, le gatekeeper peut aussi attribuer une certaine quantité de bande passante pour l'appel. Il peut agir comme un administrateur de la bande passante disponible sur le réseau. Le gatekeeper répond aux aspects suivants de la téléphonie IP :

- Le routage des appels : En effet, le gatekeeper est responsable de la fonction de routage. Non seulement, il doit tester si l'appel est permis et faire la résolution d'adresse mais il doit aussi rediriger l'appel vers le bon client ou la bonne passerelle.

- Administration de la bande passante : Le gatekeeper alloue une certaine quantité de bande passant pour un appel et sélectionne les codecs à utiliser. Il agit en tant que régulateur de la bande passante pour prémunir le réseau contre les goulots d'étranglement (bottle-neck).

- Tolérance aux fautes, sécurité : Le gatekeeper est aussi responsable de la sécurité dans un réseau de téléphonie IP. Il doit gérer les redondances des passerelles afin de faire aboutir tout appel. Il connaît à tout moment l'état de chaque passerelle et route les appels vers les passerelles accessibles et qui ont des ports libres.

- Gestion des différentes gateways : Dans un réseau de téléphonie IP, il peut y avoir beaucoup de gateways. Le gatekeeper, de par ses fonctionnalités de routage et de sécurité, doit gérer ces gateways pour faire en sorte que tout appel atteigne sa destination avec la meilleure qualité de service possible.

Ainsi, le gatekeeper peut remplacer le classique PABX. En effet, il est capable de router les appels entrant et de les rediriger vers leur destination ou une autre passerelle. Mais il peut gérer bien d'autres fonctions telles que la conférence ou le double appel. Il n'existe pas les mêmes contraintes avec un gatekeeper qu'avec un PABX. En effet, ce dernier est constitué par du logiciel et l'opérateur peut implémenter autant de services qu'il le désire. Alors qu'avec un PABX,

l'évolutivité est limitée par le matériel propriétaire de chaque constructeur, avec le gatekeeper, l'amélioration des services d'un réseau de téléphonie IP n'a pas de limites. Le grand bénéfice du développement d'un gros gatekeeper est de remplacer le PABX classique. En effet, chaque PABX utilise son propre protocole pour communiquer avec les postes clients, ce qui entraîne un surcoût. Avec le couple gateway/gatekeeper, ce problème n'existe pas. Il utilise des infrastructures qui existent, le LAN et des protocoles tels qu'IP [21].

2.2.4 Principe de fonctionnement

Depuis de nombreuses années, il est possible de transmettre un signal à une destination éloignée sous forme de données numériques. Avant la transmission, il faut numériser le signal à l'aide d'un CAN (Convertisseur Analogique-Numérique) ; le signal est ensuite transmis, pour être utilisable, il doit être transformé de nouveau en un signal analogique, à l'aide d'un CNA (Convertisseur Numérique-Analogique) [22].

La VoIP fonctionne par numérisation de la voix, puis par reconversion des paquets numériques en voix à l'arrivée. Le format numérique est plus facile à contrôler, il peut être compressé, routé et converti en un nouveau format meilleur. Le signal numérique est plus tolérant au bruit que l'analogique.

Les réseaux TCP/IP sont des supports de circulation de paquets IP contenant un en-tête (pour contrôler la communication) et une charge utile pour transporter les données.

Il existe plusieurs protocoles qui peuvent supporter la Voix sur IP tel que le H.323, SIP et MGCP. Mais les plus utilisées actuellement dans les solutions VoIP présentes sur les marchés sont le H.323 et le SIP.

2.3 Les protocoles de signalisation

2.3.1 Protocole H.323

2.3.1.1 Description générale

H.323 est un protocole de communication englobant un ensemble de normes utilisées pour l'envoi de données audio et vidéo sur Internet. Il existe depuis 1996 et a été initié par l'UIT (Union Internationale Communication), un groupe international de téléphonie qui développe des standards

de communication. Concrètement, il est utilisé dans des programmes tels que Microsoft Netmeeting, ou encore dans des équipements tels que les routeurs Cisco. Il existe un projet OpenH.323 qui développe un client H.323 en logiciel libre afin que les utilisateurs et les petites entreprises puissent avoir accès à ce protocole sans avoir à débourser beaucoup d'argent.

Le protocole H.323 est utilisé pour l'interactivité en temps réel, notamment la visioconférence (signalisation, enregistrement, contrôle d'admission, transport et encodage). Il fait partie de la série H.32x qui traite de la vidéoconférence au travers différents réseaux. Il inclue H.320 et H.324 liés aux réseaux ISDN (Integrated Service Data Network) et PSTN (Public Switched Telephone Network).

Une communication H.323 se déroule en cinq phases :

- établissement d'appel ;
- échange de capacité et réservation éventuelle de la bande passante à travers le protocole RSVP (Resource reSerVation Protocol) ;
- établissement de la communication audio-visuelle ;
- invocation éventuelle de services en phase d'appel (par exemple, transfert d'appel, changement de bande passante,…) ;
- libération de l'appel [23].

2.3.1.2 Architecture H.323

L'infrastructure H.323 repose sur quatre composants principaux : les terminaux, les passerelles (Gateways : GW), les portiers (Gatekeepers : GK), et les unités de contrôle multipoint (Multipoint Control Unit : MCU).

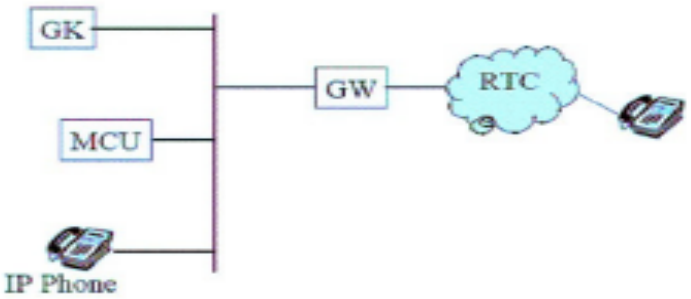

Figure 2.02 : *Architecture H.323*

- Les terminaux : Un terminal H.323 est soit un poste téléphonique IP raccordé directement au réseau Ethernet ; soit un PC (muni d'une carte son et d'un micro) sur lequel est installée une application compatible H.323. Ce composant joue un rôle clé dans VoIP car c'est à partir de lui que seront émises et reçues les conversations des utilisateurs. Le premier rôle du standard H.323 est de permettre les échanges entre les terminaux.

- Les passerelles : Elles assurent l'interconnexion avec les autres réseaux, comme H.320/RNIS, les modems H.324, téléphones classiques,… Elles assurent la correspondance de signalisation de Q.931, la correspondance des signaux de contrôle et la cohésion entre les médias (multiplexage, correspondance des débits, transcodage audio).

- Les portiers ou gardes-barrière : Ils sont des éléments optionnels dans une solution H.323. Ils ont pour rôle de réaliser la traduction d'adresse (numéro de téléphone – adresse IP) ou translation d'adresse entre les alias des terminaux et leur adresse (les alias peuvent être de type E.164 (numéro de téléphone) ou un identifiant tel qu'un nom de machine ou une adresse e-mail) et la gestion des autorisations. Cette dernière permet de donner ou non la permission d'effectuer un appel, de limiter la bande passante si besoin et de gérer le trafic sur le LAN. Les « gardes-barrière » permettent également de gérer les téléphones classiques et la signalisation permettant de router les appels afin d'offrir des services supplémentaires, ils peuvent enfin offrir des services d'annuaires.

- Les unités de contrôle multipoint : Les MCU offrent aux utilisateurs la possibilité de faire des visioconférences à trois terminaux et plus en « présence continue » ou en « activation à la voix ». Une MCU consiste en un Contrôleur Multipoint (MC), auquel est rajouté un ou plusieurs Processeurs Multipoints (MP). Le MC prend en charge les négociations H.245 entre tous les terminaux pour harmoniser les paramètres audio et vidéo de chacun. Il contrôle également les ressources utilisées. Mais le MC ne traite pas directement avec les flux audio, vidéo ou données. C'est le MP qui se charge de récupérer les flux et de leur faire subir les traitements nécessaires. Un MC peut contrôler plusieurs MP distribués sur le réseau et faisant partie d'autres MCU [23].

2.3.1.3 Les avantages et inconvénients de la technologie H.323

La technologie H.323 possède des avantages et des inconvénients. Parmi ces avantages, nous citons :

- Gestion de la bande passante : H.323 permet une bonne gestion de la bande passante en posant des limites aux flux audio/vidéo afin d'assurer le bon fonctionnement des applications critiques sur le LAN. Chaque terminal H.323 peut procéder à l'ajustement de la bande passante et la modification du débit en fonction du comportement du réseau en temps réel (latence, perte de paquets et gigue).
- Support Multipoint : H.323 permet de faire des conférences multipoint via une structure centralisée de type MCU (Multipoint Control Unit) ou en mode ad-hoc.
- Support Multicast : H.323 permet également de faire des transmissions en multicast.
- Interopérabilité : H.323 permet aux utilisateurs de ne pas se préoccuper de la manière dont se font les communications, les paramètres (les codecs, le débit…) sont négociés de manière transparente.
- Flexibilité : Une conférence H.323 peut inclure des terminaux hétérogènes (studio de visioconférence, PC, téléphones…) qui peuvent partager selon le cas, de la voix, de la vidéo et même des données grâce aux spécifications T.120 [26].

Le H.323 présente toutefois les inconvénients suivants :

- La complexité de mise en œuvre et les problèmes d'architecture en ce qui concerne la convergence des services de téléphone et d'internet, ainsi qu'un manque de modularité et de souplesse.
- Comprend de nombreuses options susceptibles d'être implémentées de façon différentes par les constructeurs et donc de poser des problèmes d'interopérabilités.

2.3.2 Protocole SIP

2.3.2.1 Description générale du protocole SIP

Le protocole SIP (Session Initiation Protocol) est un protocole normalisé et standardisé par l'IETF (décrit par le RFC 3261 qui rend obsolète le RFC 2543, et complété par le RFC 3265) qui a été conçu pour établir, modifier et terminer des sessions multimédia. Il se charge de l'authentification

et de la localisation des multiples participants. Il se charge également de la négociation sur les types de media utilisables par les différents participants en encapsulant des messages SDP (Session Description Protocol). SIP ne transporte pas les données échangées durant la session comme la voix ou la vidéo. SIP étant indépendant de la transmission des données, tout type de données et de protocoles peut être utilisé pour cet échange. Cependant le protocole RTP (Real-time Transport Protocol) assure le plus souvent les sessions audio et vidéo. SIP remplace progressivement H.323.

SIP est le standard ouvert de VoIP, interopérable, le plus étendu et vise à devenir le standard de télécommunications multimédia (son, image,…). Skype par exemple, qui utilise un format propriétaire, ne permet pas l'interopérabilité avec un autre réseau de voix sur IP et ne fournit que des passerelles payantes vers la téléphonie standard. SIP n'est donc pas seulement destiné à la VoIP mais pour de nombreuses autres applications telles que la visiophonie, la messagerie instantanée, la réalité virtuelle ou même les jeux vidéo [27].

2.3.2.2 Principe de fonctionnement

SIP intervient aux différentes phases de l'appel :

- Localisation du terminal correspondant
- Analyse du profil et des ressources du destinataire
- Négociation du type de média (voix, vidéo, données…) et des paramètres de communication
- Disponibilité du correspondant, détermine si le poste appelé souhaite communiquer, et autorise l'appelant à le contacter
- Etablissement et suivi de l'appel, avertit les parties appelant et appelé de la demande d'ouverture de session, gestion du transfert et de la fermeture des appels.
- Gestion de fonctions évoluées : cryptage, retour d'erreurs,…

Puisque nous choisirons le protocole SIP pour effectuer notre travail, nous nous appliquerons à expliquer les différents aspects, caractéristiques qui font du protocole SIP un bon choix pour l'établissement de la session, les principales caractéristiques du protocole SIP sont :

a. *Fixation d'un compte SIP*

Il est important de s'assurer que la personne appelée soit toujours joignable. Pour cela, un compte SIP sera associé à un nom unique. Par exemple, si un utilisateur d'un service de voix sur IP dispose d'un compte SIP et que chaque fois qu'il redémarre son ordinateur, son adresse IP change, il doit cependant toujours être joignable. Son compte SIP doit donc être associé à un serveur SIP (proxy SIP) dont l'adresse IP est fixe. Ce serveur lui allouera un compte et il permettra d'effectuer ou de recevoir des appels quel que soit son emplacement. Ce compte sera identifiable via son nom (ou pseudo).

b. *Changement des caractéristiques durant une session*

Un utilisateur doit pouvoir modifier les caractéristiques d'un appel en cours. Par exemple, un appel initialement configuré en voix uniquement peut être modifié en voix + vidéo.

c. *Différents modes de communication*

Avec SIP, les utilisateurs qui ouvrent une session peuvent communiquer en mode point à point, en mode diffusif ou dans un mode combinant ceux-ci.

- Mode Point à point : on parle dans ce cas-là d' « unicast » qui correspond à la communication entre deux machines.
- Mode diffusif : on parle dans ce cas-là de « multicast ». Plusieurs utilisateurs via une unité de contrôle MCU.
- Combinatoire : combine les deux modes précédents. Plusieurs utilisateurs interconnectés en multicast via un réseau à maillage complet de connexion.

d. *Gestion des participants*

Durant une session d'appel, de nouveaux participants peuvent joindre les participants d'une session déjà ouverte en participant directement, en étant transférés ou en étant mis en attente (cette particularité rejoint les fonctionnalités d'un PABX par exemple, où l'appelant peut être transféré vers un numéro donné ou être mis en attente).

e. Négociation des médias supportés

Cela permet à un groupe durant un appel de négocier sur les types de médias supportés. Par exemple, la vidéo peut être ou ne pas être supportée lors d'une session.

f. Adressage

Les utilisateurs disposant d'un numéro (compte) SIP disposent d'une adresse ressemblant à une adresse mail (sip : numéro@serveursip.com); le numéro SIP est unique pour chaque utilisateur.

g. *Modèle d'échange*

Le protocole SIP repose sur un modèle Requête/Réponse. Les échanges entre un terminal appelant et un terminal appelé se font par l'intermédiaire de requêtes. La liste des requêtes échangées est la suivante :

- Invite : cette requête indique que l'application (ou utilisateur) correspondante à l'URL SIP spécifié est invité à participer à une session. Le corps du message décrit cette session (par exemple : média supportés par l'appelant). En cas de réponse favorable, l'invité doit spécifier les médias qu'il supporte.
- Ack : cette requête permet de confirmer que le terminal appelant a bien reçu une réponse définitive à une requête Invite.
- Option : proxy server en mesure de contacter l'UAS (terminal) appelé, doit répondre à une requête Option en précisant ses capacités à contacter le même terminal.
- Bye : cette requête est utilisée par le terminal de l'appelé afin de signaler qu'il souhaite mettre un terme à la session.
- Cancel : cette requête est envoyée par un terminal ou un proxy server afin d'annuler une requête non validée par une réponse finale comme, par exemple, si une machine ayant été invitée à participer à une session, et ayant accepté l'invitation ne reçoit pas de requête Ack, alors elle émet une requête Cancel.
- Register : cette méthode est utilisée par le client pour enregistrer l'adresse listée dans l'URL To par le serveur auquel il est relié [25].

Une réponse à une requête est caractérisée, par un code et un motif, appelés respectivement code d'état et raison phrase. Un code d'état est un entier codé sur 3 digits indiquant un résultat à l'issue

de la réception d'une requête. Ce résultat est précisé par une phrase, textbased (UTF-8), expliquant le motif du refus ou de l'acceptation de la requête. Le code d'état est donc destiné à l'automate gérant l'établissement des sessions SIP et les motifs aux programmeurs. Il existe 6 classes de réponses et donc de codes d'état, représentées par le premier digit :

- 1xx = Information - La requête a été reçue et continue à être traitée.
- 2xx = Succès – L'action a été reçue avec succès, comprise et acceptée.
- 3xx = Redirection – Une autre action doit être menée afin de valider la requête.
- 4xx = Erreur de client – La requête contient une syntaxe erronée ou ne peut pas être traitée par ce serveur.
- 5xx = Erreur du serveur – Le serveur n'a pas réussi à traiter une requête apparemment correcte.
- 6xx = Echec général – La requête ne peut être traitée par aucun serveur.

2.3.2.3 Architecture SIP

L'architecture SIP définit deux grandes familles d'entités qui sont les entités utilisatrices (clients) et les entités réseau (serveurs). La figure ci-dessous illustre cette architecture [30].

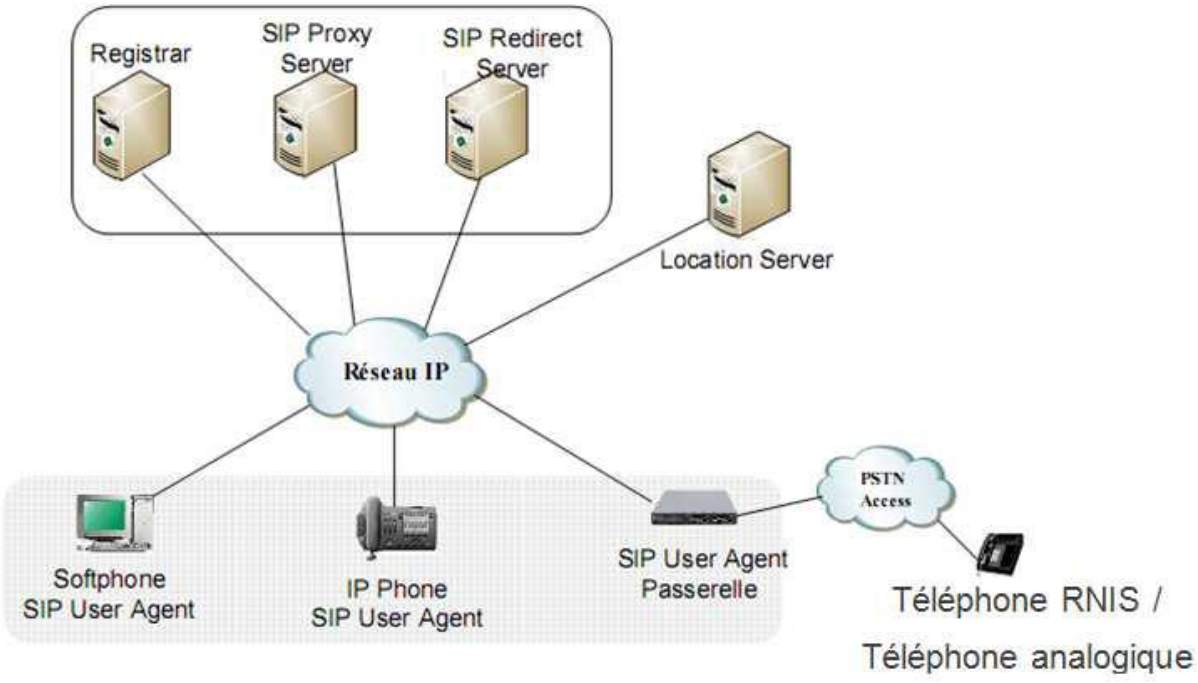

Figure 2.03 : *Entités d'une architecture SIP*

a. Clients SIP

Les clients SIP sont appelés agent utilisateur ou UA (User Agent) ou plus simplement terminal utilisateur. Chaque UA contient un UAC (User Agent Client) et un UAS (User Agent Server).

- L'UAS : il représente l'agent de la partie appelée. C'est une application de type serveur qui contacte l'utilisateur lorsqu'une requête SIP est reçue. Et elle renvoie une réponse au nom de l'utilisateur.
- L'UAC : il représente l'agent de la partie appelante. C'est une application de type clients qui initient les requêtes.

b. Serveurs SIP

SIP définit des entités logiques de type serveur faisant partie du réseau et agissant pour étendre son fonctionnement. Les serveurs SIP sont des applications qui acceptent les requêtes d'un terminal SIP. Il y a quatre types de serveurs SIP :

- Le PS (Proxy Server) ou relais mandataire, auquel est relié un terminal fixe ou mobile, agit à la fois comme un client et comme un serveur. Un tel serveur peut interpréter et modifier les messages qu'il reçoit avant de les retransmettre. Il interprète et route l'appel en direction du destinataire. Il se peut que le proxy ne sache pas où se trouve le destinataire, c'est pourquoi dans ce cas-là, il consulte un serveur de localisation. Il y a deux sortes de proxy : les proxys « stateful » et « stateless », la différence est le fait que le proxy « stateful » enregistre la position du destinataire tandis que le proxy « stateless » ne la mémorise pas. Ce qui fait que le proxy « stateful » consulte une seule fois le serveur de localisation par destination jusqu'à ce que la destination soit effacée de sa « table de routage ».
- Le RS (Redirect Server) ou serveur de direction : il réalise simplement une association (mapping) d'adresses vers une ou plusieurs nouvelles adresses (lorsqu'un client appelle un terminal mobile – redirection vers le PS le plus proche, ou en mode multicast – le message émis est redirigé vers toutes les sorties auxquelles sont reliés les destinataires). Notons qu'un Redirect Server est consulté par l'UAC comme un simple serveur et ne peut émettre de requêtes contrairement au PS.

- Le LS (Location Server) ou serveur de localisation : il fournit la position courante des utilisateurs dont la communication traverse les RS et PS auxquels il est rattaché. Cette fonction est assurée par le service de localisation.
- Le RG (Registrar) : c'est un serveur qui accepte les requêtes Register et offre également un service de localisation comme le LS. Chaque PS ou RS est généralement relié à un Registrar.

2.3.2.4 Avantages et inconvénients du SIP

Ouvert, standard, simple et flexible sont les principales atouts du protocole SIP, voilà en détails ces différents avantages :

- Ouvert : les protocoles et documents officiels sont détaillés et accessibles à tous en téléchargement.
- Standard : l'IETF a normalisé le protocole et son évolution continue par la création ou l'évolution d'autres protocoles qui fonctionnent avec SIP.
- Simple : SIP est simple et très similaire à http.
- Flexible : SIP est également utilisé pour tout type de sessions multimédia (voix, vidéo, mais aussi musique, réalité virtuelle,…).
- Téléphonie sur réseaux publics : il existe de nombreuses passerelles (services payants) vers le réseau public de téléphonie (RTC, GSM,…) permettant d'émettre ou de recevoir des appels vocaux.
- Points communs avec H 323 : l'utilisation du protocole RTP et quelques codecs son et vidéo sont en commun.

Par contre, une mauvaise implémentation ou une implémentation incomplète du protocole SIP dans les User Agents peut perturber le fonctionnement ou générer du trafic superflu sur le réseau.

Un autre inconvénient est le faible nombre d'utilisateurs : SIP est encore peu connu et utilisé par le grand public, n'ayant pas atteint une masse critique, il ne bénéficie pas de l'effet réseau.

2.4 Les protocoles de transport

2.4.1 Le protocole RTP

2.4.1.1 Description générale de RTP

RTP (Real time Transport Protocol), standardisé en 1996, est un protocole qui a été développé par l'IETF afin de faciliter le transport temps réel de bout en bout des flots données audio et vidéo sur les réseaux IP, c'est-à-dire sur les réseaux de paquets. RTP est un protocole qui se situe au niveau de l'application et qui utilise les protocoles sous-jacents de transport TCP ou UDP. Mais l'utilisation de RTP se fait généralement au-dessus d'UDP, ce qui permet d'atteindre plus facilement le temps réel. Les applications temps réel comme la parole numérique ou la visioconférence constitue un véritable problème pour Internet. Qui dit application temps réel, dit présence d'une certaine qualité de service (QoS) que RTP ne garantit pas du fait qu'il fonctionne au niveau Applicatif. De plus, RTP possède à sa charge, la gestion du temps réel, mais aussi l'administration de la session multipoint.

2.4.1.2 Les fonctions de RTP

Le protocole RTP a pour but d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie. Ceci de façon à reformer les flux avec ses caractéristiques de départ. RTP est un protocole de bout en bout, volontairement incomplet et malléable pour s'adapter aux besoins des applications. Il sera intégré dans le noyau de l'application. Il laisse la responsabilité du contrôle aux équipements d'extrémité. Il est aussi un protocole adapté aux applications présentant des propriétés temps réel. Il permet ainsi de :

- mettre en place un séquencement des paquets par une numérotation et ce afin de permettre la détection des paquets perdus. Ceci est un point primordial dans la reconstitution des données. Mais il faut savoir quand même que la perte d'un paquet n'est pas un gros problème si les paquets ne sont pas perdus en trop grands nombres. Cependant, il est très important de savoir quel est le paquet qui a été perdu afin de pouvoir pallier à cette perte ;
- identifier le contenu des données pour leur associer un transport sécurisé et reconstituer la base de temps des flux (horodatage des paquets : possibilité de resynchronisation des flux par le récepteur) ;

- identifier la source c'est-à-dire identifier l'expéditeur du paquet. Dans un multicast, l'identité de la source doit être connue et déterminée ;
- transporter les applications audio et vidéo dans des trames (avec des dimensions qui sont dépendantes des codecs qui effectuent la numérisation). Ces trames sont incluses dans des paquets afin d'être transportées et doivent, de ce fait, être récupérées facilement au moment de la phase de segmentation des paquets afin que l'application soit décodée correctement.

2.4.1.3 Avantages et inconvénients

Le protocole RTP permet de reconstituer la base de temps des différents flux multimédia (audio, vidéo,…) ; de détecter les pertes de paquets ; et d'identifier le contenu des paquets pour leur transmission sécurisée.

Par contre, il ne permet pas de réserver des ressources dans le réseau ou d'apporter une fiabilité dans le réseau. Ainsi, il ne garantit pas le délai de livraison.

2.4.2 Le protocole RTCP

2.4.2.1 Description générale de RTCP

Le protocole RTCP est fondé sur la transmission périodique de paquets de contrôle à tous les participants d'une session. C'est le protocole UDP (par exemple) qui permet le multiplexage des paquets de données RTP et des paquets de contrôle RTCP.

Le protocole RTP utilise le protocole RTCP (Real-time Transport control Protocol), qui transporte les informations supplémentaires suivantes pour la gestion de la session : les récepteurs utilisent RTCP pour renvoyer vers les émetteurs un rapport sur la QoS (gigue, délai d'aller-retour). Ces informations permettent à la source de s'adapter, par exemple, de modifier le niveau de compression pour maintenir une QoS.

2.4.2.2 Fonctions de RTCP

Parmi les fonctions qu'offre le protocole RTCP citons les suivantes :

- Une synchronisation supplémentaire entre les médias : Les applications multimédias sont souvent transportées par des flots distincts. Par exemple, la voix, l'image ou même des applications numérisées sur plusieurs niveaux hiérarchiques peuvent voir les flots gérées et suivre des chemins différents.
- L'identification des participants à une session : En effet, les paquets RTCP contiennent des informations d'adresses, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique.
- Le contrôle de la session : En effet, le protocole RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement fournir une indication sur leur comportement.

Le protocole RTCP demande aux participants de la session d'envoyer périodiquement les informations citées ci-dessus. La périodicité est calculée en fonction du nombre de participants de l'application. On peut dire que les paquets RTP ne transportent que les données utilisateurs. Tandis que les paquets RTCP ne transportent en temps réel que de la supervision.

On peut détailler les paquets de supervision en 5 types :

- 200 - SR (Sender Report) : Ce rapport regroupe des statistiques concernant la transmission (pourcentage de perte, nombre cumulé des paquets perdus, gigue,…). Ces rapports sont issus d'émetteurs actifs d'une session.
- 201 - RR (Receiver Report) : Ensemble de statistiques portant sur la communication entre les participants. Ces rapports sont issus des récepteurs d'une session.
- 202 - SDES (Source DEScription) : Carte de visite de la source (nom, e-mail, localisation).
- 203 - BYE : Message de fin de participation à une session.
- 204- APP : Fonctions spécifiques à une application.

Ces différents paquets de supervision fournissent aux nœuds du réseau les instructions nécessaires à un meilleur contrôle des applications temps réel.

2.4.2.3 Avantages et inconvénients de RTCP

Le protocole RTCP est adapté pour la transmission de données temps réel. Il permet d'effectuer un contrôle permanent sur une session et ses participants.

Par contre, il fonctionne en stratégie bout à bout, et il ne peut pas contrôler l'élément principal de la communication « le réseau ».

2.5 Codec

Le transport de la voix sur un réseau IP nécessite au préalable tout ou une partie des étapes suivantes :

- Numérisation : Dans le cas où les signaux téléphoniques à transmettre sont sous forme analogique, ces derniers doivent d'abord être convertis sous forme numérique suivant le format PCM (Pulse Code Modulation) à 64 Kbps. Si l'interface téléphonique est numérique (accès RNIS, par exemple), cette fonction est omise.
- Compression : Le signal numérique PCM à 64 Kbps est compressé selon l'un des formats de codec (Compression/ décompression) puis inséré dans des paquets IP. La fonction de codec est le plus souvent réalisée par un DSP (Digital Signal Processor). Selon la bande passante à disposition, le signal voix peut également être transporté dans son format originel à 64 Kbps.
- Décompression : Coté réception, les informations reçues sont décompressées. Il est nécessaire pour cela d'utiliser le même codec que pour la compression, puis d'effectuer une reconversion dans le format approprié pour le destinataire (analogique, PCM 64 Kbps,...).

L'objectif d'un codec est d'obtenir une bonne qualité de voix avec un débit et un délai de compression les plus faibles possibles. Le coût du DSP est lié à la complexité du codec utilisé. Le tableau ci-dessous présente les caractéristiques des principaux codecs standards de l'UIT. Les codecs les plus souvent mis en œuvre dans les solutions VoIP sont G.711, G.729 et G.723.1.

La qualité d'un codec est mesurée de façon subjective en laboratoire par une population test de personnes. Ces dernières écoutent tout un ensemble de conversations compressées selon les différents codecs à tester et les évaluent qualitativement selon la table suivante :

Qualité de la parole	Score
Excellente	5
Bonne	4
Correcte	3
Pauvre	2
Insuffisante	1

Tableau 2.01: *Mean Opinion Score (MOS)*

Sur la base des données numériques des appréciations, une opinion moyenne de la qualité d'écoute (Mean Opinion Score : MOS) est ensuite calculée pour chaque codec. Les résultats obtenus pour les principaux codecs sont résumés dans le tableau ci-dessous :

Codec	Débit (Kbps)	Score (MOS)
G.711	64	4.1
G.726	32	3.85
G.729	8	3.92
G.723.1a	6.4	3.65
G.723.1b	5.3	3.5

Tableau 2.02: *Score MOS des différents codecs VoIP*

Offrant une qualité de voix très proche, les codecs G.729 et G.723.1 se distinguent essentiellement par la bande passante qu'ils requièrent et par le retard que chacun introduit dans la transmission. Le choix d'un équipement implémentant l'un ou l'autre de ces codecs devra donc être fait selon la situation, en fonction notamment de la bande passante à disposition et du retard cumulé maximum

estimé pour chaque liaison (selon les standards de l'UIT, le retard aller (« one-way delay ») devrait être inférieur à 150 ms). Le facteur du jitter est primordial pour une bonne écoute de la Voip.

2.6 Les paramètres de la VoIP

2.6.1 La latence

La latence désigne le délai de transmission du signal de bout en bout. Plusieurs facteurs influent sur elle : la bande passante disponible, son occupation (trafic), les algorithmes de sécurisation (qui ont tendance à introduire des délais supplémentaires), etc. Trop de latence introduit des blancs dans la conversation qui font perdre son côté naturel.

La maitrise du délai de transmission est un élément essentiel pour bénéficier d'un véritable mode conversationnel et minimiser la perception d'écho.

La durée de traversée d'un réseau IP dépend de nombreux facteurs :

- Le débit de transmission sur chaque lien.
- Le nombre d'éléments réseaux traversés.
- Le temps de traversée de chaque élément, qui est lui-même fonction de la puissance et la charge de ce dernier, du temps de mise en file d'attente des paquets, et du temps d'accès en sortie de l'élément.
- Le délai de propagation de l'information, qui est non négligeable si on communique à l'opposé de la terre. Une transmission par fibre optique, à l'opposé de la terre, dure environ 70ms.

Le temps de transport de l'information n'est pas le seul facteur responsable de la durée totale de traitement de la parole. Le temps de codage et la mise en paquet de la voix contribuent aussi de manière importante à ce délai.

Il est important de rappeler que sur les réseaux IP actuels (sans mécanisme de garantie de qualité de service), chaque paquet IP « fait son chemin » indépendamment des paquets qui le précèdent ou le suivent : c'est ce qu'on appelle grossièrement le « Best effort » pour signifier que le réseau ne contrôle rien. Ce fonctionnement est fondamentalement différent de celui du réseau téléphonique où un circuit est établi pendant toute la durée de la communication.

Les chiffres suivants (tirés de la recommandation UIT-T G114) sont donnés à titre indicatif pour préciser les classes de qualité et d'interactivité en fonction du retard de transmission dans une conversation téléphonique. Ces chiffres concernent le délai total de traitement, et pas uniquement le temps de transmission de l'information sur le réseau.

Classe N°	Délai par sens	Commentaire
1	0 à 150ms	Acceptable pour la plupart des conversations
2	150 à 300ms	Acceptable pour des communications faiblement interactives
3	300 à 700ms	Devient pratiquement une communication half duplex
4	Au-delà de 700ms	Inutilisable sans une bonne pratique de la conversation half duplex

Tableau 2.03 : *Classes de qualité en fonction du temps de latence*

Le délai est très important pour avoir une bonne qualité de la conversation. Le tableau suivant montre l'influence du délai à la qualité vocale.

Délai par sens	Indice de dégradation de la conversation
200 ms	28%
450 ms	35%
700 ms	46%

Tableau 2.04: *Qualité vocale en fonction du délai*

En conclusion, on considère généralement que la limite supérieure « acceptable », pour une communication téléphonique, se situe entre 150 et 200ms par sens de transmission (en considérant à la fois le traitement de la voix et le délai d'acheminement).

2.6.2 La gigue

La gigue est le phénomène provenant de la variation de la latence. En d'autres termes, la gigue mesure la variation temporelle entre le moment où deux paquets auraient dû arriver et le moment de leur arrivée effective. A certains moments, la latence peut être faible, et la voix peut être restituée avec un effet « temps réel » satisfaisant. Puis, une congestion temporaire du réseau peut augmenter le délai d'arrivée des paquets, produisant un effet de parole hachée désagréable et rendant la conversation difficile à comprendre. Cette irrégularité d'arrivée des paquets est due à des multiples raisons dont : l'encapsulation des paquets IP dans les protocoles supportés, la charge du réseau à un instant donné, la variation des chemins empruntés dans le réseau, etc. Une solution pour éviter cela est la mise en mémoire tampon (buffer de gigue), c'est-à-dire la mémorisation préalable d'un certain nombre de paquets avant restitution sonore. L'ennui, c'est que ce processus (bufferisation) tend à augmenter les délais de bout en bout, altérant là encore l'aspect « temps réel ».

La dégradation de la qualité de service à la présence de gigue, se traduit en fait, par une combinaison des deux facteurs : le délai et la perte de paquets ; puisque d'une part on introduit un délai supplémentaire de traitement (buffer de gigue) lorsque l'on décide d'attendre les paquets qui arrivent en retard, et que d'autre part on finit tout de même par perdre certains paquets lorsque ceux-ci ont un retard qui dépasse le délai maximum autorisé par le buffer.

2.6.3 La perte et le dé séquencement de paquets

Ces problèmes sont des erreurs dans la transmission des paquets IP. Certains peuvent se perdre en cours de route, ou encore les paquets peuvent arriver dans le désordre avec une perte d'information ne permettant pas de les réordonnancer correctement. Parmi les solutions mises en œuvre pour lutter contre ces problèmes, l'émission redondante des paquets, l'analyse de leur intégrité et la mise en œuvre de processus d'interpolation pour remplacer les valeurs manquantes font partie de l'attirail disponible.

Lorsque les buffers des différents éléments réseaux IP sont congestionnés, ils « libèrent » automatiquement de la bande passante en se débarrassant d'une certaine proportion des paquets entrant, en fonction des seuils prédéfinis. Cela permet également d'envoyer un signal implicite aux terminaux TCP qui diminuent d'autant leur débit au vu des acquittements négatifs émis par le

destinataire qui ne reçoit plus les paquets. Malheureusement, pour les paquets de voix, qui sont véhiculés au-dessus d'UDP, aucun mécanisme de contrôle de flux ou de retransmission des paquets perdus n'est offert au niveau du transport. D'où l'importance des protocoles RTP et RTCP qui permettent de déterminer le taux de perte de paquet, et d'agir en conséquence au niveau applicatif.

Si aucun mécanisme performant de récupération des paquets perdus n'est mis en place (cas le plus fréquent dans les équipements actuels), alors la perte de paquet IP se traduit par des ruptures au niveau de la conversation et une impression de hachure de la parole. Cette dégradation est bien sûr accentuée si chaque paquet contient un long temps de parole (plusieurs trames de voix par paquet). Par ailleurs, les codeurs à très faible débit sont généralement plus sensibles à la perte d'information, et mettent plus de temps à « reconstruire » un codage fidèle.

Enfin, connaitre le pourcentage de perte de paquets sur une liaison n'est pas suffisant pour déterminer la qualité de la voix que l'on peut espérer, mais cela donne une bonne approximation. En effet, un autre facteur essentiel intervient ; il s'agit du modèle de répartition de cette perte de paquets, qui peut être soit « régulièrement » répartie, soit répartie de manière corrélée, c'est-à-dire avec des pics de perte lors des phases de congestion, suivies de phases moins dégradées en termes de QoS.

Le tableau ci-dessous donne un bref aperçu des valeurs acceptables en VoIP.

	Bon	**Moyen**	**Mauvais**
Délai de transit	D < 150ms	150ms < D < 400ms	D > 400ms
Gigue déphasée	G < 20ms	20ms < G < 50ms	G > 50ms
Perte de données	P < 1%	1% < P < 3%	P > 3%

Tableau 2.05: *Seuils de valeurs pour les paramètres critiques*

2.7 Points forts et limites de la VoIP

Différentes sont les raisons qui peuvent pousser les entreprises à s'orienter vers la VoIP comme solution pour la téléphonie. Les avantages les plus marqués sont :

- Réduction des coûts : En effet, le trafic véhiculé à travers le réseau RTC est plus coûteux que sur un réseau IP. Réductions importantes pour des communications internationales en

utilisant le VoIP, ces réductions deviennent encore plus intéressantes dans la mutualisation voix/données du réseau IP intersites (WAN). Dans ce dernier cas, le gain est proportionnel au nombre de sites distants.

- Standards ouverts : La VoIP n'est plus uniquement H323, mais un usage multi protocole selon les besoins de services nécessaires. Par exemple, H323 fonctionne en mode égale à égale alors que MGCP fonctionne en mode centralisé. Ces différences de conception offrent immédiatement une différence dans l'exploitation des terminaisons considérées.
- Un réseau voix, vidéo et données (Triple Play) : Grâce à l'intégration de la voix comme une application supplémentaire dans un réseau IP, ce dernier va simplifier la gestion des trois applications (voix, vidéo et données) par un seul transport IP. Une simplification de gestion, mais également une mutualisation des efforts financiers vers un seul outil.
- Un service PABX distribué ou centralisé : Les PABX en réseau bénéficient de services centralisés tel que la messagerie vocale et la taxation. Cette même centralisation continue à être assurée sur un réseau VoIP sans limitation du nombre de canaux. Il convient pour en assurer une bonne utilisation, de dimensionner convenablement le lien réseau. L'utilisation de la VoIP met en commun un média qui peut à la fois offrir à un moment précis une bande passante maximum à la donnée, et dans une autre période une bande passante maximum à la voix, garantissant toujours la priorité à celle-ci.
- Evolution vers un réseau de téléphonie sur IP : La téléphonie sur IP repose totalement sur un transport VoIP. La mise en œuvre de la VoIP offre là une première brique de migration vers la téléphonie sur IP.

Les points faibles de la Voix sur IP sont :

- Fiabilité et qualité sonore : Un des problèmes les plus importants de la téléphonie sur IP est la qualité de la retransmission qui n'est pas encore optimale. En effet, des désagréments tels que la qualité de la reproduction de la voix du correspondant ainsi que le délai entre le moment où l'un des interlocuteurs parle et le moment où l'autre entend peuvent être extrêmement problématiques. De plus, il se peut que des morceaux de la conversation manquent (des paquets perdus pendant le transfert) sans être en mesure de savoir si des paquets ont été perdus et à quel moment.
- Dépendance de l'infrastructure technologique et support administratif exigeant : Les centres de relations IP peuvent être particulièrement vulnérables en cas d'improductivité

de l'infrastructure. Par exemple, si la base de données n'est pas disponible, les centres ne peuvent tout simplement pas recevoir d'appels. La convergence de la voix et des données dans un seul système signifie que la stabilité du système devient plus importante que jamais et l'organisation doit être préparée à travailler avec efficience ou à encourir les conséquences.

- Vol : Les attaquants qui parviennent à accéder à un serveur VoIP peuvent également accéder aux messages vocaux stockés et simulatanément, au service téléphonique pour écouter des conversations ou effectuer des appels gratuits aux noms d'autres comptes.
- Attaque de virus : Si un serveur VoIP est infecté par un virus, les utilisateurs risquent de ne plus pouvoir accéder au réseau téléphonique. Le virus peut également infecter d'autres ordinateurs connectés au système.

2.8 Conclusion

Comme on a pu le voir tout au long de ce chapitre, la VoIP est la solution la plus rentable pour effectuer des conversations. Actuellement, il est évident que la VoIP va continuer à évoluer.

La téléphonie IP est une bonne solution en matière d'intégration, fiabilité et de coût. On a vu que la voix sur IP étant une nouvelle technologie de communication, elle n'a pas encore de standard unique. Chaque standard possède ses propres caractéristiques pour garantir une bonne qualité de service. En effet, le respect des contraintes temporelles est le facteur le plus important lors de transport de la voix.

Bien que la normalisation n'ait pas atteint la maturité suffisante pour sa généralisation au niveau des réseaux IP, il n'est pas dangereux de miser sur ces standards vu qu'ils ont été acceptés par l'ensemble de la communauté de la téléphonie.

CHAPITRE 3 : ETUDE CONCEPTUELLE

3.1 Introduction

Dans ce chapitre, nous allons définir la portée el les spécifications des exigences de notre système domotique. Une fois l'analyse des besoins et la spécification des exigences de notre mémoire seront élaborées, nous allons aborder la partie conception qui constitue la phase la plus importante dans le cycle de développement d'un projet puisqu'elle permet de traduire l'ensemble des exigences exposées en une solution.

Dans le cas de notre application, nous tenons à expliquer la conception de notre système domotique en étudiant les différentes interactions entre l'ensemble des entités du système.

3.2 Objectif

L'objectif de notre mémoire est de développer une plateforme domotique mettant en œuvre le protocole SIP. L'idée est donc d'utiliser SIP pour collecter des informations provenant de différents capteurs et de piloter aussi différents équipements (actionneurs). En effet, SIP est un protocole mettant en jeu la gestion des sessions mais ne gère pas les commandes que l'on veut passer. Nous souhaitons dialoguer entre serveur et clients SIP.

Notre plateforme « *Smart life avec VoIP »* consiste donc :

- En une infrastructure matérielle composée de capteurs et d'actionneurs connectés à des systèmes embarqués qui sont communicants et qui possèdent tous une connectivité IP.
- A mettre en place des passerelles entre les appliances domestiques (capteurs filaire et ZigBee, équipements X10) et le réseau IP pour permettre aux utilisateurs l'accès au réseau domestique à travers le protocole SIP. Le déploiement des passerelles nécessite le développement des logiciels adéquats dans les systèmes embarqués sous Linux.
- A développer des nouveaux services autour de la plateforme.

Notre mémoire sera intégré au final à la plateforme ToIP (Téléphonie over IP). La plateforme ToIP permet des communications VoIP mais autorise aussi l'accès vers le réseau téléphonique classique RTC (Réseau Téléphonique commuté). Le smart life avec VoIP est donc la continuité de

ToIP et l'interopérabilité entre les deux plateformes est totale car toutes deux basées sur le protocole SIP, protocole hautement interopérable.

3.3 La spécification des exigences

Pour rendre pleinement les services attendus, notre plateforme domotique doit respecter un certain nombre de contraintes. Plus globalement, la plateforme doit :

- permettre une grande hétérogénéité ;
- tolérer des comportements très dynamiques ;
- fonctionner en l'absence d'administrateur.

3.3.1 Hétérogénéité

Alors que les réseaux informatiques classiques sont formés de composants similaires (principalement des ordinateurs) comparables en termes de puissance, de stockage, de mémoire et de bande passante, les réseaux domotiques sont composés des dispositifs hétérogènes. Ils comportent aussi bien du matériel Hi-Fi que des dispositifs mobiles et du matériel informatique. Une autre différence porte sur l'hétérogénéité des moyens de communication.

La solution développée doit permettre l'interfonctionnement entre les différentes technologies domotiques (UPnP, HAVi, X10, ZigBee) qui doit être transparent à l'utilisateur final. Dans cette perspective, le protocole SIP peut assurer l'interfaçage entre les technologies domotiques via des passerelles que nous devrons développer. En plus, puisque SIP est basé sur IP, il peut être mis en application en utilisant n'importe quel langage de programmation, sur n'importe quel système d'exploitation ou plateforme matériel.

3.3.2 Nommage et adressage

Pour les appliances qui ne possèdent pas une connectivité IP, une passerelle doit être utilisée pour fournir l'interfonctionnement entre le réseau IP et les dispositifs domotiques.

Les appliances doivent avoir des adresses dans un format générique qui peut être utilisé par toute entité dans le but de communiquer avec les dispositifs domotiques indépendamment de leur type d'adressage.

3.3.3 La mobilité

Les réseaux domotiques sont particulièrement dynamiques, et ce à plusieurs titres. Tout d'abord, un réseau domotique donné évolue dans le temps en fonction des dispositifs qui le constituent.

Un réseau domotique est aussi physiquement dynamique. Les éléments qui le composent ne sont pas interconnectés en permanence : les appareils peuvent être mobiles, sous tension ou non ; les canaux de communication peuvent être bruités ou temporairement indisponibles.
Plus généralement, aucune supposition ne peut être faite sur la disponibilité d'un dispositif dans le réseau à un instant donné. Par conséquent, aucun constituant du plateforme à développer ne doit être indispensable au fonctionnement global. C'est une grande différence par rapport aux réseaux informatiques classiques, pour lesquels nous pouvons raisonnablement estimer que certains des dispositifs sont disponibles en permanence.

La mobilité implique aussi le problème de la gestion de la localisation. Le protocole SIP permet de localiser des équipements au sein d'un réseau à partir de l'enregistrement des passerelles auprès d'un serveur SIP qui est en mesure de les localiser. Par exemple, une passerelle s'enregistre à un serveur SIP en effectuant une requête. La localisation de la passerelle étant connue, différentes sessions offrant divers services pourront être ouvertes avec cette passerelle. En effet, SIP permet à un usager, indépendamment de sa localisation d'être accessible dans un réseau.

3.3.4 La fiabilité

Le protocole de communication doit fournir une flexibilité qui permet de supporter différents types de données (payload) et de transporter des commandes et des réponses de différents dispositifs gérés en réseau. SIP est un protocole qui a la caractéristique d'être extensible. Cette extensibilité lui permet de transporter une charge utile arbitraire. En effet, SIP peut être combiné à d'autres protocoles de communication, codecs ou encore formats de fichiers afin d'offrir des nouveaux services au travers des sessions SIP.

- Il doit avoir une séparation entre la couche transport et les types des données échangés.
- Puisque la plupart des communications avec les appareils gérés en réseau doivent être effectuées en temps réel, le protocole doit supporter la transmission des messages de commande.

- La notification d'évènement est très importante pour l'interaction avec les appareils gérés en réseau (par exemple : avis que quelqu'un entre dans votre maison). Par conséquent, le protocole doit supporter la souscription à des évènements et les notifications.
- Le protocole doit être capable d'encapsuler de diverses caractéristiques d'appareils. Nous utiliserons le modèle de données SOAP pour représenter les caractéristiques des différentes appliances déployées dans le réseau domotique.

3.3.5 Le mode de communication

Il y a différents modes pour agir avec les appareils gérés en réseau. Les modes d'interaction suivants sont exigés :

- Contrôle : Il doit être possible d'envoyer des commandes aux appareils. Par exemple, allumer le four et régler sa température à 180° et la durée de cuisson à 20mn.
- Requêtes : Le protocole doit assurer la demande de l'état d'appareils gérés en réseau. Par exemple, le four est-il activé ou désactivé ?
- Avis d'évènement : Le protocole doit permettre à des utilisateurs de souscrire pour recevoir des notifications quand des évènements se produisent. Par exemple, informer le mobile d'un utilisateur quand quelqu'un entre dans la maison.
- Découverte : Le protocole doit garantir à des utilisateurs de rechercher des appareils pour répondre à des exigences particulières. Par exemple, trouver un appareil qui permet de faire une tasse du café.

3.3.6 Absence d'administrateur

Enfin, les utilisateurs des réseaux domestiques sont très différents de ceux des réseaux informatiques. L'utilisateur d'un réseau informatique a souvent bénéficié d'une formation adaptée. Les appareils sont pour lui des outils de travail et il est prêt à suivre quelques procédures fastidieuses pour les maintenir en fonction. Pour les opérations complexes, un administrateur possède le niveau d'expertise adapté et des ressources dédiées.

A contrario, l'utilisateur d'un réseau domotique interagit avec des objets du quotidien. Il n'a généralement bénéficié aucune formation particulière et peut tout ignorer du fonctionnement d'un

réseau. Quand bien même, il disposerait des compétences adaptées, il ne consacrera probablement pas les ressources nécessaires pour configurer, administrer et superviser régulièrement le sien.

Les réseaux domotiques présentent donc des différences essentielles par rapport aux réseaux informatiques traditionnels, résumées dans le tableau 3.01 ci-dessous.

Réseaux informatiques	Réseaux domotiques
Dispositifs similaires	Dispositifs hétérogènes
Moyens de communication rationalisés	Moyens de communications hétérogènes
Interconnexion supposée permanente des dispositifs	Interconnexion erratique des dispositifs
Utilisateurs formés et actifs	Utilisateurs non formés et passifs
Evolutions du réseau rares et maitrisées	Evolutions du réseau fréquentes
Administrateurs	Pas d'administrateurs

Tableau 3.01 : *Différences entre réseaux informatique et domotique*

3.4 Les besoins fonctionnels

Dans ce paragraphe, nous exposerons l'ensemble des besoins auxquels doit répondre notre système domotique. En effet, étant donné la nature de notre application qui obéit à une architecture *client/serveur,* il s'agit de développer un système permettant d'utiliser et administrer la plateforme domotique soit localement par PC ou d'autre interface ; soit à distance par un mobile SIP.

L'administration sera appliquée aux différents dispositifs domotiques. En effet, notre système devra être capable de :

- découvrir les dispositifs et de leurs services ;
- fournir une description détaillée de chaque dispositif et de ses services disponibles ;
- visualiser les actions que l'utilisateur peut invoquer ;
- permettre à l'utilisateur de savoir les états actuels de ces dispositifs ;

- permettre à l'utilisateur d'être notifié sur les différents changements dans son réseau ;
- garantir à l'utilisateur l'activation et la désactivation des différents dispositifs ;
- permettre de commander les dispositifs sur le réseau.

3.5 Structure et solution retenue

En se basant sur ce qui précède, une solution qui semble conforme aux besoins exprimés et aux objectifs se résume dans un système domotique illustré par la figure 3.01.

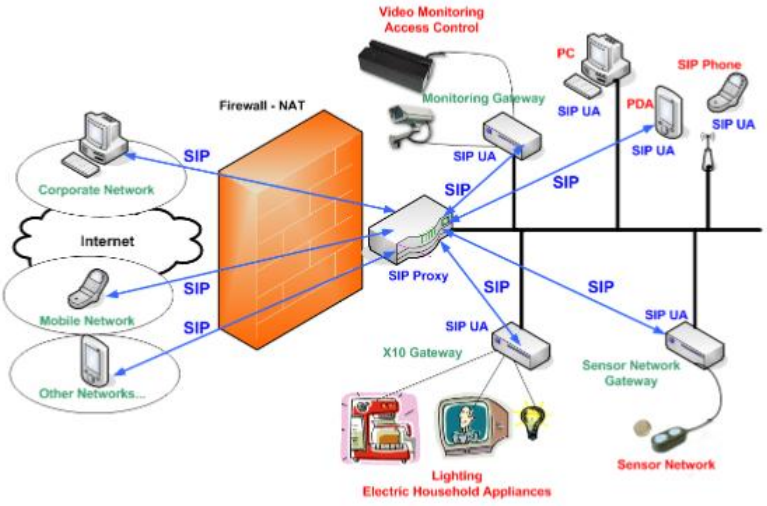

Figure 3.01 : *Plateforme smart life avec VoIP*

La plateforme domotique se compose des entités suivantes :

- Les dispositifs : Ce sont des dispositifs domotiques non IP gérés localement et à distance. Ils peuvent être des dispositifs X10, des caméras de surveillance ou des capteurs de température.
- Les passerelles SIP : Il gère les interactions entre les équipements domotiques et le monde IP.
- L'infrastructure SIP : Elle est composée de Proxy SIP, Register SIP et des User Agent SIP.

La plateforme matérielle est basée sur l'architecture SIP. Un routeur assure la redistribution sur le réseau Ethernet suivant le protocole SIP. Le réseau Ethernet sert d'ossature à la plateforme domotique avec VoIP. Toutes les communications utilisent le protocole SIP. Par l'intermédiaire de différentes passerelles, il est ainsi possible d'avoir accès à certains éléments basés sur X10,

technologie très répandue en domotique pour la commande d'appareils par courant porteur. Il pourra être aussi possible d'accéder à différents capteurs de température ou encore contrôler la vidéo surveillance.

3.6 Méthode de conception

Une méthode de conception définit une démarche reproductible qui vise l'obtention des résultats fiables. D'une manière générale, les méthodes permettent de construire des modèles à partir d'éléments de modélisation qui constitue des concepts fondamentaux pour la représentation des systèmes ou des phénomènes. Les méthodes définissent également une représentation souvent graphique qui permet d'une part de manipuler aisément les modèles, et d'autre part de communiquer et d'échanger l'information entre les différents intervenants. Une bonne représentation recherche l'équilibre entre la densité d'information et la lisibilité [31].

3.6.1 Méthode fonctionnelle

Elle consiste à définir les fonctions des composantes d'un système et leurs relations fonctionnelles. Le système est conçu d'un point de vue fonctionnel, en partant d'une vue de haut niveau, qu'on affine successivement afin d'obtenir une conception plus détaillée. L'état du système est centralisé et partagé par les fonctions qui agissent sur cet état.

3.6.2 Méthode orientée objets

C'est une méthode de conception qui permet de programmer en termes d'objets. Le système est vu comme un ensemble d'objets, plutôt que comme un ensemble de fonctions. L'état du système est centralisé, et chaque objet gère l'information concernant son propre état. Les objets disposent d'un ensemble d'attributs qui définissent leurs états, et d'un ensemble d'opérations qui permettent d'agir sur ces attributs [32].

3.7 Conception de la base de données

MERISE est une méthode de conception, de développement et de réalisation de projets informatiques. Le but de cette méthode est d'arriver à concevoir un système d'information. La méthode MERISE est basée sur la séparation des données et des traitements à effectuer en plusieurs modèles conceptuels et physiques. La séparation des données et des traitements assure

une longévité au modèle. En effet, l'agencement des données n'a pas été souvent remanié, tandis que les traitements le sont plus fréquemment.

La méthode MERISE propose une méthode de conception de développement de systèmes d'information complète, détaillée, en grande partie formalisée, qui garantit une informatisation réussie. La séparation des données et des traitements en plusieurs modèles conceptuels et physiques garantit la stabilité d'agencement des données, la possibilité de remaniement des traitements et la longévité du système.

La méthode MERISE prévoit une conception par niveau, et définit pour cela 3 niveaux essentiels :

- L'analyse : Il décrit l'ensemble des données du système d'informations sans tenir compte de l'implémentation informatique de ces données.
- Modèle conceptuel des données : Il prend en considération l'implémentation du système d'information par un SGBD (Système de Gestion de Base de Données). Ce niveau introduit la notion des tables logiques, et constitue donc le premier pas vers les tables des SGBD.
- Modèle logique des données : Il contient finalement les tables définies à l'aide d'un SGBD spécifique.

3.7.1 Le niveau conceptuel : Analyse

Notre projet consiste à recueillir des informations issues de différents types de capteurs et d'actionneurs, à distance à l'aide d'une communication IP. Dans ce cadre, nous allons besoin de savoir :

- Le nom de l'équipement.
- Le type de l'équipement, par exemple module ZigBee ou dispositif X10.
- Le port sur lequel est connecté l'équipement (port série ou port USB,…).
- L'état de l'équipement (activé, désactivé).

En plus de ces informations communes à l'ensemble des équipements, nous avons décidé de stocker des informations spécifiques aux différents types de dispositifs manipulées dans notre plateforme.

3.7.1.1 Passerelle SIP

Pour piloter à distance notre installation domotique, nous avons besoin d'une passerelle entre l'infrastructure SIP et les dispositifs. Une passerelle SIP/réseau de capteur possède les caractéristiques suivantes :

- Adresse IP.
- Nom de la passerelle.
- URI de la passerelle (adresse SIP).

Notre plateforme met en œuvre des interactions entre les passerelles SIP et les éléments suivants :

- Les UA désignent les agents que l'on retrouve dans les téléphones SIP, les softphones (logiciel de téléphonie sur IP) des PC et PDA. En théorie, on peut établir des sessions directement entre deux UA, deux téléphones par exemple. Mais cela nécessite de connaitre l'adresse IP du destinataire. Cela n'est pas idéal car une adresse IP peut ne pas être publique (derrière un NAT (Network Address Translation)) ou changer et elle est bien plus compliquée à retenir qu'une URI. Les UA peuvent donc s'enregistrer auprès des Registrar pour signaler leur emplacement courant.
- Le Registrar est un serveur qui gère les requêtes REGISTER envoyées par les UA pour signaler leur emplacement courant. Ces requêtes contiennent donc une adresse IP, associée à une URI, qui seront stockées dans une base de données spécifique au Registrar. Généralement, des mécanismes d'authentification permettent d'éviter que quiconque puisse s'enregistrer avec n'importe quelle URI.

Dans une infrastructure SIP, un proxy SIP se contente de relayer uniquement les messages SIP pour établir, contrôler et terminer la session. Une fois la session établie, les données, par exemple un flux pour la VoIP, ne transitent pas par le serveur Proxy. Elles sont échangées directement entre les UA. Un proxy SIP peut être lui aussi un serveur d'enregistrement pour les agents SIP.

3.7.2 Modèle conceptuel de données (MCD)

Le Modèle Conceptuel des Données (MCD) est la représentation simplifiée de l'ensemble des données manipulées par le système d'informations. L'intérêt de ce modèle est d'identifier la signification et la description de chaque information indépendamment de leur organisation et de

leur implantation géographique. En effet, les concepts qui apparaissent et qui sont utilisés dans le MCD sont très variables dans le temps et, à quelques exceptions près, constituent une image très fidèle des systèmes d'informations futurs. Les différents concepts utilisés dans le MCD sont :

- Entité : C'est une information majeure manipulée par l'organisme et dotée d'une existence propre et identifiable. Elle est présentée par un rectangle où figure son identifiant et ses attributs.

- Identifiant : C'est une propriété telle que, à une valeur de l'identifiant correspond une seule occurrence de l'entité. Elle sert à référencier chaque occurrence de l'entité de façon unique.

- Relation : C'est un formalisme qui définit un lien sémantique entre les entités manipulées. Elle peut être soit porteuse de données, soit non porteuse de données. On appelle dimension le nombre d'individus composant la relation. Dans le graphe du MCD, elle est représentée par un cercle portant son nom (un verbe) et les propriétés qu'elle porte.

- Cardinalité : Les cardinalités d'une relation entre entités indiquent le nombre d'occurrence maximal et minimal de participation des entités dans la relation. Le modèle conceptuel des données (MCD) a pour but d'écrire de façon formelle les données qui seront utilisées par le système d'informations. Il s'agit donc d'une représentation des données, facilement compréhensible, permettant de décrire le système d'information à l'aide d'entités.

3.7.2.1 Construction du schéma conceptuel

En s'inspirant de la spécification des besoins en données, nous pouvons définir les types d'entités et les associations de base de données.

a. Liste des entités

Nous pouvons identifier les entités citées ci-dessous :

- Un type d'entité *User_Agent* qui possède les propriétés : adresse IP, URI (adresse SIP), le nom et le type de l'agent.
- Un type d'entité *Registrar* qui a comme propriétés : adresse IP, URI et le nom du registrar.

- Un type d'entité *Device* qui possède des informations communes de tous les dispositifs domestiques et ayant comme propriétés : l'adresse IP, le nom de l'équipement, son type, l'état courant et le port sur lequel l'équipement est connecté.
- Un type d'entité *Passerelle* avec les propriétés : adresse IP, URI, le type et nom de la passerelle.
- Un type d'entité *Type d'équipement domotique_Device*; par exemple X10_Device ayant comme propriétés : code site et code dispositif.

b. *Liste des relations*

Nous pouvons distinguer les associations suivantes :

- L'association *Enregistrement_User* entre User Agent et Registrar.
- L'association *Enregistrement_Gateway* entre Passerelle et Registrar.
- L'association *Commande* entre User Agent et Passerelle.
- L'association *Associe* entre Passerelle et Device.
- L'association *Est_de_ type* entre Device et X10_Device.

c. *Le modèle conceptuel des données*

- Un utilisateur s'enregistre à un seul Registrar. Une entité User_Agent est associée vers la relation Enregistrement_User à exactement une entité Registrar. Un Registrar peut recevoir des requêtes d'enregistrement de plusieurs utilisateurs. Une entité Registrar est associée via Enregistrement_User à plusieurs entités de type User_Agent.

- Une entité Passerelle est associée via la relation Enregistrement_Gateway à exactement une entité Registrar. Une entité Registrar est associée via Enregistrement_Gateway à plusieurs entités de type Passerelle.

- Un utilisateur peut commander plusieurs passerelles SIP/réseau de capteur dans notre plateforme domotique. Une entité User_Agent est associée via Commande à plusieurs entités de type Passerelle. Une passerelle peut recevoir des requêtes de commandes de plusieurs utilisateurs. Une entité Passerelle est associée via Commande à plusieurs entités de type User_Agent.

- Une passerelle est liée à plusieurs types d'équipements domestiques. Une entité Passerelle est associée via Associe à plusieurs entités de type Device. Un dispositif est associé à une seule passerelle SIP/réseau de capteur.

- Un équipement domotique par exemple X10, module Xbee. Une entité Device peut être associée via Est_de_type à une entité X10_Device, Xbee_Module.

3.7.2.2 Modèle logique de données

Dans le modèle logique de données, les entités se transforment en relations ; les propriétés deviennent des attributs et l'identification d'une entité devient la clé primaire de la relation. Les relations permettent de traduire aussi les associations grâce aux clés étrangères.

- L'association binaire Enregistrement_User de type (0-N, 1-1) entre les entités Registrar et User_Agent se traduit par la redondance de l'identifiant de l'entité Registrar dans la relation issue de l'entité User_Agent. Le même raisonnement peut être appliqué à l'association Enregistrement_Gateway.
- L'association binaire Commande de type (0-N, 0-N) entre les entités Passerelle et User_Agent se traduit par la création d'une relation Commande qui contient comme attributs les identifiants des deux entités associées. Ces attributs constituent à eux de la clé primaire de la relation et ils sont individuellement clés étrangères.

- L'association binaire Associe de type (1-N, 1-1) entre les entités Passerelle et Device se traduit par la redondance de l'identifiant de l'entité Passerelle dans la relation issue de l'entité Device.

- L'association binaire Est_de_type (0-1,1-1) entre les entités Device et Type d'équipement domotique_Device (Par exemple : X10_Device) se traduit par la redondance de l'identifiant de l'entité Device dans la relation issue de l'entité Type d'équipement domotique_Device.

a. Le schéma relationnel

Le schéma relationnel peut être représenté comme suit :

- User_Agent (id_User, id_RegAdresse_IP_User, URI_User, Name, Type_Agent).
- Registrar (id_Reg, id_Reg, Adresse_IP_Reg, URI_Reg, Name_Reg).
- Passerelle (id_Pas, Adresse_IP_Pas, URIçPas, Type_Pas).
- Device (id_Dev, id_PasAdresse_IP_Dev, URI_Dev, Name_Dev, Type_Dev, Etet, Port).
- Type d'équipement domotique_Device (id_type d'équipement domotique, id_Device, Propriétés).Exemple : Xbee_Module (id_Xbee, id_Dev, Adresse_Xbee).
- Commande (id_User, id_Pas).

3.8 Conception de l'application

Cette étape sera réservée à la conception proprement dite du système et ce en affinant la spécification des composants de l'application et leurs interactions à travers des diagrammes permettant de représenter les interactions entre les éléments du système, en précisant la chronologie des échanges des messages durant l'exécution, et de représenter l'exécution des opérations relatives à une utilisation spécifique du système.

3.8.1 Langage UML

La méthode UML est devenue le standard industriel de la modélisation. L'UML est sous l'entière responsabilité de l'OMG (Object Management Group). Il se définit comme un langage de modélisation graphique et textuel destiné à comprendre et décrire des besoins, spécifier et documenter des systèmes, esquisser des architectures logicielles, concevoir des solutions et communiquer des points de vue.

UML unifie les notations nécessaires aux différentes activités d'un processus de développement et offre, par ce biais, le moyen d'établir le suivi des décisions prises, depuis l'expression des besoins jusqu'au codage. C'est un langage formel possédant les caractéristiques suivantes :

- Il n'est pas une notation fermée ; elle est extensible, générique et configurable par l'utilisateur.
- Un langage sans ambiguïtés.

- Un moyen de définir la structure d'un programme.
- Une représentation visuelle permettant la communication entre les acteurs d'un même projet.
- Une notation graphique simple, compréhensible même par des non informaticiens.

UML s'articule autour de plusieurs types de diagrammes, chacun d'eux étant dédié à la représentation des concepts particuliers d'un système logiciel mais, nous allons représenter seulement ceux qui sont utilisés dans notre mémoire et qui sont :

- Les diagrammes des cas d'utilisations.
- Les diagrammes de séquences.

3.8.1.1 Diagramme des cas d'utilisations

Les cas d'utilisation permettent de modéliser et de structurer les interactions entre les utilisateurs au sens large, appelés acteurs et un système.

Les cas d'utilisation représentent un moyen d'analyse des besoins utilisateurs et permettent de relier les actions faites par un utilisateur avec les réactions attendues d'un système. Plus précisément, un cas d'utilisation unitaire est une abstraction d'un ensemble de scénarios concrets effectués sur l'initiative d'un type d'utilisateurs.

Les éléments de base des diagrammes des cas d'utilisations sont :

- Les acteurs : Ils représentent un rôle joué par une entité externe (utilisateur humain, dispositifs matériels ou autre système) qui interagit directement avec le système étudié. Un acteur peut modifier et/ou consulter directement l'état du système, en émettant et/ou en recevant des messages susceptibles d'être porteurs de données.

- Cas d'utilisation : Il représente un ensemble de séquences d'action qui sont réalisées par le système et qui produisent un résultat observable intéressant pour un acteur particulier. Un cas d'utilisation modélise un service rendu par le système. Il exprime les interactions acteur/système et apporte une valeur ajoutée à l'acteur concerné.

3.8.1.2 Diagrammes de séquences

Un diagramme de séquence montre chronologiquement les interactions entre un ensemble d'objets. Chaque objet dispose d'une ligne de vie (ligne verticale). Sur ces lignes de vie, des périodes d'activités sont indiquées par des rectangles finis qui sont superposés en cas d'appel récursif [32].

3.8.2 Représentation des diagrammes des cas d'utilisations

A partir de la définition des besoins, on identifie les acteurs et leurs interactions avec le système, ce qui permet de déduire assez facilement le diagramme de cas d'utilisation général.

Le diagramme de cas d'utilisation général sera spécifié par un autre cas d'utilisation. Pour décrire la dynamique des cas d'utilisations et les documenter, on utilisera les diagrammes de séquences afin d'illustrer les scénarios d'utilisations des différents cas d'utilisations du système ce qui apportera un niveau supérieur de formalisation.

3.8.2.1 Cas d'utilisation général du système

Un cas d'utilisation spécifie une séquence d'action selon le point de vue d'une catégorie d'utilisateurs. L'étude des besoins a révélé la présence d'un acteur principal du système qui est l'User Agent SIP (SIP UA). Le diagramme de cas d'utilisation général de notre système domotique est schématisé dans la figure 3.02 ci-dessous.

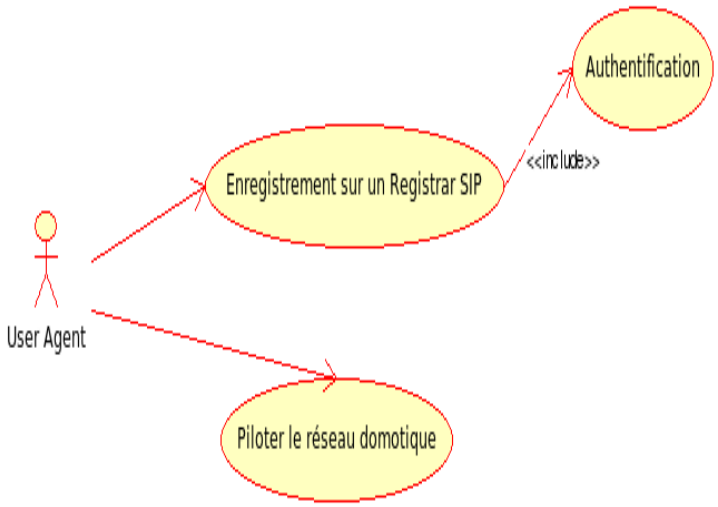

Figure 3.02 : *Cas d'utilisation générale de notre système domotique*

L'User Agent doit s'enregistrer auprès d'un Registrar SIP et s'authentifier afin de pouvoir piloter le réseau domotique soit à distance soit localement.

3.8.2.2 Cas d'utilisation « Piloter le réseau domotique »

Le fonctionnement de pilotage du réseau domotique peut être décrit par le diagramme de cas d'utilisation de la figure 3.03.

Ces différentes fonctionnalités sont assurées à travers des passerelles SIP/réseau de capteurs. En effet, après son enregistrement auprès du Registrar SIP, l'Agent SIP envoie sur le réseau des messages de découverte vers les passerelles qui permettent de découvrir les dispositifs disponibles sur le réseau ainsi que leurs services. Une fois que l'utilisateur a localisé un dispositif et ses services grâce à la phase de découverte et les informations envoyées par les passerelles, il peut procéder à la phase de souscription à un service qui lui permet de recevoir périodiquement des notifications auprès des dispositifs domestiques. L'utilisateur peut en plus envoyer des commandes et éventuellement des paramètres à un service qui tentera d'effectuer la tâche due. Ces commandes peuvent être de différents types :

- Détermination de l'état actuel d'un dispositif domotique.
- Positionnement de la valeur d'un actionneur.
- Activation ou désactivation d'un dispositif domotique.

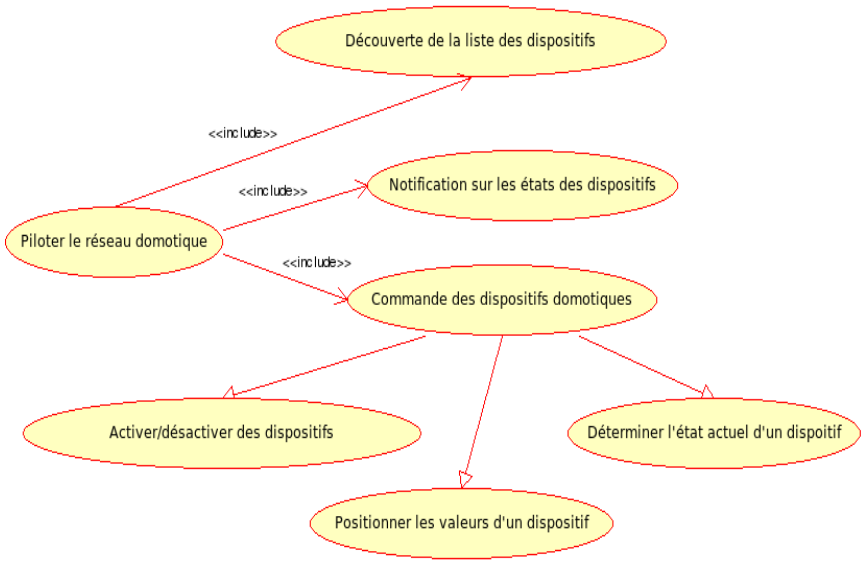

Figure 3.03 : *Cas d'utilisation « Piloter le réseau domotique »*

3.8.3 Représentation des diagrammes de séquences

Les diagrammes de séquences permettent de décrire les interactions entre les éléments de la plateforme domestique pour chaque cas d'utilisation. Dans notre cas, ces diagrammes sont liés aux diagrammes de cas d'utilisation représentés auparavant.

3.8.3.1 Enregistrement de l'utilisateur distant

Quand un utilisateur veut commander son réseau domotique à distance, il doit s'enregistrer auprès du serveur d'enregistrement SIP disponible dans le réseau. Les paramètres d'authentification et les services demandés envoyés par l'agent utilisateur SIP seront vérifiés dans une base de données liée au serveur Registrar. Une fois la vérification effectuée, un message SIP 200 OK est envoyé à l'utilisateur pour lui indiquer que l'accès est autorisé en plus d'un message indiquant la liste des passerelles sur lesquelles l'utilisateur peut se connecter. La figure 3.04 donne le diagramme de séquences de ce cas d'utilisation.

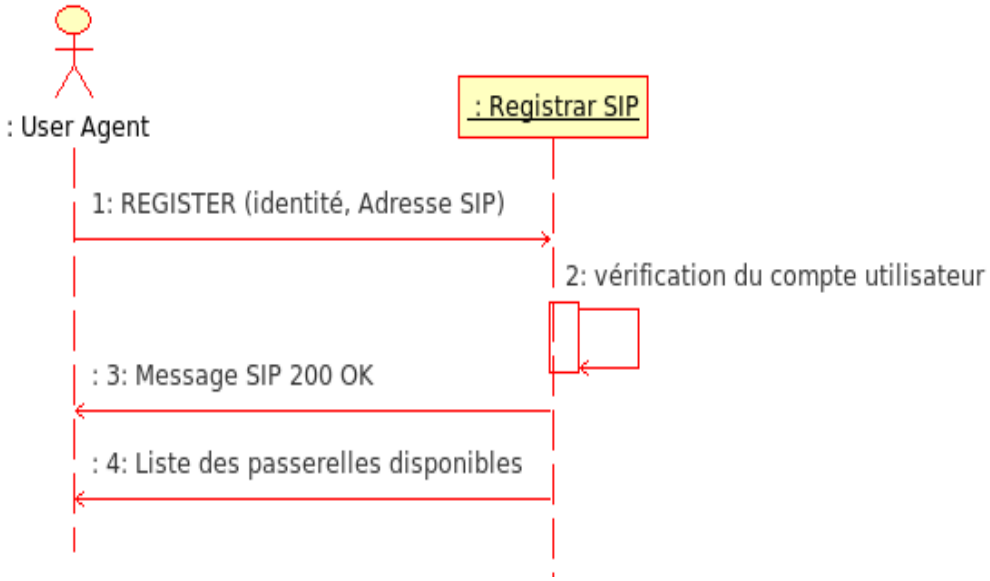

Figure 3.04 : *Diagramme de séquences « Enregistrement de l'utilisateur distant »*

3.8.3.2 Découverte des dispositifs existants dans le réseau

L'utilisateur peut découvrir les dispositifs disponibles sur le réseau domotique. En effet, après l'ouverture d'une session SIP avec la passerelle SIP/réseau de capteur à travers le proxy SIP, la

passerelle va consulter la base de données domotique pour retourner la liste des dispositifs disponibles à l'utilisateur. Cette opération est décrite par le diagramme de la figure 3.05.

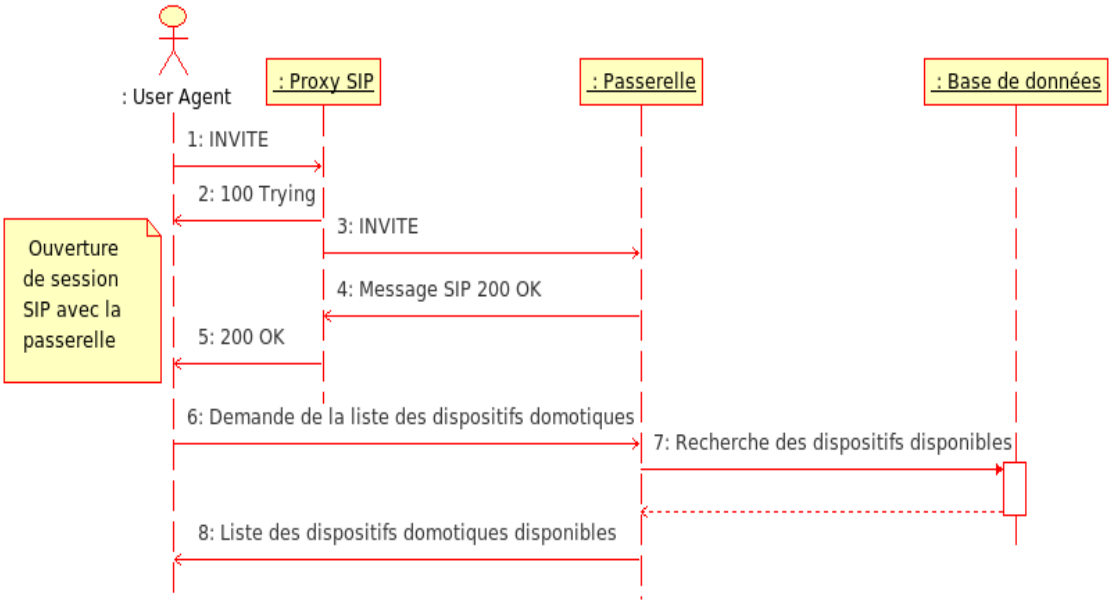

Figure 3.05 : *Diagramme de séquences « Découverte des dispositifs domotiques »*

3.8.3.3 Notification sur les états des dispositifs

Le client interroge tout d'abord la passerelle au moyen d'une requête SIP SUBSCRIBE. Si celle-ci est acceptée, le serveur en retourne le message « 200 OK » et une communication est établie pendant une durée déterminée par le champ « EXPIRE » contenu dans le « SUBSCRIBE ».

Une requête de notification est émise par un système auquel il demande des informations à travers une souscription. Ainsi, la passerelle va envoyer des requêtes de notifications comportant les informations à une certaine fréquence pendant la durée annoncée par le client. Cette opération est décrite par le diagramme de la figure 3.06.

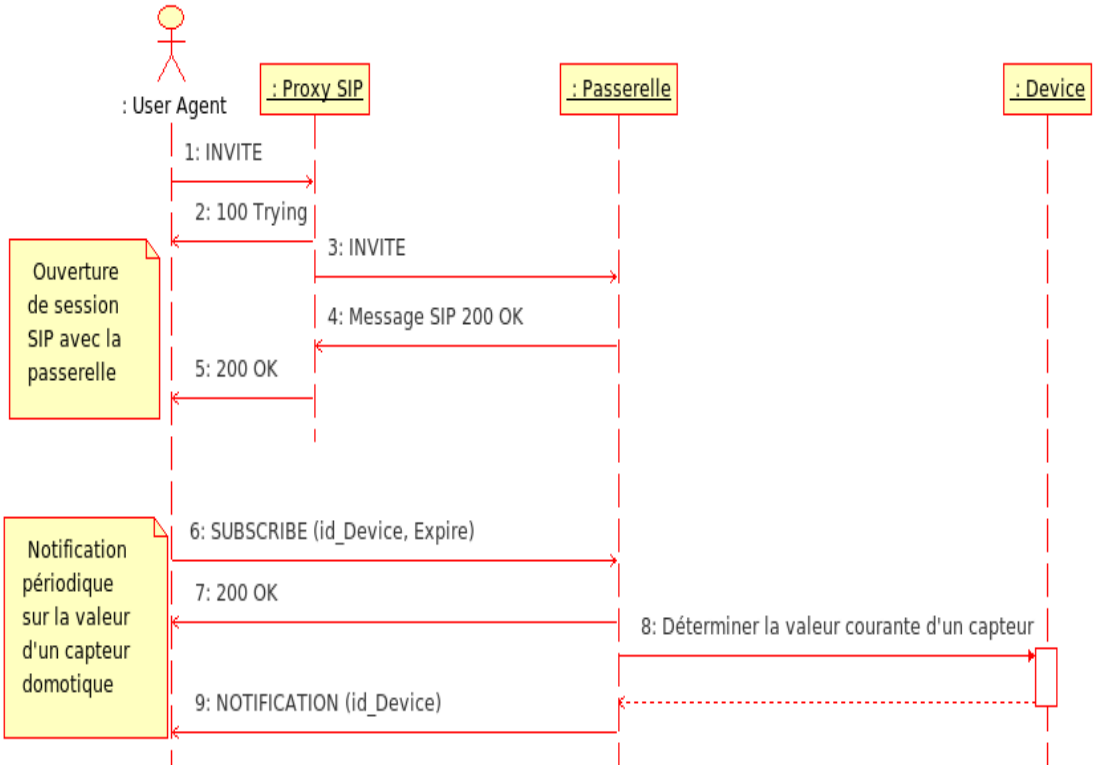

Figure 3.06 : *Diagramme de séquences « Notifications sur les états des dispositifs »*

3.8.3.4 Déterminer l'état courant d'un dispositif

L'utilisateur peut savoir l'état courant d'un dispositif disponible sur le réseau domotique. Il choisit le dispositif à partir de son identificateur (id_Device) et ensuite il valide son choix. La passerelle va consulter la base de données pour retourner l'état courant de l'équipement. La figure 3.07 décrit cette opération en détail.

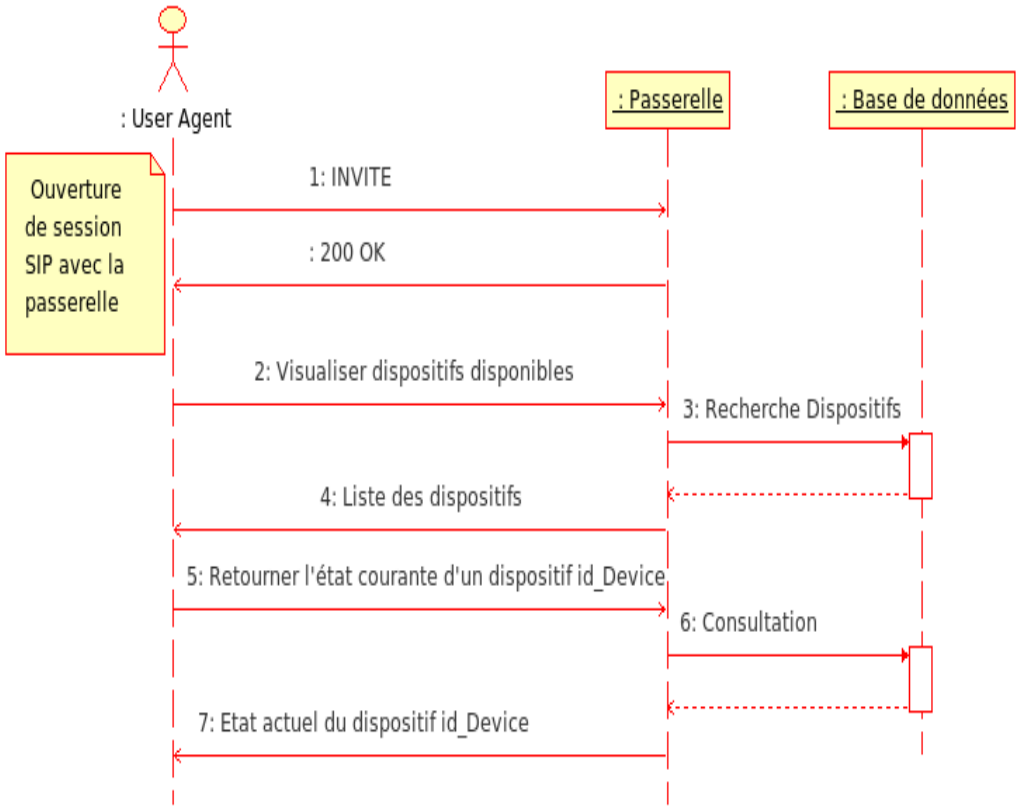

Figure 3.07 : *Diagramme de séquence « Déterminer l'état courant d'un dispositif »*

3.8.3.5 Positionner la valeur d'un dispositif

Après l'ouverture d'une session SIP avec la passerelle, l'utilisateur peut positionner les valeurs des dispositifs qu'il a la possibilité de choisir. La figure 3.08 décrit cette opération.

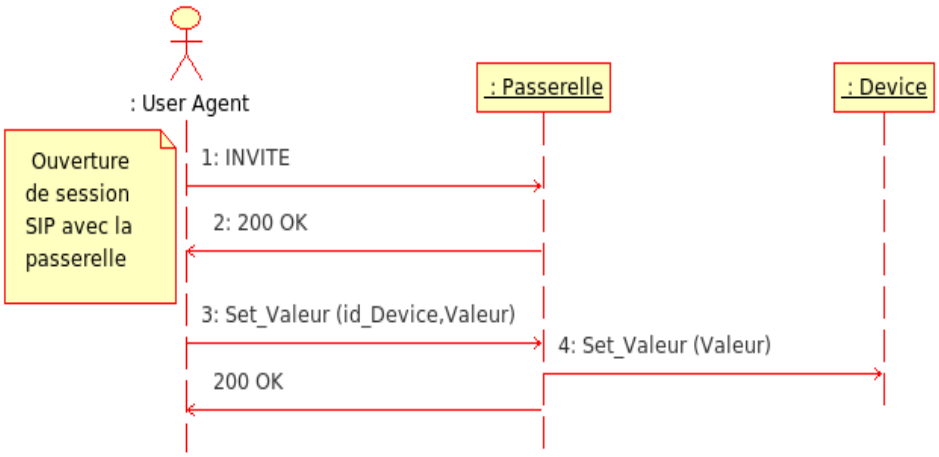

Figure 3.08 : *Diagramme de séquences « Positionner la valeur d'un dispositif »*

3.8.3.6 Activation/désactivation d'un dispositif

Pour activer un équipement dans notre plateforme domestique, l'utilisateur peut envoyer une commande ON pour un dispositif identifié par id_Device.

Pour la désactivation, il suffit d'envoyer une commande OFF. Le changement de l'état d'un équipement doit être indiqué au niveau de la base de données de notre plateforme. La figure 3.09 décrit en détail cette opération.

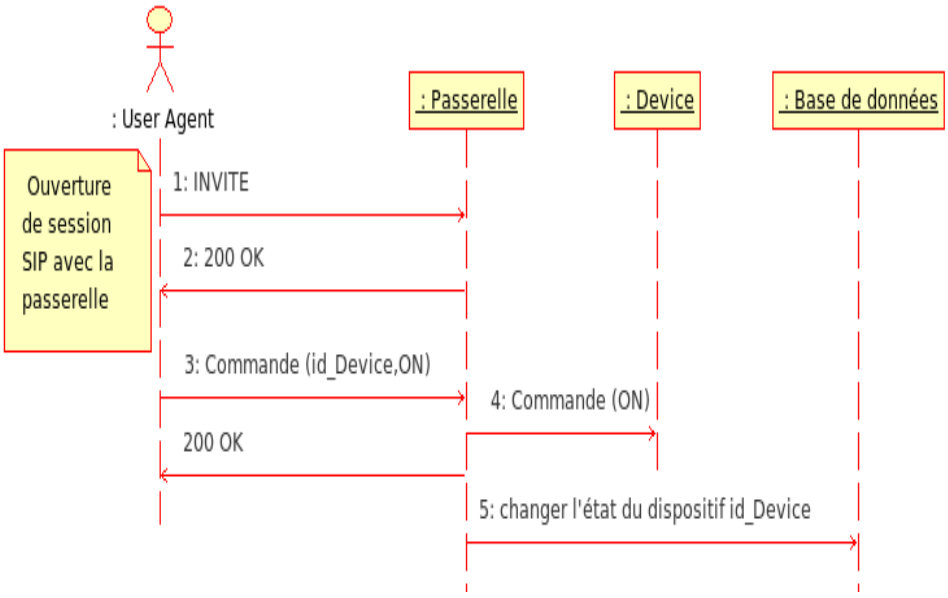

Figure 3.09 : *diagramme de séquences « Activation/désactivation d'un dispositif »*

3.9 Conclusion

Tout au long de ce chapitre, nous avons parlé de la spécification des besoins et de la conception de notre application.

L'étape de spécification des besoins nous a permis d'avoir une idée claire sur la faisabilité de notre application à travers la détermination des principales fonctionnalités de notre système. Cette étape s'avère très importante dans notre processus de développement.

Lors de la conception de notre application, nous avons exposé les différents besoins que doit répondre notre application ainsi que la solution proposée tout en évoquant l'ensemble des choix techniques et logiciels qui nous ont aidés dans la réalisation de notre application.

CHAPITRE 4 : APPLICATIONS DU SMART LIFE AVEC VoIP

4.1 Introduction

Ce dernier chapitre se consacre aux applications de notre plateforme domotique. Les passerelles SIP/réseau domotique sont implémentées sous forme des logiciels à installer sur la machine faisant office de serveur VoIP. Dans notre cas, nous utilisons l'IPBX XiVO tournant sur un système d'exploitation Debian GNU/Linux et des agents utilisateurs (User Agent) tels que smartphone et sofphone.

4.2 Architecture du réseau déployé

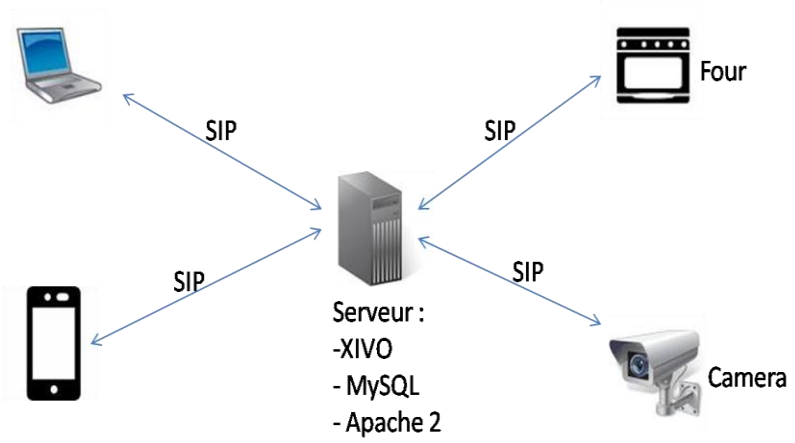

Figure 4.01 : *Schéma de principe*

L'architecture utilisée dans notre simulation est illustrée par la figure 4.01 ci-dessus.

4.3 Environnement logiciel

4.3.1 Coté serveur

4.3.1.1 DEBIAN GNU/Linux

Debian est une organisation communautaire et démocratique, dont le but est le développement de systèmes d'exploitation basés exclusivement sur des logiciels libres.

Chaque système, lui-même nommé Debian, réunit autour d'un noyau de système d'exploitation, de nombreux éléments pouvant être développés indépendamment les uns des autres, pour plusieurs architectures matérielles. Ces éléments, programmes de base complétant le noyau et logiciels applicatifs, se présentent sous forme de « paquets » qui peuvent être installés en fonction des besoins. L'ensemble système d'exploitation plus logiciels s'appelle une distribution.

La distribution Debian/GNU Linux contient environ 25 000 paquets logiciels (29 000 avec la version Squeeze) élaborés et entretenus par un millier de développeurs. Debian est réputé pour sa fiabilité et son gestionnaire de paquets original (APT), au format de fichier .deb, permettant les mises à jour et garantissant un système homogène. Debian est disponible pour une dizaine de plateformes de matériel informatique : x86, SPARC, PowerPC, MIPS, IA-64, S/390, AMD 64, ARM, Alpha et PA-RISC. D'autres architectures sont supportées, mais de manière non officielle.

La distribution Debian s'étant, à l'origine, principalement développée autour de son utilisation sur des serveurs, elle est donc particulièrement adaptée à ce rôle ; par exemple elle distingue toujours l'administrateur système de l'utilisateur.

Dans notre cas, nous utiliserons la version 6.0 de Debian pour faire tourner notre serveur VoIP. La distribution Debian est téléchargeable à l'adresse : http://www.debian.org/distrib/index.fr.html.

4.3.1.2 XiVO

XiVO est une solution Open Source publiée sous licence GPLv3. XiVO est une des distributions Linux dédiée à Asterisk. Elle intègre la base Asterisk, ainsi que certains modules complémentaires. Mais surtout, une interface Web est disponible par défaut. XiVO est basé sur Debian, et est développé par la société Avencall.

XiVO est une solution alternative complète, libre et évolutive de communications unifiées. Elle est interopérable avec la plupart des systèmes de téléphonie du marché et elle permet à tous les utilisateurs de bénéficier d'un ensemble de services évolués.

En plus des fonctionnalités téléphoniques que l'on trouve dans tout système de téléphonie professionnel, XiVO offre :

- Une interface web ergonomique d'administration, d'exploitation et de supervision du parc téléphonique

- Un serveur CTI (Customer Telephony Integration) ainsi qu'un client
- Un serveur d'approvisionnement permettant de déployer automatiquement une quarantaine de terminaux SIP du marché
- Des applications favorisant la convergence fixe-mobile

Dans notre simulation, nous avons utilisé la version 1.1.23 (lenny-xivo-gallifrey-1.1.23.iso) qui est téléchargeable sur mirror.xivo.fr/iso/archives/lenny-xivo-gallifrey-1.1.23/

4.3.1.3 MySQL

MySQL est le serveur de bases de données le plus répandu pour les serveurs web. Il allie une grande souplesse d'utilisation et de nombreuses fonctionnalités, tandis que sa mise en œuvre reste simple. Dans notre simulation, nous installerons le MySQL version 5.6 dans notre serveur.

4.3.2 Côté client

Plusieurs logiciels disponibles sur le marché peuvent être utilisés comme client SIP. Pour notre simulation, nous avons utilisé les Softphones Jitsi pour les laptops et CSipSimple pour les téléphones portables avec Android.

4.3.2.1 Jitsi

Jitsi est un logiciel libre développé en Java, qui permet d'établir des conversations audio et vidéo sur Internet via le protocole SIP.

Dans notre cas, nous utiliserons la dernière version 2.4 qui est téléchargeable à l'adresse : http://download.jitsi.org/jitsi/windows/jitsi-2.4-latest-x86.exe

4.3.2.2 CSipSimple

CSipSimple est une voix sur protocole Internet (VoIP) demande de Google Android système d'exploitation utilisant le Session Initiation Protocol (SIP). Il est open source et logiciels libres publié sous la GNU General Public License .

Autrement dit, CSipSimple est une application destinée aux smartphones ou aux tablettes équipées d'Android qui permet de passer et recevoir des appels téléphoniques par Internet.

4.3.3 Interaction entre le serveur SIP et les bases de données : AGI

AGI (Asterisk Gateway Interface) est une interface permettant de faire communiquer le plan de numérotation (extension.conf) avec des programmes extérieur à Astérisk, écrits avec des langages. Habituellement, les scripts AGI sont utilisés pour communiquer avec des bases de données relationnelles comme MySQL.

AGI est matérialisé par l'écriture de scripts qui sont exécutés dans le plan de numérotation. A chaque lancement d'un script AGI, Asterisk envoie au script un ensemble de variables avec leurs valeurs. Lorsque toutes les variables sont émises, Asterisk envoie une ligne vide pour préciser au script qu'il peut commencer.

Le script envoie les commandes et Asterisk renvoie au script, pour chaque commande émise une réponse.

4.3.4 Interaction entre php et le serveur SIP : AMI

Asterisk Manager Interface (AMI) est une interface de surveillance et la gestion système fourni par Asterisk. Il permet de surveiller en direct d'événements qui se produisent dans le système, ainsi vous permettant de demander que Asterisk effectuer une action. Les actions qui sont disponibles sont vastes et comprennent des éléments tels que le retour des informations d'état et provenant de nouveaux appels. De nombreuses applications intéressantes ont été développées au-dessus de ce que Asterisk profiter de l'AMI que leur interface principale d'Asterisk.

Asterisk Manager Interface (AMI) permet à un programme de client de se connecter à une instance d'Asterisk et exécuter des commandes ou de lire les événements sur un flux TCP / IP.

4.4 Préparation du serveur

Notre serveur est une machine virtuelle sous système d'exploitation Debian (32bits), de 512Mo de RAM dans laquelle nous avons installé XiVO, MySQL et Apache 2.

4.4.1 Installation et configuration de XiVO

4.4.1.1 Installation XiVO

Pour installer XiVO, nous avons téléchargé l'ISO depuis leur site web. Pour accéder à l'interface web, nous avons utilisé l'adresse IP de notre serveur 10.90.47.245.

Une fois que l'installation est terminée, il faut mettre à jour le système avec les commandes suivantes :

- apt-get update
- apt-get upgrade

4.4.1.2 Configuration

Pour la configuration de XiVO, nous avons passé par les étapes suivantes :

- choix de langue : anglaise ;
- acceptation de la licence ;
- configuration : cette page contient les éléments suivants :
  - hostname : xivo
  - domain name : memo03
  - password : superuser
  - address : 10.90.47.245
  - netmask : 255.255.255.0
  - default gateway : 10.90.47.1
  - dns primary : 10.90.47.1
- entités et contexte : cette page contient les champs suivants :
  - display name : spécifie le nom de l'entreprise (memo03)
  - internal calls context : spécifie le plan de numérotation des utilisateurs
- validation : à cette dernière étape, nous avons validé toute la configuration faite dans les deux étapes ci-dessus.

Après avoir validé la configuration, XiVO génére la configuration de base avant d'afficher la page d'authentification pour qu'on puisse connecter.

Figure 4.02 : *Page login de XiVO*

4.4.2 Installation et configuration de MySQL

L'installation de MySQL se fait tout simplement en lançant les commandes :

- #apt-get install mysql-server ;
- # apt-get install php5-mysql;
- # apt-get install phpmyadmin;

Puis, lancer la commande :

- # mysql –p
  mot de passe
  >Exit ;

pour vérifier que MySQL fonctionne bien.

Enfin, nous redémarrons le serveur avec la commande :

- #/etc/init.d/mysqld restart

4.4.3 Installation et configuration d'Apache 2

L'installation d'apache se fait tout simplement en lançant les commandes :

- #aptitude install apache2 ;
- #aptitude install apache2-doc ;

Ensuite, nous éditons le fichier de configuration

- /etc/apache2/httpd.conf
- /etc/apache2/apache2.conf

Afin de permettre à tout utilisateur d'accéder à notre serveur WEB sans aucune restriction et aussi que notre simulation soit dans un environnement réel pour des besoins expérimentaux.

4.5 Configuration des clients

4.5.1 Configuration de Jitsi

Les configurations des deux clients SIP se fait de la même façon ; seules les informations d'identifications des comptes changent.

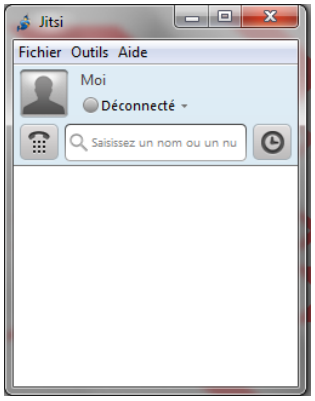

Figure 4.03 : *Première ouverture de Jitsi*

Nous allons, créer les comptes clients 3001 et 3002. Pour ce faire : Fichier/ Ajouter un nouveau compte.

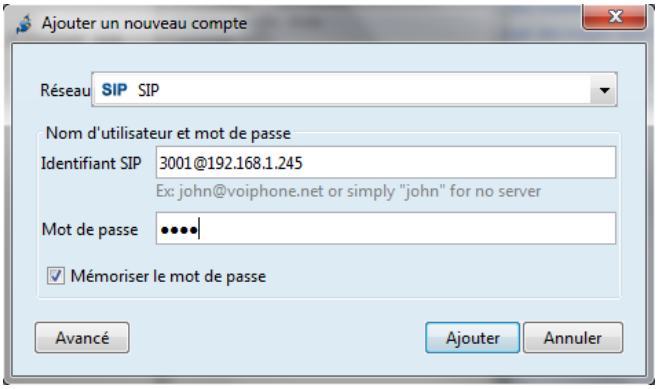

Figure 4.04 : *Création d'un nouveau compte*

Cliquer sur *Ajouter*, nous avons :

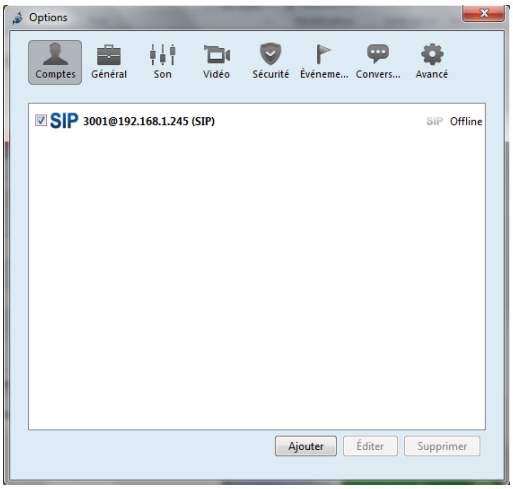

Figure 4.05 : *Compte 3001 créé*

La création du compte 3002 est la même que celle du 3001, seulement l'identification qui sera changée.

4.5.2 Configuration de CSipSimple

Pour configurer CSipSimple dans un smartphone, nous devons :

- ouvrir l'application CSipSimple déjà installé ;

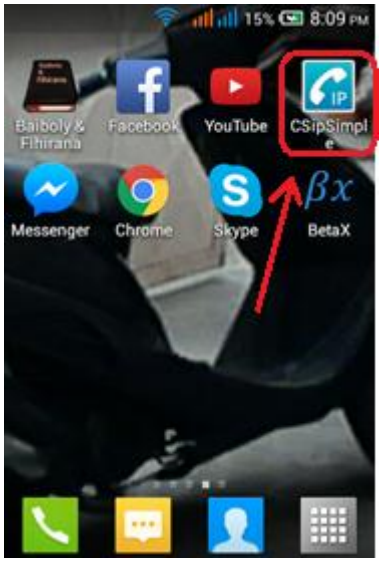

Figure 4.06 : *Application CSipSimple*

- choisir le profil de disponibilité ;

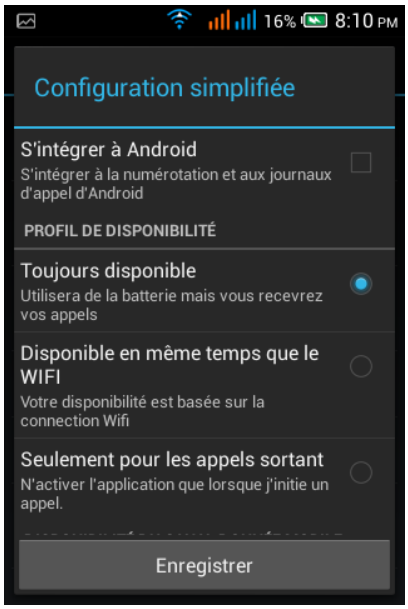

Figure 4.07 : *Interface de configuration simplifiée de CSipSimple*

- enregistrer les configurations ;

Pour créer le compte 3003, nous devons :

- choisir l'assistant : dans notre cas, nous avons choisi « *basic* » ;
- compléter les paramètres pour le compte ;

Figure 4.08 : *Paramètres du compte 3003*

- Puis *enregistrer* les paramètres ;

Figure 4.09 : *Enregistrement du compte 3003*

4.6 Simulation

Le processus que nous adoptons pour notre plateforme est comme suit :

- mise en marche du serveur ;
- interconnexion des actionneurs et outil de pilotage (client SIP) avec le serveur XiVO ;
- découverte des dispositifs ou actionneurs ; en composant le 601 à partir du smartphone (compte 3003) ou du softphone (compte 3001) ;
- choix des dispositifs : appuie sur 1 pour l'électroménager ou appuie sur 2 pour la sécurité;
- découverte des services ;
- choix des services.

4.6.1 Commande à distance d'un four

Dans la première simulation, après avoir composé le 601, nous avons appuyé sur 1 c'est-à-dire l'électroménager (four). Dans le paragraphe suivant, nous allons commander à distance un four avec un smartphone et/ou un softphone.

Pour cela,

- Le four représente l'actionnaire avec une adresse IP : 10.90.47.10 pour le réseau local et 192.168.1.10 pour le réseau Internet ;
- L'outil de pilotage ou bien l'agent utilisateur est le smartphone et/ou softphone;
- Le serveur SIP a comme adresse IP : 10.90.47.245 pour le réseau local (LAN) et 192.168.1.245 pour le réseau Internet (WAN).
- La passerelle SIP/four est l'interface AGI

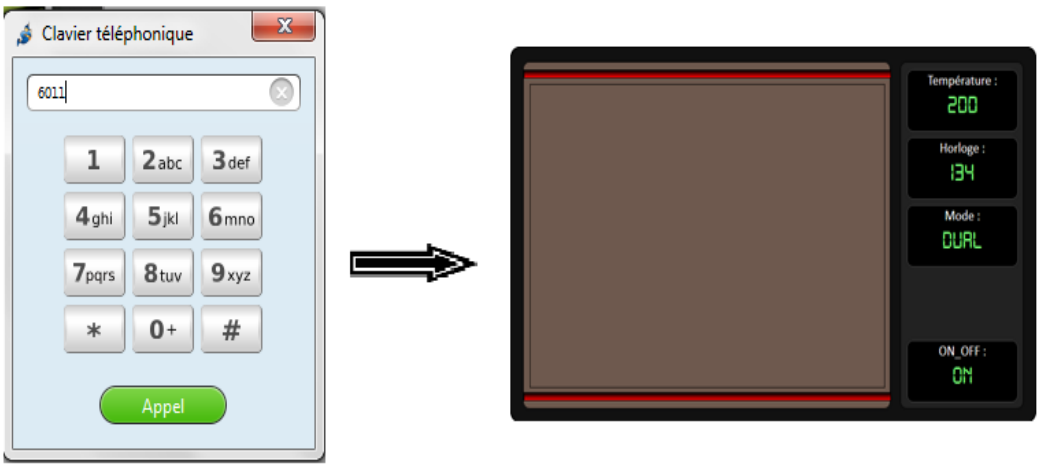

Figure 4.10 : *Commande d'un four*

Le tableau ci-dessous montre une récapitulation des numéros (codes) à appeler pour piloter à distance le four, ainsi que ces fonctions.

Numéro à appeler	Fonction	Résultat
910	extinction	Le four est éteint
911	allumage	Le four est allumé
981	lecture de la durée de cuisson	L'état actuel de la durée de cuisson est donné
982	lecture de la valeur de la température	L'état actuel de la température est donné
991	réglage de l'horloge	La valeur de l'horloge est changée
992	réglage de la température	La température prend la valeur entrée
984	détermination de l'état général du four	L'état général du four est donné

Tableau 4.01 : *Numéros pour commander à distance le four*

4.6.2 Détection d'intrusion

Pour cette deuxième simulation, nous avons choisi 2 après avoir composé 601.

Pour cela :

- La webcam représente le détecteur avec une adresse IP : 10.90.47.100 pour le réseau local et 192.168.1.100 pour le réseau Internet ;
- L'outil de pilotage est le smartphone et/ou softphone;
- Le serveur SIP a comme adresse IP : 10.90.47.245 pour le réseau local (LAN) et 192.168.1.245 pour le réseau Internet (WAN).
- La passerelle SIP/détecteur est l'interface AMI

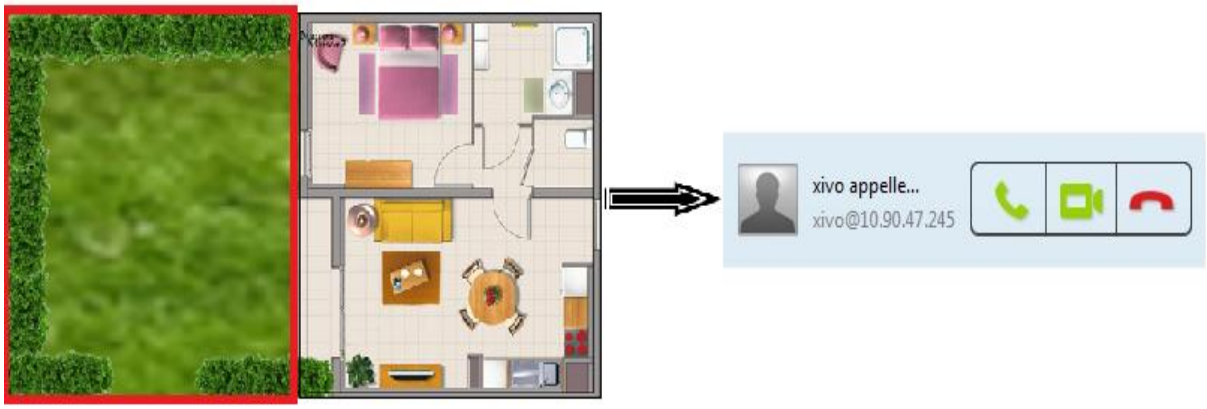

Figure 4.11 : *Détection d'intrusion*

Quand il y a un intrus dans la cours ou dans les chambres, le client SIP reçoit un appel vidéo montrant ce qui se passe à sa maison, en même temps, la police reçoit aussi un appel audio signalant qu'il y a une alerte chez une famille dont son adresse est indiquée.

Les commandes à faire pour assurer la fonction sécurité avec notre plateforme sont résumées dans le tableau 4.02 suivant.

Numéro à composer	Fonction	Résultat
710	Désactiver la sécurité dans la maison	Même s'il y a un intrus dans la maison, le client ne reçoit rien
711	Activer la sécurité dans la maison	S'il y a un intrus dans la maison, le client reçoit un appel
810	Désactiver la sécurité dans la cours	Même s'il y a un intrus dans la cours, le client ne reçoit rien
811	Activer la sécurité dans la cours	S'il y a un intrus dans la cours, le client reçoit un appel
890	Désactiver tout appel	Même s'il y a un intrus, le client ne reçoit rien
891	Activer tout appel	Quand il y a un intrus dans la cours ou dans la maison, le client reçoit un appel

Tableau 4.02 : *Commande pour la fonction sécurité de notre plateforme*

4.7 Résultats et discussion

Ici, nous avons vu que l'utilisation de notre plateforme domotique est intéressante. Mais il nous vient à l'esprit d'analyser la performance et le coût pour déployer de notre système ainsi que ses impacts dans notre pays.

La performance de notre système dépend de la performance de notre connexion internet et de notre serveur physique comportant le système XiVO. Donc, il est préférable de bien sécuriser notre serveur.

En termes de coût, le déploiement de notre système est un peu coûteux à cause de l'importation des matériels à utiliser (les logiciels à implémenter sont tous des logiciels libres). Mais ce coût sera rapidement amorti car notre dépense mensuel pour les salaires des domestiques, des agents de sécurité, la facture de la JIRAMA seront éliminés et diminués, en utilisant ce système smart life.

Par contre, l'utilisation de ce plateforme peut augmenter le taux de chômage. En effet, en utilisant ce système smart life avec VoIP, les agents de sécurité et les domestiques peuvent être licenciés car notre système arrive à faire ces travaux.

4.8 Conclusion

Au cours de ce chapitre, nous avons décrit toutes les étapes nécessaires de l'implémentation de notre système « Smart Life avec VoIP» y compris la présentation de l'environnement logiciel, afin d'aboutir à son fonctionnement, ainsi que les applications que nous pouvons faire avec notre système. Comme nous l'avons mentionné, notre système « Smart House » offre à l'utilisateur de l'application les fonctionnalités nécessaires pour piloter son réseau domotique afin d'assurer le bon fonctionnement du système.

CONCLUSION GENERALE

Actuellement, nous entendons parler d'objets connectés, d'électroménager connecté et où la démocratisation des smartphones a changé notre rapport à internet, certains concepteurs cherchent à connecter les appareils électriques et électroniques de notre maison le plus facilement possible, profitant de notre attrait pour le smartphone pour le transformer en "super télécommande". Grâce à la solution domotique, quelque soit l'endroit où nous nous trouvons dans le monde, du moment que nous sommes connectés à internet, nous pouvons regarder notre maison.

Aujourd'hui, parallèlement à l'évolution de la domotique, la téléphonie standard a peu à peu laissé sa place à la VoIP, qui, elle, repose sur la commutation par paquets et celle-ci comporte les adresses réseau de l'expéditaire et du destinataire. Les paquets VoIP qui sont transmis à travers n'importe quel réseau haut débit (wifi, 3G, 3G+…).

Pour gérer la VoIP, l'utilisation d'Asterisk est très intéressante et qui passe entre autre par la prise en charge d'un protocole standard, ouverte et très largement utilisé, le SIP. La souplesse de ce protocole SIP fournit beaucoup d'intérêts pour collecter les données des actionneurs et des capteurs.

Alors nous pouvons profiter l'alliance entre la domotique et la VoIP via le réseau internet haut débit d'un smartphone/softphone pour améliorer notre vie quotidienne qui est le but de notre plateforme « Smart life avec VoIP ».

Au terme de ce travail élaboré, nous considérons que ce projet nous a été bénéfique vu que l'utilisation de VoIP sera utile dans le domaine de la domotique. En effet, l'apport de notre étude se résume surtout dans la mise en œuvre de la sécurisation, les pilotages de divers appareils électroménagers par l'utilisation d'un serveur XiVO basé sur Asterisk et piloté par un smartphone.

Toutefois, quelques prérequis sont nécessaires, outre posséder un smartphone/softphone, les éléments dont nous souhaitons prendre le contrôle doivent être électriques ou électroniques et nous devons disposer d'une connexion Internet dans la maison.

ANNEXE 1 : EXEMPLES DES MATERIELS EN DOMOTIQUE

A1.1 Microcontrolleur ARM09

C'est une carte équipée d'un système d'exploitation Linux (Distribution Linux From Scratch) avec le support des périphériques du processeur et les principaux protocoles réseaux du marché. Elle possède de nombreuses E/S pour pouvoir connecter différents capteurs et actionneurs tel que les liaisons série et le bus USB. La carte possède aussi une interface réseau pour pouvoir remplir son rôle de passerelle. La figure A1.01 présente une carte ARM09.

Figure A1.01 : Microcontrolleur ARM09

A1.2 Capteur iButton

Ces capteurs de Dallas Semiconductor permettent une mesure et un enregistrement facile de la température ou de l'humidité. Ces capteurs sont reliés au microcontrolleur à travers des bus 1-Wire. Le 1-Wire est défini comme un bus de communication en 1 fil (plus la masse). Il a été développé par Dallas Semiconductor pour fournir une méthode de connections simple avec alimentation intégrée pour des capteurs.

Chaque composant iButton possède une clé unique 64bits qu'il identifie. Ce numéro est également gravé sur le boitier afin de les reconnaitre de l'extérieur.

Les capteurs 1-wire de Dallas transmettent leurs données numériques sur le bus. De plus, un mécanisme de CRC (Cyclic Redundancy Check) est prévu pour la sécurisation de la transmission des identifiants.

Il existe une multitude de iButtons remplissant différentes fonctions comme la mesure de la température ou de l'humidité, l'identification et l'enregistrement des mesures.

Figure A1.02 : *Capteur iButton DS1920*

A1.3 Module XBee

Ces modules sont certifiées ZigBee par l'alliance ZigBee. Tirant parti de l'attrait du faible coût et de la faible consommation d'énergie du standard ZigBee, les modules XBee de MaxStream possèdent des fonctionnalités supplémentaires : différentes options de puissance de sortie, trois options d'antennes et des outils de configuration avancés.

La gamme de produits XBee est disponible pour de nombreuses applications industrielles et commerciales, parmi lesquelles la télé-détection, l'automatisation et le contrôle des équipements. Le responable de la gestion du réseau XBee est le nœud ARM, qui prend les commandes sous format SOAP et peut exécuter les requêtes des agents SIP. La figure A1.03 présente un module XBee.

Figure A1.03 : *Module XBee*

A1.4 Module CM11

Il existe plusieurs interfaces permettant de contrôler les modules X10 à l'aide d'un ordinateur. Le module CM11 en est un. Les modules CM11 sont des modules pouvant s'interfacer sur les ports série ou USB de la passerelle SIP. Ces modules de commande assuret l'interface entre la passerelle SIP (carte ARM) et le réseau domotique.

Figure A1.04 : *Module CM11*

A1.5 Module LM12

Ce module permet de commander une lampe en faisant varier la puissance. A l'intérieur, il utilise un triac avec détection du passage par 0 pour caler la commutation. Ce module a été utilisé pour allumer des lampes dans une infrastructure domotique.

Figure A1.05: *Module LM12*

ANNEXE 2: ASTERISK

A2.1 Présentation

Asterisk est un logiciel libre sous licence GNU/GPL permettant à un simple ordinateur d'opérer en tant que commutateur téléphonique privé Il permet ainsi la téléphonie au sein d'un LAN, la messagerie vocale, les conférences, et la distribution d'appels. [12]

Asterisk implémente les protocoles H.323 et SIP, ainsi qu'un protocole spécifique nommé IAX (Inter-Asterisk eXchange). Ce protocole IAX permet la communication entre deux serveurs Asterisk ou entre un client et un serveur Asterisk. Ces protocoles peuvent être sollicités auprès d'un ISP ou auprès d'un opérateur de VoIP.

A2.2 Fonctionnalités

A ce jour, Asterisk est certainement la seule solution qui offre une telle richesse et flexibilité de fonctionnalités. En plus des fonctionnalités classiques, il propose des services plus avancés pour interconnecter les systèmes de téléphonie traditionnelle et de VoIP (donc rôle de passerelle).

Les fonctionnalités sont nombreuses, appels en mode conférence, appels en attente, enregistrement d'appel, file d'attente, heure et date d'appels, identification de l'appelant, identification de l'appelants sur appel en attente, insertion de messages vocaux dans courriels, intégration à différents types de SGBDR, liste noires, ne pas déranger, messagerie SMS, messagerie vocale, indicateur visuel de message en attente, redirection des messages vocaux par courriel, interface Web pour la gestion des messages, musique d'attente....etc. [23] [27]

A2.3 Architecture interne

Asterisk est un système flexible grâce à sa structure interne constitué de quatre APIs (Application Programming Interface) spécifiques autour du « central core system ». Celui-ci manie les connexions internes du PBX en faisant abstraction des protocoles, des codecs, des interfaces téléphoniques et des applications (d'où la possibilité d'utiliser n'importe quel hardware et n'importe quelle technologie).

La figure ci-dessous montre l'architecture interne de l'Asterisk.

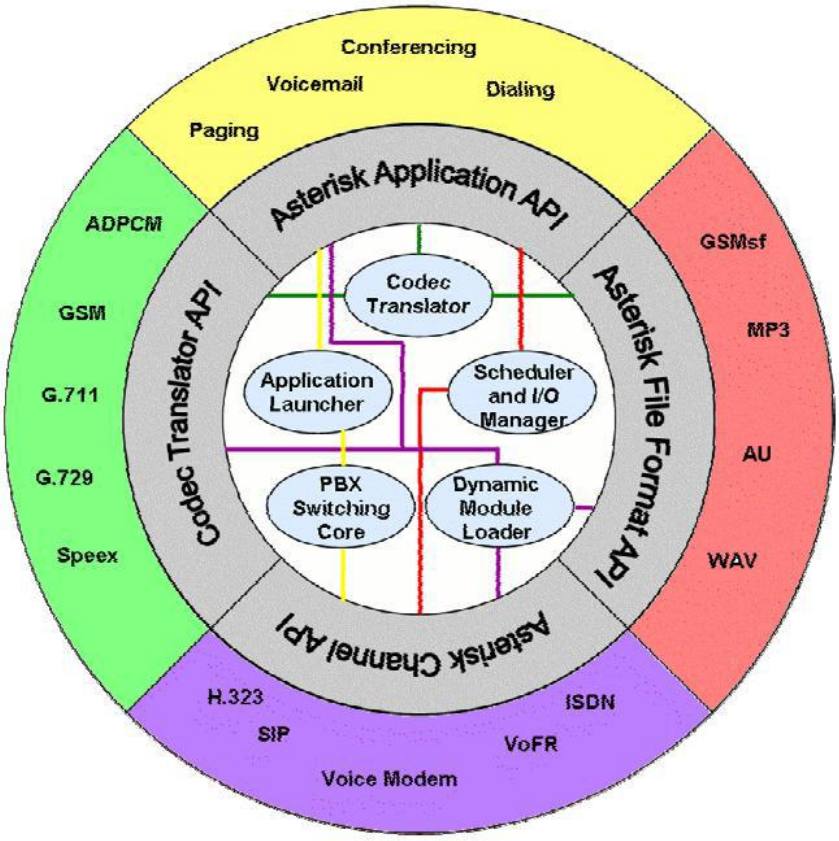

Figure A2.01 : *Architecture interne*

Asterisk joue le rôle de middleware (intergiciel) entre les technologies de téléphonie et les applications (conférence, messagerie vocale, IVR (Interactive Voice Response)), il favorise le déploiement d'environnements mixtes.

Le cœur contient 5 moteurs ayant chacun un rôle essentiel et critique dans les opérations :

- La commutation de PBX (PBX Switching Core) : fonction primaire, commute de manière transparente les appels.
- Lanceur d'applications (Application Launcher) : lance les applications qui exécutent des services pour les utilisateurs.
- Traducteur de codec (Codec Translator) : code et décode la voix, plusieurs codecs sont utilisés pour trouver l'équilibre entre la qualité audio et l'usage de la bande passante.
- Planificateur Manager d'I/O (Scheduler and I/O Manager) : planifie en bas niveau et gère les entrées/sorties pour des performances optimales.

- Dynamic Module Loader : charge les pilotes (lors de la 1ère exécution d'Asterisk, il initialise les pilotes et fait le lien avec les APIs appropriés). Après que les pilotes soient chargés, les appels commencent à être acceptés et redirigés en faisant sonner les téléphones.

L'abstraction matérielle et protocolaire passe par l'utilisation de 4 APIs :

- Channel API : gère le type de connexion, des modules dynamiques sont chargés pour travailler sur les couches basses de ces connexions.
- Application API : accomplit de manière flexible toute fonction à la demande.
- Codec Translator API : charge les modules pour supporter tous les formats (support dynamique, c'est-à-dire qu'un codec peut être utilisé pour une communication et un autre codec pour une autre communication suivant le débit de la ligne par exemple).
- File Format API : manie la lecture et l'écriture de formats de fichiers variés pour stocker dans le système de fichiers. En utilisant ces APIs Asterisk réalise une abstraction complète entre ces fonctions noyau de serveur PBX et les diverses technologies existantes (ou en développement) dans le domaine de la téléphonie. [28]

A2.3 Configuration

Pour qu'Asterisk fonctionne de manière basique, il est nécessaire de modifier les fichiers de configuration : sip.conf, extensions.conf qui se trouvent dans le répertoire **/etc/asterisk.** [25]

A2.3.1 sip.conf

Le fichier sip.conf permet de définir tous les utilisateurs SIP. Il est segmenté en sections, dont chacune débute par une étiquette (le label) entre crochets.

Le label spécial *[general]* permet d'attribuer des valeurs à des paramètres génériques, tels que le port utilisé. Le label *[user_id]* définit chaque compte d'utilisateur.

Paramètre	Description
username	Identifiant de l'utilisateur
secret	Mot de passe associé au compte
type	Indique le type de compte et les restrictions associées • *friend :* permet d'appeler et d'être appelé • *user :* permet seulement d'être appelé • *peer :* permet de définir une liaison entre deux terminaux seulement
host	Spécifie une adresse IP à partir de laquelle l'utilisateur peut accéder à son compte. La valeur *dynamic* autorise une adresse IP fournie dynamiquement. Cette valeur est donc moins restrictive.
context	Spécifie le type de routage à appliquer pour l'utilisateur. Le type de routage correspond à un contexte défini dans le plan de numérotation (extensions.conf). les communications sont donc soumises au contexte du même nom dans le fichier extensions.conf.

Tableau A2.01 : *Paramètres décrivant un compte SIP*

Voici un exemple de déclaration d'un utilisateur dans un fichier sip.conf :

[3001]
username=3001
secret=0000
type=friend
host=dynamic
context=local

A2.3.2 extensions.conf

Ce fichier contient le plan de numérotation. C'est l'élément central de la configuration du serveur Asterisk. Il définit le comportement du serveur. Maître de cérémonie ou chef d'orchestre, c'est lui qui régit les actions à entreprendre, dans quel ordre et dans quel cas, que ce soit pour un utilisateur donné ou pour l'ensemble des utilisateurs.

Ce plan concentre toute l'intelligence et la logique de fonctionnement du réseau téléphonique. C'est pourquoi il est indispensable d'en maîtriser à la fois la syntaxe et la sémantique. Il est

constitué d'un ensemble de règles, dont chacune pose les conditions de son application, ainsi que, lorsque ces conditions sont réunies, les traitements qui seront appliqués.

Le plan de numérotation répond à la question : que doit faire le serveur Asterisk lorsqu'il reçoit le flux téléphonique d'un utilisateur ? la réponse est fournie sous forme des règles qui sont structurées et dont la syntaxe est définie par les quatre éléments suivants :

- le contexte ;
- l'identifiant d'extension ;
- la priorité ;
- l'application.

Le format général d'un plan de numérotation, dans lequel se combinent ces quatre éléments, est le suivant :

[contexte_1]
exten => identifiant_d'extension_1, priorité_1, application_1
exten => identifiant_d'extension_2, priorité_2, application_2

Nous pouvons lire la première règle comme suit : « Lorsque l'extension *identifiant_d'extension_1* se présente dans le contexte *contexte_1,* nous exécutons l'action *application_1* avec la priorité *priorité_1* ».

Application	Description
Answer	Répond à un appel téléphonique entrant
Hangup	Termine une communication
Dial	Met en relation l'appelant et l'utilisateur ou le service spécifié en argument de l'application
Queue	Met en attente une communication
Record	Enregistre une communication dans un fichier son
Transfer	Transfère l'appel vers un autre poste ou service
VoiceMail	Laisse un message voacal

Tableau A2.02 : *Applications les plus courantes*

A2.4 Avantages apportés par Asterisk

Comme Asterisk est un logiciel libre sous licence GNU/GPL, on peut donc avoir son code source, les modifier à notre intérêt et il est gratuit.

ANNEXE 3 : CODE SOURCE DE LA SIMULATION

A3.1 Code web pour l'activation de l'appel audio en cas d'intrus

```
<?
/* ============================ */
/*   PHP Asterisk Peer Status   */
/* ============================ */
/*    (C) 2009 Matt Riddell     */
/*     Daily Asterisk News      */
/* www.venturevoip.com/news.php */
/*      Public domain code      */
/* ============================ */

/* Connection details */
$manager_host = "127.0.0.1";
$manager_user = "xivouser";
$manager_pass = "xivouser";

/* Default Port */
$manager_port = "5038";

/* Connection timeout */
$manager_connection_timeout = 10;

/* Connect to the manager */
$fp = fsockopen($manager_host, $manager_port, $errno, $errstr, $manager_connection_timeout);
if (!$fp) {
   echo "There was an error connecting to the manager: $errstr (Error Number: $errno)\n";
} else {

            /*            echo "-- Connected to the Asterisk Manager\n";*/
            /* echo "-- About to log in\n";*/


/*Numero */

$num = "SIP/100109701100/00261340239927";

/*$num = "SIP/3003";*/



            $login = "Action: login\r\n";
            $login .= "Username: $manager_user\r\n";
```

```
        $login .= "Secret: $manager_pass\r\n";
        $login .= "Events: Off\r\n";
        $login .= "\r\n";
        fwrite($fp,$login);

        $originate1 = "Action: originate\r\n";
        /*$originate1 .= "Channel: SIP/3003\r\n";*/
                /*$originate1 .= "Channel: SIP/100109701100/00261340239927\r\n";*/

                $originate1 .= "Channel: ".$num."\r\n";


                /* num d urgence !!!! */

        $originate1 .= "Exten: 870\r\n";

                /*          $originate1 .= "Exten: 3002\r\n"; */

        $originate1 .= "Context: default\r\n";
        $originate1 .= "Priority: 1\r\n";
        $originate1 .= "\r\n";
        fwrite($fp, $originate1);
    /*    fwrite(sleep(2)); */


    }

  fclose($fp);
  exit(0);
?>
```

A3.2 Code source pour l'activation de l'appel audio et vidéo en cas d'intrus

```
<?php


$db = mysql_connect('localhost', 'root', 'superuser') OR die('Erreur de connexion … la base');
        mysql_select_db('four_elec',$db) OR die('Erreur de selection de la base');


$sql = "SELECT * FROM secu WHERE idsecu = '1'";
//On envoie la requ?te
$req = mysql_query($sql) or die('Erreur SQL !<br>'.$sql.'<br>'.mysql_error());

        $secu_appel = mysql_fetch_array($req);

//var_dump ($data);
```

```
        $stat_appel_video=$secu_appel["secu_appel_video1"];
        $stat_appel_audio=$secu_appel["secu_appel_audio1"];



//      echo "</br>";
//      echo $allume;


if (($stat_appel_video == '0')OR($stat_appel_audio == '0')) {


        $status_appel = "OFF";


        $sqlsecuc = "UPDATE secu SET secu_appel_video1 = 1,secu_appel_audio1 = 1
WHERE idsecu = '1'" ;
        $reqtsecuc = mysql_query($sqlsecuc) or die('Erreur SQL
!<br>'.$sqlsecuc.'<br>'.mysql_error());}

else{


        $status_appel = "ON";


        $sqlsecuc = "UPDATE secu SET secu_appel_video1 = 0,secu_appel_audio1 = 0
WHERE idsecu = '1'" ;
        $reqtsecuc = mysql_query($sqlsecuc) or die('Erreur SQL
!<br>'.$sqlsecuc.'<br>'.mysql_error());}


mysql_close($db);

include 'input_secu.php';

?>

</body>
</html>
```

A3.3 Code AGI pour consulter ou paramétrer l'état général du four

```
#!/usr/bin/php -q
<?
ob_implicit_flush(false);
error_reporting(0);
set_time_limit(30);

require('include/phpagi/phpagi.php');
error_reporting(E_ALL);




$agi = new AGI();

$agi->answer();



$db = mysql_connect('localhost', 'root', 'superuser') OR die('Erreur de connexion … la base');
        mysql_select_db('four_elec',$db) OR die('Erreur de selection de la base');


$sql = "SELECT id_etat,allume,eteint,description FROM etat WHERE id_etat = '1'";
//On envoie la requ?te
$req = mysql_query($sql) or die('Erreur SQL !<br>'.$sql.'<br>'.mysql_error());

        $data = mysql_fetch_array($req);

//var_dump ($data);



        $allume=$data["allume"];
        $eteint=$data["eteint"];



if ($allume == '1'){


        $agi->stream_file("four_allum","#");
```

```
        }
else {
        $agi->stream_file("four_etteint","#");

        }

$reqtemp = mysql_query('SELECT * FROM temperature') OR die('Erreur de la requête MySQL');
        $restemp = mysql_fetch_array($reqtemp);

        $temp=$restemp['temp'];

        $agi->stream_file("val_temp");

        $agi->say_number($temp);

        $reqtimer = mysql_query('SELECT * FROM timer') OR die('Erreur de la requête
MySQL');
        $restimer = mysql_fetch_array($reqtimer);

        $time=$restimer['valeur'];

        $agi->stream_file("val_timer");

        $agi->say_number($time);


$agi->hangup();


mysql_close($db);

?>
```

BIBLIOGRAPHIE

[01] S. Lionel, « *De l'automatisme à la domotique* », 2012.

[02] A. Gential, « Domotique et confort, un état des lieux », 2001

[03] M. Weiser, « *The computer for the 21st century, ACM SIGMOBILE Mobile Computing and Communications Review* », Vol. 3, 2008.

[04] D. Sapiens, « *Etude et réalisation de la domotique* », 2013.

[05] Konnex Association, « *Présentation de la domotique et des systèmes d'automatisation de maison intelligente », 2013*.

[06] « *Les grandes fonctions de la domotique* », Cours de 4è année à l'Université de Marne-La-Vallée, 2012.

[07] « *La domotique* », cours 4è année Institut d'électronique et d'informatique Gaspard-Monge, Université de Marne-La-Vallée, 2012.

[08] F.X Jeuland, « *La maison communicante* », Editions Eyrolles, Avril 2012

[09] V. Saraswat, B. Bloom, I. Peshansky, O. Tardieu, D. Grove, « *X10 language Specification Version 2.5* », 2014.

[10] « *Le prêt à brancher de la domotique* », la maison de la domotique, 2014.

[11] Technical Background, « *HAVi* », Flammarion, 2010.

[12] J. Desbonnet, P. M. Corcoran, «*System Architecture And Implementation of a CEBus/Internet Gateway* », University College, G always, Ireland, 2012.

[13] A. Patrick, « *Le bue EIB* », Lycée Antonin, Artaud Marseille, 2012.

[14] A. Pnonphoem, « *HomeRF* », 2002.

[15] M. Ulislma, « *Introduction to Bluetooth technology* », 2005.

[16] B. Cousin, « *ZigBee, 802.15.4* », Université de Rennes, 2011.

[17] B. Sooza, «*The Jini Architecture* », Sun Microsystems, 2002.

[18] H.wong, « *Jini Technology Basics »*, 2002.

[19] S. Fontain «*Voix sur IP-VoIP* », http://www.frameip.com/voip/ , 2013

[20] Asterisk, «*Asterisk project* », https://wiki.asterisk.org/wiki/display/AST/Home, 2013.

[21] RFC 3261, «*SIP: Session Initiation Protocol* », http://tools.ietf.org/html/rfc3261, 2013.

[22] L. Ouakil, G Ryelle, « Téléphonie sur IP », 2è Edition, Eyrolles, 2005.

[23] O .Hersnet, D .Gurle, « La voix sur IP », Dunod, Paris 2006.

[24] A. Sulkin, PBX Systems for IP Telephony, McGraw-Hill Telecom: USA 2002.

[25] A. Tanenbaum, Réseaux, 4e édition, Pearson Education, Paris, 2003.

[26] Cuenot G., « *Réseaux et Informatique d'Entreprise : Le protocole H.323* », M1 RIA, 2007.

[27] « *H.323: Architecture et Protocoles* », http://www.efort.com, EFORT, 2013.

[28] S. Znaty, J.L. Dauphin « *SIP: Session Initiation Protocol* », EFORT, 2013.

[29] « *Voix sur IP – VOIP* », SebF, Novembre 2004.

[30] R. Bouzaida, « *Etude et mise en place d'une solution sécurisée* », 2014.

[31] P. Roque, « *Les cahiers de programmeur UML* », Edition Eyrolles, 2001.

[32] P.A. Muller, « *Modélisation Objet avec UML* », Edition Eyrolles, 1998.