Projet Européen SWAN : Services WiFi appliqués au NTIC (Visio, ToIp, HotSpot grand public)

David Chiron, Thomas Colombeau, Bernard Jecko, Phillipe Gaborit, Marcel Giry

Projet Européen SWAN : Services Wi-Fi Appliqués aux NTIC

David CHIRON
CISTEME : Centre d'Ingénierie des Systèmes de Télécommunications, d'ElectroMagnétisme et d'Electronique
david.chiron@unilim.fr

Philippe GABORIT
LACO - Université de Limoges
philippe.gaborit@unilim.fr

Marcel GIRY
Service Commun Informatique - Université de Limoges
marcel.giry@unilim.fr

Bernard JECKO
IRCOM équipe CREAPE - Université de Limoges
bernard.jecko@creape.unilim.fr

Thomas COLOMBEAU
CISTEME : Centre d'Ingénierie des Systèmes de Télécommunications, d'ElectroMagnétisme et d'Electronique
thomas.colombeau@creape.unilim.fr

Résumé

Notre consortium de partenaires universitaires, industriels, associations et indépendants nous a permis depuis 1999 de mener à bien des expériences techniques d'une part et de services d'autre part sur des réseaux sans fil de type Wi-Fi, ou plus performants comme des réseaux points multipoints tels que le LMDS 40 GHz (1), le WiMAX(2), voir ceux propriétaires fonctionnant en bande ISM (3). Dans le cadre de l' appel d'offre régional Practiciel soutenu par des fonds européens, un soutien aux compétences régionales nous a été attribué pour effectuer la mise en place de services innovants sur des réseaux sans fil. Lors de la rédaction du projet SWAN, nous avons initié ce dernier en réfléchissant sur des services destinés aux mêmes cibles qui compose notre consortium de partenaires, à savoir : Entreprises, Universitaires et « Grand Public ». Nous avons fait le choix de la téléphonie fixe et mobile sur IP à champs limité pour les industriels, en mettant l'accent sur le déploiement d'un commutateur téléphonique IP basé sur le logiciel open source Asterisk (4) ; parallèlement, nous avons échantillonné un ensemble de terminaux IP de divers constructeurs et testé les téléphones mobile sur une architecture Wi-Fi à commutateur centralisé du constructeur ORTRONICS (filiale du groupe Legrand, OEM d'ARUBA) (5). Nous détaillerons cette architecture puisqu'elle est déployée d'une part sur le site de la technopôle mais aussi au sein même de l'Université de Limoges. Aussi, pour compléter ce déploiement, nous avons procédé à l'installation d'un réseau de test Wi-Fi permettant d'expérimenter des moyens d'authentifications forts (Etoken) (6) et une meilleure maîtrise de la couverture radio indoor (antenne adaptée). Finalement aux beaux jours du mois de juin, nous avons déporté pendant une période de trois semaines, un accès haut débit pour permettre la couverture outdoor de la place de la république de Limoges et offert aux scolaires et au grand public un accès haut débit Wi-Fi en installant un stand et mettant à disposition pour les gens non équipés un ensemble d'ordinateurs portables Wi-Fi. Nous avons eu recours à l'installation d'un pont radio haut débit de type WiMax et nous avons associé un ensemble de bornes Wi-Fi couplées sur une seule antenne afin d'augmenter la capacité d'accueil et la bande passante ; sans négliger la fiabilisation du réseau.

Mots clefs

Wireless, Wi-Fi, WiMAX, Etoken, ToIp, Asterisk, RADIUS, Sécurité

1 Introduction

Le cœur de métier du CREAPE/CISTEME est orienté depuis plusieurs années vers les réseaux sans fils. En effet déjà en 1999 nous avons été retenu pour déployer le premier démonstrateur européen LMDS fonctionnant à 40GHz. Ce projet présenté lors des JRES 2001 reposait sur le déploiement d'une infrastructure radio de type point multipoints permettant d'interconnecter des étudiants en chambre universitaire à l'école d'ingénieur du site pour offrir des services de e-learning tels que la visioconférence. Ce démonstrateur toujours en fonctionnement à ce jour nous a propulsé au cœur du sixième PCRD dans le projet Broadwan (7) pour améliorer les performances de notre démonstrateur tant sur l'aspect radio (composants critiques) que sur l'aspect réseau (transport d'IPV6). Forts de cette expérience de capillaire radio nous avons monté, en partenariat avec la société Radiall System, un des trois démonstrateurs WiMax 3.5GHz de France Télécom à Amilly. Nous avons utilisé le matériel 802.16a - 2004 référencé AN-100 chez le constructeur Redlinecommunication (8). Nous avons également déployé un réseau en bande ISM (2.4GHz) permettant d'interconnecter à trois terminaux radio un équipement de vidéosurveillance (caméra IP) offrant un débit partagé de 8Mbit/s réel avec qualité de

service. Finalement dans le cadre de notre dernier projet SWAN, réponse à l'appel d'offre Practiciel du Limousin, nous avons monté un démonstrateur reposant sur une infrastructure complexe mélangeant matériel actif classique, pont RF de type Wimax, Architecture Wi-Fi à commutateur centralisé, association de bornes Wi-Fi derrière une antenne sectorielle, le tout utilisant des mécanismes de sécurité reposant sur l'usage de carte à puce et non uniquement sur un couple login/password. Sur ce même démonstrateur, nous avons proposé de nombreux services, comme la téléphonie sur IP fixe et Wi-Fi utilisant une base de PBX libre du nom d'Asterisk (11), l'accès Internet pour le grand public à un réseau « outdoor ». Nous allons présenter ce projet SWAN selon ces trois sous projets à savoir : téléphonie pour les entreprises, réseau d'accès pour les étudiants, et « hot-spot » grand public.

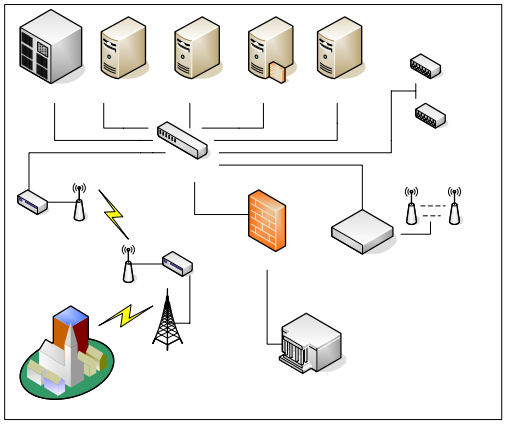


Figure 1 - *Schéma général du réseau IP mis en place*

2 Sous projet 1 : La téléphonie sur le réseau IP et Wi-Fi IP

2.1 L'architecture globale réseau

Avant tout, nous présentons ici le réseau déployé sur lequel viendront se greffer tous les équipements filaires ou sans fil. L'ensemble des services proposés est interconnecté sur un cœur de réseau utilisant un commutateur de niveau trois (routeur). Il s'agit d'un 3com 3C17701 offrant vingt quatre ports gigabits de type 10/100/1000baseT. Sont connectés sur ce cœur de réseau tous les équipements actifs pour l'ensemble du projet, à savoir le pont radio qui permet d'alimenter le cluster d'AP Wi-Fi place de la république à Limoges, le système centralisé Wi-Fi au sein de la technopôle qui offre la connectivité sans fil pour les terminaux IP-Phone Wi-Fi avec la gestion du handoover, les équipements actifs (commutateurs niveau deux HP + injecteur de courant powerdsine à la norme 802.3 af) permettant d'alimenter les bureaux du bâtiment pour y interconnecter les téléphones IP filaires, le réseau universitaire permettant de faire transiter les appels IP vers d'autres lieux, ainsi que toutes les machines nécessaires au bon rendu des services : pare feu, serveur d'authentification, proxy filtrant, portail captif, entre autres. Cette architecture a était déployée au fil des tâches du projet. Sa représentation globale est représentée sur la figure 1.

Nous n'avons pas programmé de paramètre de qualité de service dans un premier temps car l'ensemble des liens filaires et radio transite sur un réseau isolé et dédié. Aussi, la capacité de chaque lien est suffisante pour transporter l'information nécessaire. Au fil de l'article et à chaque fois que cela sera essentiel, nous décrirons plus précisément chacune des parties de cette architecture, à commencer par la partie voix sur IP.

2.2 Asterisk : un commutateur téléphonique VoIP opensource :

Lors du montage de cette partie PBX (Public Branch eXchange) nous avions plusieurs choix concernant la partie autocommutateur d'entreprises. D'une manière générale ce choix était assez limitatif, puisque hormis le PBX IP d'un constructeur, nous avions essentiellement soit en premier choix : le Call Manager ou Call Manager Express (système implémenté non plus sur un serveur mais sur un routeur) de Cisco, soit une solution libre. Attachant de l'importance au domaine open source, nous nous sommes lancés dans l'aventure avec Asterisk. Cependant d'autres nous avaient déjà montrés le chemin (9). Le but de l'exposé n'étant pas de détailler le fonctionnement d'Asterisk dans ces moindres détails, nous pouvons cependant expliquer que nous avons fait le choix du protocole SIP (plus de fonctionnalité que H323) (10) et du protocole MGCP (pour intégrer le fonctionnement de certains terminaux mobile aujourd'hui limités). Côté matériel nous avons choisis un serveur basé sur un bi-XEON 3GHz avec 1Go de RAM, un raid 1 de 73Go (un peu de place pour la messagerie vocale des utilisateurs) et bien sûr une alimentation redondante et un onduleur (les utilisateurs se plaignent lors d'une coupure du courrier électronique, ce qui n'est finalement rien en comparaison du téléphone). La particularité du serveur est qu'il offre une connectivité 64Bits sur ces bus PCI permettant de recevoir notre carte nécessaire pour nous relier sur une infrastructure téléphonique. Elle provient du constructeur Digium (11), acteur principal qui soutient le projet Asterisk. Il fournit des cartes d'accès bon marché de la simple analogique (4 ports FXO/FXS), en passant par la T0 jusqu'à une quad T2 (T0 est la dénomination d'un accès de base correspondant à 2 canaux de 64 kBit/s, T2 correspondant à un accès de 30 voies simultanées). C'est cette dernière qui équipe notre PBX ; elle permet donc de gérer jusqu'à 120 voies téléphoniques ce qui nous laisse entrevoir une montée en charge du nombre d'utilisateurs. A ce jour nous utilisons deux accès, un vers un autocommutateur MATRA 6540 situé sur un site de l'université permettant de « router » les appels inter universitaires, l'autre en attente d'une connexion vers un opérateur téléphonique. Cependant

notre serveur PBX doté d'un seul port PCI 32 bits, ils nous étaient impossible de placer plus d'une carte à quatre ports FXS pour interconnecter des téléphones classiques ou plus utiles les télécopieurs. Le logiciel Asterisk a cependant établi le protocole IAX (Inter Asterisk Exchange) permettant de tracer un lien entre PBX open source. Grâce à ce protocole, nous avons monté un autre serveur identique au premier basé sur une architecture matérielle plus simple permettant d'accueillir les cartes Quad FXS pour connecter des télécopieurs. Dans le schéma suivant, on retrouve le serveur Asterisk principal en bas, celui du haut connecté via le protocole IAX (Inter Asterisk eXchange) pour recevoir via les cartes FXS les fax et un call manager express dont nous détaillerons la raison de la présence ultérieurement.

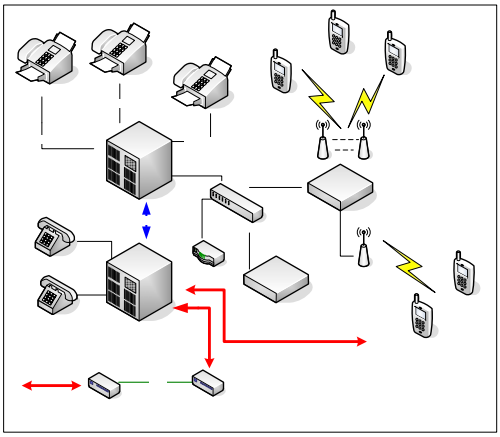


Figure 2 - *Architecture de la téléphonie sur IP avec Asterisk*

On imagine qu'avec ce même protocole il est possible d'établir des liens au travers de tunnel VPN et de disposer ces « petits » au sein de l'union européenne (pratique pour une structure ayant un fort relationnel téléphonique avec l'étranger, moins intéressant pour l'opérateur téléphonique). Parmi les nombreuses fonctionnalités d'Asterisk, on peut réaliser des « conf-call » gratuitement si on utilise le réseau Internet. Puisque nous évoquons l'aspect financier, nous sommes en train d'analyser la possibilité via des dongles et gsm bluetooth de réaliser des passerelles GSM économiques. Bien qu'au début de nos tests, la solution open source Asterisk laisse entrevoir un fort potentiel tant au niveau fonctionnalité que performance et nous continuons à exploiter de nouveaux services au fil des jours. Cependant la téléphonie sur IP reste à ce jour encore non économiquement viable pour certaines structures, principalement à cause du prix du terminal IP.

2.3 Les terminaux téléphoniques échantillonnés et leur compatibilité avec Asterisk

Notre serveur installé, nous avons échantillonnés certains terminaux. Nous ne présentons ici pas l'ensemble des terminaux existants puisque lorsque nous avons choisis certains parmi d'autres, nous avons pu constater un nombre phénoménal d'équipements tant sans fil que filaires ; d'ailleurs, depuis, de nouveaux sont apparus. Nos critères de choix se sont orientés selon la compatibilité avec Asterisk, les fonctionnalités, les doublons (certains téléphones sont quasi-identiques), l'ergonomie et le tarif. Le premier choix sans trop se tromper (terminaux référencés et testés par la communauté Asterisk) est le 7960 du constructeur Cisco (vingt postes) ; moins de tests mais quand même cité le sans fil Wi-Fi 7920 (dix postes). Le principal inconvénient de ces équipements est leur tarif élevé. A signaler au passage que l'autonomie des portables 7920 est limitée à une douzaine d'heures en veille et 2 heures en communication.

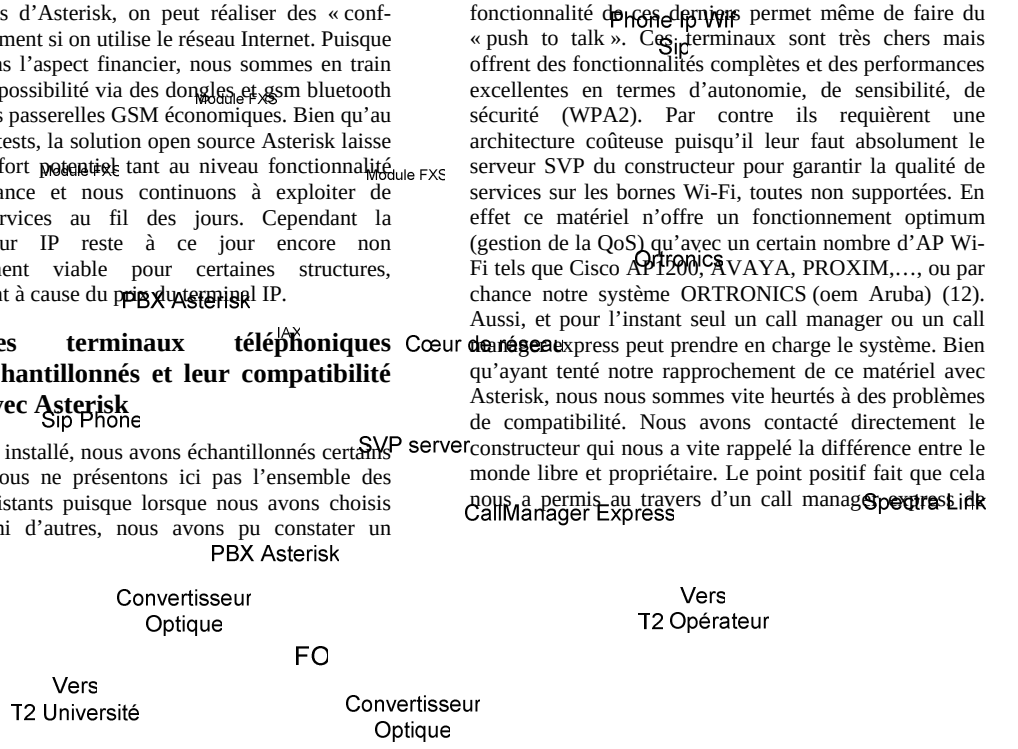
Le second constructeur identifié a était Polycom. Nous recherchions des terminaux de type araignée pour équiper des salles de conférences et nous avons choisi 4 téléphones de conférences IP400. Par la même occasion, nous avons acquis dix terminaux IP600 (équivalence aux fonctionnalités des 7960, mais plus économiques dans un rapport deux environ).

Le troisième constructeur fût Snom et nous avons approvisionné une dizaines de modèles filaires 190 et 220, de l'expérience ce sont les plus économiques des téléphones filaires échantillonnés.

Ayant acquis suffisamment de terminaux filaires, nous cherchions plus de modèle Wi-Fi et notre choix hormis Cisco n'était pas évident.

Le Quatrième constructeur fut Zyxel qui propose le téléphone Wi-Fi prestige 2000W. Leur prix est défiant toute concurrence mais les performances tant au niveau sensibilité/portée qu'autonomie sont décevantes. Nous avons interconnectés dix de ces modèles. Un point positif est que c'est le modèle qui a posé le moins de problème pour sa mise en fonctionnement (nous avons pu même réaliser une conversation de mobile à mobile via une borne Wi-Fi D-Link).

Finalement, bien que non référencé « dans le monde d'Asterisk », nous avons voulu tester le constructeur SPECTRALINK, spécialiste pour les terminaux mobiles. Nous avons échantillonnés dix i640 et dix e340. La fonctionnalité de ces derniers permet même de faire du « push to talk ». Ces terminaux sont très chers mais offrent des fonctionnalités complètes et des performances excellentes en termes d'autonomie, de sensibilité, de sécurité (WPA2). Par contre ils requièrent une architecture coûteuse puisqu'il leur faut absolument le serveur SVP du constructeur pour garantir la qualité de services sur les bornes Wi-Fi, toutes non supportées. En effet ce matériel n'offre un fonctionnement optimum (gestion de la QoS) qu'avec un certain nombre d'AP Wi-Fi tels que Cisco AP1200, AVAYA, PROXIM,…, ou par chance notre système ORTRONICS (oem Aruba) (12). Aussi, et pour l'instant seul un call manager ou un call manager express peut prendre en charge le système. Bien qu'ayant tenté notre rapprochement de ce matériel avec Asterisk, nous nous sommes vite heurtés à des problèmes de compatibilité. Nous avons contacté directement le constructeur qui nous a vite rappelé la différence entre le monde libre et propriétaire. Le point positif fait que cela nous a permis au travers d'un call manager express de



connecter ce dernier à notre solution open source sans grande difficulté.

2.4 Le déploiement sur la technopole de Limoges du système à commutateur Wi-Fi et les premiers tests

Nous présentons ici le système déployé sur le site d'ESTER technopole et nous ferons un aparté sur une structure similaire (matériel ARUBA) qui avait été déployée en multi sites sur le réseau de l'Université de Limoges dès Janvier 2005.

LEGRAND et sa filiale ORTRONICS sont partenaires du projet SWAN et nous ont mis à notre disposition un système Wi-Fi à commutateur centralisé (OR-WCU-16), accompagné d'une douzaine de bornes 802.11 a/b/g. Ces AP fonctionnent soient à 5GHz (802.11a) soit à 2.4GHz (802.11 b/g). Elles sont équipées de deux antennes de type F dual band pour la diversité. A la différence des modèles ARUBA, elles sont prévues pour être installées directement au mur à la place d'un interrupteur par exemple. Relativement plates, elles restent discrètes. Le commutateur présente huit ports POE (802.3af) et ce modèle gère jusqu'à seize bornes maximum. Nous bénéficions d'une infrastructure Ethernet catégorie 5 complète ce qui nous permet de positionner les bornes où nous le souhaitons dans le bâtiment et de profiter de la télé alimentation 48V du commutateur. Pour pimenter l'infrastructure, nous avons via un pont RF 2,4GHz connecté une entreprise du site situé à l'extérieur. Via un VLAN dédié, nous avons positionné une borne dans cette entreprise permettant la connexion de terminaux sans fil.

L'architecture réseau nous a conduit à associer à chaque participant un VLAN filaire et un autre wireless (associé au SSID).

Chacune des bornes propage l'ensemble des SSIDs (associés aux VLAN wireless), ce qui permet à chaque utilisateur de bénéficier pleinement de l'infrastructure radio quelque soit le lieu où il se trouve et d'émettre et recevoir ces appels. Les premiers tests ont d'ailleurs montré que si la couverture de deux bornes étaient adjacentes, il est alors possible de transiter d'une cellule à une autre sans coupure de la communication (handoover ou roaming). Le commutateur Wi-Fi se charge d'assurer la continuité de la connexion au niveau 2.

Une illustration du système Wi-Fi déployé est représentée sur la figure 3. On remarque que lors de la construction du réseau avec ce commutateur centralisé Wi-Fi, nous n'avons pas besoin de propager les VLAN (correspondants au SSIDs) au travers des switchs 802.1q traversés, seule la diffusion de notre vlan d'administration a suffit

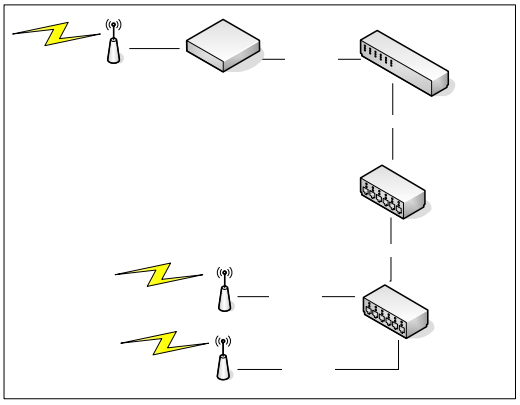


Figure 3 - *Représentation du principe de déploiement de l'équipement Wi-Fi à commutateur centralisé*

Ce système est fortement intéressant pour une administration d'un nombre important de bornes Wi-Fi. Aussi, dans le cadre de l'accompagnement du projet MIPE (Micro Portables pour les Etudiants) l'Université de Limoges a déployé un WLAN sur l'ensemble de ses sites dès Janvier 2005.

L'objectif était d'offrir une ou plusieurs zones de connexion Wi-Fi sur l'ensemble des "lieux de vie" des étudiants, sans rechercher une couverture complète des bâtiments. Une attention particulière était apportée à la facilité d'administration.

Le réseau Wi-Fi qui a été retenu à l'issue d'une consultation est composé d'un "commutateur Wi-Fi" d'origine ARUBA et d'une trentaine de points d'accès légers. Ces derniers sont raccordés au commutateur central par un tunnel GRE qui est, soit propagé sur le réseau MAN de l'Université à travers un VLAN dédié, soit routé à travers le réseau IP pour atteindre les sites délocalisés de l'Université, ou les sites des partenaires institutionnels de l'Université. Ainsi le réseau WLAN de l'Université a pu être prolongé jusqu'aux cafétérias des Restaurants universitaires.

L'authentification des étudiants (et des personnels) est assurée par un portail captif intégré au commutateur Wi-Fi qui interroge un serveur RADIUS, qui lui-même accède aux serveurs LDAP de l'établissement.

Une présentation du projet a été effectuée lors des assises 2005 du CSIESR (13)

3 Sous projet 2 : Les tests de couverture et de sécurité

Le cadre de ce sous projet concerne essentiellement la mise en place de choix techniques concernant ce qui peut être problématique sur les réseaux sans fil, à savoir les aspects couverture et sécurité.

3.1 La couverture radio Wi-Fi Indoor

Nous avons choisi d'installer un point d'accès Wi-Fi dans le hall principal de l'Institut Universitaire de Technologie de l'Université de Limoges. Ce point d'accès est un Cisco AP1200, car il permet de choisir l'antenne d'émission, celle de réception et de régler finement la puissance d'émission, paramètres nécessaires pour optimiser notre couverture radio. Nous avons donc choisi d'émettre et de recevoir sur une seule sortie et d'annihiler les effets des switchs de diversité au sein même de l'AP. Nous avons construit les jarretières coaxiales nécessaires et couplé l'ensemble à une antenne sectorielle réglable offrant des couvertures de 60 à 180° (déplacement d'un réflecteur latérale au réseau d'antennes patch) : l'idée étant de limiter la couverture radio au strict minimum. Bien sur, la solution n'est pas parfaite à cause notamment du problème de trajets multiples mais cependant elle permet de réduire la puissance au niveau de l'antenne. Parallèlement, nous sommes en train de réaliser une antenne de type omnidirectionnel à fixer au plafond, permettant d'assurer une couverture conique de 120°. Le résultat attendu est que seul les utilisateurs positionnés dans le cône de couverture reçoivent de l'information. Nous présenterons nos mesures lors de l'exposé. Bien sûr tous ces systèmes ne sont pas totalement immunisés vis-à-vis d'utilisateurs mal intentionnés équipés d'antennes YAGI et autres paraboles à fort gain.

3.2 L'authentification client par Etoken.

Aujourd'hui la plupart des moyens d'authentification se font à l'aide de couples login/password qui ont plusieurs faiblesses, comme le fait d'être distribués, le fait de pouvoir être interceptés avec un keylogger voire volés d'un simple regard. Nous avons donc réfléchi à l'utilisation d'un autre mode d'authentification qui se rapproche du fonctionnement de la carte bancaire, où le principe repose sur une carte à puce dont l'accès est forcément validé par un code pin. De telle sorte qu'il faut pour s'identifier non seulement avoir accés à un PIN mais aussi avoir un objet matériel. Une telle solution rend alors la fraude nettement plus complexe.

Nous avons donc orienté notre choix sur l'utilisation de Etoken (carte à puce) USB renfermant un certificat. Le principe repose sur un ensemble clé publique / clé privée, cette dernière ne pouvant être lue sur le Etoken qu'après validation par un code PIN. Notre client Wi-Fi se connecte sur un point d'accès qui peut être le même système que celui présentait ci-dessus ou plus simplement dans le cadre de nos tests un AP Cisco 1200, qui se comporte comme un NAS (Network Access Service) vis-à-vis d'un serveur RADIUS en amont. Le serveur envoie son certificat public.

La norme 802.1x propose plusieurs protocoles d'authenfication dont le protocole EAP-TLS qui permet l'authentification mutuelle du serveur et de l'utilisateur avec des certificats électroniques. On introduit une infrastructure de clés publiques (PKI) qui s'appuie sur une autorité de certification (gérée indépendamment) qui certifie les différents certificats utilisés par le serveur RADIUS ainsi que par les clients potentiels. On place dans le Etoken qui représente le client la clé publique de l'autorité de certification, la clé privée du client ainsi que sa clé publique munie d'un certificat de l'autorité de certification.

La PKI gère les certificats des clés ainsi qu'une liste de révocation permettant d'invalider des clés dans le temps. L'authentification mutuelle se fait alors entre le serveur RADIUS et le client, en échangeant tout d'abord les certificats de leurs clés publiques respectives, ces certificats sont vérifiés en utilisant la clé publique de l'autorité de certification. Une fois les certificats vérifiés le client envoie au serveur un challenge chiffré avec la clé publique (du serveur) que ce dernier doit déchiffrer avec sa clé privée et renvoyer au client. De la même façon le serveur envoie au client un challenge chiffré avec la clé publique du client qui doit renvoyer le challenge déchiffré par sa clé publique. Ce système permet donc au serveur et au client de s'identifier mutuellement.

La sécurité du système repose sur le fait que pour se faire authentifier un client doit avoir accès à la clé privée associé à son certificat sur le Etoken. Tous les calculs d'authentification pour le client se font directement sur le Etoken de telle sorte que la clé privée associée à un utilisateur ne sort pas du Etoken. De plus l'utilisation de la clé privée du client sur le Etoken nécessite la connaissance d'un code PIN demandé à l'utilisateur sur le poste client. Ainsi pour se faire authentifier par le serveur RADIUS un client a besoin à la fois du Etoken qui contient la clé privée associée à un client mais aussi du code PIN qui permet de lire cette clé.

Cette solution d'authentification est donc très simple d'utilisation et très adaptative et offre une sécurité plus importante qu'une simple authentification classique login/password.

Bien qu'existant depuis quelques années, cet outil nous semble sous exploité.

3.3 Les tests réalisés

Nous sommes en train de mener des tests sur une vingtaine de personnes équipées respectivement de quinze portables prêtés associés à quinze clés Etoken et cinq clés à la disposition d'intervenant extérieur muni de leur propre machine. Lors de la présence d'un portable « prêté » avec sa clé dans la zone Wi-Fi, l'utilisateur n'a besoin de connaître que le code pin associé à l'Etoken pour se connecter au réseau, code qui lui est demandé lors de son authentification. Pour un nouvel arrivant avec son matériel, il faut d'abord lui installer la clef sur un port USB (il lui faut Windows comme OS, linux étant en cours de développement pour le matériel). Ensuite lors de la première connexion, la procédure est identique à la précédente.

4 Sous projet 3 : L'accès Internet haut débit en centre ville de Limoges

4.1 Le stand et la population

Un de nos partenaires privé a implanté un espace de 100m2 de pagodes place de la république à Limoges (place où l'on trouve bon nombre de terrasse). Une douzaine de portables Wi-Fi 802.11b ont été à la disposition des visiteurs sous ces pagodes. Chacun de ces portables reçoit une clé Etoken pour permettre une authenfication identique à l'expérience de l'IUT. Parallèlement, nous avons mis à disposition un ensemble de ticket présentant des jetons de connexion à Internet valable trente minutes pour les personnes utilisants leur propre matériel.

4.2 Les modes de connexion et les services

D'un point de vue des services offerts, nous en avons proposé de deux types qui sont rattachés au mode de connexion. En effet, les personnes se présentant dans le stand et qui s'assoient devant un ordinateur portable ont une connexion sans limite (au sens temps et protocole/ports). En revanche ceux qui utilisent les tickets de connexion se voient brider à 30 minutes totales (10 minutes un jour + 20 le lendemain par exemple) d'une part et la stricte utilisation du http/https. De plus toutes leurs transactions se sont vues automatiquement filtrer de manière transparente par un serveur proxy couplé à dansguardian (14) de manière à se protéger d'une utilisation non conventionnée par le réseau Renater (téléchargement de mp3, site au contenu plus que limite, etc…). Pour scinder nos deux réseaux, nous avons propagé deux VLAN différents. De plus comme nous avions des portables (ceux du stand dédié au public) qui ne fonctionnaient qu'en mode 802.11b, pour ne pas pénaliser les plus performants (802.11g) nous avons couplé plusieurs bornes entres elles d'un point de vue RF (radio fréquence) sur une seule et même antenne sectorielle à fort gain.

4.3 Le détail de l'infrastructure réseau et radio de la place de la république

L'idée principale repose sur la séparation de type de connexion des clients : point de vue matériel et type d'authentification. En effet nous avons une borne qui broadcast les deux SSIDs associés à leur VLAN respectif et qui n'autorise que des clients OFDM (802.11g), une autre qui accepte des clients 802.11b et 802.11g et la dernière dédiée uniquement aux portables sous les pagodes. Côté Ethernet ces trois bornes sont connectées via un switch à un équipement radio de type point multipoints fonctionnant dans la bande des 5GHz et offrant un débit réel maximal de 48Mbit/s (mode utilisant la modulation QAM64 avec FEC à 2/3). Cet ensemble a était placé dans un coffret électrique étanche et positionné sur le toit des Nouvelles Galeries : une antenne dirigée vers la technopôle d'ESTER pour le pont RF et l'autre qui couvre la Place de la République en Wi-Fi. Le principe de cet ensemble repose sur le schéma suivant :

Figure 4 - *Coffret radio Wi-Fi et pont hertzien avec couplage radio des points d'accès Wi-Fi*

On aperçoit sur ce dernier les trois points d'accès relier à un coupleur 3dB figurant (zoom) sur le côté gauche de la photographie. Sur la suivante on distingue l'antenne sectorielle assurant la couverture radio jusqu'aux pagodes situées à l'arrière plan :

Figure 5 - *Vue du mat et de son antenne sectorielle (vue de détail à 90° de l'antenne en insertion en bas à droite)*

4.4 La vie du stand pendant 3 semaines

Notre stand a été opérationnel du 24 Mai au 18 Juin 2005, son ouverture publique étant le 31 Mai. Pendant toute cette période nous avons accueilli des personnes familières avec cette technologie, d'autres venant pour apprendre et comprendre et certains anecdotiquement nous demandant « qu'est qu'il faut pour s'abonner et c'est combien ! ! !». Nous avions distribué des tickets de connexions utilisables pendant trente minutes et obtenu finalement qu'une centaine de personnes qui s'en sont servis avec leur propre matériel. Nous avons eu environ quatre cents connexions sur le stand avec cinq cent trente élèves de cours élémentaire et préparatoire des écoles de la ville venu passer leur « examen Internet » en binôme.

Figure 6 - *Photographie réalisée pendant la manifestation où l'on note la présence de personnes utilisant les 2 modes de connexion (Etoken au niveau du stand en arrière plan + tickets pour ceux en terrasse)*

La manifestation ayant eu lieu au beaux jours du mois de juin, nous redoutions des problèmes dû à la chaleur puisque les bornes et le pont RF sont restés enfermés dans le coffret métallique étanche et exposés directement au rayonnement solaire pendant plus de trois semaines. Mais finalement le stand a vécu sans contrainte particulière, sachant que nous avions installé une surveillance SNMP des principaux équipements actifs en interconnectant le réseau de l'expérience avec notre système interne de monitoring réseau basé sur cacti (15).

5 Conclusions et Perspectives

5.1 Conclusion

Cette courte expérience de 18 mois nous a permis une fois de plus de mettre à profit les technologies sans fil et le monde du logiciel libre dans le but de proposer des services innovants en pleine émergence et d'associer des briques permettant de répondre aux attentes précises des utilisateurs. Nous avons réussi notre challenge et certaines idées profilent déjà dans notre consortium.

5.2 Perspectives

Ces idées ont plusieurs horizons : Asterisk fonctionnant tout à fait convenablement, ce logiciel regroupant un tas de fonctionnalités plus intéressantes les unes que les autres, nous commençons à déployer un autre serveur sur un site distant pour router nos communications inter université entre pbx. Côté industriel, le projet semble susciter un intérêt important vers les partenaires industriels locaux, certains ayant des filiales à l'étranger. Nous regardons pour l'avenir toutes les fonctionnalités et le regroupement d'intérêt économique que nous pouvons mener pour offrir une structure téléphonique centralisée riche et économe.

De l'expérience universitaire, le besoin d'antennes répondant à des cahiers des charges précis et stricts pour les stations de base (AP Wi-Fi, WiMax, LMDS,…) incite la recherche de concepts de plus en plus innovants. En parallèle, le système d'authentification à clefs devenant abordable, il est envisagé de le généraliser pour l'accès aux intervenants extérieurs et visiteurs.

Finalement, l'ouverture au grand public de l'Internet haut débit sans fil bien que moyennement satisfaisante en terme de communication et de retour d'expérience, suscite auprès des collectivités territoriales des réalisations similaires.

Affaire à suivre…

6 Remerciements

Nous tenons à remercier particulièrement les organisateurs des JRES pour nous avoir permis de présenter ce projet. Nous exprimons notre gratitude à la Région Limousin, l'Europe et l'Agence Régionale de Développement qui nous ont offert la possibilité de mener cet ensemble d'expériences dans le cadre du projet Practiciel. Nous remercions également la Mairie de Limoges qui nous a soutenu et mis à disposition la place de la République, les nouvelles galeries qui nous ont permis d'installer tous nos équipements radio, l'ensemble des partenaires du projet et particulièrement les industriels qui ont apporter « leur pierre à l'édifice » à savoir le groupe LEGRAND, la société MDS International, la sarl REGARDS pour son magnifique stand, et la société RADIALL SYSTEM.

A titre personnel, j'exprime tous mes remerciements à Messieurs Didier ROQUES, Nicolas CHEVALIER, et l'ensemble des stagiaires qui ont fait que SWAN soit une réussite.

Bibliographie

[1] David Chiron, Dans *Actes du congrès JRES2001*, pages 643-649, Lyon, Décembre 2001.

[2] http://www.wimaxforum.org

[3] http://www.manucorp.com/encyclopedie/Bandes_ISM

[4] Paul Mahler, VoIP Telephony with Asterisk, ISBN 09759992-0-6

[5] http://www.arubanetworks.com

[6] http://www.aladdin.com/etoken/

[7] http://www.telenor.no/broadwan/

[8] http://www.redlinecommunications.com/products/an100/an100.pdf

[9] http://www.voip-info.org

[10] http://www.eikonex.org/article.php3?id_article=7

[11] http://www.digium.com

[12] http://www.ortronics.com/us/products/wireless/

[13] Marcel GIRY, Nicolas VIERS : Assises 2005 du CSIESR http://www.csiesr.fr/article.php3?id_article=215

[14] http://www.pcxperience.org/dgvirus/

[15] http://www.cacti.net

Mise en forme : Puces et numéros