Stage d'IUP Génie Informatique, option Réseaux

Jean-François Rodriguez

du 31 mars au 30 septembre 2003

Wi-Fi
Expérimentations et soutien technique aux initiatives locales

Érasme
Conseil Général du Rhône

Université
Claude Bernard Lyon1

UFR d'informatique

Résumé

Ce rapport concerne mon stage d'IUP Réseau, dont le sujet comportait une partie d'expérimentations sur le Wi-Fi, et une partie de soutien technique à des initiatives locales utilisant cette technologie.

Y sont présentés le centre Érasme et les principaux travaux effectués pendant ces six mois.

Les chapitres 2 et 3 présentent le centre Érasme et le contexte du stage.

Les chapitres suivants exposent mes principales activités pendant ce stage. Ils sont classés dans l'ordre chronologique du début des missions, les quatre premières s'étant étalées sur plusieurs mois, alors que les deux dernières ont été beaucoup plus ponctuelles par comparaison.

Enfin les annexes contiennent : un glossaire des termes relatifs au Wi-Fi les plus courament utilisés, une présentation du Wi-Fi, qui fait le tour du sujet en quelques paragraphes et une procédure mise en place suite aux expériences menées lors du stage.

Table des matières

Remerciements

Ce chapitre incontournable peut être l'occasion d'exprimer une gratitude sincère envers les personnes qui ont apporté une aide, une écoute ou simplement une chaleur gratuite et généreuse.

Bien sûr, un merci particulier à Patrick Vincent, mon maître de stage, qui m'a choisi comme stagiaire et qui a su me laisser une réelle autonomie, tout en me guidant et en m'apportant l'aide et les moyens nécessaires au bon déroulement de mon stage.

Merci à Yves-Armel Martin qui a accepté ma candidature.

Je remercie également l'équipe technique d'Érasme pour leur aide inconditionnelle, et toute l'équipe pour l'accueil chaleureux et sympathique qui m'a permis de m'intégrer très rapidement.

D'autres personnes ont également joué un rôle dans ce petit épisode de ma vie. En particulier, je pense à Mehdi Hamida, Nicolas Grimler et Thomas Vénard de l'association Wireless-Lyon ; Thomas Gassilloud, Nicolas Poncet et Jean-Michel Cachard de la Maison des Jeunes de Pomeys ; Mathieu Prade, de la société INEO-Infracom ; Nicolas Prost, de la société Wisp-e ; Roger Daelemans de l'association radioamateurs F6KIO et de l'association multi-technologique de Lyon (AMT), ainsi qu'aux autres membres de ces associations ou sociétés rencontrés et que je n'ai pas cités nommément.

Ce stage a aussi donné lieu à un travail étroitement collaboratif avec Maxime Charpenne, stagiaire du DESS Réseau de l'Université Lyon 1.

Chapitre 1

Introduction

Autorisé depuis peu en France, le Wi-Fi est une technologie de transmission de données informatiques par ondes radio.

Le débit théorique du standard actuel, de 11 Mbits/seconde, et le coût relativement faible du matériel permettent d'envisager de multiples utilisations, domestiques, communautaires ou professionnelles, voire de développement du territoire.

L' "Internet sans fil" est-il possible ?

Le centre Érasme, entité du Conseil Général du Rhône, en a fait le pari, et a lancé un programme d'extension du réseau départemental par le biais du Wi-Fi.

C'est dans ce cadre que j'ai été pris en stage à Érasme : des expériences sont en cours, d'autres sont envisagées, et le programme lancé nécessite des ressources et des compétences supplémentaires.

Chapitre 2

Érasme

Érasme est une mission du Conseil Général du Département du Rhône pour le développement des Nouvelles Technologies de l'Information. Créé en 1999, sur le canton de communauté de communes de Saint Laurent de Chamousset, à Saint Clément les Places, à 45 km de Lyon, le Centre Multimédia Érasme a vu ses domaines d'intervention multipliés.

2.1 Le réseau départemental

Les Autoroutes Rhodaniennes de l'Information sont constituées d'un réseau hybride fibre/coaxial sur 289 communes du département (fig. **??**). Ne font pas partie du projet les communes déjà dans le plan câble et desservies par d'autres technologies à haut débit (Lyon, Villeurbanne, Bron, Saint Priest, St Fons, Décines, Meyzieu) et des communes n'ayant pas souhaité adhérer au projet (St Germain au mont d'or, Arnas, Riverie, Jons).

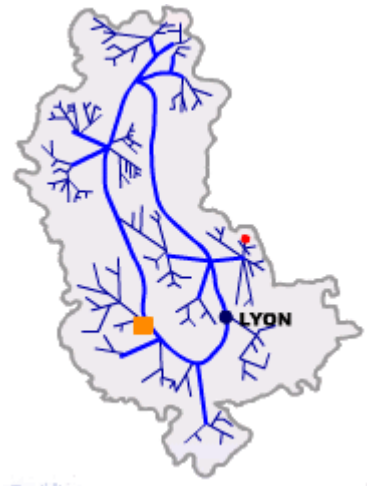

FIG. 2.1 – Le réseau départemental (le carré orange situe le centre Érasme)

Le réseau, opéré par UPC, apporte au moins un point de livraison optique par commune et couvre au moins 70 % des foyers en zone rurale. La téléphonie, la télévision et l'Internet à haut débit sont les trois services fournis. Il existe donc déjà une forte capillarité de désserte à haut débit sur le Rhône. Les bâtiments publics raccordés sont les services des communes et du département : mairies, Maisons du Rhône (décentralisation des services offerts par le département), les bibliothèques, les collèges (97) et les écoles (700).

2.2 Le Centre Serveur Départemental

Aussi appelé Centre Multimédia, il fait office de serveur de ressources brutes : images, sons, vidéos ; de documents multimédias pédagogiques (les enseignants ont leur propre page personnelle où ils peuvent déposer leurs documents et supports de cours qui seront consultables par les élèves, voir plus bas laclasse.com) ; d'un moteur de recherche ; d'un proxy Internet et d'un serveur de messagerie. Une salle de formation et un amphithéâtre permettent d'accueillir des personnes en formation. Une salle d'accès libre permet aux habitants des communes alentour d'avoir un accès à l'internet.

Le centre possède aussi une salle de prise de vue et une salle de montage vidéo, et un studio d'enregistrement et de mixage audio.

Érasme est chargé du support technique aux différents établissements mais aussi de la mise en place ou de l'aide à la mise en place de différents services comme une radio Intranet, un journal de classe, des publications de connaissances. Le routage Internet pour les utilisateurs du réseau départemental est aussi assuré par le centre.

2.3 L'expérimentation

Érasme se charge aussi d'une veille technologique et d'expérimentation à but pédagogique et de développement des technologies de la communication dans le département. Par exemple, actuellement, sont en cours des tests d'utilisation d'un lecteur/enregistreur de sons au format MP3 dans le cadre de la radio de Laclasse.com, et des tests des technologies sans fil Wi-Fi dans le cadre de l'extension du réseau filaire départemental.

2.4 Le Centre de Formation et d'hébergement

Situé dans un bâtiment séparé, il permet d'accueillir des formations, séminaires ou conférences, dans l'amphithéâtre de 80 places ou dans les salles d'informatique ou de travail. L'hébergement est également possible, avec 60 chambres individuelles et un service de restauration.

2.5 Les projets en cours

2.5.1 Laclasse.com : un portail éducatif

Laclasse.com[1] est un portail éducatif exploitant les ressources du haut débit pour fournir aux enseignants et élèves une bibliothèque multimédia et des outils de communication et de publication. Hébergé par le Centre Multimédia, il permet la mutualisation des moyens et l'accès à des contenus en ligne, facilitant l'auto-formation des élèves et des enseignants. Les enseignants des collèges et écoles du département du Rhône ainsi que les élèves de ces établissements y ont accès totalement. Les contenus libres de droit sont consultables par tout internaute en se connectant sous le nom "demo" et le mot de passe "demo". Les établissements extérieurs au département peuvent demander un compte à titre expérimental.

Les contenus (cartes, textes, sons, ...) peuvent être utilisés comme supports de cours, comme rapports d'expériences pédagogiques ou auto-formation des enseignants. Les enseignants peuvent ainsi s'échanger des cours ou des plans de cours, les élèves peuvent publier leurs recherches pour leur classe, participer à des discussions avec des élèves d'autres classes. Les parents d'élèves peuvent consulter l'agenda de la classe et entrer en contact avec les enseignants.

2.5.2 Projet Hartur

Hartur signifie : "Hypermédia d'Archives Régionales d'Actualités Télévisées sur l'Urbanisme dans le Rhône". C'est un projet hébergé au Centre Érasme, mis en place par le département du Rhône, l'Institut National de l'Audiovisuel (INA) et le Centre Régional de Documentation Pédagogique (CRDP) de Lyon à destination des 160 collèges du Département du Rhône.

[1] http ://www.laclasse.com/

Il permet la consultation en ligne d'une cinquantaine d'extraits de films vidéo sur le thème de l'architecture et de l'urbanisme. Ce service s'appuie sur une technologie innovante de navigation, "Hypermédia", développée par l'INA, qui permet d'indexer les documents vidéo et de les consulter de manière interactive, avec accès direct au passage pertinent dans le document.

Le contenu pédagogique a été réalisé sous la responsabilité du CRDP de Lyon, en liaison étroite avec le Centre Académique de Ressources pour l'Informatique Pédagogique qui relève du rectorat.

2.5.3 Rhône sans fil

Rhône sans fil est le projet d'extension du réseau filaire rhodanien, initié par Érasme. Son objectif est le raccordement en haut débit des lieux-dits et foyers isolés en zone rurale, qui ne seront pas desservis par câble en raison des coûts trop élevés d'un raccordement filaire.

2.5.4 Arbres de connaissances

ACNE signifie "Arbres de Connaissances pour une Nouvelle École". Michel AUTHIER et Pierre LEVY, mathématiciens, sociologues et chercheurs, ont mis au point le principe appelé "arbre des connaissances" et l'outil informatique permettant seul de réaliser la gestion globale des connaissances, des compétences et de la formation dans les organisations (communautés scolaires, territoriales ou sociales, entreprises ....). Un arbre de connaissances permet de faciliter l'échange réciproque de savoir entre individus et de situer l'ensemble des ses connaissances par rapport au groupe auquel il appartient. Le but est de constituer progressivement les arbres des différentes communautés concernées, à savoir :

- l'arbre de chaque classe,
- l'arbre de chaque école,
- l'arbre de chaque communauté éducative (parents, enseignants, ...)
- l'arbre de chaque village, quartier, environnement, canton ...
- l'arbre collectif de plusieurs sites (classes uniques, réseau, ...)
- l'arbre collectif de tous les sites.

2.5.5 Autres projets

Le projet Olivier est un projet qui associe le Conseil Général, l'Institut National des Sciences Appliquées de Lyon et Handicap International. Son but est de favoriser la coopération en ligne entre plusieurs établissements d'enseignement spécialisé (pour des jeunes en difficulté ou porteurs de handicap).

Le projet "Apprendre le Net à l'hôpital", porté par Handicap International, vise à apporter aux personnes hospitalisées pour une longue durée une initiation à l'utilisation de l'Internet. Trois établissements hospitaliers du Rhône sont associés à ce projet.

2.6 L'équipe

L'équipe est composée d'une dizaine de personnes. La hiérarchie (organigramme **??**) est très simple, et peu formelle, ce qui donne une ambiance sympathique, et une forme de travail dynamique basée sur la collaboration et l'initiative. Beaucoup d'idées sont échangées et discutées dans la salle de pause, de façon informelle, ce qui permet une grande liberté d'expression et par là une créativité réelle.

Cette souplesse peut paraître surprenante pour un service de l'administration, généralement rigide dans son fonctionnement, mais on peut l'expliquer par sa situation décentralisée, et par sa mission de pointe dans les domaines évoqués plus haut (projets pédagogiques, veille et expérimentation, gestion de ressources informatiques départementales).

Une partie du personnel d'Érasme a le statut de fonctionnaire, et d'autres sont employés en contrat renouvelable tous les trois ans (c'est le cas de la plupart des ingénieurs de l'équipe technique).

Dans les mêmes locaux, travaillent également des personnes rattachées à la communauté de communes, et le centre de formation et d'hébergement est géré par une autre équipe rattachée au conseil général.

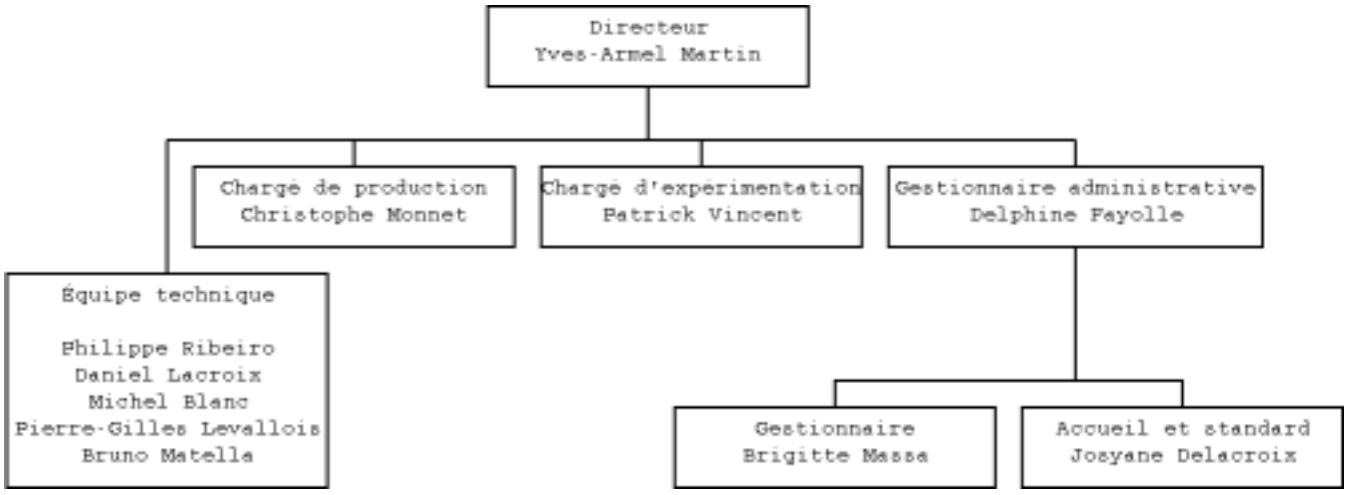

FIG. 2.2 – Organigramme

Chapitre 3

Le sujet du stage

3.1 Contexte

Du fait des limites d'extension physique du réseau câblé, des lieux-dits et des foyers en zone rurale ne seront pas desservis par le câble. Érasme étudie la possibilité de connecter ces différents lieux en haut débit par une technologie radio. L'étude des sites à desservir a permis de dégager des caractéristiques générales :

- l'existence d'un nombre important de zones à étendre
- l'existence à l'intérieur de chaque zone d'un nombre relativement faible de clients finaux
- la possibilité de liaison avec un point câblé du réseau départemental situé dans la quasi totalité des cas à moins de 3 kilomètres.

Comparée à d'autres technologies, le Wifi répond le mieux aux besoins :

- coût de déploiement limité et évolution aisée (multiplication progressive facile des infrastructures),
- bande passante partagée suffisante pour un petit nombre d'utilisateurs,
- portée de liaison suffisante (un test sur deux kilomètres a été effectué au Centre Érasme en mai 2002),
- le Département souhaite s'engager dans une voie innovante sur le plan technique et collaboratif.

Des connaissances théoriques générales sur le Wi-Fi ont déjà été acquises, et des contacts établis avec des acteurs du Wi-Fi de longue date (Wireless-Lyon[1], parmi les premiers en France), qui ont permis de concevoir l'architecture type envisagée, illustrée sur le schéma **??**.

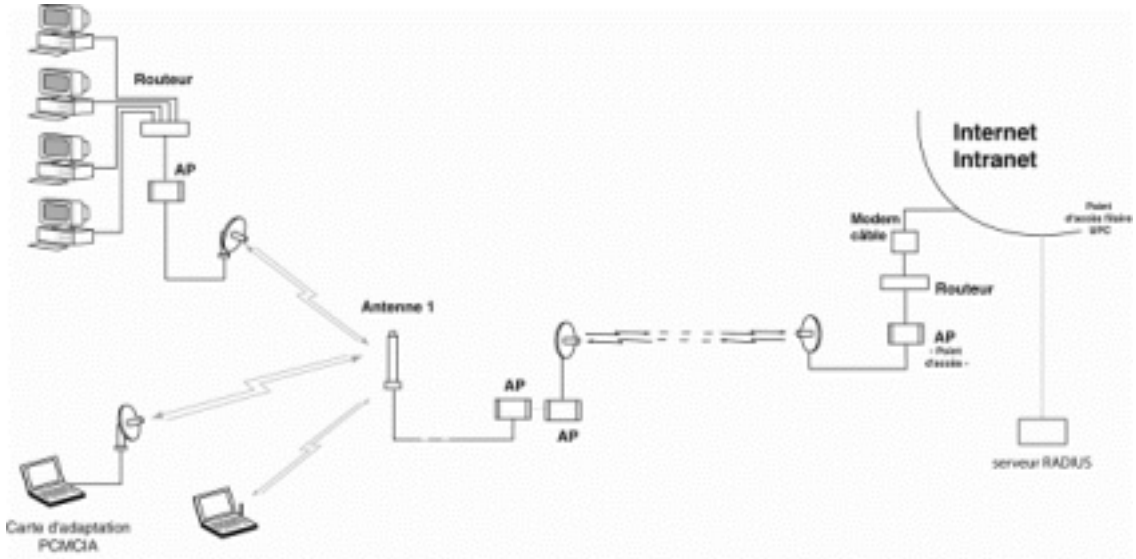

FIG. 3.1 – Architecture envisagée

[1] www.wireless-lyon.org, association affiliée à Wireless-fr (France sans fil, www.wireless-fr.org), dont le but est de déployer un réseau national autogéré, basé sur le Wi-Fi.

3.2 Les besoins

Dans un but à la fois d'expérimentation et de développement du territoire, Érasme souhaite apporter un soutien technique aux initiatives locales faisant appel au Wi-Fi, et développer un réseau humain d'échanges et de transferts de compétences.

Une partie du stage sera consacrée à cet objectif, par une aide directe aux acteurs demandeurs, mais aussi par la rédaction de modes d'emploi techniques.

De plus, des expérimentations sont nécessaires pour cerner les limites de cette technologie, pour en améliorer la compréhension et la maîtrise.

Cela constituera l'autre volet du stage.

3.3 Axes de travail envisagés

3.3.1 Expérimentations

Débit, zone de couverture et théorie de liaison

- corrélation entre les caractéristiques du matériel, la portée et le débit des données,

Qualité de liaison et interférences

- temps de réponse, fluidité des connexions et coupures,
- influence des conditions météorologiques sur la qualité des liaisons,
- interférences et recouvrement des canaux,
- itinérance (roaming),
- routage dynamique et partage de connexion, influence sur le débit,
- compatibilité entre marques différentes.

Sécurité et confidentialité

- piratage de connexions,
- configuration d'un serveur d'authentification,
- chiffrement PPTP/IPSEC sous Linux.

Étude d'architectures et configuration de matériel

- flashage de micro-programme Linksys en D-Link, analyse des expériences de Wireless-Lyon,
- configuration d'un intranet,
- réalisation d'antennes.

3.3.2 Rédaction de modes d'emploi techniques

- étude de site et théorie radio,
- cadre juridique et administratif,
- budget, choix et achat de matériel,
- configuration des architectures (partage de connexion Internet, Intranet, extension d'un réseau),
- pose et configuration du matériel,
- paramétrage réseau,
- sécurisation,
- maintenance,
- fiche comparative du matériel (performances, services, vocabulaire spécifique).

3.3.3 Support technique aux initiatives locales de déploiement Wi-Fi

- projet Maison des Jeunes de Pomeys : Intranet et partage de connexion,
- projet Rhône-Sud et Givors : partage de connexion dans les immeubles, et stands mobiles de démonstration,
- projet radio mobile de villages,

– extension du réseau filaire du collège de l'Arbresle.

Chapitre 4

Recherche documentaire

Ma première tâche a été une recherche documentaire sur la technologie Wi-Fi. Il s'agissait pour moi d'acquérir une connaissance théorique sur cette technologie que je ne connaissais pas, et également de commencer une base de connaissances que le centre Érasme désirait mettre à disposition du public.

Les limites de cette recherche ont été laissées à mon appréciation. J'ai commencé par des documents de vulgarisation pour une première approche, puis par des documents de référence, tels que les publications de l'IEEE[1] qui définissent les termes, fonctions et technologies de façon rigoureuse. Cela m'a permis d'aborder la technologie Wi-Fi au sens strict.

Il m'a fallu élargir le champ de mes recherches, pour comprendre les calculs de portée et les notions de radio-fréquence. J'ai donc aussi inclus des documents de théorie radio provenant de sources universitaires ou de radioamateurs, ces derniers étant souvent plus pratiques et accessibles.

De nombreux documents traitant des problèmes de sécurité sont issus de travaux d'universités nord-américaines, également de groupes de recherche sur la sécurité en lien avec la communauté du logiciel libre, voire de quelques sites de groupes informels de recherches de failles de sécurité informatique.

Enfin, la plupart des informations pratiques concernant le Wi-Fi et le matériel informatique associé proviennent d'associations ou de communautés Wi-Fi actives, telles que Wifi-Montauban ou Réseau Citoyen[2].

Ces recherches ont été très largement effectuées sur l'internet, et la majorité des documents trouvés est en langue anglaise.

4.1 Élaboration de la base de connaissances

4.1.1 Structure

Cette base a commencé sous la forme d'un empilement brut de liens et de documents, simplement classés par critères sur un serveur FTP.

Il nous est rapidement apparu que cela serait très difficile à maintenir et à alimenter, du fait de l'absence d'interface et des problèmes de coordination possibles.

La solution proposée par Patrick Vincent fut Spip[3], un système d'aide à la publication, interactif et séparant les tâches d'administration, de rédaction et de mise en forme. Ce choix s'est avéré très pratique, et la migration depuis la première base puis l'alimentation en nouveaux articles ont été rapides et faciles. Ce site est hébergé sur les serveurs du centre, et accessible à l'adresse "wifi.erasme.org".

Un autre avantage est que n'importe quel visiteur peut s'inscrire en ligne pour proposer des articles, ou tout simplement réagir aux articles ou poser des questions.

On peur voir, sur la capture d'écran de la page d'accueil (fig. **??**), les différentes rubriques choisies.

[1] International Electric & Electronic Engineers

[2] www.wifi-montauban.net et www.reseaucitoyen.be

[3] www.spip.net

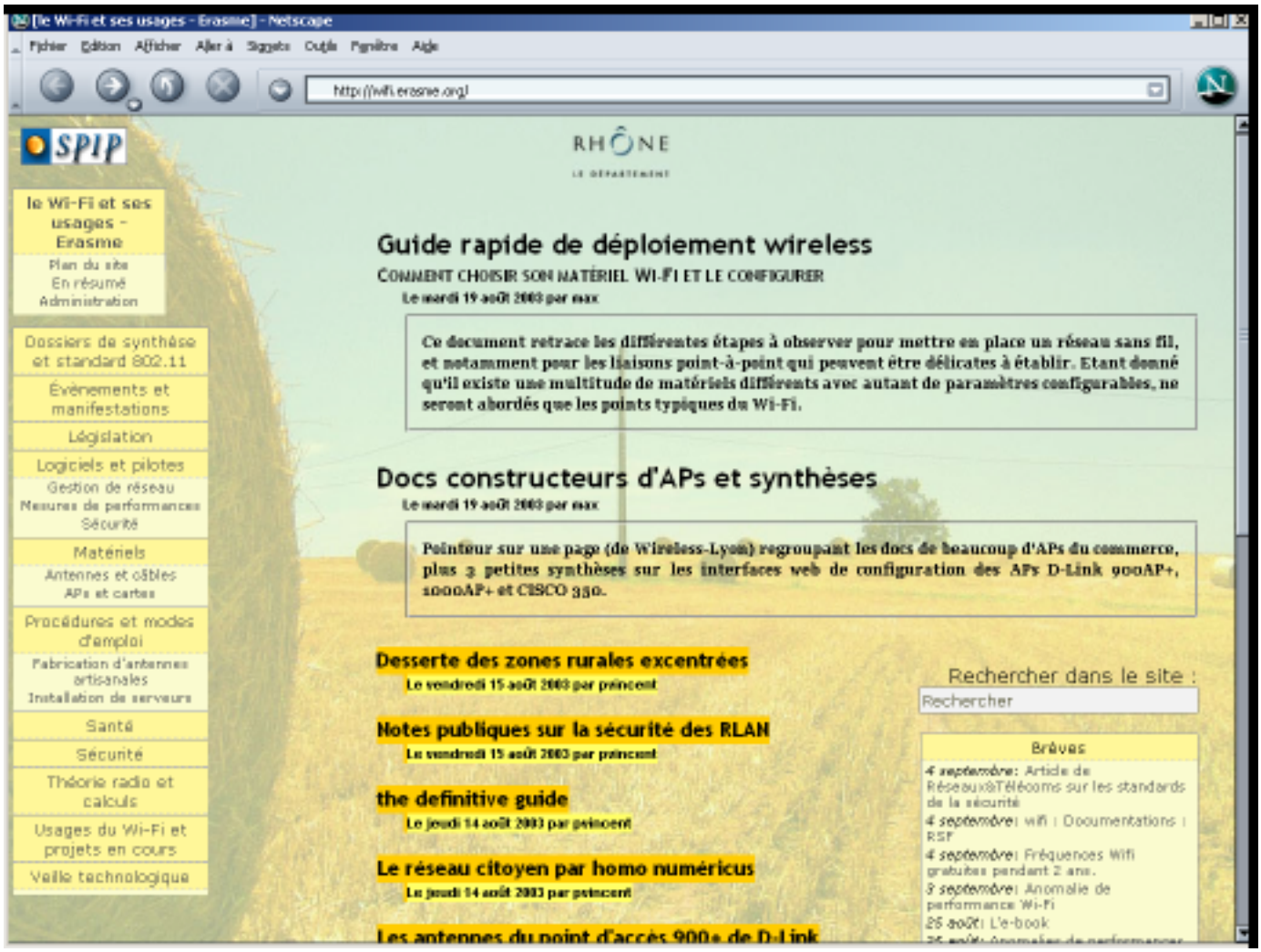

FIG. 4.1 – Page d'accueil du site contributif wifi.erasme.org

Chapitre 5

Mise en place d'un serveur d'authentification

5.1 Introduction

Une des lacunes importantes des technologies 802.11 est la sécurité. Plusieurs études ont été publiées peu après la sortie du standard, montrant la faiblesse du mécanisme de protection choisi (voir doc. [?] pour une liste d'articles).

Le mécanisme en question est le WEP, pour Wired Equivalent Privacy (protection équivalente au filaire), et sa principale faiblesse provient de l'utilisation d'un vecteur d'initialisation trop peu aléatoire. La clé de chiffrement utilisée peut être trouvée en quelques heures, par écoute passive du trafic et analyse des paquets.

Outre les faiblesses du WEP, permettant l'intrusion sur le réseau avec des outils logiciels devenus communs, mais tout de même encore réservés à des utilisateurs de portables sous Linux ou BSD, un autre problème n'a pas été pris en compte lors de la rédaction des standards. Il s'agit de l'accès au périphérique : il semble possible d'utiliser un point d'accès comme lien répéteur entre machines non autorisées. Même sans casser la clé WEP et donc sans s'associer au point d'accès, on peut établir un lien entre deux machines en ad-hoc, et utiliser un point d'accès étranger pour augmenter la portée de ce lien.

Le contrôle d'accès au périphérique n'est possible qu'avec le standard 802.1X de l'IEEE, qui gère le contrôle d'accès à la couche physique, en filtrant les données et en ne laissant passer que les paquets du protocole d'authentification, jusqu'à ce que l'utilisateur soit authentifié. Ce protocole fut d'abord élaboré pour contrôler l'utilisation de réseaux filaires, dans les cas où des prises Ethernet sont accessibles librement, comme sur les campus universitaires, par exemple.

Certains matériels supportent le 802.1X, avec le protocole RADIUS pour le serveur chargé de l'authentification.

5.2 Contexte

Dans le cadre de l'extension du réseau départemental, cette solution nous a paru la plus appropriée, en terme de coûts et de sécurité. J'ai donc reçu pour mission de tester le logiciel Freeradius, qui gère l'authentification avec le protocole RADIUS et qui est libre. L'objectif était de valider cette solution, et de rédiger une documentation, pour l'utiliser avec le standard 802.1X.

5.3 Principes

802.1X est le standard de l'IEEE qui définit le contrôle d'accès aux ressources d'un appareil d'accès au réseau.

Il fait appel à EAP, à RADIUS pour le dialogue entre cet appareil et le serveur d'authentification, et définit EAPOL (EAP Over LAN, EAP sur réseau local) pour le dialogue entre cet appareil et l'appareil qui demande l'accès au réseau.

Il est défini dans [?].

RADIUS Remote Authentication Dial In User Service (service distant d'authentification d'un utilisateur demandant une connexion) est un protocole de communication qui gère le transport d'informations :

- d'authentification,
- d'autorisation,
- de configuration.

RADIUS concerne uniquement l'authentification et la configuration. Seules ces phases sont chiffrées. Pour que le trafic normal soit chiffré par la suite, il faut que le serveur fournisse au logiciel client et éventuellement au point d'accès une méthode de chiffrement.

Radius est défini dans les rfc 2865 [?], 2866 [?], 2867 [?], 2868 [?], 2869 [?], et 3575 [?].

EAP Extensible Authentication Protocol est un protocole qui gère uniquement l'authentification, mais de façon générale. Il définit un dialogue générique, avec quatre types de données uniquement : requête, réponse, succès, échec. EAP est indépendant de la méthode d'authentification, qui est définie entre les interlocuteurs au début du dialogue. Ce dialogue est illustré par la figure **??**

L'application Freeradius peut gérer 2 méthodes d'authentification : MD5 (Message Digest version 5, cf. rfc 1321 [?]) et TLS (Transport Layer Protocol, rfc 2246 [?] et 3546 [?]).

EAP est défini dans les rfc 2284 [?] et 2484 [?], EAP/TLS est défini dans le rfc 2716 [?].

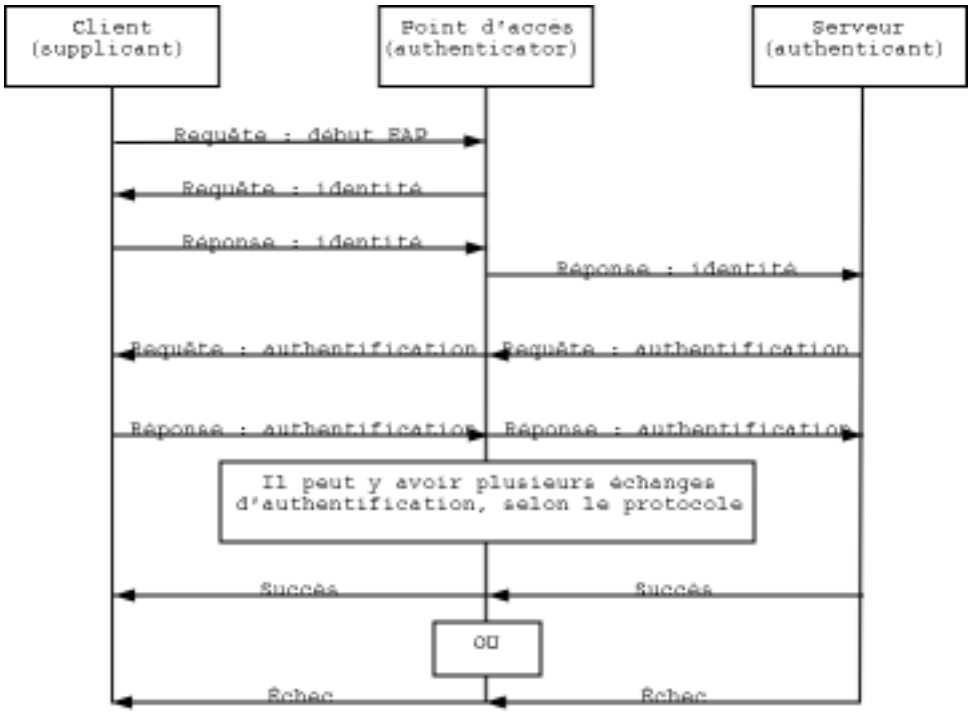

FIG. 5.1 – Dialogue EAP, à partir d'une demande d'association au point d'accès.

Les méthodes d'authentification Freeradius en gère deux avec le protocole EAP : MD5 et TLS.

MD5 permet l'authentification du client par le serveur. L'identifiant du client est connu par le serveur. Le client envoie au serveur un hachage MD5 de son identifiant

- 1. Le serveur envoie au client un défi[1].
- 2. Le client signe ce défi avec une clé basée sur son mot de passe et envoie au serveur la signature.
- 3. Le serveur signe le défi avec le mot de passe de ce client, et compare le résultat avec la signature du client. Si les deux sont identiques, le client s'est correctement authentifié auprès du serveur.

Le point faible de cette méthode est que le serveur n'est pas authentifié par le client. Une attaque peut consister à se faire passer pour le serveur, auprès du client, pour obtenir ses identifiants.

[1]Dans le contexte de l'authentification informatique, le défi est une suite de chiffres aléatoire, qui permet d'éviter la reproduction d'une session d'authentification.

TLS est une méthode dite d'authentification forte, parce qu'elle permet l'authentification mutuelle. Elle est basée sur l'utilisation de certificats, et donc sur une infrastructure à clé publique : le client doit posséder une copie du certificat du serveur, et vice-versa. Lors de l'authentification, a lieu un double défi, où chacun utilise sa clé privée pour signer le défi reçu, et vérifie ensuite avec la clé publique de l'autre que la signature reçue est correcte [2].

Articulation des protocoles Le 802.1X impose l'utilisation de EAP pour l'authentification, de RADIUS pour dialoguer avec le serveur, et de EAPOL pour le dialogue avec le client. EAP est un protocole concernant l'authentification, qui est utilisé par RADIUS pour la partie authentification, et transporté par EAPOL entre le périphérique d'accès au réseau (le point d'accès) et le client.

La figure **??** montre l'imbrication de ces standards et protocoles.

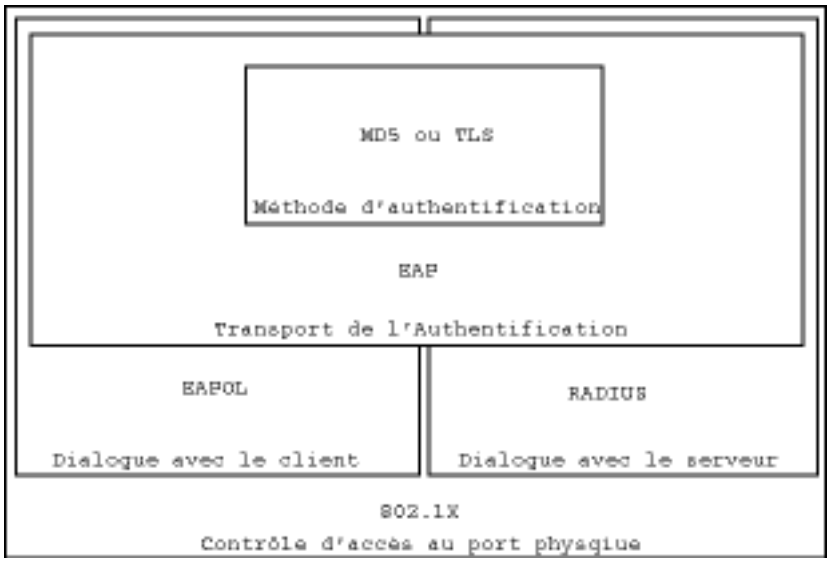

FIG. 5.2 – Articulation entre les protocoles.

5.4 Application : Freeradius

5.4.1 Étapes des expériences

Pour commencer, j'ai utilisé un serveur Freeradius déjà été installé.

J'ai cherché les fichiers et documents installés avec le logiciel, pour pouvoir m'y référer facilement au besoin. J'ai également fait une première recherche de la documentation disponible par ailleurs, sur l'internet, pour avoir des informations à jour.

La complexité des protocoles m'a amené rapidement à chercher leur définition et leur fonctionnement, donc j'ai aussi lu des synthèses et parcouru les rfc pour les comprendre.

Dès que cela a été éclairci, je suis passé aux premiers essais de mise en oeuvre, d'abord le plus simple, puis en compliquant les choses graduellement.

Par exemple, Freeradius permet de stocker les informations des utilisateurs soit dans un fichier de configuration propre au logiciel, soit d'utiliser les informations du système d'exploitation, soit de les stocker dans une base de données (plusieurs sont prises en charge, j'ai utilisé Mysql, qui est libre et considérée comme très performante). J'ai donc commencé par des essais avec des utilisateurs enregistrés dans le fichier de configuration, et avec des essais d'utilisateur du système. C'est seulement ensuite que j'ai configuré Freeradius avec la base de données Mysql.

[2] Dans les systèmes à clés publiques, chaque utilisateur a une paire de clés, une secrète, la clé privée, et une publique. On utilise la clé publique du destinataire pour chiffrer des messages que lui seul pourra déchiffrer avec sa clé privée. Pour la signature, grossièrement, il s'agit pour l'expéditeur d'utiliser sa clé privée pour chiffrer un message, que tout le monde pourra déchiffrer avec la clé publique correspondante, en sachant que c'est bien lui qui en est l'auteur.

De même, les premiers tests ont été effectués sur une seule machine, et ce n'est que plus tard que j'ai procédé à des essais par le réseau.

La première difficulté rencontrée a été la configuration avec Mysql. Déjà je ne connaissais pas ce logiciel, et en plus la configuration de Freeradius avec Mysql est peu documentée.

Quand j'ai compris et réussi cette configuration, j'ai mis en place une authentification de type MD5, simple du point de vue de l'utilisateur puisqu'elle ne fait appel qu'à un nom d'utilisateur et à un mot de passe, concepts que tous les utilisateurs d'ordinateurs intègrent rapidement et facilement (par comparaison avec le principe des certificats, beaucoup plus complexe). J'ai procédé à plusieurs essais, et découvert un problème presque irrationnel de configuration de l'interface sans fil avec l'authentification en MD5 sous Windows XP, contournable au prix de plusieurs manipulations intermédiaires[3].

Malheureusement, les mises à jour de Windows XP semblent ne plus fournir l'option d'authentification MD5. Pour que les utilisateurs du réseau puissent se connecter, il fallait donc changer de type d'authentification. Celui en vogue actuellement, et le plus fort du point de vue de l'authentification, est le système par certificats, géré par le protocole EAP/TLS.

J'ai donc entrepris de configurer Freeradius avec son module "EAP_TLS". Il fallait pour cela recompiler le logiciel, et installer une autre version du logiciel de gestion cryptographique Openssl[4] utilisé par Freeradius. De plus, comme j'ai repris ces expériences après un temps consacré à d'autres activités, j'ai préféré partir sur une base neuve, en installant un système vierge.

J'ai donc repris mes essais, avec une nouvelle méthode de prises de notes, pour que mes travaux puissent être plus facilement réutilisés.

J'ai refait rapidement les étapes précédentes, puis j'ai commencé à essayer différentes façons de compiler Openssl et Freeradius avec son module "EAP_TLS", mais aucune n'a fonctionné.

Le résultat actuel est Freeradius compilé, mais avec l'option EAP/TLS désactivée, car une erreur se produit au lancement, en lien avec l'utilisation de Openssl.

5.4.2 Méthode

J'ai commencé par prendre note de tous les fichiers du paquetage Freeradius, pour pouvoir retrouver rapidement ceux qui me servaient.

Au fur et à mesure de mes besoins, j'ai étudié les protocoles de Freeradius, ou l'utilisation du serveur Mysql, en synthétisant par écrit le fruit de mes recherches.

Enfin, j'ai également essayé de garder par écrit les modifications que j'apportais à la configuration, en copiant parfois les fichiers modifiés.

Pourtant, mes notes se révélèrent difficilement utilisables. Lorsque j'ai dû reprendre ce travail après une interruption due à d'autres activités, j'ai passé beaucoup de temps à retrouver ce que j'avais fait et où j'en étais exactement.

Il m'a fallu réfléchir à une autre façon de faire, j'ai fini par :

- partir d'une installation propre, du système comme du logiciel, et la refaire dès que les modifications devenaient trop nombreuses et compliquées,
- tester chaque modification apportée, même mineure,
- copier/coller systématiquement mes commandes et leurs résultats, en les commentant comme pour les publier (donc le plus clairement possible),
- nommer les fichiers obtenus clairement, en intégrant dans le nom une numérotation chronologique.

5.4.3 Ce qui reste à faire

Je n'ai pas encore réussi à mettre en place et à tester la gestion du protocole EAP/TLS. Il me reste deux essais à faire : créer un paquetage au format .deb, de Freeradius et de openssl-0.9.7b, pour voir si

[3] pour obtenir la fenêtre de saisie du nom d'utilisateur et du mot de passe, il faut d'abord configurer l'interface pour l'authentification par certificats, afin de pourvoir cocher une case pour dire qu'on utilise un autre nom que celui par lequel on est connecté au système. Windows essaie de se connecter, cherche un certificat, n'en trouve pas et affiche l'information. Alors seulement, on peut configurer l'authentification en MD5, et obtenir l'invite de connexion.

[4] www.openssl.org, la version stable actuelle est la 0.9.6c, et il fallait que j'utilise la version 0.9.7b, en cours de développement, pour l'utilisation de EAP/TLS

l'installation se passe mieux, ou suivre à la lettre un des deux documents d'aide sur ce sujet ([?] et [?]), avec les versions antérieures qui y sont citées.

Les voies à explorer par la suite, sont :

- l'accounting, ou journalisation, pour l'enregistrement de toutes les connexions, impératif légal quand on fournit un accès à l'internet ;
- la génération et la distribution de clés WEP dynamiques, pour rendre le décryptage du trafic plus difficile qu'avec une simple clé WEP statique ;
- les autorisations, pour donner accès à des ressources différentes selon le profil de l'utilisateur.

5.5 Autres perspectives

Face à la difficulté de mise en place de Freeradius pour gérer l'EAP/TLS, encore trop expérimental, il s'avèrera nécessaire, dans l'immédiat, d'envisager une autre solution au problème de l'authentification.

Une possibilité attrayante est l'offre de la société 6wind, qui consiste en un routeur fonctionnant en IPv6, qui gère l'authentification avec un serveur RADIUS embarqué. Outre le fait que cela représenterait une première en France, l'installation d'un réseau sans fil inter-connecté en IPv6[5] permettrait d'obtenir une réelle itinérance. Malheureusement pour la beauté et la simplicité de cette solution, l'itinérance n'est pas nécessaire pour le projet d'extension du réseau, et les coûts risquent de se révéler élevés.

Il est plus probable que soit adoptée la configuration déjà éprouvée par Wireless-Lyon, qui met en oeuvre un serveur Freeradius pour une authentification moins forte (MD5), et l'utilise pour la journalisation et les autorisations. La sécurité est garantie par un tunnel chiffré en PPTP[6]. Cette solution n'empêche pas l'utilisation d'un point d'accès pour un réseau étranger, mais il est vrai qu'on peut considérer que le risque est faible en milieu rural.

5.6 Bilan

5.6.1 Difficultés rencontrées

Du fait de la jeunesse du projet Freeradius, qui est encore en développement très actif, j'ai dû faire face à un manque de documentation pénalisant.

En particulier, la configuration du serveur pour l'emploi d'une base Mysql n'est documentée apparemment que dans un unique article dans une langue que je connaisse (l'anglais en l'occurrence).

Concernant l'utilisation de EAP/TLS, il s'agit d'un usage expérimental, qui requiert des manipulations non conventionnelles (installation de 2 versions d'openssl sur la même machine). La documentation est bien faite, mais incomplète et dépassée par l'évolution des projets Freeradius et Openssl.

De plus, les astuces de compilation font appel à des connaissances pointues que je ne maîtrise pas encore bien.

5.6.2 Acquis

Cette mission m'a permis d'acquérir des savoir-faire et des connaissances théoriques enrichissants.

Elle m'a donné l'occasion d'appréhender les différents aspects du contrôle d'accès (autorisation, authentification, journalisation), d'approfondir mes notions sur les infrastructures à clés publiques et les certificats, et de disséquer des protocoles de communications pour comprendre le fonctionnement du serveur (RADIUS, EAP, MD5, TLS).

Enfin, elle m'a permis de mettre au point une méthode de travail rigoureuse et efficace pour ce genre d'exercice.

[5] Internet Protocole version 6

[6] Point to Point Tunneling Protocol

Chapitre 6

Étude et tests à Pomeys

6.1 Introduction

Dans le cadre de l'extension du réseau départemental, le centre Érasme recherche des sites volontaires afin de mettre en œuvre avec eux la technologie Wi-Fi en support d'un projet local. Le but est pédagogique dans la démarche entreprise avec les sites volontaires, et expérimental dans la recherche des méthodes et possibilités spécifiques à cette technologie.

La Maison des Jeunes du village de Pomeys a répondu à cette demande.

Le projet final de la Maison des Jeunes est de réaliser un réseau local sur tout le village, ouvert aux habitants selon des modalités à fixer en fonction des réglementations en vigueur, et pour des usages qui restent en partie à inventer.

Érasme offre un service de support technique, pour l'étude et les tests de mise en œuvre, secondé par l'association Wireless Lyon qui a déjà une expérience dans le domaine.

6.2 Description du village

Le village est à moins de 50 km de Lyon, à l'ouest. Il est devenu depuis quelques années une zone résidentielle privilégiée, et de nombreux lotissements y ont été créés (qui ne figurent pas sur les cartes).

Le village est situé sur le flanc sud-est d'une colline. Les maisons du bourg sont pour la plupart le long de la route principale, ou en contrebas. Le clocher domine le village, mais la pente le rend invisible des maisons les plus basses.

La carte **??** et la photographie **??**rendent compte de la topographie du village.

6.3 Le dossier

Le président de la Maison des jeunes a monté un dossier présentant les objectifs, la technologie, le budget prévisionnel et les contacts déjà établis.

Le projet est pour l'instant financé à 10% par la Maison des Jeunes, à 20 % par le centre Érasme, et à 70 % par le département. Le budget total est de 3500 Euros, l'essentiel allant à l'achat de points d'accès et d'antennes.

Le dossier est disponible sur le site *wifi.erasme.org*, en deux versions de dates différentes.

6.4 Définition des besoins

Une première réunion des différents acteurs (Maison des Jeunes, Wireless Lyon et Érasme) a eu lieu à Lyon. Elle a servi à

- préciser les besoins de la Maison des Jeunes,
- discuter de la technologie Wi-Fi : les possibilités offertes, les contraintes,
- planifier grossièrement le déroulement du projet,
- le chiffrer.

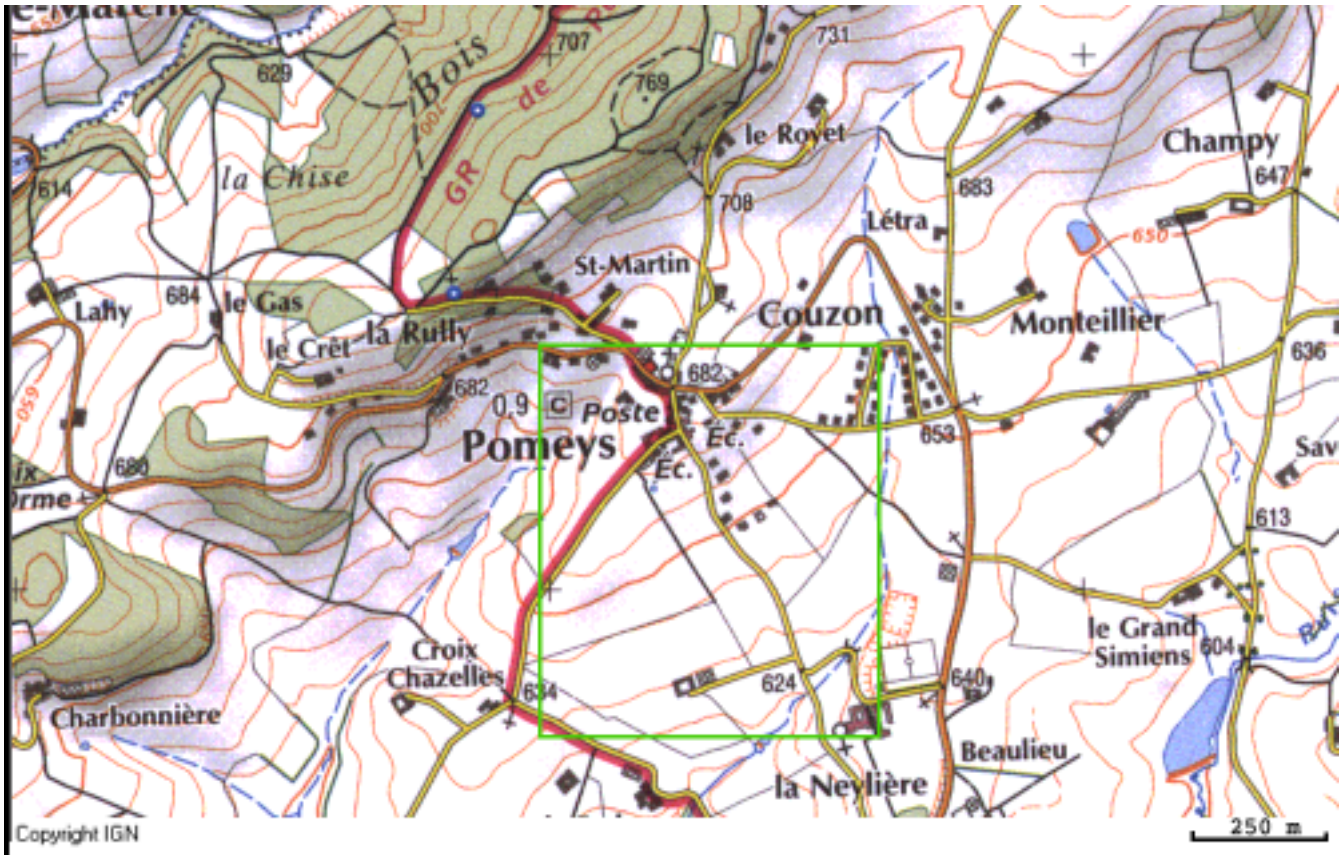

FIG. 6.1 – Carte topographique de Pomeys, et situation des expériences

Elle a permis aux représentants de Wireless-Lyon de nous informer, les stagiaires d'Érasme et les membres de la Maison des Jeunes, sur le Wi-fi en pratique, en nous parlant de leurs expériences personnelles à Lyon.

6.5 Étude du site et conception

L'étude du site s'est faite en deux fois, en même temps que des tests préliminaires.

Lors de la première réunion à Pomeys, avec des membres de l'association Wireless-Lyon et de la Maison des jeunes, nous avons fait un tour du village pour repérer la topographie du site, et les endroits les plus favorables.

L'église a tout de suite paru le lieu idéal d'implantation d'un relais central, dans un réseau en étoile. En effet, le clocher étant visible depuis presque tout le village, cela semblait le plus simple d'installer des points d'accès équipés d'antennes sectorielles [1], qui auraient couvert chacun une partie du village, un peu comme les relais de téléphonie mobile.

Des tests ont été effectués le jour-même pour valider cette première option, mais ils se sont avérés très décevants : la portée était limitée à la rue principale, directement sous l'église, et aucun lien n'a pu être établi en dehors de ça.

Le plan **??** indique en vert la portée effective de notre test avec une antenne sectorielle, et en jaune les liens directionnels testés, mais non réussis.

Pour la deuxième réunion, a été envisagée une solution de réseau à dorsale : des liaisons point-à-point entre le clocher et deux ou trois maisons bien situées appartenant à des volontaires, chacun de ces sites retransmettant en omnidirectionnel pour les utilisateurs voisins (voir le plan **??**).

[1] une antenne sectorielle a un angle d'ouverture compris entre 90 et presque 180 degrés, selon les modèles. Elle est aussi souvent nommée "antenne patch"

FIG. 6.2 – Premiers essais

Cela paraissait plus simple à mettre en pratique, puisque d'après nos premiers essais, le clocher ne pouvait pas servir à couvrir tout le village avec des antennes sectorielles.

Sur un plan du cadastre communal, les membres de la Maison des Jeunes nous ont indiqué les maisons de volontaires pour le projet (en bleu sur les plans cadastraux). Il a ensuite fallu choisir les maisons les mieux situées. Trois sites ont été retenus, pour leur situation topographique et pour la facilité d'accès, au vu des propriétaires.

Les tests de liaisons point-à-point réalisés ce jour-là ont encore été ratés (liens en jaune dans le plan **??**), mais notre méthode (ou notre manque de méthode) pouvait être cause d'erreurs. Nous sommes donc restés sur cette topologie, en cherchant à améliorer notre façon de procéder. À partir de là, nous avons continué seuls, Maxime et moi, avec les membres de la Maison des Jeunes.

6.6 Équipement du clocher et de la mairie

Dans le clocher, manquait une installation électrique permanente.

De plus, la mairie étant proche de l'église, et desservie par le réseau départemental, on pouvait envisager de faire arriver un câble Ethernet jusqu'au clocher, et d'héberger dans la mairie les ordinateurs destinés aux services de l'intranet (serveur web, serveur d'authentification, routeur, DNS et DHCP, etc). Cela permettait d'avoir toute l'infrastructure dans un endroit neutre et accessible.

Les négociations ont été faites par la Maison des Jeunes, qui a obtenu l'accord de la mairie et qui a ensuite fait faire les travaux de raccordement.

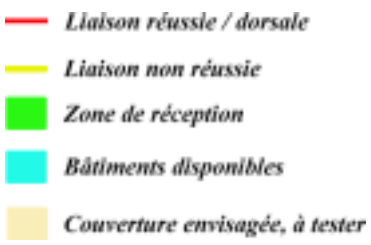

FIG. 6.3 – Légende

6.7 Tests de mise en place

Une troisième série de tests a échoué. Les liaisons testées étaient encore les mêmes, en jaune dans le plan **??**. Plusieurs hypothèses pouvaient l'expliquer :

- la proximité des antennes avec les abats-sons [2], en effet, nous tenions notre antenne directement appuyée contre les abats-sons, et nous avons appris ensuite qu'il fallait un espace libre autour de l'antenne ;
- une mauvaise configuration du matériel, dont nous ne pouvions pas être tout à fait sûrs puisque nous ne l'avions pas testée systématiquement avant l'essai ;
- de mauvaises conditions radio, tout simplement, qui auraient signifié l'impossibilité d'établir le lien ; c'est justement ce que nous voulions tester ;
- un problème de matériel, un des appareils utilisé ayant eu parfois des défaillances.

Nous avons alors décidé de remettre les essais de Pomeys à plus tard, et de procéder d'abord à des tests dans des conditions expérimentales maîtrisées. Nous sommes donc passés à la phase que je décris dans le chapitre "Tests de portée et comparatifs matériels", dans le but de pratiquer de façon répétée la mise en place d'une liaison point-à-point, en analysant la procédure et le comportement du matériel et des outils logiciels de configuration.

Quand nous avons estimé que notre méthode était au point et que notre connaissance des outils était suffisante, nous avons pris un nouveau rendez-vous avec la Maison des Jeunes.

Entre-temps, ils avaient reçu leur équipement Wi-Fi, et nous avons pu l'utiliser directement.

Les tests réalisés ont enfin été concluants, et nous avons obtenu une liaison directionnelle offrant un débit effectif de l'ordre de 5 Mbits par seconde, mesuré en téléchargeant un fichier en FTP.

Ce lien est indiqué en rouge dans le plan **??**.

6.8 Mise en place effective

Le dernier test s'étant révélé concluant, nous avons laissé aux membres de la MJC le soin de mettre en place leurs liaisons.

Notre objectif de transfert de compétences concernant le Wi-Fi est atteint : les tests ont validé la base de l'architecture à dorsale, et les membres de la Maison des Jeunes, qui ont participé à tous les essais, ont maintenant les connaissances pour continuer par eux-mêmes l'extension de leur réseau.

Les deux premières liaisons point-à-point de la dorsale ont été mises en place dans les jours suivants (liens rouges dans le plan **??**.

La photographie **??** montre la vue ouest de l'église, depuis la cheminée qui fait l'autre bout de la liaison directionnelle.

Les prochains objectifs sont la création de deux autres liens de dorsale, représentés en orange dans le plan **??**, et la retransmission en omnidirectionnel à partir des nœuds (zones circulaires en orange), pour couvrir les zones résidentielles proches.

[2] les abats-sons sont les planches inclinées qui ferment le clocher. Ils servent à protéger l'intérieur contre la pluie, et à rabattre le son des cloches vers le bas.

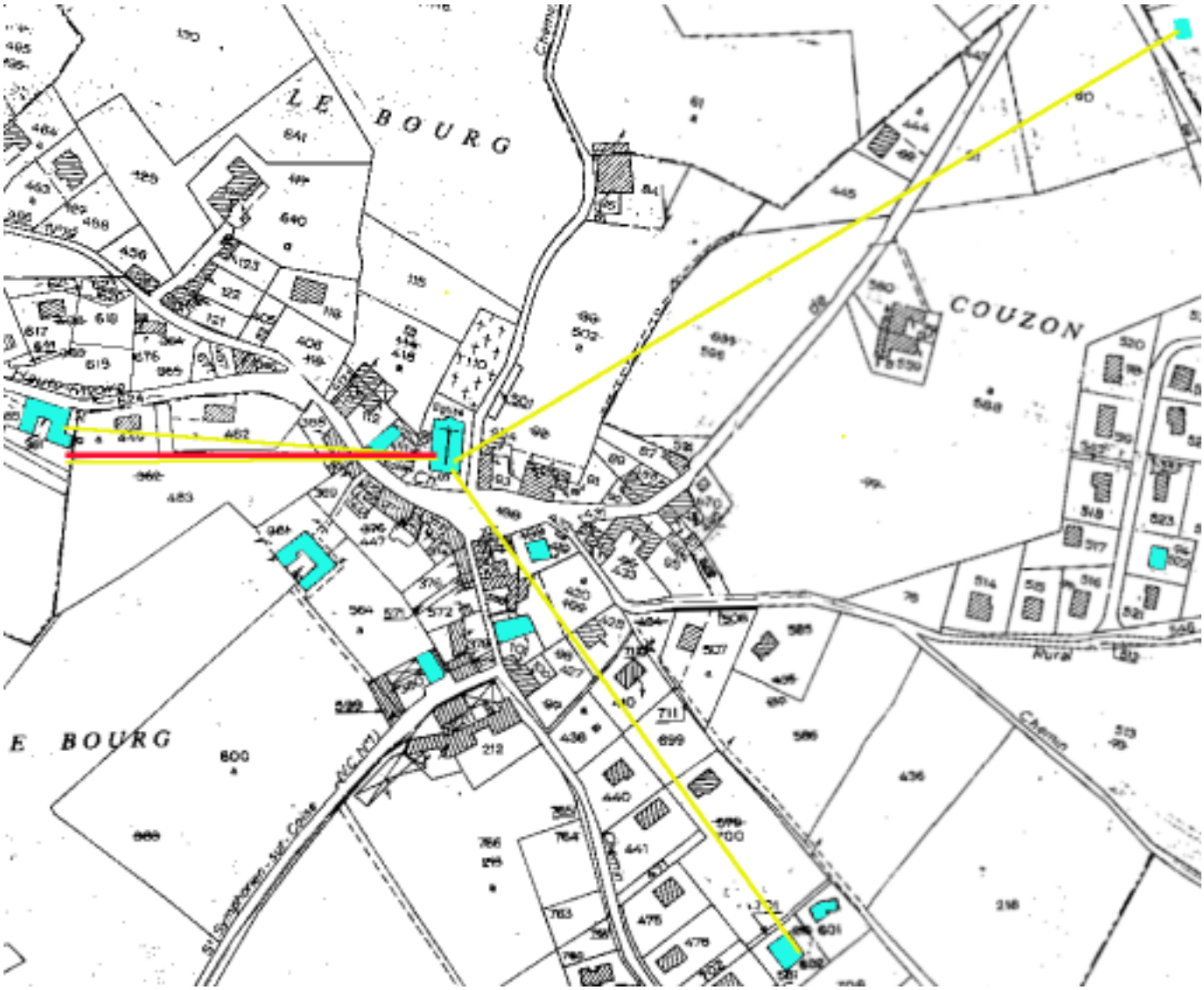

FIG. 6.4 – 2ème, 3ème et 4ème séries d'essais

6.9 Mise en place du serveur

Dans ce projet, j'ai pris en charge la rédaction de modes d'emploi pour installer et configurer un serveur web avec un Spip.

Le serveur web est Apache, et il tourne sur un système Gnu/Linux Debian. J'ai choisi ce système pour l'utiliser sur des ordinateurs aux ressources limitées et pour la puissance de son système de gestion des paquetages. Par contre, il s'agit peut-être d'un choix difficile pour une première approche, du point de vue des utilisateurs finaux.

Spip est un système d'aide à la publication de contenu web, basé sur php et mysql, qui facilite la rédaction en ligne, et qui sépare les fonctions d'administrateur(s), de rédacteurs et d'infographiste. Toutes les informations sur Spip se trouvent sur `www.uzine.net/spip`.

Pour rédiger ces aides, j'ai installé un système vierge, puis chaque paquetage nécessaire, en notant au fur et à mesure tous mes choix et mes commandes.

J'ai également écrit des introductions au système, et à un éditeur (Vi) pour modifier les fichiers de configuration.

Ces documents ont alimenté naturellement la base d'Érasme.

En partant sur ces aides, les membres de la Maison des Jeunes ont pu commencer l'installation de ce serveur. Des déplacements ponctuels sont encore nécessaires pour les aider, mais l'objectif est de leur

FIG. 6.5 – Liaisons réalisées et prochains objectifs

donner les moyens d'être autonomes, à terme.

6.10 Méthode et bilan

Ce projet a démarré alors que nous n'avions pas encore de connaissance pratique du matériel. Un des buts était justement d'apprendre par la pratique et la mise en production, et c'est en partie pour cela que l'association Wireless-Lyon y a été associée.

La mise en place d'un réseau Wi-Fi ne peut pas se faire simplement en concevant sa topologie et en le mettant en place d'après les plans obtenus. Les contraintes non maîtrisées sont en effet bien trop importantes, et obligent à passer par de nombreux tests de validation.

Nous savions cela, et c'est pourquoi la phase de conception a été très rapide : il fallait valider immédiatement la faisabilité de l'idée de départ d'un réseau en étoile autour du clocher.

Suite à l'échec de cette solution, nous avons testé la suivante : mettre en place une dorsale avec des points de diffusion terminaux.

Bien que n'arrivant pas à établir les liaisons point-à-point de la dorsale, nous avons persévéré, parce que les conditions paraissaient trop bonnes pour expliquer par elles seules nos difficultés.

À ce stade, nous avons décidé de reporter les tests suivants, et de commencer d'abord les tests de portée et de matériels prévus par ailleurs. Se déroulant dans des conditions expérimentales, et donc maîtrisées du point de vue du temps consacré et des choix de liaisons et de matériels, ceux-ci devaient permettre de nous focaliser sur des points particuliers qui pouvaient causer nos problèmes à Pomeys.

Et effectivement, nous avons pu, par ces expériences, apprendre à utiliser efficacement les outils logiciels de détection et de configuration des réseaux Wi-Fi.

En particulier, nos problèmes étaient dûs à des conflits entre le logiciel de configuration du système XP et celui du fabricant de la carte Cisco, et à une méconnaissance de leurs spécificités respectives.

FIG. 6.6 – Liaison ouest avec l'église

Dans des conditions triviales, nous arrivions toujours à résoudre ces problèmes de façon empirique. Mais dans les conditions de tests sur le site-même, à Pomeys, nous ne pouvions pas faire la part des choses entre un mauvais paramétrage logiciel et les problèmes de radio.

De plus, un point d'accès s'est révélé instable, même après la mise à jour de son micro-programme [3].

Ce n'est qu'après quelques demi-journées d'expérimentations que nous sommes retournés à Pomeys. Nous avons enfin pu établir une liaison point-à-point entre le clocher et une maison.

6.11 Conclusion

En démarrant ce projet avec des spécialistes du domaine, nous avons pu éviter les pièges qui nous auraient fait perdre beaucoup de temps. Cependant, nous avons été confrontés à des problèmes de configuration et de mauvaise connaissance du matériel, qui nous ont obligés à repenser notre façon de procéder et qui nous ont guidés dans les phases d'expérimentation du matériel.

Techniquement, le travail en équipe au début, puis en autonomie par la suite a été très formateur, puisqu'il m'a permis d'appréhender précisément les savoirs-faires nécessaires à l'installation d'un réseau Wi-Fi et de les acquérir ensuite par la pratique directe.

Sur le plan humain, j'ai pu conduire un projet avec un autre stagiaire, Maxime Charpenne, de façon consensuelle et complémentaire dans l'approche, et le mener jusqu'à la réussite auprès du client qu'était la Maison des Jeunes.

[3] le programme embarqué chargé de son fonctionnement, souvent appelé "firmware"

Chapitre 7

Tests de portée et comparatifs matériels

7.1 Introduction

Dans le cadre des expérimentations et des projets en cours, nous avons besoin de connaître le matériel disponible.

Ce besoin a plusieurs causes. D'abord, il nous faut mesurer l'écart entre les données théoriques et la réalité matérielle et physique.

Ensuite, nous devons être capables de faire un choix raisonné parmi les principaux modèles de périphériques Wi-Fi disponibles sur le marché, que ce soit par rapport à des besoins spécifiques, ou pour conseiller des utilisateurs d'un point de vue rapport qualité/prix plus général.

Enfin, nous avons vu, lors de nos tests à Pomeys, que nous ne maîtrisions pas encore le matériel utilisé, ainsi que les outils et méthodes de configuration, nous avions donc besoin de les manipuler pour nous les approprier.

Nous avons procédé à des essais comparatifs, en mesurant le débit effectif comme critère de performance.

7.2 Matériel

Le matériel à notre disposition est composé, pour les périphériques Wi-Fi, de cartes PCMCIA Cisco Aironet 350, avec prises MMX pour connexion d'antennes extérieures, et de points d'accès de différentes marques et modèles :

- Cisco Aironet 340 et 350,
- D-Link DWL-900AP+, DWL-1000AP+ et DWL-2000AP,
- Linksys WAP-54G et
- Zyxel Zyair B-1000 et B-2000
- Trendnet TEW-210APB.

Plusieurs antennes ont été testées :

- 2 paraboles (grilles, directionnelles) Doradus,
- 2 yagis (directionnelles) Micronet et 2 Cisco,
- 2 patchs (sectorielles) AFT, 1 Centurion et 1 Cisco,
- 1 omnidirectionnelle Doradus et 1 autre de marque non référencée

Les différents types d'antennes sont illustrés dans le tableau **??**.

Nous avons parfois été limités dans nos possibilités de tests par un manque ponctuel de connectique adéquate. La connectique n'est pas encore bien standardisée [1], et la disponibilité de connecteurs adaptés a été mise en défaut, quand le matériel était utilisé pour d'autres manipulations.

[1] 3 standards se disputent le marché : les types N, TNC, et SMA, avec des variantes "RP" (Reverse Polarity), pour les points d'accès, les cartes PCI et les antennes, et MMX pour les cartes PCMCIA


grille


yagi


patch


omnidirectionnelle

TAB. 7.1 – Les principaux types d'antennes

7.3 Méthode

La méthode s'est mise en place de façon un peu empirique : nous avons d'abord fait quelques essais de lien point-à-point distants, puis nous avons pu déterminer nos besoins matériels (tels que radios portatives, pied d'appareil photo, un chapeau, etc) et établir une liste d'essais comparatifs.

Les paramètres pris en compte pour comparer le matériel sont :

- le modèle d'appareil,
- la puissance d'émission,
- le canal d'émission (la fréquence),
- le modèle d'antenne.

Nous avons aussi calculé la PIRE[2], pour qu'il soit possible de faire un comparatif avec les calculs théoriques.

Les premiers tests ont été faits à une distance d'environ 920 mètres, mais un bosquet limitait la vue. En me décalant de 200 mètres, j'ai trouvé un endroit idéalement placé pour la vue, et à une distance de 1000 mètres (voir la carte : fig. **??**).

Pour chaque essai, nous avons effectué un transfert de fichier chronométré, parfois 2 ou 3, en utilisant le protocole d'échange utilisé par Windows[3]. Nous avons ainsi pu calculer le débit utile offert par la connexion Wi-Fi testée.

Une solution plus pratique aurait consisté à utiliser le protocole FTP, comme nous l'avons fait à Pomeys, mais nous avions fait les premières séries comme cela, et il nous a semblé préférable de conserver les mêmes conditions par la suite, dans un souci de cohérence.

En fig. **??** est représentée une capture de notre tableau d'essais.

Pour la procédure de mise en place d'un lien point-à-point, se référer à l'annexe *Comment mettre en place une liaison point-à-point.*

7.4 Résultats et bilan

Nous n'avons pas encore analysé les données enregistrées. Cependant, quelques grandes lignes ressortent de notre expérience.

D'abord, en étant à vue, un lien Wi-Fi d'un kilomètre est très réalisable dans le respect des conditions de l'ART[4], qui limitent la puissance émise (PIRE) à 100 mW.

Ensuite, les débits observés étaient assez homogènes entre les différents modèles, de l'ordre de 4 Mbits par seconde, alors que les observations de puissances reçues variaient parfois du simple au double. Cette contradiction apparente nous a d'abord surpris, mais en fait, tant que la puissance restait suffisante pour éviter le repliement[5], le débit n'avait pas de raison de varier. S'agissant du choix du matériel, une première

[2]Puissance Isotrope Rayonnée Équivalente, c'est la puissance émise par l'appareil, en sortie d'antenne, qui tient compte des pertes dues au câble et du gain de l'antenne.

[3]SMB Server Message Block ou CIFS Common Internet File System, qui permet le "partage" de fichiers

[4]l'Autorité de Régulation des Télécommunications est l'instance nationale chargée de réglementer les télécommunications.

[5]mécanisme qui permet de changer de débit, voire de type de codage, pour pallier à la faiblesse du signal reçu. Le débit est réduit en faveur d'une meilleure correction des erreurs.

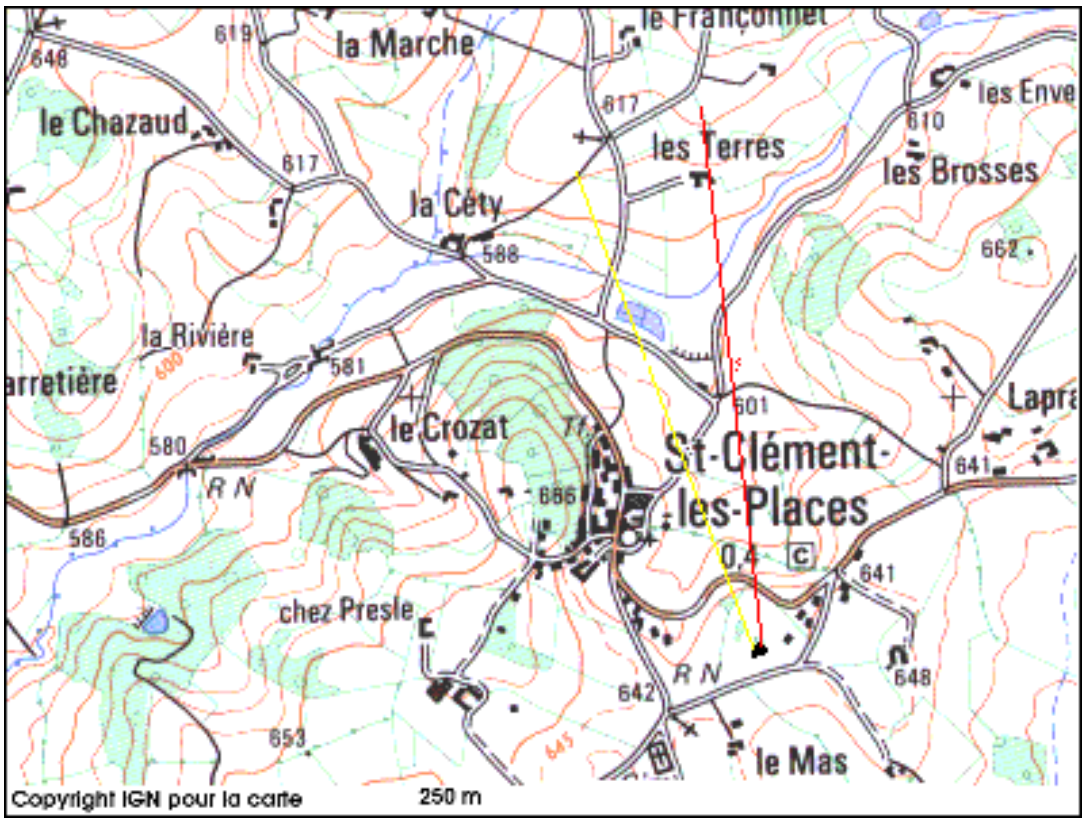

FIG. 7.1 – Situation géographique - La liaison jaune est celle de la première série d'essais, la rouge, celle des suivantes.

conclusion permet de dire qu'on peut laisser de côté la question de la qualité du périphérique radio, pour s'intéresser plus particulièrement aux fonctions et services fournis, qui diffèrent d'un modèle à un autre. Des tests de charge, avec plusieurs clients par point d'accès, menés par Maxime Charpenne, pourront confirmer ou corriger cette conclusion.

Nous avons également pu prendre la mesure de l'inconstance du medium : d'un transfert à l'autre, nous avons parfois observé des écarts significatifs sans qu'aucun changement dans les configurations ne puisse l'expliquer. Dans deux cas, cela a pu s'expliquer par la suite, par la mise en cause d'un périphérique défaillant, mais il reste beaucoup de paramètres non maîtrisés, dûs au medium même (interférences, distorsions diverses du signal, environnement de façon assez générale). Cela ne remet pas en question l'intérêt du Wi-Fi, mais cela rend plus difficile la mise en œuvre effective, par rapport à l'apparente facilité du premier abord.

Enfin, de façon plus générale, je dirai que ces tests ont mis en évidence la nécessité d'une méthode. De nombreuses fois, nous avons passé beaucoup de temps avant de réussir la liaison radio, avant même de pouvoir mettre en place la liaison réseau pour procéder au transfert de fichier.

Ce n'est qu'en adoptant la procédure décrite en annexe que nous sommes arrivés à obtenir ce lien radio immédiatement, dans les conditions favorables dans lesquelles nous avons mené l'expérience.

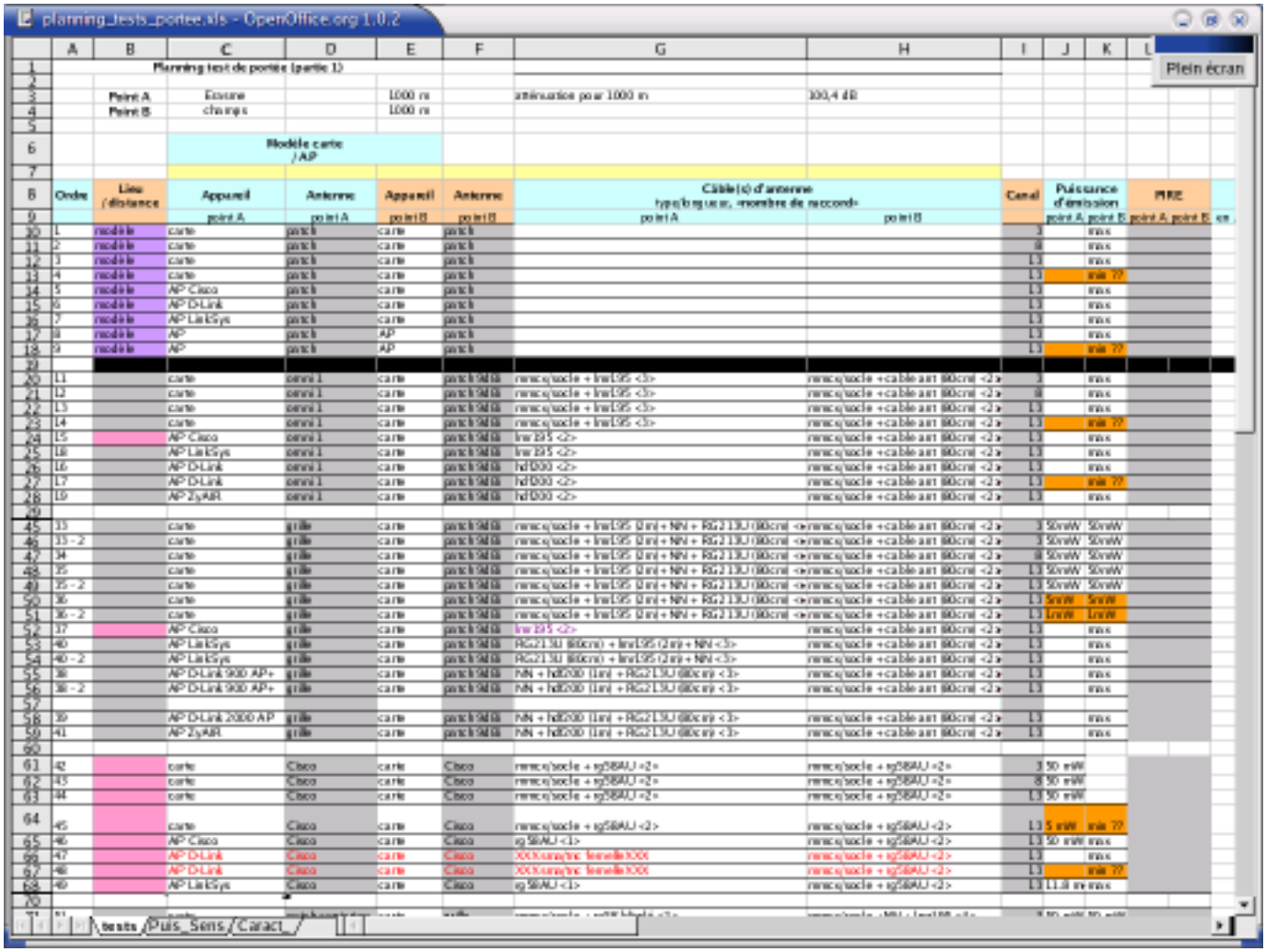

FIG. 7.2 – Tableau des tests comparatifs

Chapitre 8

Journée Wi-Fi

8.1 Introduction

Le centre Érasme a organisé une journée de présentation du Wi-Fi, le 14 juin 2003. À cette occasion, ont été mises à contribution toutes les ressources du centre.

Il s'agissait de faire connaître le Wi-Fi dans un cadre rural, par le biais de conférences, de stands et d'ateliers.

Mon rôle prévu pour la journée était l'animation, avec Maxime Charpenne, d'un atelier de fabrication d'antennes.

8.2 Préparation

Pour participer à la préparation de cette journée, j'ai rédigé des synthèses destinées à être affichées sous forme de posters.

J'ai également mis en place des serveurs pour un réseau local de démonstration des usages du Wi-Fi : un serveur Samba pour le partage de fichiers, un serveur RADIUS pour l'authentification, un serveur DHCP et un DNS pour le fonctionnement du réseau. Ce travail a été fait avec Michel Blanc, administrateur du réseau départemental, et j'ai aussi reçu une aide précieuse de Nicolas Grimler pour un problème de configuration de PHP.

Enfin, pour me préparer pour l'animation de l'atelier, j'ai suivi une formation pratique et théorique d'une demi-journée avec une association de radioamateurs d'EDF-GDF : nous avons revu les paramètres importants pour une antenne de type dit "Ricoré"[1], nous avons pu mesurer l'efficacité d'un prototype avec des appareils de mesure spécialisés et nous avons fabriqué chacun une antenne "Ricoré".

FIG. 8.1 – Une antenne "Ricoré"

[1] ce nom vient de la marque qui commercialise son produit dans les boîtes les plus adaptées qu'on trouve en France

FIG. 8.2 – L'intérieur de l'antenne "Ricoré"

8.3 Déroulement de la journée

Avant le début de l'atelier de fabrication d'antennes, j'ai terminé la configuration et la vérification du réseau de démonstration, et informé les animateurs de cet atelier de l'architecture mise en place et de l'utilisation du service d'authentification.

Puis j'ai intégré mon poste d'animateur, et j'ai passé l'après-midi à expliquer les principes de l'antenne et à guider les participants dans les manipulations de préparation et de soudure des éléments constitutifs de l'antenne "Ricoré".

8.4 Conclusion

La journée Wi-Fi d'Érasme a reçu un écho dans toutes les communautés "wifistes" de France, signe que ce type d'événement répond à un besoin.

Cette journée a été l'occasion pour moi d'affronter de grosses charges de travail pendant la préparation du réseau de démonstration, et de collaborer avec d'autres membres de l'équipe, et aussi avec des membres de Wireless-Lyon que je ne connaissais pas.

L'animation de l'atelier de fabrication d'antennes m'a confronté à des problèmes de gestion de ressources, qui étaient juste suffisantes, et à des difficultés variables selon les individus, qui n'avaient pour la plupart aucune connaissance théorique ou pratique a priori.

Chapitre 9

Raccordement de bâtiments au collège de Champagnat

9.1 Introduction

Le Collège de Champagnat, à St-Symphorien-sur-Coise, a fait appel à Érasme pour relier les réseaux locaux de deux bâtiments distant de 200 m environ..

Cette demande a eu lieu en début juillet, au moment où les réseaux ne sont pas utilisés, et pour nous au moment où nous commencions à être au point sur la pratique du Wi-Fi.

Naturellement, cette mission a été menée avec Maxime Charpenne.

9.2 Déroulement

Nous nous sommes d'abord rendus sur place avec Patrick Vincent, pour un premier contact avec M. Patrick Gonont, professeur et responsable du réseau informatique, ainsi que pour le repérage des lieux.

Nous avons alors évalué la faisabilité de la liaison, qui paraissait simple à mettre en place, et avons pu lister les besoins matériels.

Nous y sommes retournés Maxime et moi, lorsque M. Gonont nous a informés de l'arrivée de son matériel et de l'équipement des lieux (raccordement au réseau, mâts pour les antennes, alimentation électrique).

Le lien point à point a été mis en place sans problème, en suivant notre procédure mise au point lors des tests comparatifs, et nous attendons un retour d'information de M. Gonont, ce qui devrait être possible avec la reprise de l'activité scolaire.

Chapitre 10

Conclusion

Le Wi-Fi est une technologie récente, utilisable en France depuis seulement quelques mois, qui apporte beaucoup de possibilités nouvelles. En particulier,elle réduit notablement les coûts d'installation d'un réseau, surtout en extérieur où elle évite les tranchées.

De plus, le coût relativement faible des périphériques met cette technologie à la portée de nombreuses personnes. En cela, le Wi-Fi peut amener une évolution des usages (notamment vers plus de partage et de possibilités d'expression), qu'il sera intéressant d'observer dans les mois et années à venir.

Le reproche qu'on peut faire à cette technologie, est de n'être pas encore réellement prête pour l'usage professionnel : le lien radio n'est pas fiable, surtout dans la plage de fréquences libres utilisées, car soumis à trop d'aléas et de possibilités d'interférences ; sans parler de la faiblesse des mécanismes de sécurité, qui perdurera certainement encore plus d'un an en pratique, malgré le travail de l'IEEE et de la Wifi-Alliance.

Ces limites restreignent pour l'instant l'usage du sans-fil à des cas très précis, généralement en parallèle avec un réseau filaire, ou à des usages de loisirs.

Dans tous les cas, l'adoption du Wi-Fi ne pourra se faire à une échelle plus importante qu'en opérant de façon organisée : le manque de fiabilité impose une redondance des liens et des protocoles de routage adaptés[1], comme pour l'internet, et le partage d'une bande de fréquence impose soit une conception globale du réseau, soit des accords entre les parties opérant sur un même territoire, quelle qu'en soit l'échelle, pour éviter les interférences.

Soit le Wi-Fi imposera un dialogue entre les acteurs qui se l'approprient (entreprises, milieux associatifs et particuliers), apportant une évolution positive d'une partie de la société, soit il faudra imposer l'ordre, et mettre un terme aux promesses sociales de cette technologie.

Ce que le stage m'a apporté

Techniquement :

- problématiques réseaux : une meilleure compréhension des couches ISO, dans les faits, qui correspondent à des standards différents de l'IEEE ; aspects spécifiques à la radio : portée, atténuation, théorie, interférences ;
- Windows XP : utilisation, configuration et analyse réseau, serveur ftp, gestion générale ;
- Gnu/Linux : utilisation courante, divers problèmes rencontrés et surmontés, installations logicielles, compilations, outils de réseaux (serveurs web, DHCP, DNS, SAMBA, base de données, ssh)
- identification des besoins des utilisateurs : expression avec le web, partage de fichiers, courrier électronique, accès internet ;

Personnellement :

- travail en équipe lors des tests,
- travail autonome sur freeradius et lors de la recherche documentaire,
- beaucoup d'analyses et de synthèses, lors de la sélection des documents référencés et parfois résumés dans la base,
- recherche documentaire et lecture de l'anglais,

[1] cf. le protocole AODV rfc 3561 [?] pour une voie en cours d'exploration

– recherche de méthodes d'expérimentation.

Ce stage s'est déroulé dans une ambiance agréable, et les tâches accomplies étaient intéressantes et multiples.

Annexe A

Glossaire des termes du Wi-Fi

- 802.11b : standard de l'IEEE relatif à la bande 2,4 GHz (débit théorique de 11 Mb/s)
- 802.11a : standard de l'IEEE relatif à la bande 5 GHz (débit de 54 Mb/s)
- Hiperlan 2 : norme européenne relative à la bande 5 GHz.

De nouvelles normes sont en préparation : 802.11g évolution de la 802.11b avec un débit plus élevé, 802.11h évolution de la 802.11a avec l'introduction de qualité de service

- Antenne associée à l'appareil : antenne nécessaire pour émettre (et recevoir) les signaux radio. Cette antenne est caractérisée par des paramètres tels que :
  - son gain : il mesure l'amplification du signal,
  - son secteur angulaire : il mesure la zone d'émission du signal ; le secteur angulaire peut varier de 0ř dans le cas des antennes directives permettant de relier deux points (liaison point à point), à 360ř dans le cas des antennes omnidirectionnelles qui permettent d'émettre un signal radio dans une cellule circulaire (liaisons point multipoint).
- Itinérance ou Roaming : acheminement des appels. Un accord de roaming entre un opérateur A et un opérateur B permet qu'un appel émis par un abonné de l'opérateur A soit acheminé par l'opérateur B. B envoie à A les informations de facturation. L'accord prévoit les conditions de reversement entre opérateurs pour le service fourni. Les accords de roaming permettent à un opérateur d'offrir une continuité de service à ses clients y compris sur des zones dans lesquelles il n'a pas déployé de ressources.
- Carte WiFi PCMCIA : carte 802.11b insérée dans l'ordinateur portable ou le PDA. Elle gère la liaison avec le point d'accès.
- Carte WiFi PCI : carte 802.11b insérée dans l'ordinateur de bureau. Elle gère la liaison avec le point d'accès.
- Point d'accès (ou AP, ou borne RLAN) : installation qui permet à un utilisateur de se connecter par une liaison radio en 2,4 GHz ou en 5 GHz à un réseau haut débit par exemple à un réseau Ethernet ou un accès ADSL.
- PIRE : puissance isotrope rayonnée équivalente, puissance de rayonnement moyenne du point d'émission en sortie d'antenne
- RLAN : Radio Local Area Network (terminologie de la normalisation des télécommunications), traduit en français par Réseaux locaux radioélectriques
- Radius : protocole d'authentification très utilisé dans Internet, disponible sur un serveur centralisé.
- WLAN : Wireless Local Area Network, en français "réseaux locaux sans fils" (terminologie de la normalisation du monde Internet, par exemple de l'IEEE qui élabore la norme 802.11), il s'agit de la version sans fil des réseaux informatiques locaux. Les termes RLAN et WLAN sont parfois employés l'un pour l'autre, l'un (RLAN) trouve son origine dans les télécommunications et est réservé aux bandes de fréquences 2,4 GHz et 5 GHz, l'autre (WLAN) est un terme plus général qui est utilisé par les acteurs de l'Internet pour tous les réseaux sans fil.
- WEP : Wired equivalent privacy, seul protocole de sécurisation de 802.11, jugé insuffisamment fiable ; une version WEP 2 est en préparation. Devrait être remplacé par le protocole de cryptage

- WPA (Wifi protected access) : standard élaboré par la Wi-Fi Alliance pour remplacer le WEP dans l'immédiat, en attendant une évolution du standard de l'IEEE (802.11i en particulier).
- WiFi : Label d'un consortium industriel américain le ń Wi-Fi Alliance ż anciennement WECA ("Wireless Ethernet Compatibility Alliance"). Ce label atteste la conformité des produits au standard 802.11b.
- WISP : fournisseur d'accès à Internet utilisant les technologies d'accès sans fil WLAN.

Annexe B

Le Wi-Fi en 12 points

B.1 Définition

Le Wi-Fi est une technologie permettant la transmission de données informatiques sans fil et à haut débit.

B.2 Architectures

Le déploiement d'un réseau Wi-fi permet de reproduire l'ensemble des applications liées à l'utilisation d'un réseau Ethernet classique mais ... sans fil. Il existe deux types d'applications principales liées aux technologies radio : l'extension d'un réseau existant et le partage de ressources.

B.2.1 Étendre un réseau existant

Des liaisons point à point de plusieurs kilomètres permettent de prolonger un réseau local ou éventuellement d' amener l'Internet haut débit là où personne ne le propose. Prenons l'exemple de deux écoles distantes, à vue, possédant chacune un réseau informatique et désirant mettre en commun leurs réseaux. Le Wi-fi , par le biais d'une liaison directionnelle (point à point) permet de relier les deux infrastructures (fig. **??**), en réduisant les coûts de 10 à 100 fois par rapport à un raccordement câblé.

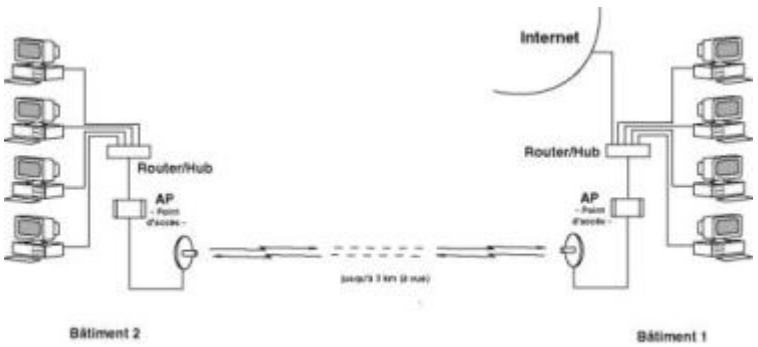

FIG. B.1 – Liaison directionnelle entre deux réseaux locaux

B.2.2 Partager une ressource réseau

La seconde consiste à mutualiser des éléments réseaux (fichiers, images, films, applications, matériel, connexion Internet) entre plusieurs usagers.

Cinq voisins désirent par exemple de partager un accès Internet haut-débit, en toute légalité selon le contrat passé avec leur fournisseur d'accès : une liaison omnidirectionnelle Wi-Fi va permettre de mutualiser facilement l'accès à cette ressource (fig. **??**). Dans ce cas, le débit de la connexion sera partagé entre les utilisateurs simultanés.

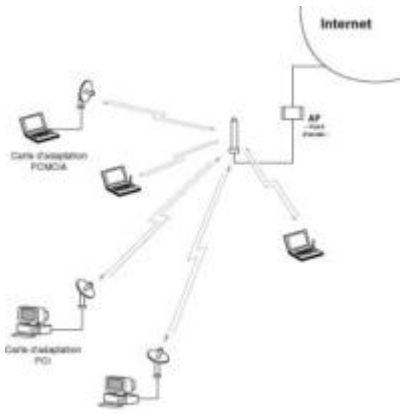

FIG. B.2 – Partage de ressources

N'importe quelle ressource peut être partagée de la sorte : imprimante, scanner, serveur de données, permettant par exemple la mise en place d'un site contributif de données à l'échelle d'un village ou d'un quartier.

L'utilisation du Wi-Fi a permis de s'affranchir de la contrainte de câblage et de la mise en place d'un switch ou d'un hub mais aussi de réduire considérablement les délais de déploiement.

B.3 Avantages et Inconvénients

Les avantages du Wi-Fi : peu coûteux, facile à déployer, évolutif, apporte les avantages de la mobilité. Les inconvénients du Wi-Fi : nécessite d'être à vue pour les longues portées, est sensible aux interférences, nécessite de mettre en place des protocoles de sécurité complets.

B.4 Standards

Le mot Wi-fi, abréviation du terme "Wireless Fidelity", est une dénomination commerciale pour désigner l'ensemble des produits du marché répondant aux standards 802.11 b et g de l'IEEE et inter-opérables entre eux.

Le standard 802.11b, déjà bien déployé actuellement, fournit un débit théorique de 11 Mbits/seconde. Le 802.11g, qui apparaît sur le marché depuis quelques mois (printemps 2003), permet théoriquement un débit de 54 Mbits/seconde.

B.5 Matériel

Une connexion Wi-Fi se présente sous la forme d'une antenne, reliée à un périphérique actif Wi-Fi, lui même connecté au réseau existant ou à un ordinateur. Cet élément actif assure la conversion des données (ondes radio <-> données numériques) entre l'antenne et le matériel ou réseau informatique. Il peut s'agir d'un concentrateur, nommé point d'accès ou AP, ou de cartes clientes PCI ou PCMCIA (voir fig. **??**) directement insérées dans les ordinateurs.

Il n'y pas de site *d'émission* et *de réception* en Wi-Fi : tous les éléments échangent des données de manière bidirectionnelle (en half-duplex).

B.6 Mode de connexion

Il existe deux modes de communication possibles entre les différents éléments d'un réseau Wi-Fi :

– le mode infrastructure, basé sur l'utilisation d'un point d'accès servant de point de concentration radio. Dans ce cas, les informations envoyées entre les différentes stations transitent toutes par le point d'accès.
– le mode ad-hoc, permettant à plusieurs stations équipées de cartes Wi-Fi de communiquer directement entre elles. Des possibilités de routage dynamique existent.

B.7 Canaux et fréquences

Le Wi-Fi utilise la gamme de fréquence du 2,4 Ghz pour transmettre des données entre les couples point d'accès / antenne. Cette bande de fréquence comporte 14 canaux de largeur 22MHz. Du fait du recouvrement des canaux, trois seulement sont utilisables simultanément à proximité[1], comme on peut voir sur le schéma de recouvrement (fig. **??**)..

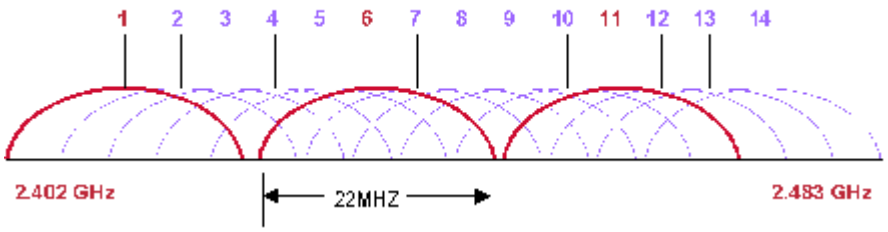

FIG. B.3 – Canaux du Wi-Fi et recouvrement

B.8 Débit

Les débits de données disponibles s'échelonnent de 1 à 54 Mbits/seconde en théorie, avec un maximum de 11 Mbps pour le standard 802.11b, 54 pour le 802.11g. Dans la pratique, on observe un débit de l'ordre de la moitié, par rapport au débit théorique.

Il s'agit d'un débit mutualisé (partagé entre les utilisateurs).

Le mécanisme de repliement permet, si les conditions sont mauvaises (distance trop grande ou interférences par exemple), de revenir à un débit moindre utilisant un codage plus robuste, pour conserver la connexion.

B.9 Puissance d'émission et portée

En l'état actuel des autorisations, la puissance d'émission des couples point d'accès / antenne Wi-Fi (la PIRE, Puissance Isotrope Rayonnée Équivalente) est fixée à 100 mW, permettant d'atteindre en extérieur des portées de l'ordre de 3 km en liaison directionnelle et 800 m en desserte omnidirectionelle à 11Mbps.

[1] cependant, on peut jouer sur la polarisation des antennes pour multiplier les possibilités

TAB. B.1 – Deux AP (D-Link et Linksys), une carte PCI et une carte PCMCIA

B.10 Sécurité

Le standard 802.11b met en œuvre un mécanisme de chiffrement nommé WEP (Wired Equivalent Privacy), qui utilise l'algorithme de chiffrement RC4. Le WEP permet un chiffrement sans perte importante de débit, mais il est très faible du point de vue de la sécurité, et peut être cassé en quelques heures par écoute passive et analyse du trafic enregistré.

Il existe des solutions alternatives propriétaires plus sûres, comme TKIP de Cisco, mais le mieux pour conserver la liberté de choix du fournisseur est d'utiliser une des formules suivantes, cumulables :

- l'authentification des utilisateurs au moment de la connexion sous forme de couple login/mot de passe (MD5) ou de certificat (TLS), et la distribution de clés WEP dynamiques. Cette formule nécessite le déploiement d'un serveur d'authentification (RADIUS),
- le chiffrement des données de bout en bout, par encapsulation : tunneling IPsec ou PPTP.

Les constructeurs travaillent actuellement sur un standard de gestion de la sécurité plus sûr, nommé WPA (Wifi Protected Access), en attendant le standard 802.11i qui est en cours d'élaboration à l'IEEE.

B.11 Santé

Selon les sources de l'ART, *"les antennes Wi-Fi rayonnent avec une puissance maximale de 100 mW, très inférieure par exemple aux antennes GSM dont la puissance, elle même relativement faible par rapport à d'autres sources d'émission radioélectrique, est de l'ordre de quelques dizaines de watts."* Ce point de vue semble partagé par la plupart des analystes officiels.

A titre d'indication nous avons évalué qu'une antenne Wifi de 100mW placée à 1 mètre rayonnait de manière équivalente à un téléphone portable 1W placé à 3 mètres !

B.12 État des autorisations

En France, seules les fréquences correspondant aux 13 premiers canaux (sur les 14 du Wi-Fi) sont autorisées.

Depuis le 25 juillet 2003, les statuts particuliers accordés à certains départements ont été généralisés, et l'utilisation de ces fréquences est libre dans la limite des puissances émises, indiquées dans le tableau **??**. Les expérimentations de réseaux Wi-Fi ne sont plus soumises à autorisation, mais doivent simplement être déclarées auprès de l'ART[2].

<table>
<tr><th>Fréquence (MHz)</th><th>Canal</th><th>Intérieur</th><th>Extérieur</th></tr>
<tr><td>2400

2454</td><td>1

9</td><td rowspan="2">100 mW</td><td>100 mW</td></tr>
<tr><td>

2483</td><td>

13</td><td>10 mW</td></tr>
</table>

Tab. B.2 – Limites de puissance autorisées

[2]Autorité de Régulation des Télécommunications

Annexe C

Comment mettre en place une liaison point-à-point

Au cours des différents tests, à force de faire des erreurs souvent bêtes et coûteuses en temps perdu, nous avons adopté une méthode pour réussir une liaison directionnelle rapidement, ou au moins pour pouvoir diagnostiquer un échec comme étant dû à de mauvaises conditions radio.

C.1 Conditions requises

Il faut être au moins deux !

Les points à relier doivent être à vue, sans obstacle[1]. Certains obstacles comme les lignes électriques ou les poteaux ne gêneront pas trop pour des distances courtes (200-500 m). La distance maximale, pour une liaison utilisable en respectant les limites de puissance, doit être d'environ 3 km.

L'idéal est de disposer :

- de deux ordinateurs portables,
- de deux cartes Wifi PCMCIA disposant de prises pour brancher des antennes,
- de radios portatives (talkies-walkies), au pire de téléphones portables,
- de mâts ou de pieds suffisamment mobiles pour faire l'azimutage, nous utilisions pour cela un pied d'appareil de prise de vue, sur lequel l'antenne était tout simplement scotchée,
- d'un logiciel d'analyse de la puissance et de la qualité du signal, idéalement par graphe ou signal sonore en temps réel (nous utilisions le client propriétaire des cartes Cisco – fig. **??**, mais le client de Windows avec ses barres vertes est déjà un indicateur relativement fiable),
- éventuellement d'un logiciel de détection de réseau Wifi, comme Network Stumbler(www.netstumbler.com, attention, pas compatible avec toutes les cartes), qui permet de détecter le signal même s'il est trop faible pour qu'on puisse s'y associer,
- évidemment de toute la connectique nécessaire !

C.2 Procédure

- 1. Régler la configuration logicielle et les points d'accès, et tester le bon fonctionnement, avant de se séparer. S'il y a un doute, vérifier le sens de polarisation des antennes : en les tenant face à face, il faut les faire tourner autour de l'axe imaginaire de la liaison radio, pour déterminer dans quelle position le signal est le meilleur[2].
- 2. Une fois séparés et en place, lancer le logiciel de détection de réseau Wi-Fi, et faire l'azimutage[3] grossièrement, jusqu'à être averti qu'un réseau est capté.

[1] Cela est vrai en milieu rural; par contre, en ville, les bâtiments environnants peuvent servir de "guide d'ondes", et permettre des liaisons indirectes, un tel cas nous a été rapporté par Wireless-Lyon.

[2] La polarisation est verticale ou horizontale (ou encore circulaire, plus rare, c'est alors le sens de rotation qui détermine la polarisation). Deux antennes dont la polarisation diverge de 90degrés ne peuvent pas se transmettre d'énergie radioélectrique, il faut qu'elles soient polarisées de la même façon.

[3] réglage de la position des antennes

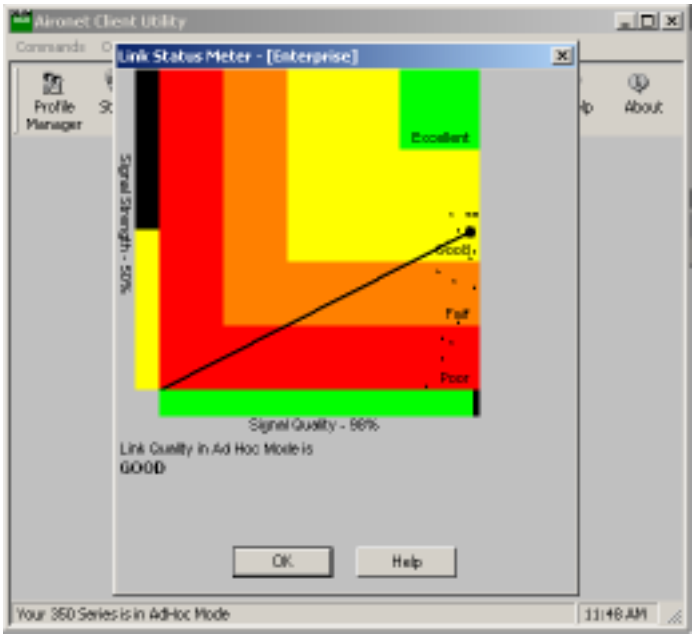

FIG. C.1 – L'outil de Cisco pour visualiser l'état de la connexion

- 3. arrêter le logiciel de détection et lancer l'outil de visualisation d'état de connexion [4], pour affiner l'azimutage **d'un côté à la fois**. Il faut rechercher une puissance élevée, le rapport signal/bruit n'étant pas significatif tout seul. Il faut également obtenir une connexion réseau, vérifiable par ping, puis par transfert de fichier (ce qui indique la stabilité du lien).
- 4. Une fois l'azimutage optimal trouvé, on peut fixer les antennes et brancher les appareils définitifs,
- 5. procéder à une vérification de la connectivité avec les points d'accès pour finir.

[4] il y a en effet un risque de gêne mutuelle, comme nous l'avons remarqué entre le client Cisco et NetStumbler