Projet de déploiement du réseau WiFi sur le campus de l'INT

Céline Ayraud
Benjamin Leroux
François Delepine
Guillaume Peigne
Charles Delalonde
Florent Mathé

10 mai 2003

Table des matières

Table des figures

Chapitre 1

Analyse des besoins

1.1 Introduction

1.1.1 Contexte et objectifs du projet

Le Wi-Fi (Wireless Fidelity) est un nom générique désignant des technologies de réseaux sans fil. Aujourd'hui, l'INT commence à envisager d'implémenter ce type de technologie sur son campus. Concrètement, ce projet vise à permettre aux élèves, aux permanents ainsi qu'aux visiteurs occasionnels de l'INT de se connecter au réseau et à Internet via leur ordinateur portable, ou leur PDA (Portable Digital Assistant).

Afin de mener à bien ce projet, la Direction de l'INT a chargé un groupe d'élèves de deuxième année de mener une étude préparatoire sur ce sujet durant la "Semaine Projet".

L'étude est divisée en quatre sous-projets, qui correspondent chacun à un aspect du projet :

- définition précise du contexte juridique de l'INT et de la législation en vigueur pour l'utilisation du Wi-Fi dans le cadre d'un établissement publique.
- définition précise des différents besoins internes à l'INT en terme de mobilité et de réseaux sans fil.
- étude d'une solution de sécurisation du réseau sans fil.
- étude d'une solution de déploiement et d'offre de services.

1.1.2 La technologie Wi-Fi

Le Wi-Fi est une norme permettant de transporter des informations par ondes radios. Derrière ce terme se cache un ensemble de normes (802.11X) définissant de manière rigoureuse les communications entre les éléments d'un réseau sans fil. En clair, cette technologie vous offre les portes de la "mobilité IP", à savoir être présent sur un réseau et avoir accès à ses services sans avoir besoin d'être relié par un câble à une prise réseau.

Les possibilités d'utilisation d'une telle technologie sont très variées. Tout simplement, cela permet par exemple de pouvoir se connecter à Internet, avec son ordinateur portable ou son PDA, sur la terrasse de la cafétéria, ou dans le forum, entre autres. Cela vous permet d'être mobile et de disposer de l'accès sur toute la zone géographique de l'INT, comme le montre le schéma en page suivante.

1.1.3 L'analyse des besoins

Ce dossier a pour objet l'analyse des besoins, réalisée par notre équipe de huit collaborateurs. Conformément au cahier des charges qui nous a été proposé, et en accord avec la Direction de l'INT, maître d'ouvrage, nous avons élaboré un guide d'entretien et planifié une série de rendez-vous avec un ensemble d'interlocuteurs. L'objectif était de cerner les besoins en terme de Wi-Fi des différentes populations de l'INT. Le cahier des charges distinguait judicieusement trois types de besoins différents :

- connexion de personnes de passage, « hotspot », notamment participants aux colloques et vacataires
- connexion des permanents
- connexion des élèves

Nous aborderons tout d'abord le travail préalable aux interviews, à savoir la rédaction du questionnaire et le choix des personnes à interviewer. Ensuite, nous examinerons les résultats des interviews par catégories de besoins. Enfin, nous proposerons une synthèse de notre étude ainsi que des recommandations en terme de déploiement et de communication.

1.2 La mise en place du questionnaire et de la liste d'interviewés

Notre équipe, préalablement au travail d'interviews, a rédigé un questionnaire et déterminé une liste de personnes à interviewer. Ce travail était crucial : étant donné l'ampleur de la population considérée, il faut poser les bonnes questions aux bonnes personnes.

1.2.1 La liste des personnes à interviewer

Notre objectif était d'avoir une vision globale des populations de l'INT, afin de pouvoir dresser une liste de personnes significatives en terme de besoins en Wi-Fi. Nous sommes partis des 3 populations définies dans le cahier des charges :

- les personnes de passage
- les permanents
- les élèves

Nous avons ensuite identifié des sous groupes au sein de ces trois catégories principales. L'arborescence suivante dresse le panorama des populations identifiées :

Personnes de passage

- Colloques : Olivier Berger, Chantal Vallet, Jean-Claude Lafont
- Vacataires : Gilles Fauré, Sidonie Hill
- Personnes de l'extérieur en contact avec l'incubateur : Sébastien Cauwet, Louis Marmillon
- Autres (Service International, ...etc) : Beverley Delsine

Permanents

- Administration
- Ecoles
- INT Management : Laurent Hua, Aline Salierno, Christelle Cornu
- Telecom INT : Gérard Carnat, Christian Camilleri, Claude Vilard
- Services : Régine Bélliard, Marie-Christine Monget, Jean-Claude Lafont
- Maisel : Christian Camilleri, Brice Proucelle

Enseignants chercheurs

- Responsables de département : Jean-Paul Goulvestre, Louis Lasoudris, Fabienne Canal
- Autres : Nel Samana, Jérôme Boudy, Jean-Pierre Vidal, Olivier Epinette, Jean-Maurice Bruneau, Chantal Vallet

Elèves

- Résidant à la Maisel : N Guetta N zore (EI1), Isabelle Elhadji Toumane (EI2), Laetitia Kanga (EM1), Nizar Rouatbi (EI2), Arnaud Janvier (EI1), Soufiane Kelly (EI2), Stéphanie Prineau (EM1)
- Extérieurs : Nicolas Men (EM2), Cyril Perissol (EI2), Wasfi Jaouad (EI3), Julien Brajard (EI3), Denis Rebeyrat (EM2), Jorma Leteurtrois (EI2), Louis Marmillon (EM2), Vincent Khoury (Master), Ayadi Achraf, (Thésard)
- Formation Continue : Jean-Claude Violette
- Bibliothèque : Régine Bélliard

1.2.2 Le questionnaire

Après avoir déterminé une liste significative de personnes à interviewer, nous avons rédigé un questionnaire type (cf. annexes).

Les personnes à contacter ayant un statut différent, nous avons délibérément choisi un questionnaire général qui puisse s'adapter à tout le monde. Certaines questions n'ont pas été posées à certains interlocuteurs (exemple : questions 7, 8, 9), car elles concernent des populations particulières.

Dans ce questionnaire, nous avons décliné une série de questions qui va du général au particulier : nous commençons par évaluer le degré d'utilisation d'Internet de l'interviewé ; ensuite, nous lui demandons en quoi le Wi-Fi pourrait lui être utile par rapport à son utilisation quotidienne d'Internet. Enfin, nous demandons concrètement où il compterait se connecter, et à quelle fréquence.

Ce questionnaire a servi de fil conducteur pour mener nos entretiens, sans forcément se tenir rigoureusement aux questions. Notre idée était de poser des questions ouvertes, qui puissent conduire l'interviewé à se demander si un réseau Wi-Fi lui serait utile, en fonction de son statut dans l'école. Cela donnait souvent lieu à une discussion moins formelle qu'un simple questionnaire, dans laquelle l'interviewé exprimait ses besoins en terme de réseau Wi-Fi.

1.3 Les résultats des interviews

1.3.1 Les personnes de passage

Définition de la population

La population observée est constituée des vacataires, participants à des colloques ou visiteurs de l'INT. Cette étude se concentre sur une population mobile (limitée ds le temps).

Au sein de cette population il faut séparer les utilisateurs vacataires ayant une relation contractuelle avec l'INT et un visiteur occasionnel. En effet, le premier, à l'occasion de la signature du contrat peut être informé des technologies implémentées à l'INT. Le visiteur occasionnel peut participer à un colloque sans avoir de liens avec l'administration de l'école.

Ainsi, les stratégies et les réactions par rapport à cette technologie sans fil diffèrent.

Pour obtenir une représentation large de l'avis de ces populations, nous avons interrogé six personnes. Jean-Claude Lafont, responsable des relations entreprises, Olivier Berge organisateurs de colloques autour du libre (système de charte) et des vacataires Gilles Fauré professeur de Culture Japonaise et Sébastien Cauwet responsable de l'incubateur.

Avantages du WIFI pour cette population

Pour Sébastien Cauwet ou Jean Claude Lafont, le WIFI et son installation ne changera pas leur utilisation d'Internet car ils se connectent principalement de leur bureau. Par contre, ils s'accordent pour dire que les entreprises visitant l'incubateur, ou les membres du Challenge Projets Entreprendre aimeraient sûrement avoir un accès Internet pendant leur passage à l'INT.

En ce qui concerne les colloques, les avis sont unanimes : le WIFI est une obligation. Pour Beverley Delsinne, recevoir une conférence de l'IEEE cet été doit se faire avec un accès aux technologies les plus récentes. En effet, la réception de colloques constituent une véritable vitrine de la technologie de notre école. Monsieur Verge, organisateur de colloque indique que l'accès au Wifi permettrait aux gens des colloques de vérifier leurs messages mais aussi, de consulter le site de la conférence, le programme et réagir sur Internet à la présentation des intervenants.

Par ailleurs, les conférenciers pourraient être plus performants en évitant les problèmes de logistique (disquette, câbles...).

Pendant le colloque, les questions des participants pourraient être postées sur un forum et les questions seraient filtrées puis synthétisées par un assistant du conférencier. Le Wifi serait donc un outil de participation pour les conférences de l'INT.

Pour prévenir les problèmes de sécurité, une charte d'utilisation pourrait être signée au début de la conférence. Celle-ci indiquerait les problèmes de sécurité inhérents au WIFI et responsabiliserait donc les utilisateurs, tout en leur indiquant les dangers éventuels en matière de sécurité.

Dans le cadre de ces conférences, les participants pourraient louer où emprunter ces cartes Wifi auprès d'une structure de l'INT. Pour éviter tout problème d'administration, il faudrait bien entendu que ces cartes soient auto configurables. Ainsi, vacataires et participants ou organisateurs de colloques s'accordent pour favoriser l'implantation de la technologie.

Cela constituerait une promotion de notre école et encouragerait la participation aux colloques. Cependant, nos interlocuteurs mettent en garde sur l'utilisation de la technologie dans certaines conditions.

Inconvénients

La sécurité du réseau constitue la première réticence de cette catégorie. En effet, vacataires comme participants de colloques s'inquiètent de la fiabilité du réseau.

De plus les vacataires redoutent une utilisation détournée de la technologie pendant les cours.

Enfin, certain professeurs s'inquiètent du débit limité du Wifi qui, dans le cadre de contenu trop lourd peut provoquer un ralentissement du réseau.

1.3.2 Les enseignants chercheurs

Description

Les personnes interrogées sont les enseignants-chercheurs permanents de l'INT.

Utilisation actuelle des ressources réseau et Internet

Tous les permanents de l'INT disposent d'un bureau au sein de l'école. Ils sont équipés en matériel informatique et ont accès aux réseau Internet et Intranet. De plus, si tous ne possèdent pas de portable, les départements en possèdent un certain nombre à usage collectif. A l'opposé, certains départements tels que Samovar ou Informatique ont déjà équipé tout leur personnel de portable Wifi.

Utilisation actuelle du réseau

L'accès Internet offert par l'école est principalement utilisé pour des applications telles que http et e-mail. Un certain nombre, pour des besoins professionnels utilisent le ftp et les forums de discussion. D'autres font appel aux e-learning pour concevoir leurs cours et proposer aux étudiants d'autres supports d'apprentissage. Plus rares sont ceux qui ont une utilisation complète d'Internet, faisant appel au streaming vidéo ou à la visioconférence. Tous soulignent cependant l'intérêt qu'ils portent aux services de l'Intranet, tels que l'accès à la bibliothèque ou la communication entre les départements.

Nouvelles utilisations liées au Wifi

L'intérêt du Wifi réside dans son absence de câble. Cela semble moins lourd en terme de mobilité. Beaucoup remarquent qu'ils perdent beaucoup de temps à se connecter lorsqu'ils ont besoin d'un portable pour leur cours et que toutes les informations dont ils peuvent avoir besoin ne sont pas disponibles. Ils regrettent d'avoir à charger ces informations sur leur disque dur avant leur cours et espère qu'un réseau Wifi résoudra ces problèmes. Certains professeurs évoquent la possibilité de poursuivre leur recherche à la bibliothèque directement à partir de leur portable.

Au niveau pédagogique, certains professeurs pensent que le Wifi permettrait de développer des modules plus interactifs, de désengorger les salles TP et d'assister les étudiants à distance, leur permettant ainsi d'avancer à leur rythme. Ils soulignent cependant le danger d'élargissement de la fracture numérique entre élèves équipés Wifi et élèves ne pouvant s'équiper. Ils redoutent de plus l'utilisation détournée de la part des élèves d'un accès Internet permanent pendant les cours (chat, téléchargement de vidéos,...), soulignant que déjà lors de cours en salle TP, les étudiants ne peuvent s'empêcher de consulter leurs mails et de surfer sur le Web.

Importance de la Sécurité

Les enseignants sont globalement confiants quant à la sécurité d'un tel réseau. Les applications qu'ils utilisent ne requièrent pas un très haut niveau de protection. Ils souhaitent cependant s'assurer que leurs données personnelles resteront protégées.

Exigences en termes de débit et de qualité de service

Les enseignants sont conscients de la perte de débit engendrée par le Wifi. Ils pensent cependant globalement que les applications dont ils ont besoin peuvent s'en contenter. Toutefois, tous soulignent qu'il est hors de question de revenir en arrière en proposant un débit moindre au quotidien. Ils ne veulent pas être otages d'une technologie encore balbutiante, redoutent les problèmes de congestion et avouent être habitués à un grand confort d'utilisation.

Conclusion

En ce qui concerne leurs besoins propres, les enseignants considèrent globalement plutôt le Wifi comme un gadget, compte tenu de la performance du réseau actuel.

De plus, s'ils sont en mesure d'imaginer des applications pédagogiques au Wifi, ils redoutent un élargissement de la facture numérique parmi les étudiants et des utilisations détournées par ceux qui seraient équipés.

Les enseignants sont surtout convaincus qu'un tel réseau constitue principalement une vitrine pour l'INT et soulignent son importance pour l'image extérieure de l'école. Nombreux sont alors ceux qui nous ont rappelé l'importance des services à développer pour crédibiliser cette vitrine.

1.3.3 Les élèves

Description

Par « élèves » nous entendons en fait trois catégories :

- les « Maisel », qui résident sur le campus
- les « extérieurs » qui résident en dehors du campus et sont présents uniquement pour les cours
- les « FC » qui suivent une formation continue, dispensée par INT entreprise

Interlocuteurs

Pour avoir un avis général des élèves nous avons essayé d'en rencontrer beaucoup (nous en avons interrogé une quinzaine) et tenté de diversifier l'échantillon. Nous avons donc interviewé des élèves-ingénieurs des élèves-managers, des mastères, des thésards, de toutes les promotions (la liste exacte est en annexe).

En ce qui concerne la formation continue, nous n'avons pas pu interroger de « FC » car il n'y avait pas de formation en cours. Nous avons donc interrogé Jean-Claude Violette, directeur d'INT entreprise qui dispense ces formations continues. Nous avons également interrogé pour le service documentaire Régine Belliard, responsable de la bibliothèque, qui nous a entretenu sur les besoins des élèves dans ce lieu .

Utilisation des ressources

les « Maisel » sont pratiquement tous reliés au réseau de la Maisel, ils utilisent quotidiennement Internet et le réseau local , en priorité pour le web et le mail, mais aussi pour les jeux en réseau, le chat, le transfert de fichiers, le e-learning...

Les « extérieurs » utilisent aussi beaucoup Internet, chez eux et par le biais des salles TP.

En ce qui concerne la bibliothèque, les élèves peuvent y utiliser le Web en général pour rechercher des informations. Ils ont également accès a des revues électroniques et des bases de données d'informations (Arcentel, Europresse...).

Les « FC » disposent d'un compte MCI quand ils sont là pour plusieurs mois et se connecte par le biais de salle TP au réseau, par exemple pour garder contact avec leur entreprise par le biais des mails , du web...

Le Wifi ? oui mais pourquoi ?

les « Maisel » sont déjà connectés par le réseau filaire. Pour la plupart ils ne voient pas vraiment l'intérêt du Wifi dans leur chambre mais annoncent que celui ci leur permetterait de gagner en mobilité.

Les «extérieurs » utilisent également les ressources filaires de l'école et la solution leur convient. Ceux d'entre eux qui possèdent déjà un portable aimeraient utiliser le Wifi pour plus de mobilité et pour accéder plus facilement aux ressources. Par exemple, dans le cas de salles TP engorgées, on peut imaginer une salle banalisée avec Wifi ou les élèves pourraient venir travailler avec leur portable.

Cette utilisation est loin d'être anecdotique. Depuis quelques années beaucoup d'élèves possédent un ordinateur portable et le nombre des élèves équipé augmente fortement d'une année sur l'autre. Aujourd'hui on peut dire que environ 30

Pour cette population, l'intérêt du Wifi est indéniable. Grâce à lui, la pratique de l'internet et du réseau peuvent se généraliser fortement. Les extérieurs équipés pourront ainsi profiter des ressources en matière

d'Internet et de réseau local de l'INT. Plus généralement les élèves désirant travailler en groupe (sur un projet par exemple) pourront se réunir dans des lieux auparavant inexploitables : la bibliothèque, les salles de jeu calme à la Maisel, le foyer, l'extérieur.

Tous les élèves interrogés se déclarent fortement intéressés par une éventuelle location à l'année de cartes Wifi. Si MCI ou MiNET met en place une telle opération, nul doute que la majorité des possésseurs d'un portable utiliseront ce service.

Les « FC » ont besoin de se connecter à Internet et possèdent souvent un portable. Le Wifi pourrait être la solution idéale, surtout si on intègre la location de cartes appropriées. Mr Violette propose l'installation d'une borne d'accès publique ouverte connectée en Wifi pour le côté « démonstrateur de nouvelles technologies ».

Les élèves, de manière générale, ne perçoivent pas de nouvelles utilisations qui seraient générées par l'installation du Wifi. Ils voient juste l'aspect pratique, par exemple ne plus avoir de chercher une prise, et l'aspect mobile qui leur permettera de travailler ou ils le désirent.

Mais on peut tout de même envisager de nouvelles utilisations, comme le travail en groupe sur ordinateurs portables reliés grâce au Wifi, par exemple en salles banalisées, à la Maisel, en extérieur, à la cafétéria.

Besoins en Wifi

De manière générale, les élèves ne réclament pas de besoin en sécurité particuliers. Ils n'échangent généralement pas de données confidentielles.

Les élèves, habitués au réseau filaire, ne veulent pas perdre de débit ou de qualité de service en passant à la technologie Wifi.

Pour des raisons évidentes de limitation de budget, les élèves sont principalement rebutés par le prix du matériel permettant d'accéder à la technologie Wifi. C'est pourquoi, ils sont très intéressés par la location éventuelle de cartes Wifi, qui pourrait se faire par le biais du département MCI ou de l'association MiNET.

Les élèves ne paraissent pas s'inquiéter d'un éventuel impact sur la santé.

Les emplacements

les « Maisel » ne semblent pas particulièrement intéressés par un accès Wifi de leur chambre, étant donné qu'il sont déjà satisfaits de leur connexion filaire. Dans son entretien, Mr Camilleri déclare que le U6, sera construit avec le réseau filaire, parce que les coûts d'installation sont peu importants si elle se déroule en même temps que la construction du bâtiment.

Les lieux qui reviennent souvent dans les discours des élèves sont :

- le forum, parce qu'il constitue un lieu de passage évident
- des salles de cours banalisées pour désengorger les salles Tp, soit pleines soit fermées.
- le foyer : les élèves qui désirent travailler avec leur portable dans les locaux associatifs pourraient l'utiliser.
- l'extérieur (en particulier la célèbre « butte au lapin »)
- la cafétéria est évoquée sans plus.
- La bibliothèque

En ce qui concerne la bibliothèque, le Wifi permettrait de se libérer des contraintes filaires (nombre de postes limité, emplacements peu pratiques). La technologie a déjà été mis en place avec succès dans d'autres écoles, comme l'ESC Reims, l'ESC Marseille et l'ESC Rouen. Dans ces lieux, le service est bien utilisé, principalement par les étudiants qui possèdent des portables récents compatibles avec le Wifi.

Pour l'INT Entreprise et la formation continue, il serait utile d'installer le Wifi dans le nouveau bâtiment F, afin de proposer l'accès aux personnes en formation, pendant leur temps libre.

De manière générale, les élèves apparaissent comme passifs face à l'éventuelle implémentation de la technologie Wifi à l'école. Ils sont prêts à utiliser la technologie si on leur prête le matériel nécessaire, mais ne vont pas pour autant modifier leurs habitudes d'utilisation du réseau et de l'Internet. Les élèves possédant un portable, donc plus facilement équipés, sont beaucoup plus demandeurs. D'où l'importance de la mise en place d'une location de cartes Wifi à l'année.

Les deux endroits à retenir, pour l'installation, sont la bibliothèque et des salles banalisées ou les élèves pourront venir travailler avec leur propre matériel.

Il ne faut surtout pas négliger l'impact promotionnel, le Wifi constitue une vitrine technologique indispensable dans une grande école d'ingénieur. Cet accès serait un plus pour le programme de formations continue donc il faudrait, en priorité, implémenter le Wifi au bâtiment F.

1.3.4 L'Administration

Description

Les personnes interrogées appartiennent à la direction de l'INT. On peut distinguer plusieurs services : le service de scolarité, le service documentaire, la maison des élèves, les services de communication avec l'extérieur. Les besoins varient suivant le service étudié.

Utilisation actuelle des ressources réseau et Internet, niveau d'équipement

Les bureaux de la Direction sont équipés d'au moins d'un ordinateur fixe et la plupart des personnes interrogées disposeraient d'un ordinateur mobile et voire même d' équipements Wifi. Des salles de réunion sont dorénavant équipées de bornes Wifi.

Après une dépouille de nos interviews, nous avons constaté que ces équipements étaient utilisés principalement pour la communication et surtout pour les emails.

Aussi, la plupart utilise le réseau Intranet davantage par rapport au réseau Internet pour lire l'actualité du campus ou de leur département, leur email et consulter certaines informations comme les emplois du temps et les autres services en ligne.

Très peu utilise les protocoles de transferts de données comme le FTP. Ces protocoles sont en fait transparents pour les utilisateurs qui l'utilisent occasionnellement.

Une partie minoritaire utilise la visioconférence pendant que d'autres sont perplexes sur le bon fonctionnement de cette technologie. Quant aux jeux en ligne, chat, et forums très peu les utilisent.

Utilisation du Wifi

Pour la plupart de nos interlocuteurs le Wifi est une solution pour remplacer tous les fils et câbles qui pullulent dans toutes les salles de cours et de réunion et qui rendent souvent pénible la connexion de certains équipements. Certains pensent que le Wifi pourrait servir de vitrine technologique pour l'INT et d'autres affirment qu'il s'agit d'un gadget de plus.

Concrètement, par exemple, le Wifi permettrait de relier plus facilement l'ordinateur portable au vidéoprojecteur sans faire appel à la logistique.

Ce serait aussi une solution pour connecter les non permanents à savoir les vacataires, les membres des colloques et les visiteurs.

implémentation du Wifi

Les interlocuteurs sont pour le Wifi à condition que leurs exigences en matière de sécurité, santé et débits offerts soient remplies. Pour eux l'équipement nécessaire à l'utilisation du Wifi devra être fourni par l'école et principalement par le service MCI. Ils n'ont pas personnellement de contraintes budgétaire comparés aux étudiants.

Les avis divergent quant à la détermination du niveau de sécurité du futur réseau. Les responsables de la scolarité demande un niveau élevé de sécurité pour interdire certains accès aux élèves comme les bases de données des notes. La maison des élèves demande aussi un niveau semblable à cause des nombreuses applications métiers qu'elle utilise gérer les logements des étudiants. Pour les autres un minimum de sécurité pour évite que les mails ne soient pas lus par tous est amplement suffisant.

Habitué au Gigabit Ethernet actuel, une infime partie des personnes interrogées sont pour le statut quo ou un débit meilleure à cause notamment des outils E-learning développés par la cellule multimédia qui sont adaptés pour un réseau 10/100 Mbits. Mais à part ce groupe les autres pensent qu'ils n'auront pas besoin d'un grand débit pour leur application.

1.4 Synthèse et recommandations

1.4.1 Synthèse des besoins exprimés

Après avoir interrogé sur le sujet une quarantaine de personnes, nous sommes en mesure d'annoncer les premières impressions.

Les enseignants/chercheurs et les élèves utilisent énormément les ressources de l'Internet et du réseau local aujourd'hui, par le biais du réseau filaire. Le passage à la technologie WIFI ne modifiera pas leurs utilisations, mais permettra juste de rendre l'usage plus simple et plus confortable. Plusieurs exemples s'offrent à nous comme désengorger les salles de TP au profit de salles de cours avec accès WIFI ou simplifier le branchement des ordinateurs portables en salle de réunion. Pour les élèves, possésseurs d'un portable, l'accès à la technologie Wifi s'annonce comme un grand plus dans leur utilisation quotidienne d'Internet et ils sont très demandeurs d'un tel service.

L'importance d'une éventuelle implémentation du WIFI à l'école se trouve plutôt du côté de la communication. Beaucoup d'interlocuteurs ont mentionné l'effet démonstratif de cette nouvelle technologie, vis-à-vis des entreprises en visite à l'INT.

C'est pourquoi les principaux utilisateurs du WIFI sur le campus semblent d'abord les « personnes de passage » : les vacataires, les participants aux colloques, les visiteurs... Ceux-ci pourront alors accéder aux ressources Web et mail en accès libre.

La communication sur le sujet s'annonce comme primordiale dans le cas d'une installation du WIFI .En effet certains départements ont déjà équipés leurs membres de cartes WIFI mais celles-ci sont sous utilisées. Autre exemple, certaines bornes, ouvertes au public, existent déjà dans le forum sans que personne ne le sache. La bibliothèque permet déjà aux élèves munis d'un portable de se connecter à Internet par câble sans que cela ne soit précisé.

De par son accès libre, le WIFI oblige les administrateurs du réseau à veiller à la sécurité. Les interlocuteurs rencontrés ont tous signifié des inquiétudes à ce sujet. L'équipe « sécurité » devra mettre en place un plan d'implémentation qui garantisse une parfaite gestion du réseau à ce sujet.

Toutes les applications déroulant de la technologie WIFI doivent aussi nécessairement s'inscrire dans le cadre juridique associé. En effet des problèmes découlent de l'ouverture des ressources aux visiteurs occasionnels. D'où l'intérêt de définir ce cadre avant l'implémentation.

1.4.2 Besoins potentiels

Les entretiens n'ont pas révélés de nouvelles utilisation du réseau liées à l'installation d'un accès Wifi à l'INT. Les différentes personnes interrogées n'avaient sans-doute pas suffisamnet de recul sur la technologie pour vois l'impact que cette technologie pourrait avoir sur leurs habitudes de travail.

On peut pourtant envisager d'autres applications au Wifi que la simple consultation de pages Web ou de mails :

- salle de TP mobile (chariot comprenant 24 portables ou 24 PDA équipés de cartes Wifi et un access point à brancher sur le réseau filaire)
- accéder aux rétroprojecteurs
- visite de l'INT par PDA (plan + explications en fonction de l'endroit où vous êtes
- systèmes d'urgence (liés à la localisation)
- localisation et gestion du matériel informatique à distance
- localisation des personnes

1.4.3 Qualité de service

Une connexion par Internet, qu'elle soit par réseau câblée ou Wifi, suppose un certains nombres d'applications. Celles-ci exigent un niveau de sécurité adaptée à l'utilisation que tous peuvent ou ne peuvent pas en faire, ainsi que le débit leur permettant de fonctionner correctement.

Services demandés

Il faut donc bien entendu fournir les applications de base, comme l'accès à l'Internet général (http) et aux e-mails. De nombreux utilisateurs potentiels expriment par ailleurs leur désire d'utiliser des applications ftp, plus gourmandes en terme de débit.

Les élèves et les permanents expriment globalement le même type de besoins. Ils souhaitent avoir accès aux services de l'Intranet au quotidien (emplois du temps, menu du restaurant administratif et cours en ligne) et envisagent d'en développer de nouveaux (réservation d'un véhicule, d'un barco ou de matériel audiovisuel en ligne). Ils demandent de plus la possibilité de réaliser une recherche documentaire et de réserver les ouvrages dont ils peuvent avoir besoin sans se déplacer à la bibliothèque.

En outre, toutes les personnes interrogées voient dans le Wifi la solution aux problèmes d'engorgement des salles TP, à condition de donner aux élèves l'accès aux plates-formes et logiciels privés de l'INT, leur offrant la possibilité de réaliser leur travail dans de bonnes conditions. Ou bien cela permettrait de réserver l'accès de ces salles aux étudiants ayant un projet, plutôt qu'à ceux qui ne veulent que consulter leurs mails. Cependant il faut alors résoudre le problème du partage des imprimantes, des fax ou des scanners.

Certains professeurs ont exprimé la possibilité de mettre en place des modules plus interactifs, voire des visioconférences en libre accès avec des universités étrangères.

En ce qui concerne les visiteurs extérieurs, lors de colloques par exemple, il est important de leur offrir un accès à Internet et aux données de leur entreprise car ceux-ci en sont très demandeurs. Il peut être aussi très intéressant de leur offrir un service de localisation au sein des bâtiments de l'INT.

Enfin, les stagiaires en formation continue ou les vacataires de passage souhaitent avoir accès aux cours et aux ressources de l'INT aux même titres que les élèves.

Question du débit

Toutes les personnes interrogées reconnaissent être habituées à un grand confort d'utilisation en terme de débit. Elles sont donc hostiles à une baisse significative du débit et redoute les problèmes de congestion.

Ainsi il conviendra de limiter l'accès aux applications les plus gourmandes en débit (téléchargement de vidéos par exemple ou de gros fichiers de données).

1.4.4 Sécurité

Les exigences en matière de sécurité varient grandement selon les personnes interrogées et les applications envisagées.

Pour des applications tels que http, transfert de données non confidentielles, email, les besoins en terme de sécurité ne semblent pas très élevés. Par contre, les utilisateurs exigent que leurs données personnelles soient protégées contre le piratage et l'espionnage. Elles redoutent de mettre en partage leurs fichiers. De plus il convient de fermer complètement l'accès aux bases de données confidentielles des services de direction et d'administration, ainsi qu'aux données sécurisées et aux brevets de l'incubateur, ces données étant trop sensibles pour les diffuser sur un réseau relativement ouvert.

Un autre problème de sécurité vient à être soulevé. Il faut être conscient que la scolarité dans cette école est payante, il semble donc normal que les ressources internes de l'école, telles que les cours en ligne ou les revues électroniques payantes mises à disposition des élèves et permanents par la bibliothèque, ne soient pas ouvertes au public. Hors aujourd'hui toute personne disposant d'une adresse IP fournie par l'école, ce qui sera le cas lorsque l'on se connectera au réseau Wifi de l'INT, peut accéder à ces données. Il existe ici un véritable problème de contrôle des droits d'accès.

1.4.5 Répartition géographique de la technologie WIFI au sein du campus de l'INT

Pour résumer ce qui a été dit précédemment, voici les besoins géographiques de la technologie WIFI par catégorie de personnes :

- pour les vacataires et membres de colloques : dans le forum, les amphis.
- pour les enseignants/chercheurs : non nécessaires
- pour la direction : le batiment de direction (Dir)

- pour les élèves : une ou deux salles à titre expérimentales pour désengorger les salles de TP (installer dans les salles du bâtiment A ou dans les salles E00), ainsi que la bibliothèque.

Voici un plan du campus INT avec la répartition géographique du déploiement de la technologie WIFI :

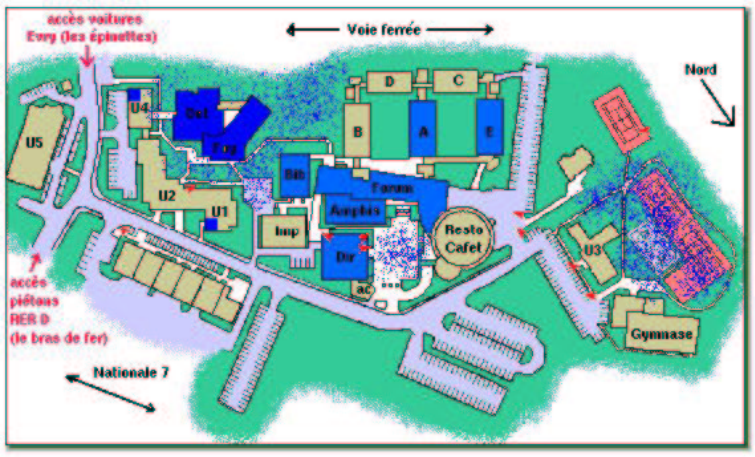

FIG. 1.1 – Répartition géographique des zones à couvrir (en bleu)

1.4.6 Tableaux récapitulatifs des besoins à l'INT

Il est possible de synthétiser les besoins exprimés par les différentes population de l'INT sous la forme d'un tableau.

Catégorie	Besoins Wi-Fi	Localisation du besoin	Importance
Elèves	Accéder à Arcentel et aux services de la bibliothèque ;	Bibliothèque ;	+++
	Pouvoir exploiter les zones de travail que constituent les salles de jeux calmes de la MAISEL et la bibliothèque avec un accès au Web ;	Salle de jeux calmes, foyer, Bibliothèque ;	++++
	Pouvoir accéder à Internet et aux services de l'INT sans avoir à aller dans des salles TP souvent engorgées ;	Forum, salle banalisée, cafétéria, amphithéâtres, salles E00 ;	+++
	Pouvoir profiter des zones extérieures du campus en été et travailler dehors ;	Butte aux Lapins ;	++
Formation Continue	Pouvoir offrir l'accès Web/mail aux professionnels ;	Bâtiment F ;	+++
	Image de marque, vitrine technologique ;	Bâtiment F, forum, cafétéria, Cours d'Honneur, amphithéâtres ;	+++
Permanents	Simplifier l'organisation de réunion ;	Salles de Réunion, bâtiment DIR ;	+++
	Exploitation dans le cadre de projet de recherche ;	Départements, laboratoires ;	++
	Utilisation de leur poste de travail en bibliothèque ;	Bibliothèque ;	++
	Accessibilité aux rétroprojecteurs en cours ;	Amphithéâtres, salles E00 et A ;	+
	Utilisation Web/mail ;	Forum, cafétéria, extérieurs ;	++++
Vacataires	Ne restent pas suffisamment longtemps pour avoir un besoin différent des autres "visiteurs" ;	Forum, cafétéria	++
Visiteurs	Accéder aux ressources Web et mail le plus facilement possible ;	Forum, cafétéria, amphithéâtres, E00, extérieurs ;	++++
Colloques	Accéder au programme et ressources du colloque ;	Forum, amphithéâtres, E00, extérieurs, cafétéria ;	+++
	Dialoguer avec les autres participants, poser des questions à l'intervenant (concept de "forum virtuel") ;	Lieu du déroulement du colloque ;	+++
	Visionner en temps réel les supports d'une présentation ;	Lieu de déroulement du colloque ;	++
	Consultation Web et mail comme les autres visiteurs ;	Forum, amphithéâtres, cafétéria, extérieurs ;	++++
Incubateur	Pouvoir accéder à des services internes de l'INT, aux mails et au Web ;	Forum, cafétéria, extérieur de l'incubateur ;	+

FIG. 1.2 – Tableau récapitulatif des besoins

1.4.7 Plan de lancement

Cependant, monsieur Lasoudris nous a alerté sur les modalités d'implantations d'un tel projet. Il souligne l'importance d'une volonté politique et d'une campagne d'accompagnement. Celle-ci inclurait communication sur le projet et formation des utilisateurs. Car fournir la technologie aux utilisateurs ne suffit pas pour qu'elle soit adoptée.

Aussi, nous recommandons un plan de communication en plusieurs phases comprenant :

- L'annonce officielle du projet
- L'inauguration animée par la direction
- La semaine de formation

La variable humaine est donc de première importance, du fait notamment que le projet rassemble les compétences de services (et de départements) différents. Leur personnel pourra donc être amené à travailler davantage ensemble. Cette partie visera à découper le projet en plusieurs phases de développement. Pour chacune d'entre elles nous effectuerons une brève présentation.

L'annonce officielle du projet

Cette nomination s'inscrit dans une campagne de communication. Ainsi, l'existence d'un réseau WIFI pourrait être spécifiée sur les plaquettes de l'INT et sur la page d'accueil du site web (scolarité, admissibles). Cette communication devra s'orienter, à la fois, vers les élèves mais aussi les enseignants chercheurs et bien entendu tous les visiteurs occasionnels de l'INT.

L'inauguration du projet

Celle-ci devra être lancée par la direction de l'école pour démontrer l'engagement dans ce projet. Cependant une grande présentation officielle ne suffira pas à initier un projet de tel envergure. Il faudra l'associer à des ateliers de formations où les gens apprendront les utilisations possibles de cette technologie, ou ils pouraient être aider à configurer leur carte WIFI. Enfin, pour conserver un aspect ludique, nous pourrions imaginer un jeu récompensé par du matèriel WIFI.

La semaine de formation

Afin d'assurer un suivi de l'inauguration du projet, une équipe devra assister les personnes désireuses de connaître où installer la technologie sur leur ordinateur personnel. Pour informer les dates de déroulement de cet atelier, il est nécessaire d'utiliser tous les moyens de communication interne (TV, mail, affiche ...).

Pour tout ceux qui ne pourront pas profiter de cet atelier, il est important d'avoir une page Internet expliquant toutes les configurations sur les différents systèmes (Windows XP, 2000, 98, 95, Linux Debian, Red Hat, Mandrake, Ipaq, Mac, ...). Cette page devra également contenir une adresse électronique (Wifi@int-evry.fr par exemple) et une liste de FAQ (Questions fréquemment posées).

Lors des colloques à l'INT, il sera important d'avoir en location des cartes WIFI compatibles avec le réseau de l'INT et avoir un panneau grand format expliquant les paramètres de configuration et les possibilités du réseau de l'INT. Pour garantir une bonne utilisation, les participants signeront au début du colloque une charte de fonctionnement du réseau Wifi mis en place pour l'occasion. Pour l'arrivée des participants des colloques il sera également envisageable que des élèves fassent un mini atelier de configuration pour les participants du colloque.

Plus généralement, pour générer l'utilisation du Wifi, les élèves semblent très intéressés par la location de cartes Wifi. Ces cartes seraient loués à l'année, soit par MCI à l'inscription, soit par MiNET lors de l'adhésion.

Chapitre 2

Analyse du contexte juridique

2.1 Introduction

En amont du déploiement d'un réseau Wi-Fi sur l'INT et son campus, de nombreuses questions juridiques se posent. Ce type de réseau est très novateur et il serait l'un des premiers du genre dans une grande école. Cependant, par son rôle important dans le secteur des télécommunications, l'INT se doit de respecter scrupuleusement la loi et ne peut pas prendre les libertés qui ont pu être prises par d'autres établissements.

La demande d'une analyse du contexte juridique a donc été formulée dans le cahier des charges de l'étude. Nous allons tout d'abord étudier l'INT et ses caractérisitiques, avant de faire une première série de remarques d'ordre général. Ensuite, une étude complète du cadre législatif français et des préconisations européennes sera menée. Finalement la dernière partie synthétise le cadre juridique applicable à l'INT, compte tenu des besoins révélés et du déploiement proposé.

2.2 L'INT et ses particularités

2.2.1 L'INT

L'Institut National des Télécommunications est un acteur important du secteur des télécommunications il est donc impératif de respecter les lois en vigueurs et particulièrement les recommandations de l'ART.

Le déploiement de réseau sans fil doit tenir compte de la mission de l'INT, à savoir l'enseignement et la recherche. Il va donc falloir réfléchir entre autre à l'accès au réseau sans fil par des personnes participant à des évènements extérieurs à la mission de l'INT (cas de La Poste récemment).

On peut d'ores et déjà établir deux catégories de personnes : celles ayant et celles n'ayant pas de compte MCI.

- Personnes possédant un compte MCI (que l'on nommera par la suite GFU, Groupe Fermé d'Utilisateurs) :
  - Les permanents, qu'ils soient enseignants ou chercheurs ;
  - Les élèves de manière générale (EI, EM, Mastères etc.) ;
  - Les différents employés de l'INT ;
  - Certains vacataires ;
- Personnes ne possédant pas de compte MCI :
  - Les participants aux différents colloques ;
  - Certains vacataires ;
  - Les élèves venant passer leurs oraux ;
  - Les visiteurs de manière générale.

Un autre point délicat dans le déploiement du réseau sans fil est le fait de déborder sur la voie publique. En effet la rue Charles Fourier n'appartient pas en totalité à l'INT. Pour ce qui est de la partie appartenant à l'INT il s'agit d'un domaine privée, il y a donc moins de problème. Par contre pour le reste de la rue, le problème peut attirer notre attention pour être en accord avec les différentes réglementations et notamment celle du ministère de la défense.

2.2.2 Premières remarques

Cette partie du document contient quelques remarques, d'ordre général ou juridique.

Le terme Wi-Fi

Le terme Wi-Fi (ou Wi-Fi) est une marque déposée par Wifi Allicance <http ://www.weca.net>. Son utilisation est donc soumise au droit des marques. Par exemple, l'association Wifi-Paris a changé de nom

pour devenir Paris-SansFil. Le but de l'appellation Wi-Fi est de certifier le matériel répondant à la norme IEEE 802.11b.

Les prestations Wi-Fi

Tout fournisseur de prestation Wi-Fi publique s'engage à garantir une qualité et une disponibilité de service satisfaisante. Il doit aussi garantir la neutralité des services vis-à-vis du contenu des messages transmis sur leur réseau et le secret des correspondances, en assurant notamment l'intégrité de ces messages. Ainsi, les agents de maintenance du réseau doivent être aussi mis au courant de leur responsabilité face au secret des correspondances. De plus, le fournisseur se doit d'informer ses utilisateurs des moyens par lesquels ils peuvent sécuriser leur connexion ainsi que leur coût.

Responsabilité des utilisateurs

La mise en place d'un réseau Wi-Fià l'INT devra s'accompagner d'une bonne communication à l'égard des utilisateurs, notamment en terme de responsabilité. Ainsi, il serait bon de rappeler à l'utilisateur les condition d'utilisation du résau, et ce aussi souvent que possible. Ce qui suit est donc une proposition visant à compléter l'actuelle charte dutilisation des resources informatiques.

Tout utilisateur du réseau sans fil mis en place par l'Institut National des Télécommunications s'engage à respecter les règles suivantes :

- L'utilisateur s'engage à respecter les chartes en vigueur à l'INT et notamment la charte informatique ainsi que la charte Renater disponibles en ligne http ://www.int-evry.fr/chartes ou en format papier auprès du service informatique.
- L'utilisateur s'engage à ne pas créer de réseau sans fil et notamment à ne pas ajouter de bornes sans l'accord de la Direction représentée par son service informatique. Il ne peut que se raccorder à un réseau sans fil déjà existant.
- L'utilisateur s'engage à ne pas utiliser un matériel ne respectant pas la réglementation de l'ART (Autorité de régulation des Télécommunications) sur les réseaux sans fils. En particulier, l'utilisateur doit veiller à ne pas émettre de signaux de puissance dépassant les niveaux de puissance de 100 mW en intérieur et 10 mW en extérieur.
- L'utilisateur s'engage à ne pas volontairement émettre des signaux ayant pour but de brouiller ou de réduire les performances du réseau sans fil.
- L'utilisateur s'engage à respecter la confidentialité des messages transitant sur le réseau et s'engage à ne pas commettre d'écoutes sur le réseau.
- L'utilisateur est invité à utiliser des solutions de cryptographie pour faire transiter ses données. Des solutions et des informations concernant la sécurité des réseaux sans fil sont mises à disposition de l'ensemble des utilisateurs par le service informatique de l'INT.
- L'utilisateur est invité à se documenter sur les effets des ondes électromagnétiques sur la santé. Des informations sont également disponibles au service informatique. A titre de rappel, il est rappelé que le principe de précaution implicite est de rigueur. Toute exposition inutile aux ondes doit être évité.

Il reste néanmoins la question de sanction en cas de non respect, notamment par un externe.

Recherche dans les écoles ayant commencé des démarches similaires

Un cadre juridique commun est ressorti après avoir contacté les écoles de management de Nancy, Bordeaux et Grenoble.

En effet dans ces trois cas seuls les élèves, les professeurs et l'administration ont accès à l'utilisation du Wi-Fi. Les extérieurs sont exclus de ce réseau car non répertorié par le service informatique. Les écoles de Bordeaux et Grenoble n'émettent qu'à l'intérieur des bâtiments, l'école de Nancy émet aussi sur le campus dans les limites de ce dernier. Dans tous les cas une procédure d'identification a été mise en place par login/mot de passe.

Ces écoles correspondent donc à un cadre juridique précis qui est celui du réseau privé auquel seul le groupement fermé d'utilisateurs a accès. Dans ces conditions, aucune licence n'est alors nécessaire.

L'impact sur la santé

Selon 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 radioéléctriques, est de l'ordre de quelques dizaines de watts. Ces émissions ne représentent donc pas de risque majeur.

Recherche pour le groupe de sécurisation

Depuis novembre, pour mieux sécuriser les échanges et amplifier les moyens de lutte contre la cybercriminalité, l'usage de la cryptographie va devenir totalement libre. Les conditions d'exercice et de responsabilité des acteurs (hébergeurs de sites, fournisseurs d'accès et opérateurs de télécommunications) seront par ailleurs précisées. La responsabilité civile et pénale des hébergeurs ne pourra ainsi être mise en cause que dans des hypothèses limitées et clairement définies. On peut alors se référer à l'article 18 du chapitre Ier du titre III du projet procède à la mise à jour complète de la réglementation touchant la cryptologie, jusqu'ici définie par l'article 28 de la loi n° 90-1170 du 29 décembre 1990 modifié par la loi n° 96-659 du 26 juillet 1996.

L'article 18 qui fixe le cadre général du contrôle de l'importation, de la fourniture, de l'utilisation, et de l'exportation des moyens de cryptologie, est un cadre général basé sur trois régimes : un régime de liberté, un régime de déclaration et un régime d'autorisation. Comme dans la loi précédente, la définition et le champ d'application de ces régimes sont renvoyés à des décrets.

Le projet assouplit grandement les modalités de contrôle des moyens de cryptologie par rapport aux dispositions en vigueur (décret n° 98-101 du 24 février 1998, décrets n° 99-199 et n° 99-200 du 17 mars 1999) :

- en libéralisant totalement l'utilisation des moyens de cryptologie quels qu'ils soient ;
- en libéralisant totalement l'importation, la fourniture et l'exportation des moyens de cryptologie assurant des fonctions de signature ;
- en abrogeant le régime d'autorisation pour la fourniture des autres moyens de cryptologie et en allégeant le régime de la déclaration.

2.3 Le cadre législatif Français et Européen

2.3.1 La législation Française

Depuis le 12 novembre 2002, il est possible de déposer des dossiers auprès de l'ART afin d'obtenir une licence d'expérimentation d'un réseau Wi-Fi. Pour le moment, ces demandes font l'objet d'un examen au cas par cas par le ministère de la Défense puis d'une autorisation par la ministre déléguée à l'Industrie en charge des télécommunications, mais la transposition en droit français de la nouvelle directive européenne relative au régime d'autorisation, prévue en 2003, pourrait changer les conditions d'octroi des licences. Ces licences ne sont néanmoins pas à demander dans le cas d'un réseau indépendant. Pour un établissement scolaire comme l'INT, la problématique se pose justement de savoir si l'on considère un réseau privé ou ouvert au public, puisqu'il serait en effet intéressant que des gens de passage dans l'école, des vacataires, puissent également profiter du réseau Wi-Fi établi.

Si d'autre part l'INT devient fournisseur de prestation Wi-Fi publique, il lui faudrait s'engager à garantir une qualité et une disponibilité de service satisfaisantes. Il devra aussi garantir la neutralité des services vis-à-vis du contenu des messages transmis sur leur réseau et le secret des correspondances, en assurant notamment l'intégrité de ces messages. Il aura également un devoir d'information vis-à-vis de ses utilisateurs sur les conditions contractuelles de fourniture de ses services et notamment des conditions de durée, de renouvellement et de qualité des services. N'oublions pas également que le terme Wi-Fi est une marque déposée par Wi-Fi Allicance, le but de cette appellation étant de certifier le matériel répondant à la norme IEEE 802.11b. Son utilisation est donc soumise au droit des marques et l'appellation « Wif'INT » pourrait ainsi poser problème.

Les RLAN pour les projets de développement local

Afin de connecter des installations radioélectriques dans la bande de fréquences 2,4 GHz, y compris en extérieur, des licences expérimentales en application de l'article L.33-1 du code des postes et télécommunications sont délivrées. Ces réseaux sont établis à titre expérimental (18 mois).

L'Autorité de Régulation des Télécommunications (ART) instruit pour le compte du ministre les demandes d'autorisation. Les demandes peuvent être présentées par des personnes physiques ou des personnes morales de droit privé ou de droit public, lorsque les dispositions législatives et réglementaires leur permettent d'exercer une telle activité. En outre, elle assure un suivi de ces expérimentations.

La bande de fréquences utilisée par les installations radioélectriques est la bande 2400-2483,5 MHz. Ces réseaux peuvent utiliser une puissance de 100 mW sur toute la bande de fréquence, à l'extérieur comme à l'intérieur des bâtiments. Le ministère de la Défense a demandé qu'en raison des contraintes liées à la défense et à la protection du territoire, les réseaux émettant en extérieur soient installés en respectant une distance de protection dès lors qu'ils sont situés à proximité d'un site jugé sensible.

Chaque projet fait l'objet d'une demande de licence expérimentale auprès de l'ART au titre de l'article L. 33-1 du code des postes et télécommunications en vue de l'établissement et l'exploitation d'un réseau ouvert au public. Toute demande fait l'objet d'un examen qui comprend la consultation, durant un délai d'un mois, du ministère de la Défense. Les autorisations au titre des expérimentations peuvent être délivrées pour une période de 18 mois. Les nouvelles directives européennes devraient être transposées en droit français au plus tard le 24 juillet 2003. Les textes de transposition préciseront les obligations des opérateurs de réseaux et celles applicables aux expérimentations. D'ici là, ces dernières seront conduites selon les décisions de l'ART.

Les demandes d'autorisation expérimentale doivent comporter (voir les détails en annexe)ndexAutorisations :

- Les informations relatives au demandeur : son identité (dénomination, siège social, pour les sociétés : immatriculation au registre du commerce et des sociétés et extrait Kbis, statuts, la description et identification de l'équipe, coordonnées d'un correspondant), le cas échéant la description des activités existantes et partenariats dans le domaine des télécommunications ;
- les autorisations dont dispose éventuellement déjà le demandeur ;
- La description des caractéristiques techniques du projet, telles que : topologie du réseau avec le schéma du site, caractéristiques et nombre de chaque équipement, zone de couverture de chaque borne, normes utilisées, canaux utilisés dans la bande 2400-2483,5 MHz, la présentation du réseau de desserte et les points d'accès à ce réseau ;
- La carte détaillée du réseau avec l'indication de la situation des bornes et la description précise de la zone de couverture ;
- l'occupation du domaine public envisagée ;
- Les autorisations nécessaires s'il y a lieu pour l'établissement des installations ;
- La description des services offerts aux utilisateurs, leurs conditions commerciales, ainsi que le nombre et les caractéristiques des utilisateurs potentiels ;
- Les informations justifiant la capacité technique à réaliser le projet, ainsi que les partenariats envisagés ;
- Les conditions financières dans lesquelles le projet est réalisé, ainsi que les partenariats financiers envisagés ; le coût du projet ainsi que les ressources nécessaires au financement devront être justifiés ;
- Les partenariats commerciaux et institutionnels ;
- Le calendrier de déploiement, de mise en service et d'ouverture commerciale de l'expérimentation.

Les dossiers seront transmis au chef du Service Opérateurs et ressources de l'Autorité de Régulation des télécommunications, (7, Square Max Hymans, 75730, Paris cedex 15) en deux exemplaires. Une version électronique sera également adressée à `Delphine.Fraboulet@art-telecom.fr`. Le circuit de traitement du dossier pour les projets de développement local est le suivant :

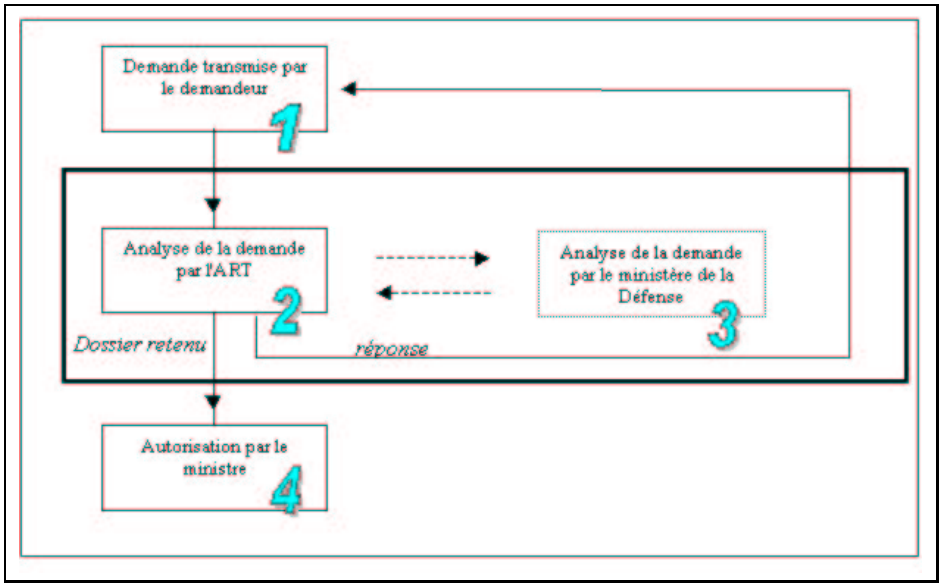

FIG. 2.1 – ART - Circuit du traitement du dossier

Les éventuelles demandes de fréquences devront être faites par une procédure spécifique si le demandeur souhaite disposer de ressources hertziennes dans les bandes de fréquences réservées à cet effet en dehors de la bande 2,4 GHz (renseignements benoît.leclapart@art-telecom.fr). Les dossiers seront transmis pour information à l'Agence nationale des fréquences lorsque l'expérimentation conduit à utiliser les fréquences avec des seuils de puissance rayonnée supérieurs aux maxima définis dans les décisions d'attribution des fréquences de la bande 2.4GHz.

Les RLAN pour les lieux de passage (hotspots)

L'utilisateur doit se conformer aux décisions n° 02-1008, 02-1009 pour la bande de fréquences 2,4 GHz. Ces fréquences sont attribuées sans aucune garantie de protection et les installations doivent respecter les dispositions qui peuvent s'appliquer en matière d'installations radioélectriques (règles d'urbanisme par exemple).

Deux cas de figure se présentent :

- raccorder des bornes RLAN à un réseau ouvert au public existant (ou raccordement par un opérateur déjà autorisé).
- établir un nouveau réseau pour relier des bornes RLAN dans des lieux de passages ("hotspots") pour la fourniture de services au public.

Dans le premier cas, les installations radioélectriques terminales n'utilisant pas des fréquences spécifiquement assignées à leur utilisateur sont établies librement dès lors qu'elles ne nécessitent pas l'établissement d'un réseau ouvert au public. Les utilisateurs peuvent installer, sous leur responsabilité, des bornes d'accès pour partager un même accès haut débit, à condition qu'ils aient l'accord préalable de leur fournisseur d'accès à Internet.

Dans le second cas, une autorisation est nécessaire quand une société, qui ne possède pas de licence d'opérateur de réseau ouvert au public, souhaite établir un nouveau réseau d'accès ayant pour objet de relier des bornes RLAN entre elles ou utiliser un réseau privé existant, transformant ainsi sa qualification réglementaire. L'Autorité propose alors à la ministre chargée des télécommunications d'attribuer des autorisations expérimentales d'une durée de 18 mois, sans préjudice des dispositions issues de la transposition des nouvelles directives européennes qui devrait intervenir au plus tard le 24 juillet 2003.

Cas des établissements scolaires

Si la borne est raccordée à un réseau public, les décisions permettent l'installation de bornes sans autorisation, à condition bien sûr que le fournisseur de l'accès haut débit soit d'accord et que les bornes soient conformes aux limitations de puissance précisées dans les décisions. Si la borne est raccordée à un réseau indépendant, par exemple celui d'une collectivité locale, alors cela change la nature de ce réseau qui est prévu pour des usages privés. La problématique n'est pas liée au Wi-Fi, c'est un problème général qui doit trouver une clarification dans le futur cadre réglementaire. C'est la question de savoir si des réseaux reliant des écoles, des universités, des bibliothèques doivent être considérés comme des réseaux privés, ou au contraire comme des réseaux ouverts au public.

Les informations à fournir sont les mêmes que pour un projet de développement local. D'autre part, les dossiers doivent comporter l'engagement que le projet est conforme aux décisions d'utilisation et d'attribution des fréquences des bandes de fréquences 2,4 GHz (décisions n°02-1008 et 02-1009). Les dossiers sont à adresser au même endroit.

Les RLAN pour les réseaux indépendants (réseaux privés)

Les réseaux indépendants utilisant des fréquences non spécifiquement assignées à leur utilisateur sont établis librement, à la condition de respecter les décisions de l'ART n° 02-1008 et 02-1009 pour la bande 2,4 GHz. Il est possible dans les départements libéralisés d'établir des réseaux indépendants sur le domaine public, sans demande d'autorisation préalable, avec une puissance isotrope rayonnée équivalente (PIRE) limitée à 100 mW dans la bande 2400-2454 MHz et 10 mW dans la bande 2454-2483,5 MHz. La demande d'utilisation de fréquences est réservée uniquement à l'utilisation de la bande 2446,5-2483,5 MHz (ou 2454-2483,5 MHz) à l'extérieur des bâtiments, sur les propriétés privées ou le domaine privé des personnes publiques, avec une puissance limitée à 100 mW.

2.3.2 La transposition des directives européennes

Les nouvelles directives européennes devraient être transposées en droit français au plus tard le 24 juillet 2003. Celles-ci pourraient changer les conditions d'octroi des licences. Néanmoins, ces directives visant à faciliter le déploiement des réseaux RLAN, ne devraient pas entraver les démarches de demande de licence, au contraire. Les textes de transposition préciseront les obligations des opérateurs de réseaux et celles applicables aux expérimentations.

D'ici là, ces dernières seront conduites selon les décisions de l'ART. L'ART est censée appliquer la loi et non la faire, mais dans les circonstances actuelles on assiste plutôt à une confusion des deux. En effet, l'Europe étant loin d'être claire sur le sujet du Wi-Fi, l'ART est amenée à prendre ses propres décisions en attendant une certaine régularisation, qui, quant à elle, ne devrait pas changer grand chose aux pratiques appliquées jusque-là.

L'exploitation d'un réseau RLAN se fonde donc sur des bases mouvantes et il est bien souvent précisé que les entreprises privées et publiques doivent anticiper les risques juridiques liés à l'établissement et à l'exploitation de ce type de réseau. Néanmoins, tout semble mener à l'assouplissement du cadre juridique de l'établissement des réseaux RLAN.

D'une part, les équipements du ministère de la Défense dans la bande 2,4 GHz migrent progressivement vers d'autres bandes de fréquences afin de pouvoir consacrer les fréquences ainsi libérées aux utilisations civiles dont les RLAN. Et d'autre part, les collectivités locales notamment pensent au Wi-Fi comme une solution alternative de bonne envergure pour les zones rurales et poussent l'ART à ?uvrer dans leur sens en leur accordant des licences.

2.4 Synthèse et recommandation

2.4.1 Cadre réglementaire et évolutions

Cadre réglementaire actuel

La réglementation française concernant les réseaux locaux sans fil était jusque là l'une des plus contraignantes d'Europe. Mais avec les récentes décisions de l'ART, elle s'assouplit. Dans cette réglementation, les réseaux locaux sans fil communément appelés WLAN, sont dénommés RLAN (Radio Local Area Network), ou RLR (Réseaux Locaux Radio-électriques).

L'ART s'est exprimé en Novembre 2002 concernant l'utilisation du Wi-Fi sur la bande 2.4 Ghz. Les fournisseurs de services et les opérateurs peuvent fournir des services de connexion sur les lieux de passage, et cela sans demande d'autorisation particulière. Les réseaux ouverts au public ne peuvent être établis que dans le cadre d'expérimentations, après demande d'autorisation et pour une durée maximale de 18 mois. Globalement, dans les DOM TOM et 38 départements français (maintenant étendu à 58, voir en annexe), il est possible d'utiliser pleinement Wi-Fi en intérieur comme en extérieur.

L'Essonne faisant partie des départements libéralisés depuis le début de cette année, nous pouvons nous interroger sur la législation concernant un déploiement de RLAN sur l'INT

Les perspectives d'évolution du cadre réglementaire

De nouvelles décisions de l'ART attendues au cours des 24 prochains mois devraient encore assouplir le cadre juridique de l'établissement des réseaux sans fil de type RLAN. A partir de 2004, les réseaux sans fil RLAN devraient pouvoir être exploités sur tout le territoire en utilisant la totalité de la bande de fréquence 2,4 GHz en intérieur et en extérieur, en fonction du résultat des discussions qui vont être menées par l'ART avec le Ministère de la Défense.

A l'issue de la période d'expérimentation de 18 mois, l'ART devrait faire un nouveau point de situation sur la base des bilans d'expérimentations qui seront communiqués par chacun des titulaires d'une autorisation. Dans cette attente, les entreprises privées et publiques concernées doivent rester vigilante et anticiper les risques juridiques liés à l'établissement et à l'exploitation de ce type de réseaux, afin d'éviter les mésaventures des pionniers du Wi-Fi comme l'association Provence Wireless, contrainte à la désinstallation immédiate du réseau WI-FI de la commune de Mane sous peine de sanctions pénales et avec un préjudice financier important.

D'ici là, la législation est toujours stricte, et toute infraction risque une peine de six mois d'emprisonnement et de 30 000 euros d'amende. L'ART est donc dans une période de réflexion, elle se basera sur les résultats des expérimentations et sur les décisions européennes pour adapter la loi française.

2.4.2 Le cas de l'INT

Le problème

Pour conclure quant à la faisabilité du projet, l'INT est censé entrer dans une des catégories envisagées par l'ART. Pressée par l'Union européenne de tenir ses engagements et afin de favoriser le développement du Wi-Fi, la France a entamé le processus de modification de sa législation sur les fréquences radio. Jusqu'alors, seuls les particuliers, les entreprises ou les collectivités territoriales pouvaient utiliser les technologies de réseau sans fil pour installer un réseau destiné à leur usage propre, à l'intérieur de leurs immeubles. Les nouvelles dispositions, prises en accord avec le ministère de la Défense, autorisent l'usage de bornes de réseaux Wi-Fi, pour la fourniture au public de services Internet haut débit, en particulier dans les lieux de passage, hot spots (gares, aéroports, centres d'affaires, etc.).

Voici ces 3 catégories :

Les RLAN pour les projets de développement local

Ce cadre concerne un déploiement permettant à quiconque de se connecter, y compris les participants d'un colloque à l'INT Chaque projet fait l'objet d'une demande de licence expérimentale auprès de l'ART (au titre de l'article L. 33-1 du code des postes et télécommunications) en vue de l'établissement et l'exploitation d'un réseau ouvert au public. Cette démarche concerne majoritairement les agglomération ou les localités désireuses de remédier ainsi à des zones de territoire mal desservies par les réseaux existants, ce qui n'est pas vraiment le cas de l'INT.

La demande de licence expérimentale est donc compliquée, et de plus, elle n'est valide que 18 mois. Nous ne savons pas encore quelles seront les modalités de renouvellement.

Les RLAN pour les lieux de passage (hotspots)

Suite aux multiples attentes qui ont été exprimées lors de la consultation publique sur l'utilisation des réseaux radioélectriques mise en oeuvre par l'ART, cette dernière a adopté le 7 novembre 2002 les décisions permettant l'utilisation de réseaux Wi-Fi pour la fourniture au public de services Internet haut débit, en particulier dans les lieux de fort passage du public (dits "hot spots") comme les gares, les aéroports, les centres d'affaires ou encore les hôtels.

Ce cas concerne les fournisseurs de services et les opérateurs autorisés qui vont pouvoir installer sans autorisation des bornes d'accès utilisant les technologies de la bande des 2,4 GHz, à l'intérieur comme à l'extérieur des bâtiments, sous réserve du respect de certaines conditions techniques (notamment de puissance sur des fréquences données).

Une telle autorisation est cependant nécessaire quand une société (c'est le cas de l'INT ne possédant pas de licence d'opérateur de réseau ouvert au public, souhaite établir un nouveau réseau d'accès ayant pour objet de relier les bornes entre elles ou d'utiliser un réseau privé existant, transformant ainsi sa qualification réglementaire.

L'Autorité souhaite proposer à la ministre chargée des télécommunications d'attribuer dans ces cas des autorisations expérimentales d'une durée de 18 mois, sans préjudice des dispositions issues de la transposition des nouvelles directives européennes qui devrait intervenir au plus tard le 24 juillet 2003. Globalement, l'ouverture du réseau de l'INT à des extérieurs pourait se faire dans ce cadre.

Les RLAN pour les réseaux indépendants (réseaux privés)

Il est possible dans les départements libéralisés (dont fait partie l'Essonne) d'établir des réseaux indépendants sur le domaine public, sans demande d'autorisation préalable, avec une puissance isotrope rayonnée équivalente (PIRE) limitée à 100 mW dans la bande 2400-2454 MHz, à l'intérieur et à l'extérieur, ce qui est la cas dans le projet envisagé. La demande d'utilisation de fréquences est réservée uniquement à l'utilisation de la bande 2446,5-2483,5 MHz (ou 2454-2483,5 MHz) à l'extérieur des bâtiments, sur les propriétés privées ou le domaine privé des personnes publiques, avec une puissance limitée à 100 mW.

Le cas de l'INT est donc spécial, en effet, si on souhaite connecter uniquement l'ensemble des élèves et des permanents, nous pouvons alors parler de groupe fermé d'utilisateur (GFU), et nous considérer comme un réseau privé.

Si nous voulons aussi permettre aux participants d'un colloque de se connecter, nous sommes alors entre le Hot spots et le réseau public, sachant qu'ils nécessitent l'attribution d'une licence. Après discussions avec Céline Chérifi, travaillant auprès de l'ART sur l'attribution des licences publiques expérimentales WI-FI, il s'avère que l'INT en permettant l'accès à Internet à des personnes extérieures au G.F.U entre dans le cadre d'un réseau public. En effet, selon elle, le fait que l'INT partage l'accès du G.F.U avec un public extérieur fait sortir l'INT du cadre juridique d'un hot spot.

Une solution

Après plusieurs entretiens avec des membres de l'ART (Céline Chérifi et Daniel Quintin), la solution légale la plus simple serait de présenter le déploiement du WI-FI sur l'INT comme la superposition d'un réseau privé (ayant un Groupe fermé d'utilisateur) et d'un Hotspot.

L'INT s'intègre sans problème dans le cadre juridique du réseau privé. En effet on peut considérer la population des élèves, des permanents (enseignants et chercheurs) et l'administration comme un groupe fermé d'utilisateur.

La notion de G.F.U reste encore très floue au niveau juridique. Les difficultés rencontrées pour déterminer un G.F.U reposent sur l'appréciation portée sur la définition d'un groupement fermé d'utilisateurs (G.F.U.) ; celui-ci est entendu comme un groupe qui repose sur une communauté d'intérêt suffisamment stable pour être identifiée et préexistante à la fourniture de service de télécommunications. On comprend bien alors que se pose pour le législateur dans la pratique le problème des limites du rôle d'un G.F.U. : limites quantitatives relatives au nombre d'utilisateurs potentiels, limites relatives à la connexion de plusieurs G.F.U. entre eux. Les dispositions législatives et réglementaires en vigueur sont génératrices de flou sur ces points ; ceux-ci sont examinés, cas par cas, par l'ART avec un esprit de large ouverture et ce d'autant plus que la loi de réglementation a strictement encadré les motifs de refus d'autorisation, tant en ce qui concerne les réseaux ouverts au public, que la fourniture des services au public ou que les réseaux indépendants.

Le groupement fermé d'utilisateurs de l'INT entre tout à fait dans cette définition à travers les chartes signées par les utilisateurs du réseau.

En ce qui concerne l'accès Internet sans fil pour les extérieurs au G.F.U de nombreux problèmes se posent comme nous l'avons vu précédemment. La solution la plus simple dans un premier temps est de déposer une demande de licence Hotspot. Céline Cherifi nous a conseillé de lui envoyer le dossier dans un premier temps, elle pourra alors nous donner un premier avis global, et en cas, nous aider à le reformuler pour rentrer dans les critères et de s'assurer de la bonne formulation de cette demande. Le risque étant en effet que l'Autorité n'accepte pas qu'un G.F.U partage sa connexion avec des extérieurs.

En cas de refus, la dernière solution serait alors de se munir d'une licence publique expérimentale beaucoup plus difficile à obtenir. En effet le projet de développement du Wi-fi sur le campus de l'INT n'entre pas dans les priorités définies par l'Autorité que nous avons évoqué précédemment.

2.4.3 Recommandations

Même si il est probable que l'usage fait aujourd'hui des RLAN (dans les limites de la loi) détermine en partie la législation à venir, l'INT se doit d'être en accord avec la loi.

La législation actuelle peine à rattraper le développement technologique et commercial du Wi-Fi, c'est pourquoi il n'existe pas encore de réel cadre pour des déploiements comme celui souhaité par l'INT et de plus beaucoup d'installations se font en désaccord avec la loi.

Il faut aussi tenir compte de l'évolution annoncé des textes, en se basant à la fois sur les futurs textes européens, et sur les leçons tirées des différentes expérimentations. Le cadre définitif en France devrait apparaître d'ici 24 mois.

Ainsi, la solution proposée d'un réseau privé couplé à un Hotspot est la meilleure solution actuelle. Avant tout déploiement, Il faudra prendre contact avec l'ART pour se tenir à jour avec la loi, et particulièrement Céline Cherifi qui accepte de prendre du temps pour étudier notre dossier avant de faire la demande.

Chapitre 3

Etude des méthodes de sécurisation

Introduction

Quels que soient les réseaux considérés, il existe toujours trois critères essentiels auxquels il faut s'intéresser : la disponibilité (capacité à délivrer le service), la fiabilité (capacité à assurer la continuité du service) et la sécurité (protection des données échangées, confidentialité).

Pour que le fonctionnement du réseau soit performant il ne faut négliger aucun de ces trois points. Nous nous sommes principalement intéressés à la sécurité des réseaux, mais il est évident que ces trois paramètres sont intimement liés.

Un système d'informations peut être soumis à différents types d'attaques : les catastrophes naturelles, les accidents, et les malveillances. Le rôle des personnes en charge de la sécurité est d'évaluer les différents risques pour le système, et de chercher des solutions permettant leur neutralisation. Si ce point est négligé, cela peut avoir un coût énorme pour l'utilisateur du système. Dans le cas des entreprises, un dysfonctionnement du réseau ou une intrusion extérieure malveillante peuvent causer une immobilisation des services ou de la production, la destruction de fichiers essentiels (comptes, base de données clients, etc.), entre autres. Dans le cas de l'INT, on peut imaginer qu'un piratage du réseau de l'école permettrait au cyber-délinquant de modifier (par exemple) les fichiers des élèves (notes, données d'état civil), ou les cours en ligne, bref, de causer de graves dysfonctionnements dans l'activité de l'école.

Malgré son importance capitale, la sécurité des réseaux n'est pas le domaine le plus médiatique de ce secteur. Pour une raison simple : on a tendance à sous estimer le nombre d'attaques ou de violations des services, pour la bonne et simple raison que les victimes ne s'en vantent pas, car cela serait avouer qu'il existe une faille dans leur réseau. Mais il ne faut pas se leurrer, les attaques sont beaucoup plus fréquentes qu'on ne le croit. Il faut aussi préciser que les techniques des pirates évoluant à une vitesse incroyable, il faut que les équipements de sécurité soient évolutifs. Il faut rester vigilant, même s'il est très difficile pour ne pas dire impossible de suivre les cyber-délinquants d'un point de vue technologique.

Le grand problème de la sécurité n'est pas uniquement de garantir l'inviolabilité d'un réseau. En effet, cela ne doit pas impliquer d'investissements trop importants, ni contraindre utilisateurs et administrateurs à des procédures lourdes et compliquées. Il s'agit de trouver un équilibre entre ces différents critères, en sachant à l'avance qu'un réseau n'est jamais parfaitement sécurisé.

3.1 Analyse des besoins et des risques

Avant toute tentative de resolution technique des problèmes qui nous occupent, il nous faut analyser les besoins des utilisateurs envisagés, et en déduire les risques résultants, en considérant les spécificités des réseaux sans fils.

3.1.1 Analyse des besoins et contraintes spécifiques

Ce qui doit le plus nous interpeller dans les besoins formulés, c'est la distinction entre deux types de population :

- Les personnes participant aux colloques, pas forcément connues à l'avance (mais filtrées à l'entrée, comme d'habitude, donc facilement listables)
- Les personnes internes à l'INT, clairement identifiées par l'intermédiaire de leur compte MCI.

Ces deux types d'utilisateurs ont bien entendu des besoins spécifiques et différents en terme d'accès aux ressources, de confidentialité et d'authentification.

Il y aura tout d'abord des ressources réseau mises à la disposition des personnes non membres de l'INT, comme les participants à des colloques ayant lieu dans le cadre de l'école.

L'idée serait de les laisser accéder aux services de base que sont l'accès à Internet (http, https), et le courrier électronique (smtp, pop3, imap) en leur interdisant l'accès au reste. Ils n'ont par exemple pas besoin d'un accès au réseau local, ni d'un accès ftp extérieur. On part du principe que ces personnes se contenteront des deux services cités précédemment.

Il n'existe pas de gros besoin de confidentialité dans ce cas, les données échangées n'étant ni particulièrement sensibles pour leur utilisateur, ni vitales pour le fonctionnement de l'école. Un mécanisme de

cryptage de données n'est donc pas prioritaire. On peut envisager de faire signer aux usagers précités une charte de comportement (prolongement de la charte MCI).

Les demandes des permanents de l'INT, des vacataires et des élèves sont plus grandes. Ces personnes souhaitent, en plus des services évoqués précédemment, accéder aux voisinages réseau, aux serveurs des départements ainsi qu'à d'autres services.

On constate qu'ici, on devra développer une infrastructure beaucoup plus sécurisée. Même si le besoin de confidentialité n'est pas beaucoup plus élevé que pour le réseau précédent, il va en revanche falloir accentuer le processus d'authentification. En effet, le réseau fonctionnera avec les comptes MCI (comme pour le réseau filaire actuel), qui se caractérisent par un ensemble login/mot de passe spécifique à chaque utilisateur.

Dans tous les cas ces deux types d'utilisateurs seront soumis aux mêmes risques, les réseaux étant souvent soumis aux mêmes genres d'attaques.

3.1.2 Attaques auxquelles un réseau informatique est exposé

Outre les pannes de matériel, on peut classer les différents risques en plusieurs catégories :

- **Inondation** : engorgement du réseau nuisant à son fonctionnement, jusqu'à empêcher tout son fonctionnement. Il peut être involontaire, en cas de fortes demandes simultanées des utilisateurs ou consciemment provoqué par des utilisateurs (déni de service).
- **Intrusion** : consiste à profiter d'une faille d'un serveur pour s'introduire sur une machine avant de modifier son fonctionnement ou de profiter de cette machine pour en attaquer d'autres. L'attaquant peut installer sur la machine une porte d'accès lui permettant de revenir (backdoor), ou simplement chercher à détruire les informations qu'il contient (bombe logique).
- **Ecoute (sniff)** : consiste à écouter les données qui circulent sur le média afin de récupérer des informations potentiellement utiles (mots de passe ...) . Si ces données sont cryptées, il faudra les décrypter (cassage de clef par force brute ...) avant qu'elles ne soient exploitables.
- **Usurpation d'identité / vol de sessions** : consiste à profiter des faiblesses de protocoles pour se faire passer pour un autre utilisateur, et donc de profiter de ses droits.
- **Programmes "nocifs" (virus, vers)** : programmes infectant des fichiers exécutables et se diffusant au travers un réseau en se reproduisant.

Ces attaques sont les plus communes, et s'appliquent a tous les réseaux de données. Elles font partie des risques à envisager, meme si, du fait des specificiés des reseaux sans fil, il vient s'en greffer de nouvelles.

3.1.3 Les failles spécifiques au Wifi

Brouillage et saturation

Le wi-fi étant un média partagé, cela le rend d'autant plus sensible aux attaques et aux interceptions. Il existe deux types de normes pour le Wi-fi, qui utilisent des fréquences d'émission différentes : la norme 802.11a utilise la fréquence de 5Ghz, alors que la norme 802.11b utilise la fréquence 2.4Ghz. Mais dans les deux cas, c'est une fréquence fixe, et la bande passante est limitée pour les deux (54Mbits/sec pour le 802.11a, et 11Mbits/sec pour le 802.11b), et il est donc aisé de saturer le réseau par des émissions parasites. Une antenne pirate peut ainsi émettre sur les fréquences précédemment citées pour créer des interférences et brouiller le signal. Cette menace est à prendre au sérieux, puisqu'une antenne pirate est facile à mettre en place. Il est cependant possible de détecter ce genre d'émissions.

Detournement de trafic

Un autre problème posé par le fait que le Wifi utilise un média partagé est la possibilité de détournement du trafic. En effet, il suffit à quelqu'un d'installer une antenne redirectrice aux limites du domaine de couverture pour détourner le trafic vers un autre endroit, et monopoliser la bande passante. L'installation d'antennes relais tout comme l'installation d'antennes émettrices de trop forte puissance sont des dangers spécifiques au Wifi.

Fragilité logistique

En dehors des failles spécifiques au caractère aérien du wi-fi, il nous faut penser qu'au point de vue logistique, celui-ci est très contraignant. En effet, il faut pour obtenir un réseau performant disposer des bornes (ou points d'accès) assez régulièrement, et ces équipements doivent impérativement être protégés (des vols, des dégradations diverses,...). En effet, ils représentent les nœuds du réseau wi-fi et sont par conséquents indispensables à sa bonne marche. Il faudra donc réfléchir à des solutions de protection des bornes (mise en hauteur, couverture par une gaine, installation à l'interieur d'une armoire scellée)

Un algorithme de cryptage peu performant : le WEP

Une autre faille d'importance dans le Wifi se situe au niveau du WEP. Cet algorithme de cryptage des données, utilisé dans le wi-fi (norme 802.11) présente un gros défaut de conception qui sera vu plus en détails dans la partie suivante.

Toutes ces failles font qu'un réseau wi-fi est encore plus fragile qu'un reseau filaire, donc plus difficile a proteger. Il nous faut reflechir à tous les risques encourus dans le cadre d'une telle installation, et decider pour lesquels nous devront appliquer un traitement prioritaire.

Nous avons donc pour l'instant listé les differents dangers qui guettent notre réseau. Il nous reste à décrire par quoi ces attaques se traduisent-elles en terme de gênes pour l'utilisateur ou l'administrateur

3.1.4 Risques encourus

Les attaques d'intrusion et par virus visent les clients et serveurs, l'utilisation de Wi-Fi n'introduit donc pas de failles de sécurité.

L'attaque par congestion

- brouillage des fréquences par un émetteur pirate pour empêcher les utilisateurs d'accéder aux bornes d'accès.
- Flood des machines et/ou équipements présents sur le réseau. Conte tenu de la bande passante accessible à chaque client Wi-Fi, il faut coordonner l'action de nombreux attaquants pour arriver à perturber un réseau. Cette attaque présente donc peu de risques.

Ecoute

Les faiblesses du protocole WEP font qu'il est facile de décrypter les données captées (des programmes automatisant la procédure existent)

Voici le tableau de classification des risques encourus :

Attaque	Difficulté à mettre en œuvre	Difficulté à contrer	Dégâts possibles	Probabilité	Evaluation du risque couru
Congestion	++	+++	++	+	+
Intrusion	++/+++	++	+++	+	+/+++
Ecoute	+	++	++	+++	+++
Usurpation d'identité	+++	++	++	+	+
Virus...	++	+	+++	++	+

FIG. 3.1 – Risques encourus par le Wep

3.2 Technologies permettant d'établir un niveau de sécurité

De nombreuses technologies conçues pour améliorer la sécurité des réseaux sont utilisables dans le cas de ce reseau Wi-Fi.

3.2.1 Charte

interêt

Le point faible de tout réseau informatique réside plus dans le facteur humain que dans les solutions techniques mise en place. En effet, il est bien plus simple pour un pirate de se procurer le mot de passe et le login d'une personne négligeante plutôt que de s'introduire sur un réseau en essayant de forcer les défenses techniques en place. En outre, de nombreux malfaiteurs agissent par jeu ou défi, il est donc important de prévoir des sanctions à leurs égards.

Les utilisateurs sont la plus grosse faille existante de tout système. Lorsque l'on désire déployer un réseau WI-FI, il est important d'intégrer cette remarque et de se demander quelles sont les règles de bonne conduite, les chartes qui engagent la responsabilité des utilisateurs à mettre en place pour assurer un niveau de sécurité acceptable.

Ainsi quelque soit la solution technique adoptée, les utilisateurs réguliers ou marginaux du réseau seront sensibilisés et conscients de ce qui est permis et de ce qui ne l'est pas. La signature d'une charte est nécessaire pour éviter tous les problèmes liés à la négligence des utilisateurs. Elle permet également de rejeter la responsabilité d'un acte malveillant ou inconscient sur l'utilisateur plutôt que sur l'organisme qui gère le reseau.

Plus concrètement, un utilisateur marginal se connectant lors d'un colloque à l'internet se doit de respecter la charte RENATER qui interdit certaines pratiques sur le WEB (comme l'usage de logiciels de peer to peer).

Charte

Une charte existe déja à l'INT pour les élèves et le personnel. Il serait bon de l'adapter pour les participants aux colloques.

Cette charte précise pour l'instant les conditions d'accès aux ressources informatiques, la confidentialité des informations, les droits de propriétés et de licences de logiciels, l'utilisation des ressources informatiques, l'utilisation d'INTERNET et de RENATER, des règles particulières et un aperçu des sanctions applicables.

Pour un réseau Wifi qui serait ouvert lors de colloques, certaines modifications doivent être apportées :

- **Conditions d'accès aux ressources** : Les participants aux colloques ont accès à l'INTERNET exclusivement et uniquement pendant la durée du colloque.
- **Confidentialité des informations** : Il est interdit de tenter d'intercepter les communications, ainsi il est interdit sur un réseau Wifi de sniffer le trafic ou de tenter tout autre démarche visant à intercepter des données qui ne sont pas destinées à l'utilisateur.
- **Droits de propriété et de license des logiciels** : Chaque intervenant est responsable de sa machine et des logiciels présent sur cette dernière. Il n'est pas possible de copier des logiciels compte tenu de l'accès disponible pour l'intervenant (WEB exclusivement).
- **Utilisation des ressources informatiques** : Rien à changer.
- **Utilisation d'Internet et de RENATER** : La charte RENATER doit être respectée (préciser le lien vers cette charte).
- **Règles particulières** : Il est interdit de brouiller les communications en emettant des signaux parasites. Il est également interdit de créer un autre access point que celui présent à l'Institut.

3.2.2 Limitation d'accès (firewalling)

L'utilisation d'un firewall permet de limiter les services disponibles aux utilisateurs en fonction de l'adresse du serveur qui le gère et du port TCP à contacter. Une politique de sécurité efficace consite à

bloquer tous les ports et adresses possibles en créant des exceptions pour les services que l'on veut rendre disponibles.

3.2.3 Cryptage

Le cryptage permet, à l'aide d'un mécanisme de clés publiques ou privées, de garantir la confidentialité des données échangées en faisant en sorte que seuls les propriétaires des clés adéquates soient en mesure de décrypter un message. De tels procédés doivent accorder un soin particulier au traitement des clés, qui ne doivent être ni trop faciles à deviner ni susceptibles d'être écoutées par un tiers.

le WEP

Le WEP (Wired Equivalent Privacy) est le protocole de sécurité standard offert par la norme 802.11B. Il permet de crypter les données à l'aide d'une clé de 64 ou 128. Mais en réalité, ces clés contiennent un vecteur d'initialisation (IV) de 24 bits ce qui réduits les clés précédentes à 40 et 104 bits repsectivement. Ce cryptage est basé sur l'algorithme RC4. Chaque terminal possède une clé secrète partagée. Avant d'être envoyé, un message est d'abord crypté à l'aide de la clé secrète : le générateur aléatoire (PRNG(RS4)) est initialisé à l'aide du vecteur d'initialisation et génère ainsi une clé aléatoire. Celle-ci est appliquée au message à envoyer à l'aide de la fonction XOR, ce qui nous donne le texte crypté (Cyphertext). La trame émise est donc composée de ce cyphertext accompagné du vecteur d'initialisation correspondant.

Ainsi le WEP offre d'indéniables avantages en protégeant d'attaques simples et permet l'authentification sécurisée ainsi que le cryptage des transmissions. De plus il existe des modes d'authentification.

D'un coté, l' « Open System » est idéal pour les conférences, ou les bornes d'accès publiques, car il n'est pas sécurisé et aucun échange de clé n'est nécessaire : seule la connaissance du SSID permet la connexion, SSID qui est en permance diffusé en clair dans des trames appellées Beacons.

De l'autre, le mode « Shared Key », plus intéressant, se base sur un système de clé secrète partagée. La station qui désire se connecter au point d'accès (AP), lui envoie une requête d'authentification . L'AP en retour, lui envoie une trame de 128 bits d'un texte aléatoire, à laquelle la station doit renvoyer une trame d'authentification contenant le texte crypté à l'aide de sa clé secrète partagée. Par la suite, l'AP décrypte le texte et le compare au texte envoyé initialement. Si le texte a été crypté correctement, cela signifie que la station a la bonne clé secrète partagée, et elle est donc authentifiée.

En effet, ce protocole a récemment fait l'objet d'attaques opérationnelles qui ont montré que dans sa forme initiale, ce protocole n'est absolument pas sûr.

Tout d'abord, une attaque lors de l'authentification peut être effectuée : il suffit d'écouter le message de test envoyé en clair à la station désirant s'identifier ainsi que le message crypté renvoyé au point d'accès. En appliquant la fonction XOR et un certain algorithme au deux messages, on peut retrouver la clé.

Ensuite, une autre attaque passive utilise uniquement les paquets chiffrés inteceptés, en écoutant le réseau et en stockant dans une table chaque IV associé à sa clé, pour pouvoir ainsi déchiffrer tous les autres messages transitant par ce réseau.

Ainsi si le WEP ne garantit pas une sécurité parfaite, il doit quand même être utilisé (car il assure un protection minimale et il est gratuit) mais être associé à d'autres protocoles de sécurité, comme le VPN (Virtual Private Network) et un système d'authentification et autorisation RADIUS (Remote Access Dial-Up User Service).

EAP

L'EAP-TLS (Extensible Authentification Protocol Transport Layer Security) est une propriété définie dans la norme IEEE 802.1x (norme de l'IEEE permmetant la mise en place de procédures d'authentification).

L'EAP-TLS permet de parer à l'une des plus grandes failles du WEP qui utilise une même clé de chiffrement dans tout le réseau, ce qui rend le réseau vulnérable. Tandis que l'EAP-TLS permet à l'issue de la procédure d'authentification, de générer dynamiquement une clé de chiffrement propre à la station qui vient de s'authentifier. Cette clé est ensuite utilisée pour chiffrer les transmissions entre cette station et le point d'accès. Un renouvellement périodique et automatique des clés peut être demandé.

Cette voie ne garantit certes pas une sécurité absolue, mais elle rend les attaques plus difficiles grâce au changement régulier des clés.

A l'heure actuelle, trop peu de machines clientes sont dotées du système EAP-TLS, qui n'est d'ailleurs compatible qu'avec Windows XP ou Xsupplicant (Linux). Il n'est donc pas envisageable pour l'instant d'implémenter EAP dans notre réseau. Mais, 802.1x étant devenue une norme IEEE depuis peu, la fonctionnalité EAP devrait se standardiser aussi bien sur les machines clientes que sur les bornes d'accès.

3.2.4 Authentification

Pouvoir procéder à l'authentification sûre d'un utilisateur est un élément indispensable de la sécurité d'un réseau, qui permet à chaque utilisateur d'accéder aux services auxquels il a droit, et à aucun autre. L'authentification par adresse MAC (adresse physique de la carte Wi-FI du client) n'offre pas de sécurité puisqu'il est possible de changer l'adresse de nombreuses cartes.

Pour combler ce problème, d'autre protocoles existent, parmis lesquels le Radius.

RADIUS (Remote Authentication Dial-In User Service) est un protocole normalisé qui fournit des services d'authentification, d'autorisation et de gestion des comptes pour l'accès réseau à distance. Un client RADIUS, généralement un serveur d'accès réseau à distance utilisé par un fournisseur de services Internet (ISP, Internet Service Provider), envoie des informations concernant l'utilisateur et la connexion à un serveur RADIUS. Le serveur RADIUS authentifie et autorise la demande du client RADIUS.

On peut appliquer ce protocole pour notre WLAN en traitant les demandes de connexion comme une connexion à distance. Au départ développé pour les dial-up remote access, RADIUS peut être maintenant utilisé par les bornes d'accès.

RADIUS n'est pas sans failles. Mais la majorité de ses failles sont davantage liées à la configuration du serveur RADIUS qu'au protocole lui-même. Cependant RADIUS est très répandue, car c'est la meilleure solution pour l'authentification, en particulier lorsqu'elle est combinée avec EAP.

3.2.5 VPN

VPN (Virtual Private Network) est un protocole destiné à autoriser un client à accéder à un serveur ou à une application distante, en passant par des réseaux dans lesquels la sécurité n'est pas assurée mais en offrant un bon niveau de sécurité de bout en bout.

Pour offrir un tel service, il faut mettre en place une association de sécurité entre le client et le serveur de façon à authentifier les deux entités de l'association puis à créer un chemin sécurisé entre les deux entités au travers d'un réseau non sûr.

Le VPN consiste à mettre en place un chemin privé virtuel sécurisé appelé tunnel entre le client et le serveur. Chaque entité est identifiée et les données sont cryptées par la mise en œuvre du procédé d'encapsulation.

Les protocoles de VPN les plus répondus sont PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), IPSec.

Si l'on souhaite assurer au sein d'un réseau local sans fil la confidentialité des transmissions et le contrôle d'accès, on devrait obtenir une architecture où chaque paire de stations souhaitant communiquer doit bâtir un tunnel sécurisé. Mais il est difficile de mettre en place une telle architecture. Pour simplifier, tout en garantissant un bon niveau de sécurité, il faut obliger une station souhaitant se connecter à établir un tunnel avec une passerelle avant de pouvoir communiquer avec le reste du réseau.

Cette configuration du réseau permet de déployer des bornes assurant des fonctions de base, sans pour autant remettre en cause la sécurité puisque tout est contrôlé au niveau de la passerelle.

De plus il serait intéressant de séparer physiquement le réseau local qui supporte les points d'accès de celui du réseau principal pour garantir une sécurité maximale, ainsi on limiterait les points d'attaque possible.

Du point de vue de l'architecture, une solution basée sur de l'EAP / radius necessite l'utilisation de bornes d'accès compatibles avec ces protocoles, alors qu'une solution basée sur du tunneling VPN peut se contenter de bornes d'accès plus simples, mais necessite en plus l'utilisation d'une passerelle.

3.3 Description d'une solution de sécurité

L'analyse des besoins exprimés par les utilisateurs potentiels d'un réseau wi-fi sépare clairement deux populations aux besoins disctincts :

- des personnes de passage, qui ont essentiellement besoin d'un accès web et mail. En outre, comme ces personnes ne sont pas clairement identifiées, il est necessaire de s'assurer qu'elles ne puissent avoir accès à des serveurs privés.
- Des internes (enseignants, permantents, élèves), qui, en plus d'un accès web et mail souhaitent pouvoir profiter des voisinages reseaux et accéder aux serveurs des départements (en fonction des services auxquels ils ont droit)

La facon la plus simple de répondre aux besoins de ces deux populations est de créer deux reseaux distincts. Le premier, ouvert, ne laisse accès qu'à un nombre restreint de services, alors que le deuxième nécessite une authentification mais accorde la possibilité d'accéder à des services plus étendus.

Pour disposer de deux types d'accès, l'un libre et l'autre sécurisé la norme Wi-fi ne nous laisse d'autre choix que de réaliser deux réseaux Wi-fi distincts.

3.3.1 Un réseau ouvert

Topologie du réseau :

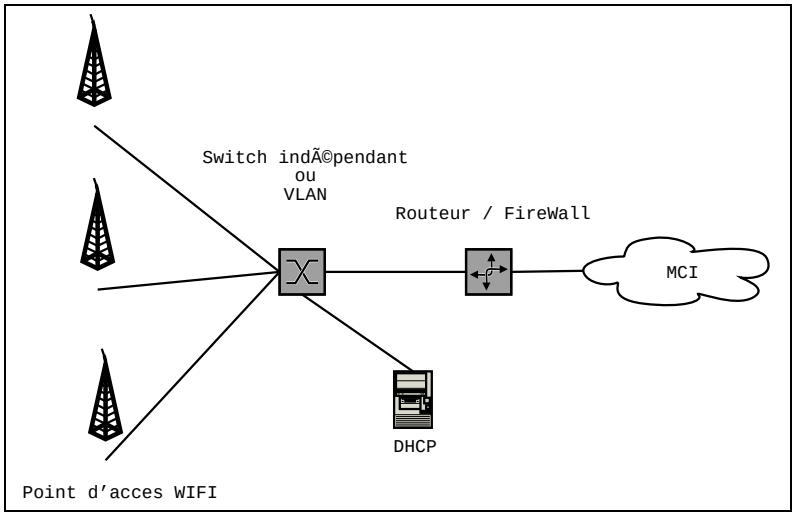

FIG. 3.2 – Architecture d'un réseau ouvert

Les points d'accès Wi-fi devront être connectés sur un réseau ethernet indépendant du réseau de l'INT, en utilisant soit des VLANs (réseaux virtuels), soit du matériel indépendant.

Attribution d'adresse IP :

Les postes Wi-fi se verront attribuer des adresses IP dans l'un des sous réseaux dont dispose l'INT. Il s'agit d'adresses IP publiques ce qui permet de réduire les coûts en évitant le déploiement d'un serveur proxy ou d'un NAT.

Un serveur DHCP devra donc être configuré pour cette zone. Il est important de noter que si celui ci est placé derrière le Firewall ou le routeur, il faudra laisser passer les broadcasts DHCP à travers celui-ci (udp 67/68).

Securité Wifi basique :

Il est possible de limiter les accès sur ce réseau ouvert afin d'en restreindre l'utilisation aux personnes de l'INT et aux personnes autorisées.

Pour cela il suffit :

- d'activer le WEP.
- de désactiver le broadcast du SSID par la borne.

Ainsi une personne voulant se connecter au réseau doit disposer au minimum du SSID et de la clef WEP. Il est bien évident que cela n'apporte que peu de sécurité supplémentaire, néanmoins cela constitue une barrière basique et simple pour protéger un minimum ce réseau d'abus de personnes extérieures. De plus cette méthode est simple et rapide à mettre en œuvre et ne nécessite pas de configuration complexe ni des clients, ni des points d'accès.

Enfin pour augmenter éventuellement la sécurité, il est possible de procéder à une rotation des clefs à intervalles prédéterminés sans grand désagrément pour les utilisateurs.

Restriction des services disponibles :

La limitation des services disponibles se fera quant à elle par l'utilisation d'un Firewall et/ou de règles de filtrage IP d'un routeur.

En effet le but du réseau ouvert est de permettre aux internes et extérieurs (colloques) d'avoir accès aux principaux services de base (HTTP,MAIL). Néanmoins il n'est pas question de leur permettre d'avoir accès a plus de ressources , ni de pénétrer le réseau interne de l'INT. Par conséquent les services et ports que le routeur et/ou le Firewall devront laissés passer sont :

- 80/tcp http
- 8080/tcp http/proxy
- 443/tcp https
- 25/tcp smtp
- 110/tcp pop-3
- 143/tcp imap2
- 443/tcp https
- 993/tcp imaps
- 995/tcp pop3s

Ce routeur devra être considéré comme externe au réseau interne de l'INT et connecté en conséquence.

Attention : Le FireWall ou routeur devra aussi se charger d'empêcher les clients du réseaux Wi-fi ouvert de se connecter à la banque d'abonnement de la bibliothèque. Cette restriction est dûe à la méthode utilisée par ces sites pour identifier les connections (Contrôle sur l'IP).

Il est également intéressant de prévoir un accès FTP (21/tcp) ou Telnet (23/tcp) depuis une machine d'administration de l'INT afin de pouvoir configurer les bornes Wi-fi à l'aide de scripts plutôt qu'à travers l'interface HTTP des bornes.

3.3.2 Le réseau sécurisé

Topologie du réseau

Les points d'accès Wi-fi devront être connectés sur un réseau ethernet indépendant du réseau de l'INT. Celui-ci devra aussi être indépendant du réseau Wi-fi ouvert, en utilisant soit des VLANs, soit du matériel indépendant. Contrairement au cas précédent, cette méthode n'est pas seulement utilisée pour la sécurité, mais destinée à faciliter le roaming.

Sécurité Wifi avancée

Il est primordial de sécuriser l'accès au réseau sécurisé dès le client et le point d'acces. Pour cela on utilisera les fonctionnalités de sécurité de la couche 802.1x si on utilise la norme 802.11b ou 802.11g non certifiée et les fonctionnalités de la couche 802.11i si on utilise la norme 802.11g CERTIFIE.

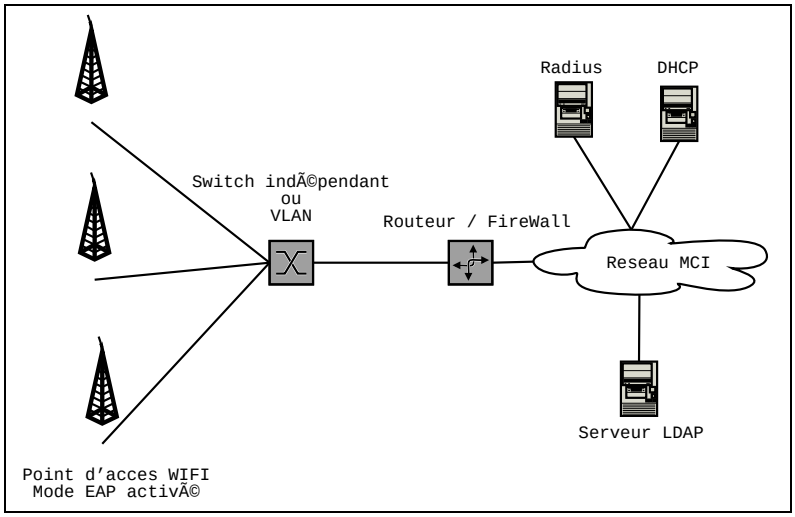

FIG. 3.3 – Architecture d'un réseau fermé

De plus les points d'accès doivent être compatibles EAP-TLS. Cette configuration technique nous permet d'utiliser un serveur RADIUS pour autoriser la connexion de clients aux points d'accès Wifi, ainsi que l'échange de clefs de cryptage de session entre le point d'accès et le client.

L'application simultanée de ces deux concepts permet d'obtenir un réseau sûr dans la mesure où seul les utilisateurs dûment authentifiés sont autorisés à se connecter aux bornes sécurisés.

Et que toutes les transmissions entres le client et le réseau sont chiffrées.

En toute logique, on pourrait donc intégrer ces bornes directement sur le réseau interne de l'INT. Néanmoins cette solution n'est pas retenue pour deux raisons :

- cela complique le Roaming : Nécessité d'implanter un protocole de routage type Mobile IP à cause des changements de sous réseaux.
- cela crée un risque concernant la sécurité : Durant les tests avec l'une des bornes prêtées par le département RST, celle-ci s'est ré-initialisée suite à un problème électrique et toutes les fonctions de sécurités furent désactivées (configuration par défaut).

Pour ces deux raisons il est préférable de créer un réseau ethernet spécial pour le Wi-fi sécurisé, disposant de son propre plan d'adressage IP (sous réseau dédié) ce qui permettra de faciliter le roaming, les bornes Wi-fi se comportant comme des ponts de Couche 2, et de mettre en place des règles de FireWall supplémentaires, dans la mesure où l'on ne peut pas faire totalement confiance à ce sous réseau.

Ces règles supplémentaires restent à définir et doivent faire l'objet d'un audit de sécurité plus poussé afin de définir les domaines et services réellement sensibles et nécessitant des mesures de sécurité particulières par rapport au Wi-fi.

Déploiement :

Actuellement le déploiement de ce réseau s'avère quelque peu complexe. En effet les produits conformes avec les normes 802.11g et i ne sont pas encore très répandus sur le marché. Le support de ces normes par les matériels clients (carte Wi-fi) reste encore partiel et complexe. Les clients supportant actuellement de façon opérationnelle l'authentification EAP sont :

- Windows XP
- Linux et la famille des *BSD (xsupplicant)
- Le support pour les autres OS ne semble pas encore mature.

Néanmoins la norme devrait se stabiliser d'ici juillet 2003. Les grands fabricants et Microsoft ont déjà annoncé la disponibilité de client EAP-TLS avec leurs produits, voir la possibilité d'upgrader les bornes existantes (ex : CISCO).

En plus de cet actuel mauvais support par les clients, le déploiement de l'EAP-TLS implique la distribution de clés de certification à chaque client. Cette procédure peut s'avérer complexe et fastidieuse si elle n'est pas convenablement pensée. Une étude supplémentaire est nécessaire quand à la méthode de distribution de ces certificats, le problème n'étant pas de les générer mais de les distribuer aux clients de façon sure et simple. Ce qui n'est pas un problème technique mais humain, la procédure d'installation des clefs restant quelque peu complexe pour des utilisateurs novices même lorsqu'elle est bien documentée.

3.3.3 VPN

Compte tenu des contraintes d'utilisation liées au VPN, la solution proposée ci dessus, à base d'authentification radius, semble préférable. Une soilution à base de VPN peut cependant être également étudiée.

3.4 Protection assurée par les mesures proposées

On peut globalement estimer l'efficacité des mesures proposées :

	Inondation	Intrusion	Ecoute	Usurpation d'identité / vol de sessions	Virus...
Réseau ouvert	Faible	Bonne	Faible	Faible (WEP désactivé) / Moyenne (WEP activé)	moyenne
Réseau privé	Faible	Bonne	Faible (sans EAP) / Bonne (avec EAP)	Bonne	moyenne

FIG. 3.4 – Efficacité des méthodes de sécurisation

Cependant, de telles estimations à priori necessitent d'etre validées par un ensemble de tests.

Mais il existe aussi un certain nombre de logiciels capables de hacker les serveurs, en décrivant le processus de piratage, détectant ainsi les failles et erreurs de configuration éventuelles pour permetre aux administrateurs de les combler avant qu'un vrai pirate ne les exploite. Ces logiciels peuvent aussi tester les firewall, les passerelles, scanner les ports des serveurs, ou sniffer les données échangées sur le réseau. D'autres logiciels sont disponibles pour tester le cryptage WEP et la facilité avec laquelle un pirate peut être capable de casser ce code. Il est également possible de faire appel à un cabinet pour mettre en œuvre cette phase de tests.

3.5 Perspectives d'évolution et évolutivité du matériel

3.5.1 La norme 802.1x

De nombreux problèmes de sécurité sont présents dans la norme actuelle 802.11. Notamment au niveau de l'authentification et du transport des données. Le WEP est bien trop facilement craquable. Une nouvelle norme 802.1x, poussée par des constructeurs et des éditeurs de logiciels, se met en place actuellement et tente de résoudre ce genre de problèmes.

Cette norme distingue trois entités : le client, l'authentificateur et le serveur d'authentification. L'authentification se fera par un serveur RADIUS en utilisant le protocole EAP. Néanmoins même si cette technologie semble être la prochaine étape, puisque les constructeurs l'intègre aujourd'hui, des failles de sécurité existent encore et le recours au VPN sera encore nécessaire.

Ces failles viennent de la présence des deux protocoles 802.11 et 802.1x et permettent les attaques de type vol de session et usurpation d'identité (par attaque de type « man in the middle ».

L'arrivée de la norme 802.1x a permis de résoudre le problème lié au WEP présent dans le 802.11 mais n'est pas totalement sécurisée non plus. Pour avoir une sécurité totale il faudrait ajouter l'usage du VPN. Il serait bon d'investir dans du matériel supportant cette norme tout simplement parce qu'elle deviendra le standard. Mais il est certain qu'elle ne constitue pas une solution miracle.

3.5.2 Evolutivité des matériels

Comme il l'a été énoncé précédemment, les constructeurs ont tendance a adopter certaines normes avant qu'elles soient certifiées (par exemple la 802.11g, dans le cas de Cisco), ce qui pose deux problèmes.

Premièrement, on se retrouve face à de gros problèmes de compatibilité entre les équipements des différents constructeurs (tant qu'une nouvelle norme n'aura pas été clairement posée, la multiplication des différences continuera). On pourra donc se retrouver dans le cas ou un client muni d'un matériel du constructeur alpha ne pourra pas se connecter à notre réseau du fait que nos points d'accès fournis par le constructeur beta utiliseront une autre norme. Dans le cas du réseau ouvert que nous voulons mettre en place, il s'agit d'un probleme préoccupant.

Le deuxieme probleme qui doit nous occuper est l'evolution possible des matériels. Au moment de l'installation du réseau, il nous faudra investir dans un nombre important de points d'accès. Si, du fait de l'évolution des normes, ceux ci s'averent obsolètes dans les deux ans qui viennent, l'investissement consenti sera un sacrifice vain. Il nous faut donc faire très attention à l'évolution des décisions de l'IEEE, et décider avec soin de la date de mise en place de notre réseau, afin de s'assurer que la norme utilisée sera viable, ou que les équipements utilisés seront evolutifs.

Conclusion

Les reseaux Wi-Fi n'assureront jamais le même niveau de sécurité qu'un réseau filaire, cependant, il existe des protocoles qui permettent d'assurer une sécurité relative en fonction des besoins spécifiques au réseau. Dans le cas d'un déploiement de Wi-Fi sur l'INT, où il faut répondre à deux demandes différentes, il est necessaire de déployer deux réseaux à vocations distinctes. Il est possible d'assurer un niveau de sécurité suffisant sur un reseau ouvert, à condition de fortement limiter les services accessibles, et cela sans imposer de trop fortes contraintes sur l'utilisateur ou sur l'administration.

Un reseau fortement sécurisé et offrant les mêmes fonctionnalités que le reseau filaire est plus complexe à mettre en œuvre au vue des technologies normalisées au moment de la réalisation de cette étude, mais est actuellement réalisable. Cependant, de nouvelles normes en cours de développement devraient, dans un futur proche, faciliter la mise en œuvre de ce genre de réseaux. Il est donc conseillé d'attendre l'émergence de ces normes avant de réaliser un reseau sécurisé, d'autant plus que la demande des utilisateurs ne semble pas encore tout à fait mûre.

Chapitre 4

Plan de déploiement

4.1 Etat de l'art

Nous allons tout d'abord présenter les différentes normes qui existent (les normes standardisées et les non standardisées). Puis nous allons décrire de façon plus détaillée les principales normes qui existent actuellement. Enfin nous terminerons par expliquer la solution retenue en prenant en compte différents paramètres, à savoir : les résultats de l'étude des besoins, la sécurité, l'évolutivité.

A l'heure actuelle, quelques normes ont été développées et d'autres normes en cours de développement viennent s'ajouter à celles-ci afin de les améliorer sur différents critères. Nous allons donc présenter d'abord les principales normes existantes, puis les normes qui sont en cours de développement.

Les normes existantes sont les suivantes :

802.11	L'ancêtre du réseau sans fil, sur 2,4 GHz modulation DSSS (Direct Sequence Spread Spectrum) ou saut de fréquence (aucune norme imposée), d'un débit de 2 Mb/s et pratiquement pas inter opérable de constructeur à constructeur.
802.11a	historiquement le second projet de réseau Ethernet sans fil sur 5 GHz, disposant d'une bande passante physique de 54 Mb/s, mais dont la sophistication a fortement retardé l'industrialisation.
802.11b	premier réseau Ethernet sans fil inter opérable, sur 2,4 GHz, offrant un débit physique de 11 Mb/s (modulation DSSS, accès par CSMA/CA et détection de porteuse)
802.11g	adaptation d'ofdm aux réseaux 802.11b, mode "turbo". Haut débit (54 Mbit/s théoriques) sur la bande des 2,4 GHz apportant également les mécanismes de code de protection par redondance (PBCC). Norme en voie d'achèvement, prévu pour juin 2003.

FIG. 4.1 – Table des principales normes Wi-fi

Il existe des normes "additives" ou "améliorantes". Il s'agit des normes qui viennent se rajouter aux normes citées précédemment dans le but d'apporter diverses améliorations.

4.1.1 802.11a

Norme mise en place par l'IEEE, elle utilise elle aussi la bande de fréquence des 5Ghz, et utilise la même technique de multiplexage orthogonal que Hiperlan2. Cependant, ses performances sont loin d'être aussi bonnes, et si elle promet un débit théorique de 54 mbps, le débit réel atteint ne dépasse pas 18mbps.

Les systèmes de sécurité utilisés effectivement par les constructeurs sont soit basés sur la norme 802.1x de lEEE, soit sur le WEP, réputé comme particulièrement peu fiable. L'IEEE est en train d'achever de définir la norme 802.11e qui permettra d'apporter une qualité de service aux protocoles 802.11a 802.11e et 802.11g.

L'offre commence à se diversifier en France, même si elle reste nettement moins conséquente qu'aux Etats-Unis. Cependant les prix proposés restent bien supérieures aux matériels de la norme la plus utilisée actuellement, c'est-à-dire 802.11b.

4.1.2 802.11b

Présentation

Le premier standard international du LAN sans fil est le 802.11, il fonctionne dans la bande de fréquence ISM (2,4-2.4835 GHz en Europe). La réglementation Française impose une limitation de puissance d'émission à 100mW en utilisation interne ou en externe dans un domaine privé, si on se limite à la première plage de fréquences. Sinon, l'émission est limitée à 10mW.

Le standard 802.11b est une amélioration de la norme 802.11 (débits max. de 1 et 2 Mbit/s) qui permet d'atteindre deux vitesses supplémentaires 5.5 et 11 Mbit/s. L'architecture, les fonctions et les services de

802.11c	Complément de la couche MAC améliorant les fonctions "pont", reversé au Groupe de Travail 802.11d (Travaux suspendus).
802.11d	Adaptation des couches physiques pour conformité aux exigences de certains pays particulièrement strictes (essentiellement la France et le Japon) (travaux suspendus).
802.11e	Norme en voie d'achèvement apportant un complément de la couche MAC qui apporte une qualité de service (QoS) aux réseaux 802.11a, b et g. Par exemple, la transmission synchrone (voix)
802.11f	document normatif décrivant l'interopérabilité inter constructeur au niveau de l'enregistrement d'un point d'accès (AP) au sein d'un réseau, ainsi que les échanges d'information entre AP lors d'un saut de cellule (roaming). Norme en voie d'achèvement. Il s'agit donc de travaux sur le protocole Inter Access Point Protocol qui doit permettre aux points d'accès de dialoguer entre eux.
802.11h	Amélioration de la couche MAC visant à rendre compatible les équipements 802.11a avec les infrastructures Hiperlan2. 802.11h s'occupe notamment de l'assignation automatique de fréquence de l'AP et du contrôle automatique de la puissance d'émission visant à éliminer les interférences entre points d'accès (à ne pas confondre avec un asservissement de la puissance d'émission de l'AP en fonction de la force du signal du client, tel que c'est le cas pour le MMAC IsWan japonais). De plus, 802.11h gère une adoption des technologies DFS (Dynamic Frequency Solution) et TPC (Transmit Power Control), pour une conformité avec les normes Européennes.
802.11i	Amélioration au niveau MAC destiné à renforcer la sécurité des transmissions sur les bandes fréquences 2,4GHz (802.11b et 802.11g) et 5GHz (802.11a), et se en améliorant le protocole de cryptage WEP (Wireless Equivalent Privacy). Norme composée de nombreuses étapes de travail ne devant pas s'achever avant la fin 2003.
802.11j	Convergence des standards américain 802.11 et européen Hiperlan, tous deux fonctionnant sur la bande de fréquence des 5 GHz
802.1x	Sous-section du groupe de travail 802.11i visant à l'intégration du protocole EAP (authentification) dans les trames Ethernet (indépendamment de tout protocole PPP, contrairement aux accès RAS conventionnels). 1x permet l'usage d'un serveur d'authentification de type Radius

FIG. 4.2 – Tables des normes additives/améliorantes

base du 802.11b sont les même que le standard 802.11 car la révision b n'affecte que la couche physique, ajoutant seulement des débits supérieurs.

Principe de multiplexage

Au niveau de la couche physique la norme 802.11b, utilise la technique de signalisation en séquence directe appelé aussi DSSS (Direct Sequence Spread Spectrum).

Recouvrement et interférences

Les données sont transmises intégralement, sur un seul des trois canaux possibles, le fait de ne pouvoir utiliser que 3 canaux différents impose de faire un choix d'affectation des canaux, afin d'éviter tout recouvrement par des canaux trop proche afin d'éviter les interférences.
Pour palier au bruit on utilise une technique de codage 'chipping', chaque bit de données est converti en une série de motif de bits redondants appelés 'chips'. Cette technique de codage assure le contrôle d'erreur, et peut récupérer la majorité des erreurs sur le canal de transmission, ce qui minimise d'autant les demandes de retransmission. Ce qui fait que l'on peut dire que le protocole 802.11b est très robuste.

Avantages	Inconvénients
Moins cher que l'Hiperlan2	Débit réel décevant
QoS et sécurité bientôt fourni par 802.11e et 802.11i	Effectivement peu compatible avec 802.11b
Evolutif	

FIG. 4.3 – Avantages et inconvénients de la norme 802.11a

Débits

Le débit théorique est de 11 Mbit/s. En pratique, on atteint les 6 Mbit/s effectifs.

Technique d'accès

Accès par CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) et détection de porteuse. Le protocole CSMA/CA tente d'éviter les collisions en imposant un accusé de réception systématique des paquets (ACK), ce qui signifie que pour chaque paquet de données arrivé intact, un paquet ACK est émis par la station de réception.

Ce protocole CSMA/CA fonctionne de la manière suivante : la station qui souhaite émettre explore les ondes et, si aucune activité n'est détectée, attend un temps aléatoire avant de transmettre si le support est toujours libre. Si le paquet est intact à la réception, la station réceptrice émet une trame ACK qui, une fois reçue par l'émetteur, met un terme au processus. Si ACK n'a pas été détectée par la station émettrice (parce que le paquet original ou le paquet ACK n'a pas été reçu intact), une collision est supposée et le paquet de données est retransmis après attente d'un autre temps aléatoire.

CSMA/CA permet donc de partager l'accès aux ondes. Ce mécanisme d'acusé de réception explicite gère aussi très efficacement les interférences et autres problèmes radio.

Evolutivité

A l'heure actuelle la norme la plus utilisée est la 802.11b, mais cette norme arrive en fin de vie elle va très certainement être supplantée par la 802.11g qui offre des débits théoriques 5 fois supérieurs. Par contre une partie du matériel 802.11g est prévu pour rester compatible avec cette norme ce qui implique que la 802.11b devrait faire partie du paysage des réseaux sans fils pendant quelques années encore.

Avantages et inconvénients

Inconvénients :
La limitation du 802.11b à 3 fréquences « non recouvrantes » oblige l'administrateur à disposer des équipements utilisant une même bande parfois dans des périmètres forts proches les uns des autres, provoquant des risques d'interférences. Les réseaux 5 GHz, dont le 802.11a et Hiperlan2, disposent de 8 canaux « non recouvrant », ce qui permet d'éloigner le plus possible les points d'accès utilisant la même bande. Les risques de brouillages mutuels sont alors pratiquement inexistants. Cette norme ne permet pas de haut débit lorsque plusieurs utilisateurs utilisent le même point d'accès simultanément.

Avantages :
La norme 802.11b est entièrement définie par IEEE ce qui n'est pas encore le cas pour les autres. C'est la plus répandue et la moins chère actuellement ; elle est donc adaptée à une utilisation haut débit pour un faible nombre de personnes ou bas débit pour un nombre plus conséquent.

4.1.3 802.11g

La norme 802.11g étant une évolution de la norme 802.11b, nous ne détaillerons que les améliorations qu'elle apporte, ainsi que les avantages et les inconvénients de cette norme.

Les améliorations apportées
La norme 802.11g fonctionne dans la même bande de fréquence (bande ISM 2.4Ghz) que la norme 802.11b, elle présente le gros avantage d'avoir un débit plus élevé 52Mbit/s soit cinq fois plus que la norme 802.11b. La plupart des spécialistes pensent que d'ici la fin de l'année cette norme aura supplanté l'actuel 802.11b.

La bande de fréquence de la norme 802.11g étant la même que pour la 802.11b, la différence entre les deux se situe au niveau du codage. En effet la 802.11g utilise une technique de modulation à porteuses multiples appelée "OFDM" (Orthogonal Frequency Division Multiplexing). Le principe de cette technique est de multiplexer des signaux orthogonaux en fréquence, l'orthogonalité sert en suite à les démultiplexer facilement.

4.1.4 802.11i

Cette norme apporte des mécanismes supplémentaire pour améliorer la sécurité d'un système 802.11. Elle porte sur quatre directions :
- Intégration du standard IEEE 802.1x permettant de gérer l'authentification et l'échange de clés dans un réseau IEEE 802.11
- Gestion et création de clés dynamiques à partir d'une clé initiale
- Complémentation du WEP pour améliorer le contrôle d'intégrité de chaque paquet
- Utilisation dans la norme IEEE 802.11 du nouveau standard de cryptage AES (Advanced Encryption Standard) pour un chiffrement sûr.

L'intégration du standard IEE 802.1x à 802.11 va permettre de profiter de mécanismes d'authentification et de distribution de clés. Le standard 802.11 de 1997 utilise des clés statiques. L'obtention d'un bon niveau de sécurité passe par la gestion de clés dynamiques. Pour cela 802.1 utilise un nouveau protocole, TKIP, qui devrait fournir une meilleure protection.

4.1.5 Hiperlan 2

L'Hiperlan2 est une norme européenne mise en place par l'ETSI (European Telecommunications Standards Institute) parallèlement au 802.11a de l'IEEE, et ayant vocation à succéder au 802.11b, en utilisant la technique de multiplexage orthogonale OFDM lui permettant d'atteindre des débits théoriques de 54 mbps (megabits par seconde). C'est un système assez performant, puisqu'il attend en pratique des débits de 38 mbps, bien meilleurs que les débits effectifs du 108.11a (cf ci-dessous)

En terme de sécurité, l'hiperlan2 implémente une authentification individuelle avec une clé crypté par session, et supporte des procédures de cryptage comme le PKI. Il intègre également une gestion de la qualité de service (QoS) permettant le transfert audio ou video.

Cependant, peu de matériel est disponible à l'heure actuelle, d'une part car les fabriquants les plus importants sur le marché son Américain, et suivent donc plutôt les normes de l'IEEE (802.11a par exemple dans le même domaine de fréquence) ; et d'autre par parce que la législation permet encore difficilement d'émettre dans la bande des 5Ghz, utilisée par l'armée et en particulier par les radars. Et un certain nombre de constructeurs ont arrêté leur production à l'arrivée de la norme américaine 802.11a. Par ailleurs, la quantité produite étant faible, le matériel est cher, en particulier face à des technologies comme le 802.11a.

Avantages	Inconvénients
Débit réel excellent	Prix d'installation exhaustif
Bonne gestion de la sécurité	Peu de matériel disponible
Gestion de la QoS	Pas encore pleinement compatible avec les normes 802.11

FIG. 4.4 – Avantages et inconvénients de la norme Hiperlan 2

4.2 Les solutions retenues

Nous avons à notre disposition un large choix de normes. Nous devons choisir la norme qui répond le mieux à nos besoins. En premier lieu, nous souhaitons déployer un réseau sans fil à haut débit, ce qui nous donne une idée préalable de la norme à choisir. En effet, deux normes permettent actuellement de disposer d'un réseau sans fil à haut débit : la norme 802.11a et 802.11g.

Nous allons présenter les caractéristiques de chacune de ces deux normes, afin d'en élire une. Nous tenons à préciser que nous ne prenons pas en compte la norme 802.11i qui est toujours au stade expérimental et qui n'est pas encore normalisée.

4.2.1 La norme 802.11a : Haut Débit, Haute Capacité

En occupant la bande de fréquences des 5 GHz et en utilisant la modulation OFDM, la norme 802.11a fournit trois avantages par rapport à 802.11b. Tout d'abord, elle augmente le débit maximal par canal (il passe de 11 à 54 mbps). Ensuite, le nombre de canaux disponible pour la norme 802.11a est de 8 alors que leur nombre est de 3 pour les normes 802.11b et 802.11g. Enfin, la largeur de bande totale disponible pour la bande de 5 GHz est plus grande que celle pour la bande de 2.4 GHz, 83.5 MHz contre 300 MHz. Par conséquent, un réseau sans-fil basé sur 802.11a peut supporter un plus grand nombre d'utilisateurs haut débit simultanés sans risque de conflit.

Cependant, ces avantages ne vont pas sans contreparties en terme d'interopérabilité et de portée. Du fait qu'ils opèrent dans des bandes de fréquence différentes, les produits 802.11a et 802.11b ne sont pas compatibles. Par exemple, un point d'accès à 2.4 GHz (802.11b) ne fonctionne pas avec une carte réseau utilisant la norme 802.11a. Cependant, ces deux standards peuvent certainement co-exister. Ainsi, un utilisateur de 802.11a et un autre de 802.11b, se servant de points d'accès distincts connectés sur le même réseau local, peuvent opérer dans le même espace physique et partager les ressources du réseau (accès Internet, etc.).

En revanche, la portée des points d'accès 802.11a est moins importante que celle des 802.11b, du fait de la fréquence de fonctionnement élevée des produits 802.11a (5 GHz). On aura ainsi besoin d'un plus grand nombre de points d'accès 802.11a pour couvrir la même surface. Cependant, les tests montrent que les produits 802.11a maintiennent une performance d'environ 3 fois plus élevée que celle des produits 802.11b dans les environnements clos.

802.11g : Haut débit dans la bande des 2.4 GHz

Le standard 802.11g apporte les avantages de haut débit tout en maintenant une compatibilité avec les équipements existants de la norme 802.11b. 802.11g fonctionne dans la même bande de fréquence et avec la même modulation DSSS que 802.11b. Par contre, 802.11g ajoute une modulation OFDM aux débits élevés.

Ainsi, une carte réseau 802.11g pourra fonctionner avec un point d'accès 802.11b et un point d'accès 802.11g fonctionnera avec les cartes réseau 802.11b à des débits allant jusqu'à 11 Mbps. En revanche, pour profiter d'un débit de 54 Mbps, le point d'accès et la carte réseau doivent être tous deux des produits normalisés 802.11g.

L'inconvénient de 802.11g est sa plus petite capacité, à l'opposé de 802.11a, à servir un grand nombre d'utilisateurs de WLAN haut débit. La modulation OFDM autorise des hauts débits mais la largeur de bande totale disponible pour la bande de fréquence de 2.4 GHz reste la même car 802.11g est encore restreint à 3 canaux, contrairement aux 8 qui sont disponibles dans la bande de 5 GHz.

Choix d'une norme WLAN

La norme 802.11a offre beaucoup d'avantages par rapport à la norme 802.11g. Les 8 canaux non recouvrants de la norme 802.11a permettent un déploiement facile et souple des points d'accès. Les réseaux sans fils basés sur cette norme sont capables de supporter un grand nombre d'utilisateurs haut débit. Mais le grand inconvénient de cette norme est que ses équipements fonctionnent dans la bande de fréquence de 5Ghz. Ceci empêche la compatibilité entre les points d'accès basés sur cette norme et la majorité des portables qui existent actuellement sur le marché et qui sont équipés de cartes 802.11b. En revanche, la norme 802.11g assure cette compatibilité. La coexistence des utilisateurs équipés de cartes 802.11b et 802.11g sur un réseau 802.11g est tout à fait possible.

D'autre part, les deux standards 802.11b et 802.11a peuvent parfaitement coexister à condition d'installer des points d'accès 802.11b et des points d'accès 802.11a. L'inconvénient majeur de cette solution est qu'elle entraîne des charges supplémentaires considérables.

Nous optons donc pour la norme 802.11g qui permettent, avec une seule et unique infrastructure, la coexistence entre les produits 802.11b très répandus sur le marché et les équipement 802.11g.

4.2.2 Récapitulatif des besoins par population

L'INT envisage d'implémenter un réseau Wi-Fi sur son campus pour permettre aux élèves, aux permanents ainsi qu'aux visiteurs occasionnels de l'INT de se connecter au réseau et à Internet via leur ordinateur portable, ou leur PDA (*Portable Digital Assistant*). Nos collègues de l'équipe "besoin" ont cerné les envies et attentes des ces utilisateurs potentiels. Ces besoins ont été demandés pour les types d'utilisateurs suivants : les personnes de passage, les permanents, les élèves et la direction. Sous forme d'un questionnaire l'ensemble des besoins a été fixé pour chacun des types d'utilisateurs. Il en découle une liste de besoins et d'exigences sur le réseau Wi-Fi à créer pour chaque utilisateur :

- Les personnes de passage :
  - accès à Internet pendant leur passage a l'INT
  - accès a leur boite mail
  - interaction via Internet
  - échange de données via le réseau Wi-Fi
  - besoin de matériel facile d'utilisation
  - sécurité du réseau pour empêcher les abus
  - Haut Débit sur le réseau
- Les permanents :
  - facilité de connexion et d'utilisation
  - accès a leurs données via le réseau
  - sécurisation du réseau pour empêcher les abus
  - Haut Débit sur le réseau
- Les élèves :
  - accès aux ressources
  - besoin de matériel facile d'utilisation
  - mobilité accrue dans l'INT
  - Haut Débit
- La direction :
  - sécurité
  - qualité de service

  - 2 réseaux bien différents : l'un ouvert, facile d'accès mais fortement limité, l'autre complet mais sécurisé "au maximum"

On remarque que tous ces besoins sont sectorisés dans des lieux précis :
- Le forum
- Les salles de cours banalisées pour désengorger les salles TP, pleines ou fermées.
- Le foyer
- L'extérieur (en particulier la célèbre « butte au lapin »)
- La cafétéria
- La bibliothèque
- Le bâtiment F

En conclusion on peut voir que les besoins sont en général :
- Une facilité de connexion, d'accès aux données et d'utilisation.
- Un Haut Débit en fonction des services ou accès proposé.
- Une sécurité très efficace pour interdire les abus éventuels des différents utilisateurs
- Et au final deux réseaux avec des services et une sécurité différente.

4.2.3 Mise en place effective du réseau

Etude topologique

Grâce à la synthèse de l'analyse des besoins, nous avons identifié l'ensemble des zones à couvrir. Ces zones ont été repérées sur des plans de masse du campus qui ont été mis à notre disposition (ces plans sont disponibles en annexes). Nous avons ensuite procédé en deux temps.
Nous avons d'abord repéré les zones qu'il fallait couvrir. Ce premier repérage ne tenait pas compte d'un quelconque découpage en cellules. Il s'agissait de localiser géographiquement le réseau à deployer, qui s'étend finalement sur une bonne partie du campus, depuis le foyer des élèves jusqu'à la cafétéria.
Ensuite nous avons effectué une série de tests (qui seront détaillés dans la partie suivante) afin d'évaluer pratiquement la portée des équipements. Les premiers test ont plutôt permis de se faire une bonne idée des portées. Ensuite nous avons commencé à refléchir au découpage en cellules de la zone de couverture.
Enfin ces deux étapes ont été analysées et intégrées au plan de décision du placement des points de connexion. Cette étape de synthèse est détaillé dans la suite de l'étude.

Tests : démarches et résultats

Grâce au matériel dont nous avons disposé cette semaine, nous avons réalisé une série de tests, en intérieur et en extérieur. Le protocole de test a toujours été le même. Nous avons principalement evalué la portée des points d'accès et/ou des antennes en mesurant la qualité du signal reçu. Outre la qualité du lien radio, nous avons mesuré la qualité du lien réseau en utilisant deux outils :
- la commande `ping`, qui évalue la qualité de la transmission, en calculant notamment les pertes subies
- le protocole de transfert de fichiers `ftp`, qui permet de se faire une bonne idée du débit effectif de la liaison.

Les tests en intérieur ont été réalisés avec des points d'accès (Netgear ME 401) sans antenne supplémentaire ; en extérieur nous avons utilisés une antenne omnidirectionnelle Cisco avec le point d'accès du même constructeur (Aironet 350). Les clients étaient munis de carte PCMCIA, Netgear et Lucent Technologies ; il s'agissait d'ordinateurs portables sous Windows (2000 et XP) et sous Linux (Debian / Noyau 2.4.20).

Les résultats sont récapitulés dans le tableau ci-dessous.

Choix effectif des points de connexion et attribution des canaux

Cette étape a été déterminante dans notre plan de déploiement. A partir de l'étude topologique réalisée auparavant, nous avons proposé un découpage en cellules de notre zone de couverture. Les facteurs décisifs ont été les suivants :
- couverture performante des lieux de passage (forum, amphithéâtres, extérieur du foyer, direction...)
- affectation optimisée des canaux

Intérieur	Bibliothèque	En plaçant une borne au centre de l'espace de travail, on arrive à couvrir la totalité de la bibliothèque. Le signal est de très bonne qualité dans l'espace ouvert et il reste très acceptable dans les bureaux.
	Bâtiment DIR	Avec deux points d'accès, la totalité du bâtiment est couverte avec un signal de bonne qualité. En plaçant les bornes à l'extérieur des bureaux, la zone de couverture s'agrandit et on peut faire capter le signal jusque dans l'intérieur des bureaux les plus excentrés.
	Forum et Amphithéâtres	Un point d'accès permet de couvrir la totalité d'un amphi et même davantage. On peut donc facilement couvrir les amphis et le forum. Cependant pour assurer un service capable de supporter la charge, il faudra plusieurs bornes, ce qui nécessite une bonne attribution des canaux.
Extérieur	Toit du foyer	En plaçant l'antenne en ce point et en adaptant la puissance d'émission, on peut couvrir l'extérieur du foyer ; ceci inclut notamment la "butte aux lapins", tout le contour du foyer ainsi que les bancs derrière la bibliothèque
	Toit du bâtiment DIR	Avec une antenne sur le toit terrasse, on couvre une partie assez importante du campus, qui s'étend de la cour d'honneur à l'entrée du foyer. A noter le problème d'émission sur une partie de la rue Charles Fourrier.

FIG. 4.5 – Récapitulatif des résultats des tests

– configuration optimisée des puissances d'émission des antennes et des points d'accès

Le choix des canaux se doit d'être rigoureux afin d'éviter les problèmes d'interférences. Les raisons techniques de nos choix sont expliqués dans la suite du rapport. Ils permettent le recouvrement de certaines cellules, comme par exemple celles des amphithéâtres qui sont inclues dans la cellule "extérieure".

En ce qui concerne la configuration des puissances d'émission, nous avons dû respecter divers critères. Les deux principaux concernent l'obligation de ne pas faire déborder la zone de couverture sur l'extérieur du campus (notamment pour des contraintes liées à la législation) et la limitation volontaire du diamètre de certaines cellules afin d'optimiser les recouvrements.

La synthèse de cette étape est représentée sur la carte disponible en annexes. L'explication de la position des 16 bornes est expliquée ci-dessous.

– 1 et 2 : Ces bornes desservent le batiment F, et elles émettent à 50mW, de manière à couvrir le batiment en intégralité.

– 3 et 4 : Ces bornes couvrent les salles communes du batiment U5, leur puissance est réglée à 30mW, car on les place au sous sol, et que les murs absorbent beaucoup de signal.

– 5 : Cette borne dessert les salles communes du batiment U4, avec une puissance de 30 mW. La borne est placée dans le couloir du rez-de-chaussée.

– 6 : Le foyer est couvert par cette borne, comme celle ci doit couvrir la totalité du foyer, la puissance est réglée à 50mW.

– 7 : Cette borne est située en extérieur, elle sera équipée d'une antenne plus performante, mais sera limitée à une puissance d'émission de 10mW pour des raisons de législation.

– 8 : La salle de jeux du U1 est couverte par cette borne, située dans le couloir pour éviter de trop dépasser vers l'extérieur. On laisse par contre une puissance de 30mW, ce qui permet de couvrir aussi la cuisine du batiment U1, et d'optimiser l'utilisation de cette borne.

– 9 : La borne de la bibliothèque émet à une puissance de 30mW, mais couvre plus que la bibliothèque, notamment à cause des fenètres, ce qui fait qu'elle dessert aussi une partie de l'extérieur du batiment.

– 10 et 11 : Ces bornes desservent les amphithéatres 10 et 11, nous avons choisi de placer deux bornes pour des raisons de débit, on obtiendrait des débits trop faibles avec une seule borne, si les deux salles étaient occupées. Ces deux bornes seront placées au niveau du projecteur, au milieu des salles, pour couvrir correctement les salles. La puissance de ces bornes sera de 30mW, et la portée du signal vers l'extérieur est limitée par l'absence de fenêtres ou d'ouvertures.

– 12 : Une borne est suffisante pour couvrir l'intégralité du batiment de direction, en la placant au centre du batiment. un emplacement au niveau de l'escalier au second niveau convient parfaitement, car il permet de couvrir tous les bureaux, ainsi que la salle de réunion. La puissance requise est de 50mw, car les cloisons métalliques reduisent la puissance du signal dans les bureaux. Par contre, les extérieurs du batiment seront très peu couverts, de par la présence des cloisons metalliques.

– 13 : Cette borne est celle qui se situe le plus en hauteur, elle couvrira la plus grande partie des extérieurs, que l'on veut desservir, ainsi que le forum. La fréquence choisie est imposée par la législation, car on émet au delà de 10mW en extérieur. La puissance nécessaire pour couvrir la zone est de 30mW, avec une antenne d'extérieur.

– 14 : Le restaurant de l'INT et la cafétaria sont couverts par cette borne, qui aura une puissance de 30mW, puissance nécessaire de par la présence d'équipements perturbateurs tels que les fours micro-ondes.

– 15 : Une borne couvre les salles E0010 et E0020, celle ci emettant à 30mW, ce qui est nécessaire pour desservir les salles, ainsi que la cour intérieure des batiments A,C et E.

– 16 : Finalement, une borne est placée au U3 pour les étudiants de ce bâtiment ainsi que pour une éventuelle utilisation extérieure.

4.2.4 Prévention des problèmes d'interférences

D'après la littérature, les problèmes des interférences est à prendre en compte lorsqu'on fait le choix d'une topologie à cellules recouvertes, ce qui signifie que les zones de couvertures des points d'accès se chevauchent. Il faut alors configurer les bornes de manière à leur faire utiliser des fréquences différentes. Dans notre cas (pour le 802.11g comme pour le b), la bande de fréquence ISM est telle que seuls 13 canaux sont disponibles. Cependant il faut utiliser des canaux totalement séparés afin d'éviter tout recouvrement de fréquences. En pratique, il reste 3 canaux disponibles pour mettre en place une topologie avec recouvrement des zones couvertes.

Ce constat théorique rend possible la mise en place de deux réseaux wifi sur une même zone géographique réduite. Pour le cas de la couverture de l'amphithéâtre, on peut envisager plusieurs points d'accès : certains permettant un accès au réseau ouvert et d'autres donnant accès au réseau sécurisé interne.

Cependant, la coexistence de plusieurs réseaux demande une affectation stricte des canaux. Cette affectation peut se voir perturbée par les réseaux de recherche des différents départements. Ainsi lors des tests effectué dans le forum, on perçoit systématiquement les bornes du département RST. La présence des réseaux de recherche n'est pas un problème majeur. En effet les clients peuvent, par le système de gestion des connexions sans fil de leur terminal, choisir le réseau auquel ils veulent se raccorder.

Enfin pour les sources extérieures d'interférences, *i.e.* les systèmes utilisant la même bande de fréquence, on peut craindre des problèmes avec les fours à micro-ondes de la cafétéria. Cependant ces fours sont une source très localisée et temporaire. On peut donc prévoir des perturbations discontinues, ce qui

n’affectera qu’une zone limitée du réseau.

4.3 Le matériel : points d'accès et cartes

4.3.1 Matériel adapté

Le choix du protocole s'est orienté vers un réseau LAN sans fil IEEE 802.11g à un débit de 54Mbps plutôt que 802.11a pour conserver une compatibilité maximum avec les cartes WiFi les plus courantes. Nous nous intéressons donc uniquement au matériel compatible avec la norme 802.11g. Ce matériel est en phase de développemenet et est sujet à d'éventuelles modifications suivant l'évolution de la normalisation définitive de 802.11g, contrairement à celui adoptant le 802.11b. Nous nous sommes donc attachés à l'évolutivité des équipements en fonction de l'évolution de la norme 802.11g.

Il existe plusieurs types de points d'accès compatibles avec la norme 802.11g sur le marché, mais il y en a peu qui supportent la norme de sécurisation 802.1x et EAP en dehors de celle de Cisco. Nous avons recherché les autre AP "sécurisables" existantes.

Voici une présentation des équipements les mieux adaptés à nos besoins chez les principaux constructeurs (Cisco, D-Link, Buffalo et Netgear). Nous ne présentons que les access points et les cartes d'accès.

4.3.2 D-Link

Carte DWL-G650

Norme Compatible 802.11b et 802.11g.

Caractéristiques Encryptage WEP 64/128bits.

OS supportés Drivers pour Microsoft Windows.

Prix constaté 75 €.

Point d'accès DWL-2000AP

Norme Ce point d'accès fournit un accès à un réseau LAN sans fil IEEE 802.11g.

Sécurité Encryptage WEP sur 64, 128 et 256 bits.
Contrôle d'accès des noeuds connectés (filtrage des adresses MAC non autorisées, liste des adresses MAC des noeuds connectés).
Support de la norme 802.1x et WPA.

Antenne Il a une antenne SMA reverse intégrée, détachable et pouvant donc être remplacée par une antenne extérieure. La portée en espace libre est de 100m en intérieur et de 400m en extérieur.

Roaming Prise en charge transparente d'une cellule à l'autre.

Alimentation Externe.

Fonctionnalités supplémentaires Serveur DHCP intégré.
Mise à jour firmware par client TFTP.
Administration via navigateur web.

Prix constaté 200 €.

4.3.3 Buffalo

Carte WLI-CB-G54

Norme Compatible 802.11b et 802.11g.

Caractéristiques Encryptage WEP 64/128bits.
Roaming supporté.

OS supportés Drivers Microsoft Windows exclusivement.

Prix constaté 50 €.

Point d'accès WBR-G54

Norme Accès à un réseau LAN sans fil IEEE 802.11g ("Proposed Draft Standard". Compatibilité assurée avec la norme IEEE 802.11b. De plus, le constructeur s'engage à changer ou upgrader gratuitement le matériel en cas de changement des fonctions matérielles spécifiées par la future norme IEEE 802.11g.

Sécurité Encrypatage 64/128bits WEP.
Registre d'adresse MAC.
Filtrage dynamique de paquets.
Dectection des intrusions avec Intrusion Detector Firewall.

Antenne Puissance de 32mW. Portée de 50 à 570m en extérieur selon le débit (de 54Mbps à 1Mbps) et de 20 à 125m en intérieur.

Roaming Non spécifié.

Alimentation Externe.

Fonctionnalités supplémentaires Administration par interface web.
Support VPN.
2 ans de garantie.

Prix constaté 120 €.

4.3.4 Netgear

Carte WAG511

Norme Compatible avec les normes 802.11b, 802.11a et 802.11g ("Draft").

Caractéristiques Roaming supporté.
Encryptage WEP 128bits pour le 802.11b et jusqu'à 152bits pour le 802.11a et le 802.11g.
Supporte le VPN.
Mise à jour future pour supporter AES et WPA.

OS supportés Drivers Microsoft Windows exclusivement.

Prix constaté 80 €.

Point d'accès WG602

Norme Support de la norme 802.11g et 802.11b.

Sécurité Encryptage WEP 128bits.
Filtrage d'adresse MAC.
Support de 802.1x et WPA avec une mise à jour future du firmware.

Antenne Détachable.

Roaming Supporté.

Alimentation Externe.

Fonctionnalités supplémentaires Garantie de 3 ans.

OS supportés Drivers fournis uniquement pour les systèmes Microsoft Windows.

Prix constaté 110 €.

4.3.5 Cisco

Point d'accès Aironet 1100

Norme Norme 802.11g supportée avec mise à jour prévue lors de la normalisation définitive du 802.11g.

Sécurité Encryptage WEP 40 ou 128bits.
Authentification fondée sur 802.1x et EAP exploitant les listes d'accès utilisateurs.
Permet d'utiliser un serveur RADIUS pour le registre des connexions utilisateurs.
Assure une protection contre les attaques passives et actives.
Support des réseaux locaux virtuels (VLAN).
Intègre un proxy.
Accès Tenet, FTP, TFTP via l'interface de commande Cisco.

Antenne Antenne dipolaire à réception multiple intégrée.
Puissance d'émission réglable jusqu'à 100mW.

Roaming Qualité de service assurée.

Alimentation Externe ou en ligne via Ethernet.

Fonctionnalités supplémentaires Segmentation du réseau jusqu'à 16 groupes d'utilisateurs.
Gestion centralisée possible à partir de nombreuses applications CiscoWorks.
Interopérabilité avec les systèmes de gestion de réseaux compatibles SNMP.
Permet de basculer de façon transparente vers un point d'accès de secours.
Evolutivité garantie permettant d'intégrer de futures technologies, telles que la norme 802.11g ou l'AES.
Intégration de solution anti-vol par fente de sécurité.
Client DHCP intégré.
Serveur HTTP avec nouvelle interface web de type navigateur.

Prix constaté 600 €.

4.3.6 Solution proposée

Points d'accès

Au vue des performances des équipements Cisco par rapport aux autres constructeurs et d'après les besoins évoqués en terme d'évolutivité et de sécurité, le choix est clairement orienté vers des points d'accès Cisco malgré leur prix largement supérieur. En effet, la mise en place d'un réseau public implique la nécessité de pouvoir isoler le réseau WLAN du réseau de l'INT. Pour ce faire, la solution adaptée est d'utiliser le réseau filaire déjà établi et de former un réseau privé (VLAN) entre les points d'accès, ce qui élimine une bonne partie des équipements précédemment décrits.

Pour pouvoir assurer une évolution de ce réseau public vers un réseau interne avec authentification, il est nécessaire de s'assurer que le matériel choisi soit évolutif et capable de supporter les normes de sécurité comme 802.1x et EAP.

Et enfin, la taille de la zone à couvrir implique l'utilisation de plusieurs points d'accès, or pour éviter toute zone d'interférences, nous devons veiller à ce que ces différents AP ne couvrent pas la même zone. La puissance des AP est donc un élément important dans le choix du matériel et la possibilité de régler celle-ci est un avantage certain.

En considérant l'ensemble de ces contraintes, Cisco est le seul constructeur à proposer une solution complète pour la mise en place d'un réseau sécurisé avec une mise à jour garantie.

Cartes

Afin de créer un besoin et de faire connaître les possibilités du WiFi à l'INT, il pourrait être intéressant de proposer le prêt de cartes aux visiteurs et aux vacataires lors de leur interventions nécessicitant un accès au réseau.

Les offres porposées par les constructeurs sont équivalentes au niveau des perfomances et du prix. Le choix entre les cartes précédemment présentées est donc laissé au client.

4.4 Le matériel : antennes

Il existe plusieurs sortes d'antennes. Chacune est déterminée par leur fréquence d'émission, leur gain, leur prix . Ces antennes sont placées directement après le point d'accès afin d'étendre sa zone de couverture du réseau Wi-Fi. Nous allons faire le détail des offres des antennes ainsi que leurs caractéristiques propres.

4.4.1 Antennes 802.11b/g

Fréquence (MHz)	2300-2650
Gain (dB)	14
Puissance maxi (W)	500
Diamètre maxi du mât (mm)	55
Longueur (m)	0.98
Poids (Kg)	0.7
Prix	110 €

FIG. 4.6 – Caractéristiques des antennes hélices (802.11b/g)

Antennes hélices

Fréquence (MHz)	2300-2500	2300-2500	2300-2500	2300-2500	2400-2500
Gain (dBi)	13	17	29	21.5	24
Faisceau 3 dB	18°	18°	15°	12°	10°
Dimension (cm)	46*25	51*51	61*61	76*76	91*91
Poids (Kg)	2.5	3	3.5	4	5
Prix	42 €	44 €	54 €	66 €	80 €

FIG. 4.7 – Caractéristiques des antennes paraboliques (802.11b/g)

Parabole

Fréquence (MHz)	2300-2500	2300-2500	2300-2450
Gain (dBD)	10	14	18
Puissance maxi (W)	100	100	50
Angle d'ouverture			
-verticale :	54		13
-horizontale :	67		15
Dimension (mm)	130*130	220*330*15	330*330
Poids (Kg)	1.3	1.5	1.7
Prix	75 €	85 €	185 €

FIG. 4.8 – Caractéristiques des antennes panneaux (802.11b/g)

Panneaux

Antennes omnidirectionnelles

Les antennes omnidirectionnelles ont la particularité d'avoir un rayonnement à 360°.

Fréquence (MHz)	2300-2500	2300-2500	2400-2500
Gain	7 dB	8 dBi	11 dBi
Puissance maxi (W)	50	50	
Hauteur (m)	0.06	0.039	1.50
Poids (Kg)	2.35	0.370	
Prix	169 €	99.50 €	295 €

FIG. 4.9 – Caractéristiques des antennes omnidirectionnelles (802.11b/g)

Fréquence (MHz)	2400	2400	2400
Gain	5 dBi	7.5 dBi	9 dBi
Dimension (mm)	80*100		120*90*20
Poids (Kg)	0.1	0.17	0.5
Prix	35 €	43 €	52 €

FIG. 4.10 – Caractéristiques des antennes patchs (802.11b/g)

Patchs

Antennes sectorielles

Les antennes sectorielles sont destinées à assurer la couverture d'une zone bien déterminée, en raison d'une ouverture importante.

Fréquence (MHz)	2400	2400	2400
Gain	12 dBi	13 dBi	14 dBi
Ouverture	120°*15°	90°*15°	120*90*20
Dimension (cm)	49*17*9	49*17*9	49*17*9
Poids (Kg)	2.2	2.2	2.2
Prix	255 €	255 €	255 €

FIG. 4.11 – Caractéristiques des antennes sectorielles (802.11a)

4.4.2 Antennes 802.11a

Antennes omnidirectionnelles

Antennes directives

4.5 Pour conclure

D'un point de vue de la faisabilité technique, ce projet de déploiement d'un réseau WiFi est tout à fait réalisable. Notre étude propose la mise en place d'un réseau sans-fil qui permet de couvrir une partie

Fréquence (MHz)	5000	5000	5000
Gain	7 dB	10 dB	13 dB
ROS	1 :1.8	1 :1.8	1 :1.8
Hauteur (cm)	18	50	100
Poids (Kg)	0.8	1.2	1.9
Prix	160 €	234 €	360 €

FIG. 4.12 – Caractéristiques des antennes omnidirectionnelles (802.11a)

Fréquence (MHz)	5000	5000	5000	5000
Type	Parabole	Parabole	Panneau	Panneau
Gain	20 dB	27 dB	8 dB	14 dB
Ouverture	7°	4°	80°	40°
Dimension (cm)	51*51	91*91	12*12*1.5	22*33*1.5
Poids (Kg)	2	4.15	0.30	1.16
Prix	50 €	80 €	80 €	145 €

FIG. 4.13 – Caractéristiques des antennes directives (802.11a)

importante du campus, en tenant notamment compte des lieux de passage et des lieux les plus fréquentés.

Chapitre 5

Synthèse de l’étude

Introduction

Cette synthèse a pour objet de finaliser l'étude menée du 07/04/2002 au 11/04/2003 concernant la mise en oeuvre d'un réseau de type Wi-Fi sur le campus de l'INT. Son but est donc de proposer une solution, en partant des besoins exprimés par les différentes populations circulant dans l'enceinte de l'INT, tout en répondant à diverses questions qu'engendre nécessairement un tel déploiement : aspects juridiques, aspects de sécurisation, etc.

Rappelons que la technologie Wi-Fi est extrêmement jeune et innovante. Cependant, si elle est séduisante par de nombreux aspects, il ne faut pas perdre de vue les réalités et les problèmes engendrés par l'introduction d'une nouvelle technologie dans un établissement aussi complexe que l'INT. Nous tâcherons donc de répondre clairement à la question suivante : l'introduction de la technologie Wi-Fi est-elle pertinente à l'INT, et si oui, sous quelle forme ?

Afin de répondre à cette problématique, nous commencerons par synthétiser les besoins exprimés par les différentes populations interrogées à l'INT. A partir de cette synthèse, nous serons en mesure de proposer un déploiement adapté, un cadre juridique, et une solution de sécurisation envisageable. Enfin, nous pourrons conclure sur les évolutions possibles du déploiement proposé.

5.1 Quels sont les besoins de l'INT par rapport au Wi-Fi ?

5.1.1 Tableaux récapitulatifs des besoins à l'INT

Il est possible de synthétiser les besoins exprimés par les différentes population de l'INT sous la forme du tableau exposé à la page 21.

Ce tableau montre donc bien qu'il existe un champ d'exploitation pour le Wi-Fi à l'INT, notamment pour ce qui est de la consultation des services classiques, soit le Web et le mail. Cette utilisation serait surtout localisée dans :

- Le forum ;
- Les amphithéâtres ;
- Certaines salles de cours dont les E00 ;
- Les extérieurs : Butte aux Lapins, Cours d'Honneur ;
- La cafétéria ;
- Le bâtiment de la Direction, et les salles de réunion ;

Les services à offrir sur ce réseau seraient donc dans l'ordre de priorité :

1. L'accès aux pages Web ;
2. L'accès aux mails (sous toutes ses formes : *pop, smtp, imap, webmail*) pour tout le public présent sur campus : étudiants, permanents, visiteurs ;
3. L'accès aux ressources intranet sécurisées : accessibles uniquement aux internes.

Il existe donc bien un besoin exprimé à l'INT, besoin qui semble géographiquement localisable, facilitant ainsi les possibilités de déploiement. Au delà de ces besoins exprimés avec plus ou moins d'enthousiasme par les personnes interrogées, on peut également parler de l'existence d'un besoin latent.

5.1.2 Existence d'un besoin latent

Il existe en effet chez les populations de l'INT une forte volonté de mobilité, qui ne devient complètement solutionnée que par l'introduction de technologies sans fil tel que le Wi-Fi. Cette volonté de mobilité s'exprime largement à travers certains chiffres que nous avons pu recueillir.

Tout d'abord, le département des Moyens Communs Informatiques (MCI) nous confirment la croissance des volumes de commande pour le matériel informatique mobile :

	Ordinateurs Fixes	Ordinateurs Portables
1er Marché Public 2001	104	24
2nd Marché Public 2001	100	27
1er Marché Public 2002	135	44
2nd Marché Public 2002	18	27

FIG. 5.1 – Composition des appels d'offres de MCI sur les deux dernières années

Actuellement, les conditions d'acquisition de PDA (*Portable Digital Assistant*) pour un certain nombre de permanents de l'INT est également à l'étude.

Les statistiques de l'association M*i*NET permettent de mettre en valeur cette volonté de mobilité chez les élèves :

Année	Nombres d'ordinateurs portables
2000	50
2001	95
2002	130

FIG. 5.2 – Nombre d'ordinateurs portables raccordés au réseau de la MAISEL par M*i*NET par année

Chez les élèves également, le besoin de mobilité est fort, et croissant. On peut donc raisonnablement dire que le Wi-Fi va venir soutenir ce besoin de mobilité. Dans ce sens, même si le Wi-Fi n'amènera pas dans un premier temps de nouvelles utilisations des ressources informatiques de l'INT, il augmentera le confort des utilisations actuelles.

D'autre part, les technologies sans-fil sont l'une des tendances lourdes de l'industrie des télécommunications. Les usages de ces technologies émergeront d'ici une à deux années, avec des offres de carte PCMCIA/GPRS par exemple. Avec la technologie Wi-Fi, l'INT possède une opportunité pour se poser en tant que leader technologique dans le domaine, en tant que pionner du sans fil. Cette image serait facilement capitalisable par l'établissement, et aurait un impact extrêmement positif sur les entreprises comme sur les élèves potentiels.

5.1.3 Conclusion sur les besoins et les services à offrir.

Pour conclure, les populations qui se sont montrées les plus enthousiastes par rapport à la connexion Wi-Fi à l'INT sont évidemment les plus mobiles. Les participants à des colloques et les visiteurs d'une manière générale apprécieraient énormément la possibilité d'accéder à leurs ressources Web et à leurs mails. Pour les populations sédentaires à l'INT, le besoin est globalement moindre, mais le service serait également apprécié. La plus grosse demande vient des instances de Direction et d'encadrement, qui y voient un moyen de faciliter considérablement l'organisation de réunion, et de simplifier la synchronisation de leurs différents outils de travail : PDA, portables, PC fixes, etc... Enfin, on a vu que la mobilité des individus à l'INT était une tendance de fond que l'implantation de la technologie Wi-Fi à l'INT permettrait de favoriser.

A partir de là, les services que devra offrir cet accès sont facilement identifiables : il s'agit du Web et du mail en priorité, puis des ressources internes dans un second temps. Les accès Web/mail devront être aussi simples et faciles d'accès que possible.

Au delà des besoins fonctionnels des agents, c'est également l'aspect "vitrine technologique" qui a été souvent cité dans nos entretiens. Il est vrai que l'implantation d'un tel réseau serait extrêmement novateur, et permettrait à l'INT de capitaliser sur une image de modernisme et de leader technologique, attirante à la fois pour les élèves et pour les entreprises.

5.2 Proposition technologique

5.2.1 Services proposés

Compte tenu de la teneur des besoins de l'INT, et de la jeunesse de la technologie Wi-Fi, nous estimons qu'il serait positif de réaliser un premier déploiement. Il couvrirait largement les zones retenues par l'étude des besoins, à savoir :

- Le forum ;
- Les deux amphithéâtres ;
- Les salles E00 ;
- Les extérieurs : butte aux lapins, Cours d'Honneur ;
- La bibliothèque ;
- Les salles de jeux calmes MAISEL ;
- Le foyer associatif ;
- Le bâtiment de la Direction ;

Les services offerts après ce premier déploiement seraient uniquement l'accès au Web, aux services mails (protocoles *pop, smtp, Imap, webmail*), et aux serveurs IRC (*Internet Relay Chat*). En effet, 95% des besoins se concentrent autour de ces utilisations. On pourra dans un deuxième temps étudier la possibilité d'accéder à l'intranet et aux services départementaux, dans un cadre de sécurisation bien plus développé.

5.2.2 Déploiement géographique

Au contraire de l'offre de service qui se fera donc en deux temps, le déploiement physique se fera lui en une seule fois sur les zones énumérées ci-dessus. La carte du campus en annexe offre une bonne représentation de ce déploiement. La technologie Wi-Fi fonctionne grâce à des "points d'accès", sortes d'émetteurs radio. Ces points ont été placés de façon à couvrir un maximum de surface interne, tout en débordant le moins possible sur la zone publique. On peut visualiser la carte de déploiement global en annexe, page 73.

5.2.3 Technologie et matériel recommandé

La technologie recommandée dans le cadre de ce déploiement est la future norme *802.11g*. Cette technologie est sur le point d'être standardisée par l'IEEE, et présente de nombreux avantages par rapport à la technologie actuelle, le 802.11b. Outre les possibilités de *roaming* qu'elle offre (possibilité pour le terminal de recevoir le signal d'émission tantôt d'une borne A, tantôt d'une borne B, de façon transparente), cette technologie offre des débits de l'ordre de 54 Mb/s contre 11 Mb/s pour le 802.11b.

En terme de matériel, nous n'avons pu que tester du matériel des marques Cisco et Netgear. Toutefois, nous recommandons sans hésiter le matériel Cisco. Les raisons qui motivent cet avis tiennent à la position de leader technologique du constructeur, et à la fiabilité de ses équipements. La firme Cisco en effet participe activement à l'établissement des normes Wi-Fi, et dans ce sens, les standards adoptés par Cisco seront supportés par la plupart des matériels du marché, faisant disparaître les risques d'incompatibilité

avec d'autres marques. En outre, le service MCI comme l'association M*i*NET ont tout deux été très satisfait du matériel Cisco avec lequel ils travaillent depuis plusieurs années. Le matériel Cisco propose enfin un certain nombre d'outils de configuration, permettant d'agir sur la puissance d'émission, ou de détecter le zones de congestion du réseau, qui lui confèrent un véritable plus sur le marché.

5.2.4 Sécurisation du réseau

La sécurisation du réseau est un réel problème, et ce d'autant plus qu'il s'agit de Wi-Fi et que l'on souhaite ouvrir le réseau au publique. C'est notamment à cause de ces problèmes de sécurité, et des limitations de la technologie Wi-Fi dans son état actuel que nous avons choisi de repousser dans un premier temps l'accessibilité aux services internes. Concrètement, s'il fallait faire cohabiter un réseau sécurisé avec un réseau publique, il faudrait doubler toutes les bornes d'accès. Or, cette option n'est pas envisageable en l'état actuel de l'art, car les bornes se brouilleraient entre elles. Nous avons donc choisi de n'offrir qu'un réseau publique dans un premier temps, dans la mesure où celui-ci est en mesure de solutionner 95% des besoins exprimés.

Nous avons choisi de laisser l'accès au réseau aussi libre (et donc aussi simple) que possible, tout en limitant strictement les services accessibles, au Web, au mail et à l'IRC, et en contrôlant les volumes générés sur le réseau. Cela implique donc la présence d'un firewall filtrant les flux sortant et entrant sur le réseau, et d'une solution de *shaping* afin d'éviter la congestion de la connexion Internet ou la saturation de certains points d'accès. Ces processus devraient donc permettre de limiter les actes malveillants pouvant être commis depuis l'intérieur du réseau.

Ensuite, afin d'assurer un minimum de confidentialité des communications, nous conseillons de favoriser autant que possible les protections par chiffrement. Il peut s'agir du WEP, propre à la technologie Wi-Fi, comme du SSL, qui permet une protection des couches applicatives. Même si ces méthodes ont leur limite, elles représentent un rempart satisfaisant pour bon nombre des tentatives d'interception.

5.2.5 Évaluation des coûts

La proposition de déploiement décrite ci-dessus a l'avantage d'être très peu coûteuse. En effet, la couverture totale des zones précisées auparavant nécessiterait la mise en place d'une quinzaine de bornes, et de deux antennes. Si l'on se base sur du matériel Cisco, on peut chiffrer ainsi le coût d'acquisition du matériel nécessaire à la mise en place du réseau :

- 15 bornes *Cisco Aironet 1100 Series* au prix unitaire de 600 € TTC, soit un total de 9600 € TTC ;
- 2 antennes *Cisco AIR-ANT2506* au prix unitaire de 140 € TTC, soit un total de 280 € TTC ;

On arrive donc à un coût d'acquisition total de 9880 € TTC, soit environ 65 500 FF

5.3 Dans quelle cadre juridique ce réseau pourrait-il se déployer ?

5.3.1 Un cadre juridique expérimental

La modernité du projet d'étude est souligné par ses aspects juridiques, où l'on constate que la législation accuse un lourd retard par rapport à la technologie. En France, l'ART n'a mis en place que des législations provisoires, permettant de combler un peu le vide juridique entre le présent et la future législation européenne. Pour la technologie Wi-Fi, deux choses sont à retenir :

- Le département de l'Essonne figure dans la liste des départements pour lesquels l'utilisation de la bande de fréquence des 2,5 Ghz a été libéralisé : l'utilisation de la technologie Wi-Fi est donc possible.

– Pour les réseaux sans-fil basés sur les technologies Wi-Fi, comprenant une ouverture au public, il existe une licence expérimentale dite de *hot-spot*.

Le réseau que nous proposons de mettre en place comporte à la fois un accès privé, et un accès public. Le premier accès rentre tout à fait dans le cadre des "RLAN privés" définis par l'ART, et ne nécessite pas d'autorisation particulière, tant que l'on reste dans le cadre géographique du campus. Le second accès rentre dans une logique d'ouverture et de partage du réseau au public. Cette ouverture ne pourra se faire légalement qu'après l'acquisition d'une licence de type *hot-spot*.

L'acquisition de cette licence est soumise à très peu de contraintes, mais elle n'est attribuée qu'au cas par cas. Le dossier à déposer comporte essentiellement un descriptif technique du réseau (type de bornes d'accès employées, position, hauteur, puissance, etc.). L'exploitation de cette licence ne semble pas être soumise à une obligation en terme de qualité de service ou de sécurisation. En outre, le coût d'acquisition est nulle.

5.3.2 Des risques subsistent

Si cette licence expérimentale semble être à la portée de l'INT, il faut bien prendre conscience de son caractère transitoire et temporaire. Elle n'est valable que 18 mois, sans que des modalités de renouvellement aient été mises en place. Sur ce point, l'ART semble vouloir attendre que l'Europe montre la direction à prendre.

D'autre part, si l'obtention de cette licence permet à l'INT d'ouvrir son réseau au public, il lui faut l'autorisation de son fournisseur d'accès Internet pour partager cette ressource. Le réseau RENATER semble toutefois permettre le partage de la ressource. Cependant, l'INT reste seule responsable des utilisations de sa connexion Internet. Si donc une utilisation publique du réseau se trouvait être frauduleuse, l'INT serait considéré comme pleinement responsable.

5.4 Les développements futurs du réseau Wi-Fi

Une fois ce premier déploiement effectué, plusieurs projections sont permises pour l'avenir. Tout d'abord, la première évolution consistera sans-doute à créer au sein du réseau une partie complètement sécurisée et authentifiée afin de permettre aux internes d'avoir accès aux serveurs départementaux et aux services locaux. A partir de là, il n'y aura pas de différence pratique entre le réseau filaire et le réseau sans fil.

De manière simultanée, on pourra commencer à développer de nouvelles utilisations du réseau grâce au Wi-Fi. Ainsi on peut imaginer la conception d'une offre de services à destination des colloques. Par exemple, avec un accès Wi-Fi durant une conférence, on peut offrir un service de "forum virtuel", sur lequel les participants pourront poser leurs questions directement à l'intervenant. Une tierce personne se chargerait d'agréger les questions, pour ensuite les soumettre au conférencier. D'une autre façon, les professeurs pourront commencer à réellement envisager des modules de e-learning à intégrer à leurs cours.

Dans un cadre plus interne, un certain nombre d'applications logistiques ou organisationnelles sont concevables, depuis la géolocalisation de certains matériels, jusqu'à la mise en place d'agendas partagés beaucoup plus dynamiques que l'actuel système d'emplois du temps.

Dans un avenir un petit peu plus lointain, ce sont toutes les applications dites *VoIP* qui pourront être envisagées. Ainsi, la mise en place d'un système de communication téléphonique mobile interne devient imaginable, permettant de réduire les coûts engendrés par une flotte de GSM.

Toutes ces pistes sont données à titre anecdotique : l'introduction de la technologie Wi-Fi favorisera l'apparition de nouveaux comportements chez les utilisateurs du réseau, et suscitera de nouvelles demandes. Il serait présomptueux de vouloir prédire ces demandes, mais il n'en reste pas moins que le Wi-Fi offre à l'INT un formidable champ de développement et d'expérimentation.

En conclusion...

La conclusion de cette étude est assez claire, avec des aspects positifs qui contrebalancent largement les quelques points négatifs qui existent. On doit notamment noter que :

- Le cadre juridique est incertain et sujet à changement.
- Faire cohabiter un réseau public et un réseau interne sécurisé est difficilement faisable dans l'état actuel de l'art.
- La mise en place d'un tel réseau va obliger MCI comme l'association M*i*NET à adapter une partie de la configuration actuelle du réseau.
- L'INT reste la seule responsable de l'utilisation qui est faite de ses ressources informatiques.

Toutefois, un grand nombre de points viennent défendre la mise en place d'une telle solution.

- Il existe bel bien un besoin à l'INT que la technologie Wi-Fi permettrait de combler.
- Le déploiement d'un tel réseau dans un cadre scolaire serait pratiquement une première en France.
- Il permettrait de poser l'INT en tant que leader technologique, et non pas suiveur.
- 95% des besoins exprimés relèvent de l'accès web et du mail.
- Ce réseau pourrait être ouvert simplement au public visiteur de l'INT, sans difficulté technique ou juridique majeure, avec tout de même un certain niveau de sécurité.
- Les applications développable pour un tel réseau sont nombreuses, et permettraient de faciliter à la fois des fonctions d'enseignement comme de logistique.

L'INT reste seul maître du choix à faire dans la problématique qui nous concerne. Quoiqu'il en soit, nous affirmons qu'il existe des besoins à l'INT que le Wi-Fi pourrait venir satisfaire, dans un cadre technique, juridique et sécuritaire satisfaisant, le tout pour une somme relativement modique.

Annexe A

Annexes

A.1 Annexes de l’analyse des besoins

A.1.1 Questionnaire type

Connaissez vous le WIFI ?

a.Présentation de la plaquette réalisée par l’association Minet sur le projet

Quelles sont vos utilisations des réseaux Internet et Intranet (du plus au moins utilisé)

a.http
b.FTP
c.Jeux en réseaux
d.E-Mail
e.Visio conférence
f.E-Learning
g.Chat (Messagerie Instantanée)
h.Forum
i.Serveurs partagés
k.Autre :

Est-ce que le WIFI modifierait votre utilisation de ces applications (élargissement) ?

Est-ce que le WIFI apporterait de nouveaux contextes d’utilisation ?

Quel est votre niveau de sécurité pour ces applications ?

Quelles sont vos réticences ?

a.Santé
b.Sécurité
c.Prix
d.Débit (par rapport au débit actuel) / Qualité de service

Si vous êtes vacataire ou participant d'un colloque seriez vous prêt à louer un équipement WIFI ?

Seriez vous prêt à équiper les membres de votre département ?

Est-ce que le WIFI pourrait servir l'ensemble de vos stagiaires (formation continue). Sous quelle forme souhaiteriez vous le mettre en place ?

A quel endroit utiliseriez vous l'accès WIFI, combien de fois par jour ?

a.RA
b.Amphi
c.Cafétéria
d.Salle de cours
e.Bibliothèque
f.Forum
g.Autre :

A.2 Annexes de l'analyse juridique

- Annexe 1 : Tableau récapitulatif du cadre réglementaire des RLAN
- Annexe 2 : Liste des 58 départements métropolitains libéralisés
- Annexe 3 : Détail de la demande de licence expérimentale
- Annexe 4 : Décision n° 02-1008 de l'ART
- Annexe 5 : Décision n° 02-1009 de l'ART
- Annexe 6 : Tableau récapitulatif sur les puissances autorisées
- Annexe 7 : Informations à fournir pour une demande de réseau expérimental dans un hotspot

A.3 Annexes de l'étude de déploiement

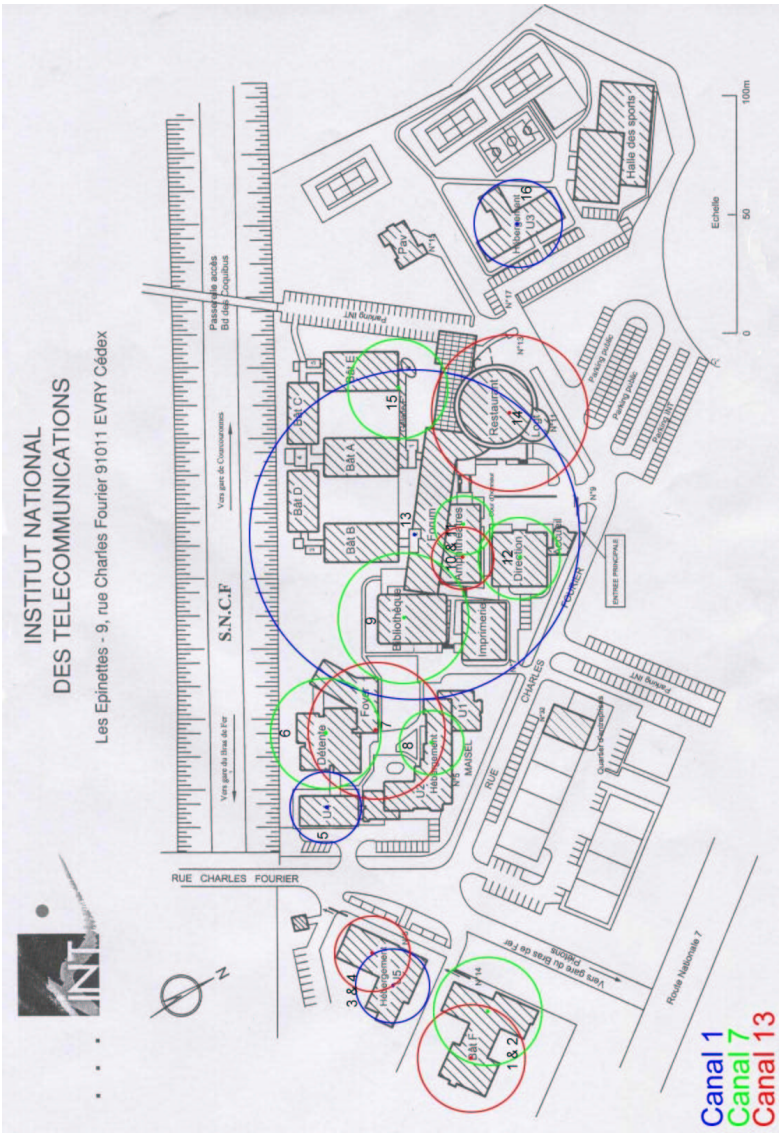

FIG. A.1 – Le déploiement géographique des bornes et les zones de couverture

Index

O

P

Q

R

S

T

V

W