CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE REGIONAL RHÔNE-ALPES

CENTRE D'ENSEIGNEMENT DE GRENOBLE

MEMOIRE

présenté par David ROUMANET

en vue d'obtenir

LE DIPLÔME D'INGENIEUR C.N.A.M.

en INFORMATIQUE

NOMADISME ET SÉCURITÉ SUR LES RÉSEAUX INFORMATIQUES

Soutenu le …décembre 2005

JURY

Présidente : Mme Véronique Donzeau-Gouge

Membres : M. Eric Gressier
M. Jacques Courtin
M. Jean-Pierre Giraudin
M. André Plisson
M. Eric Jullien

Mes remerciements :

Durant ce stage, j'ai pu évoluer dans un environnement très instructif et dont le cadre ouvert m'a permis d'obtenir tout les renseignements et toute l'aide dont j'avais besoin. Cette année de travail au sein de l'équipe réseau du CICG restera dans mon esprit pour longtemps.

Je tiens malgré tout à remercier plus particulièrement :

- Le CNAM qui facilite l'acquisition de compétence et l'évolution dans le cursus éducatif de nombreux étudiants déjà engagés en entreprise,
- Christian LENNE auquel je suis redevable d'un sujet passionnant et qui m'a assuré des conditions de travail idéales au sein du CICG,
- Eric JULLIEN, qui s'est beaucoup investit dans son rôle de tuteur, et dont les suggestions, le positivisme et les conseils m'ont beaucoup aidés,
- Tous les membres du département réseau du CICG qui, chacun dans leur domaine, m'ont apporté une aide pour la réalisation pratique de mon projet (notamment Raoul DORGE, Patrick PETIT, Jean-Luc DEMOISSON),
- ma femme Béatrice pour m'avoir motivé à continuer mon cursus ingénieur puis à m'avoir encouragé dans les moments difficiles ainsi que mon fils qui m'a permit de relativiser les problèmes : je leur dédie ce mémoire.
- les membres du jury qui consacre une grande partie de leur temps aux auditeurs du CNAM, notamment pour les épreuves de mémoires et de probatoires,
- les différentes communautés "Wi-Fi Grenoble", "Wi-Fi CRU", "ARREDU", "FreeRADIUS" (en particulier Rok PAPEZ du réseau ARNES pour son aide précieuse dans le projet de connexion au réseau EduRoam) et "Open Office" pour les différentes aides et améliorations d'applications.

TABLE DES MATIÈRES

1 INTRODUCTION....1

2 PRÉSENTATION....2
2.1 Définitions....2
2.1.1 Définitions liées au nomadisme....2
2.1.1.1 nomadisme....2
2.1.1.2 Itinérance (roaming)....3
2.1.1.3 Mobilité....3
2.1.1.4 Interopérabilité....3
2.1.2 Définitions de la sécurité....3
2.1.2.1 Identification....3
2.1.2.2 Authentification....4
2.1.2.3 Autorisation....4
2.1.2.4 Accounting....4
2.1.2.5 cryptologie....4
2.2 Constats sur le nomadisme informatique....5
2.2.1 Statistiques et évolutions....5
2.2.2 Récapitulatif....8
2.3 Répercussions sur la sécurité....8
2.3.1 Les attaques classiques....9
2.3.1.1 Attaques externes....9
2.3.1.2 Attaques par ingénierie sociale....9
2.3.1.3 Attaques par infection....10
2.3.2 Les attaques sans fil....10
2.3.2.1 War-driving....10
2.3.2.2 War-chalking....10
2.3.2.3 brouillage....11
2.3.2.4 arp-poisoning....11
2.4 Conclusion....11

3 CAHIER DES CHARGES....12
3.1 Définition de l'environnement....12
3.1.1 Rôles du CICG....12
3.1.2 Département réseau....13
3.1.3 Les différents réseaux....14
3.1.3.1 Réseau TIGRE....14
3.1.3.2 Réseau AMPLIVIA....15
3.1.3.3 Réseau RENATER....15
3.1.3.4 Réseau GEANT....15
3.1.3.5 Réseau EDUROAM....16
3.2 Analyses et classifications....16
3.2.1 Classification des utilisateurs....16
3.2.2 Classification des équipements....17
3.2.3 Classification des accès géographiques....18
3.3 Description de l'architecture d'origine....19
3.3.1 Architecture VPN interuniversitaire....19
3.3.2 Adressage et sécurité....20
3.4 Spécifications des besoins....20
3.4.1 Contraintes....20
3.4.1.1 Contraintes techniques....20
3.4.1.2 Contraintes législatives....21
3.4.1.3 Contraintes collectives....21
3.4.2 besoins....22
3.4.2.1 Utilisation standard....22

3.4.2.2 Utilisation étendue....23
3.4.2.3 Salubrité des postes....23
3.4.2.4 Résumé des besoins....23

4 NORMES ET INFORMATIONS....25
4.1 Introduction....25
4.2 Nomadisme et mobilité....26
4.2.1 Modèles de réseaux....26
4.2.2 Normes communes....27
4.2.2.1 Norme IEEE 802.1q....28
4.2.2.2 Norme IEEE 802.1x....29
4.2.3 Normes réseaux filaires....31
4.2.3.1 Réseaux point à point et multipoint....31
4.2.3.2 IEEE 802.3....32
4.2.3.3 Les accès via réseau téléphonique....33
4.2.3.3.a RTC....33
4.2.3.3.b DSL....33
4.2.4 Normes réseaux sans fil....34
4.2.4.1 Modulations et codages....35
4.2.4.1.a Modulation d'amplitude (Amplitude Modulation)....35
4.2.4.1.b Modulation de fréquence (Frequency Modulation)....35
4.2.4.1.c Modulation de phase (Phase Modulation)....35
4.2.4.1.d Les symboles....36
4.2.4.2 Distances et interférences....37
4.2.4.2.a Distances....37
4.2.4.2.b interférences....37
4.2.4.3 Étalement de spectre....38
4.2.4.3.a FHSS....38
4.2.4.3.b DSSS....38
4.2.4.4 Les réseaux sans fil 802.11....39
4.2.4.4.a Généralités sur le 802.11....40
4.2.4.4.b Les spécifications de fréquences du standard 802.11....41
4.2.4.4.c Le fonctionnement du standard 802.11....42
4.3 Sécurité....45
4.3.1 Chiffrement....46
4.3.1.1 algorithmes à chiffrement symétrique....46
4.3.1.1.a RC4....46
4.3.1.1.b DES....46
4.3.1.1.c AES-Rijndael....47
4.3.1.2 Algorithmes à chiffrement asymétrique....47
4.3.1.3 fonctions de hachage et de signature....48
4.3.1.3.a Fonction de hachage....48
4.3.1.3.b Fonction de signature électronique....49
4.3.2 Authentification, Autorisation et accounting....49
4.3.2.1 Différentes méthodes d'authentification....49
4.3.2.1.a Mot de passe....50
4.3.2.1.b One Time Password....50
4.3.2.1.c Biométrie....50
4.3.2.1.d Carte à puce....50
4.3.2.1.e Single Sign On....51
4.3.2.2 Architecture AAA....51
4.3.2.3 Structure d'authorité de certification....52
4.3.3 Tunnels et Réseaux Virtuels Privés....54
4.3.3.1 SSL (Secure Socket Layer)....54
4.3.3.2 IPSec (Internet Protocol Secure)....54
4.3.3.2.a AH (Authentication Header)....54
4.3.3.2.b ESP (Encapsulating Security Paiload)....55
4.3.3.3 PPTP (Point to Point Tunneling Protocol)....56
4.3.3.4 EAP....56

4.3.3.4.a EAP-TLS....57
4.3.3.4.b EAP-TTLS et EAP-PEAP....58
4.3.3.5 VLAN....60

5 SOLUTIONS ET DÉPLOIEMENT....61
5.1.1 Solution de base....61
5.1.2 Solution étendue....61
5.1.3 Tronc commun au deux solutions....62
5.2 Authentification....62
5.2.1 Présentation....62
5.2.1.1 Steel Belted Radius (Funk Software Inc.)....62
5.2.1.2 Microsoft IAS (Microsoft)....63
5.2.1.3 Radiator (OSC)....63
5.2.1.4 FreeRADIUS (Alan DEKOK)....63
5.2.2 Déploiement dans la solution....64
5.2.3 Installation de base....64
5.2.4 configuration EAP-TTLS....65
5.3 Portails captifs....65
5.3.1 M0n0wall et pfSense....66
5.3.1.1 Installation et configuration....66
5.3.1.2 Les avantages....67
5.3.1.3 Les inconvénients....67
5.3.2 Talweg....67
5.3.2.1 Installation et configuration....67
5.3.2.2 Les avantages....68
5.3.2.3 Les inconvénients....69
5.3.3 Squid....69
5.4 Réseaux Virtuels Privés....69
5.4.1 VPN Cisco 3030....69
5.4.2 VPN SSL F5 Networks....69
5.4.3 Solution WPA....69
5.5 Gestion du projet....70
5.5.1 Développement....70
5.5.2 Organisation....71
5.5.3 Communication....72
5.5.3.1 Communication interne....72
5.5.3.2 Communication externe....73
5.5.4 Architecture finale déployée....74
5.6 Perspectives et projections....75

6 CONCLUSION....77
6.1 Projections....77
6.2 Conclusion personnelle....77

7 ANNEXES....78
7.1 Les groupes de travail de l'IEEE....78
7.2 Valeurs de fréquences et puissance d'émission....78
7.3 Caractéristique de la modulation DSSS....79
7.4 Différences et similitudes entre protocoles VPN....79

INDEX DES ILLUSTRATIONS

Illustration 1: Répartition des fonctions mobiles en entreprise....5
Illustration 2: Équipement des personnes mobiles en entreprise (2004)....6
Illustration 3: Principaux freins au développement des réseaux mobiles....6
Illustration 4: Nombre de hotspots déployés....7
Illustration 5: Symboles utilisés dans le war-chalking....11
Illustration 6: Organigramme du CICG....13
Illustration 7: Dorsale haut débit Metronet....14
Illustration 8: schéma des réseaux gérés par le CICG....14
Illustration 9: Architecture Wi-Fi et VPN de Grenoble Universités....19
Illustration 10: Statistiques virales du 1er semestre 2005....23
Illustration 11. : les couches OSI et TCPIP....27
Illustration 12: Fonctionnement des réseaux locaux virtuels....28
Illustration 13: Insertion champs vlans sur une trame Ethernet....29
Illustration 14: Le standard 802.1x et ses protocoles....29
Illustration 15: Trame 802.1x....30
Illustration 16: Fonctionnement du protocole 802.1x....30
Illustration 17: Les couches EAP....31
Illustration 18: Les topologies filaires....32
Illustration 19: Mécanisme CSMA/CD....33
Illustration 20: Spectre de fréquences et longueurs d'ondes....34
Illustration 21: Les différentes modulations....35
Illustration 22: Extrait d'un datasheet d'un composant électronique....36
Illustration 23: débits en fonction de la distance en 802.11....37
Illustration 24: les différentes perturbations des ondes....38
Illustration 25: étalement de spectre....38
Illustration 26: Les différentes familles de réseaux sans fil....39
Illustration 27: logo de certification Wi-Fi....40
Illustration 28: Chevauchement des fréquences en 802.11b/g....41
Illustration 29: Exemple de répartition de canaux....42
Illustration 30: Les couches du standard 802.11....42
Illustration 31: Les différents modes de connexion 802.11....43
Illustration 32: Protection de communication entre les points d'accès....43
Illustration 33: Fonctionnement de CSMA/CA....44
Illustration 34: Fonctionnement d'un algorithme de chiffrement symétrique....46
Illustration 35: Fonctionnement d'un algorithme de chiffrement asymétrique....48
Illustration 36: Fonctionnement d'un mécanisme de hachage....48
Illustration 37: Les deux modèles d'architecture AAA....51
Illustration 38: symbole cadenas pour le protocole HTTPS....53
Illustration 39: Les modes transport et tunnel d'IPSec....54
Illustration 40: Structure de l'en-tête AH....55
Illustration 41: Structure de l'en-tête ESP....55
Illustration 42: Format de trame EAP....56
Illustration 43: Authentification EAP-TLS....58
Illustration 44: Authentification EAP-TTLS....59
Illustration 45: interface de Steel Belted Radius....62
Illustration 46: Interface d'IAS de Microsoft....63
Illustration 47: synoptique de fonctionnement FreeRADIUS....65
Illustration 48: architecture typique m0n0wall....66
Illustration 49: architecture Talweg....67
Illustration 50: exemple de ré-écriture de liens sous Talweg....68

Illustration 51: Gestion de projet par diagramme de Gantt..... 70
Illustration 52: Progression du travail dans le temps.....71
Illustration 53: Cycle de la roue de Deming.....71
Illustration 54: Organisation d'idées..... 72
Illustration 55: Exemple de "weblog" employé pour le projet STAR.....73
Illustration 56: Architecture finale..... 75

INDEX DES TABLES

Tableau 1: Lieux et mobilité..... 7
Tableau 2: localisation et usage des services.....18
Tableau 3: Table des fonctionnalités par besoins.....24
Tableau 4: Le modèle ISO..... 26
Tableau 5: Echelle de qualité de signal.....37
Tableau 6: les amendements du standard 802.11.....40
Tableau 7: Les principales différences de transmission 802.11..... 41
Tableau 8: Débits contatés avec deux stations 802.11b (source IMAG-LSR).....45
Tableau 9: Points forts des différents algorithmes utilisés avec EAP..... 57

1 INTRODUCTION

L'évolution de l'informatique durant les trente dernières années est allée croissante : les transistors ont remplacé les lampes, les circuits imprimés ont réduit les câblages, les réseaux ont modifié les approches centralisées et Internet est devenu un continent virtuel incontournable.

Durant cette évolution, il n'est pas facile de déterminer si c'est la technique qui a fait progresser les méthodes de travail ou bien l'inverse. Le constat actuel montre seulement que nous ne sommes que dans une étape transitoire dans l'emploi de ces technologies : L'ENIAC[1] et ses 19000 tubes représente l'ère préhistorique de notre planète mais l'intégration des circuits intégrés et la convergence des technologies (comme la vidéo-conférence, les réseaux sans fils, la biométrie, l'analyse vidéo, etc) n'ont pas encore fini de progresser.

Dans ce contexte, l'Homme vit dans un monde en perpétuelle mutation et cherche à adapter son mode de vie à l'évolution des méthodes de travail. Dans un présent ou les contrats d'embauches précisent que le lieu de travail est une région voir même un pays, la technologie devient un moyen de garder un lien, une attache avec ses proches : trains à grande vitesse, téléphones mobiles, courrier électronique, vidéo-conférence...

D'un autre coté, elle nous rend esclave du temps : envoi de rapport depuis la maison, saisie de commandes et consultation des stocks en temps réel pour garantir un délai aux clients, supervision de structures en permanence (astreintes)... sont les contre-parties que la technologie mobile apporte à l'Homme itinérant.

Désormais dans l'ère du service, l'homme sédentaire de l'ère industrielle est devenu une sorte de "cro-magnon" remplacé par un homo-sapiens bientôt capable de se déplacer, de voyager, de partir, de parcourir des distances importantes tout en restant en liaison permanente.

Ce mémoire s'attache à introduire les notions nécessaires à la compréhension de cette évolution puis à définir un cadre de travail. Ensuite nous présentons les techniques existantes ainsi que quelques solutions qui s'appuient dessus. Enfin la mise en oeuvre dans le cadre du CICG est détaillée et nous terminons par les perspectives d'avenir.

1 ENIAC : Electronic Numerical Integrator and Computer, premier ordinateur au monde fonctionnant à lampes . 30 tonnes, 72m² (1946)

2 PRÉSENTATION

Ce qui a fait la force de l'homme, c'est sa capacité à se déplacer, à voyager et découvrir des domaines inconnus. Toutefois, cette force est accompagnée d'une grande faiblesse : il est difficile à l'Homme de ne pas communiquer avec sa communauté, de ne pas tisser de liens et de perdre de vue son entourage.

Ainsi, il y a des hommes sédentaires et d'autres nomades. Certains peuples dits "nomades" semblent ne pas avoir d'attaches à un lieu mais sont rattachés à une communauté : en réalité, le nomadisme évolue et sa définition également.

Le nomade rencontre généralement des problèmes lors de ses voyages : passage de frontières, contrôles d'identité et de nationalité, gestion des échanges locaux et transports de produits interdits. Ces problèmes sont souvent liés aux lois et à la sécurité des pays traversés. En effet, la sécurité est probablement un des termes les plus opposés au nomadisme dont la particularité ne permet pas l'établissement de règles générales.

La première partie de ce chapitre donne la définition du nomadisme et de la sécurité tel quelle est utilisé dans ce mémoire. Ensuite, nous verrons les usages des utilisateurs nomades et enfin les répercutions sur la sécurité.

2.1 Définitions

En informatique, les termes sont souvent utilisés par abus de langage ou encore il peut s'agir d'anglicismes. Ainsi de nombreux articles emploient des mots dont la signification n'est pas exacte ou bien complètement fausse. Parfois, l'abréviation anglaise est utilisée (et souvent reconnue) et d'autre fois, c'est l'abréviation française (généralement moins connue) : les interprétations des termes ne sont parfois pas identiques ou alors vaguement communes. Ce chapitre a pour objet de définir les termes et abréviations employés dans ce mémoire et détailler les abus de langage parfois utilisés.

2.1.1 Définitions liées au nomadisme

Le nomadisme est un mot qui existe depuis plusieurs dizaines d'années. La notion de nomadisme est connue de tous. L'utilisation récente des technologies sans fil et la force des commerciaux pour clamer les qualités d'un produit change toutefois le sens de certains mots.

De plus, de nouveaux mots apparaissent pour qualifier un concept nouveau, une technologie récente ou une solution inédite. L'intégration de ces termes par les français est souvent plus rapide que par les académiciens...

2.1.1.1 nomadisme

L'encyclopédie Microsoft Encarta donne comme définition du nomadisme :"n*omadisme, mode de vie des populations non sédentaires, caractérisé par des déplacements cycliques ou périodiques afin d'assurer leur subsistance*". Cette définition, ne correspond pas à priori à la définition de "client nomade" utilisant l'informatique ou la téléphonie. Et pourtant, la population active est souvent amenée dans le cadre du travail à se déplacer pour toutes sortes de motifs qui seront énumérés plus loin.

Toutefois, le terme nomadisme qui est employé dans ce rapport se rapporte plus à la notion de mobilité ou d'itinérance : elle correspond au déplacement d'un utilisateur et éventuellement d'un terminal sur un ou plusieurs réseaux informatique.

2.1.1.2 Itinérance (roaming)

Le terme "itinérance" n'existe pas dans les dictionnaires actuels (Larousse, Petit Robert...). Il s'agit d'un terme dérivé du mot itinérant qui signifie "*qui va d'un lieu à un autre pour accomplir sa tâche*"

L'itinérance est une "*fonction reliée à un système de téléphonie cellulaire, qui consiste à permettre à l'abonné d'un réseau d'utiliser son appareil dans une zone autre que celle où il a été enregistré, mais dans laquelle il peut être localisé.*" ; cette définition du site du Grand dictionnaire terminologique de l'Office Québécois de la langue française[2] est classé dans la partie télécommunication.

Par extension, l'itinérance sera employé dans ce rapport pour les systèmes informatiques dont les fonctions permettent à un utilisateur de se connecter à son système d'information à partir d'un autre réseau.

2.1.1.3 Mobilité

Aucun dictionnaire n'intègre une définition liée à l'informatique, la définition courante étant "*caractère de ce qui est mobile ; qui a la capacité de se déplacer, de se mouvoir*". Ce terme est fréquemment cité en entreprise dans l'expression "mobilité géographique" est qui traduit la capacité de changer de lieu de travail.

En informatique, le terme mobilité est la traduction du terme anglais "roaming". Alors qu'en téléphonie le terme itinérance est plus facilement employé, le mot mobilité est plus employé en informatique et en réseaux.

Toutefois, la mobilité sur les réseaux sans fil n'entraîne pas forcément un déplacement de l'utilisateur et de son équipement pendant la communication bien que cela soit aussi possible. Cela peut correspondre à un utilisateur immobile (dans un bureau, une réunion, un amphithéâtre) loin de son lieu de connexion habituel.

2.1.1.4 Interopérabilité

L'interopérabilité s'appuie sur des règles précises pour faciliter la mise en oeuvre de système, de conception différente. Les objets ou les équipements peuvent ainsi opérer ensemble et fournir un ensemble de services minimums.

Cette notion implique l'utilisation de normes et de standards (dont les définitions sont données plus loin).

2.1.2 Définitions de la sécurité

"*Situation politique, économique, matérielle ou morale dont tout risque ou tout danger est exclu*" explique le dictionnaire Focus-Bordas et qui complète cette définition par "*Dispositif destiné à éviter tout accident*".

C'est actuellement la préoccupation majeure des entreprises dans lesquelles on trouve désormais une fonction dédiée à la sécurité des systèmes d'information. Bien sûr, cet idéal étant plutôt utopique, la sécurité s'appuie sur des techniques et des méthodes permettant de limiter au mieux les risques et dangers connus.

2.1.2.1 Identification

L'identité est un ensemble d'élément qui permettent de reconnaître un individu (ex: Jean Dupont) ou une entité (ex: Coca-cola). Toutefois, une identité peut-être copiée (les vendeurs de soda au cola le savent bien) et les contre-façons existent.

2 http://www.granddictionnaire.com/

L'identifiant est un élément normalisé associé à une identité : le numéro INSEE est un identifiant unique en France. Une adresse MAC est également un numéro unique désignant un seul équipement. Il est malheureusement facile de copier ou forger un identifiant : la sécurité ne peut pas être assurée par un identifiant.

2.1.2.2 Authentification

Pour s'assurer qu'un identifiant est bien présenté par l'identité qu'il représente, il faut l'authentifier.

L'authentification est donc un procédé permettant à un individu ou une entité de prouver son identité : la photo pour une carte nationale d'identité, une empreinte digitale, vocale ou rétinienne pour des systèmes perfectionnés ou encore un mot de passe ou une carte à puce pour les méthodes les plus courantes.

L'authentification repose sur la notion d'un secret partagé ou d'éléments infalsifiables.

2.1.2.3 Autorisation

Pour accéder à un environnement sécurisé, il est nécessaire d'avoir une autorisation. L'autorisation correspond généralement à une fonction dans cet environnement. En informatique, les droits fournis à un utilisateur authentifié sont liés à son rôle et éventuellement au moyen employé pour ce connecter. D'autre part, les ressources ont aussi des limitations d'accès propres qui permettent des accès personnalisés. Ainsi, pour plusieurs personnes ayant un rôle d'étudiant, une seule pourra accéder à sa ressource courrier. La notion de groupe permet, inversement, d'autoriser un ensemble de personnes à accéder à une ressource sans aucune déclaration individuelle.

2.1.2.4 Accounting

L'accounting est un terme anglais qui se traduit littéralement par "comptabilité" mais la signification du terme est plutôt "traçabilité". L'accounting permet de suivre le fonctionnement d'un réseau en fournissant des statistiques sur la charge globale, le nombre d'utilisateurs actifs, les accès rejetés, etc.

En terme de sécurité, l'accounting est fondamental : en effet, l'ASSI[3] et l'entreprise étant responsable des fautes commises à partir de leur réseau, il est nécessaire de pouvoir déterminer avec précision qui utilise un système et à quelle moment.

2.1.2.5 cryptologie

La cryptologie est la science des écritures secrètes et des messages chiffrés. Elle comprend la cryptographie et la cryptanalyse.

Cette science utilise un vocabulaire souvent mal utilisé ou dont les anglicismes sont venus remplacer les termes français.

La liste ci-dessous redonne la définition exacte de ces mots et leur équivalent anglais (entre parenthèses) [WEB001].

- Cryptographie (cryptography) : du grec *kruptos*, caché, et *graphein*, écrire. Science du chiffrement. La loi française définit les prestations de cryptologie comme étant "*toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en information ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet*"[4].
- Cryptanalyse (Cryptanalysis) : Art de déchiffrer les messages codés (sans obtenir de manière officielle le mécanisme ou le code utilisé).

3 ASSI : Agent de Sécurité de Systèmes d'Information
4 Article 28 de la loi 90-1170 du 29 décembre 1990 modifiée

- Chiffrement (encryption) : Ensemble de méthodes permettant de rendre un message incompréhensible. Les anglicismes suivants sont parfois employés : cryptage et crypter (à la place de chiffrer). Les anglais emploient aussi le terme encipher (et decipher pour déchiffrer).
- Stéganographie (Steganography) : La stéganographie consiste à cacher un message dans un document anodin afin qu'il passe inaperçu. Actuellement, il est facile de cacher un fichier texte dans une image jpeg par exemple.
- Cryptogramme (CipherText) : texte codé résultant du chiffrement.
- Texte en clair (Plaintext) : texte original.
- Challenge : employé dans le sens de défi, il représente une épreuve qu'il faut réussir pour obtenir un avis positif. Le chiffrement d'un ensemble de données de taille limité est un challenge.

2.2 Constats sur le nomadisme informatique

Le nomadisme est désormais entré dans notre vie quotidienne : téléphone cellulaire portable, organiseur, ordinateur portable... personne n'y échappe et toutes les tranches d'âge sont visées. La mobilité apporte des services nouveaux quelque soit la localisation de l'utilisateur : SMS, logos et sonneries personnalisés, accès aux services météorologiques, horaires de trains, cours de la bourse, actualités, messages vocaux...

2.2.1 Statistiques et évolutions

La mobilité touche de plus en plus de personnes en entreprise. Les fonctions les plus nomades sont les commerciaux mais aussi les dirigeants et les intervenants pour maintenance. Le tableau ci-dessous présente la répartition par fonction (s*ource Louis Harris "les entreprises, la mobilité et les NT" en 2004, cité dans le livre blanc sur la mobilité en entreprise*) :

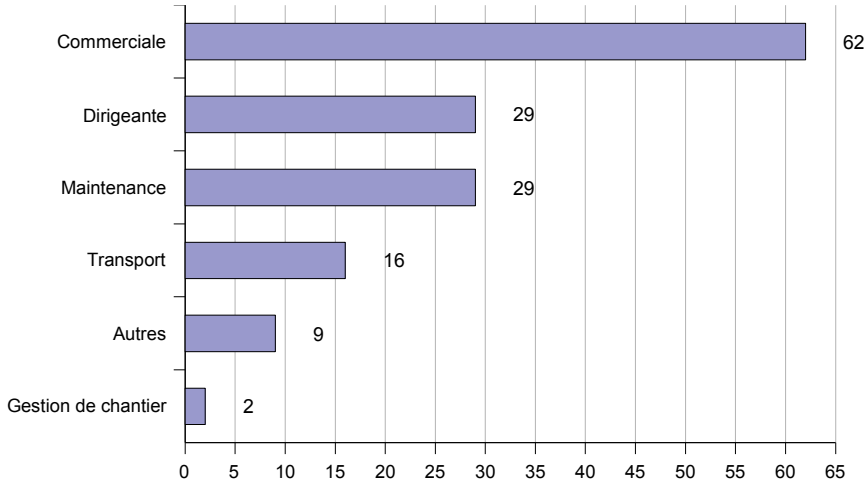


Illustration 1: Répartition des fonctions mobiles en entreprise

Cette évolution est liée à l'accroissement de productivité des individus ce qui entraîne de nouveaux usages. Ces usages entraînent à leur tour de nouvelles applications. Les usages principaux sont le passage de commandes, l'accès aux inventaires ou aux bases clients, la récupération de notices et d'informations et la prise de décision en temps réel.

D'autre part, la mobilité implique l'utilisation d'un terminal : téléphone, PDA, ordinateur portable... et il est intéressant de constater la notion de mobilité est très associé aux téléphones mobiles, comme le montre le tableau suivant (*source Louis Harris "les entreprises, la mobilité et les NT" en 2004, cité dans le livre blanc sur la mobilité en entreprise*) [LIBL04]:

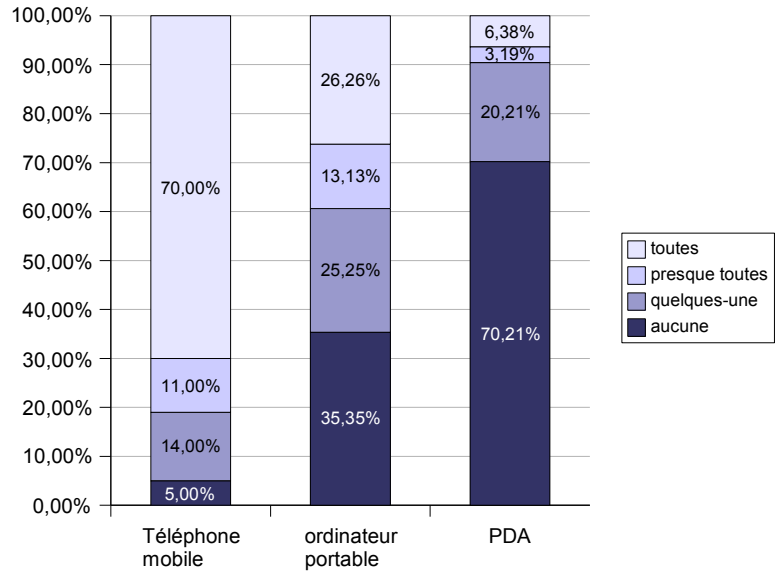


Illustration 2: Équipement des personnes mobiles en entreprise (2004)

Cette faible pénétration des ordinateurs portables et des PDA s'explique toutefois par les raisons qui freinent le développement des solutions mobiles. Il apparaît notamment (toujours d'après Louis Harris) que le coût de mise en place, la sécurité et la complexité de la mise en oeuvre sont les arguments les plus bloquants, comme le montre l'illustration suivante :

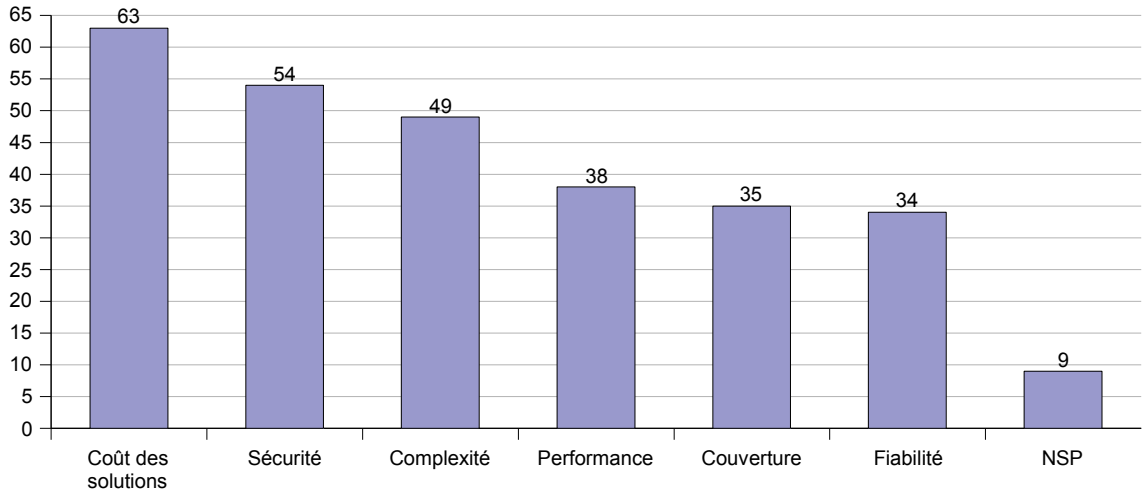


Illustration 3: Principaux freins au développement des réseaux mobiles

Le retour sur investissement et l'interopérabilité sont également des obstacles : les entreprises ne peuvent accepter des solutions hétérogènes dont la maintenance grève le budget.

Mais encore, les entreprises attendent des avantages de ces technologies mobiles. D'après IBM Business Consulting Services, il y a huit axes de bénéfices :

- Qualité des données (mise à jour régulières, diminution des doubles saisies, plus d'informations collectées, informations plus précises),
- Productivité (diminution des coûts administratifs, diminution des interventions nécessitant une deuxième visite, ordonnancement plus efficace, outillage et pièces corrects, re-planification dynamique),
- Accès à l'information sur site (accès direct aux informations pertinentes et à jour, moindre dépendance vis-à-vis des processus papier),
- Pilotage de la performance (suivi des niveaux de service, assistance et retour d'informations individualisés, clôture des interventions plus précise)
- Lien avec l'entreprise (facilité de communication, renforcement du sentiment d'appartenance)
- Service client (moins de pénalités pour non-respect des rendez-vous, meilleur respect des engagements, moins d'opportunités perdues)
- Sécurité des agents (possibilité de suivre les agents en zones sensibles ou les travaux avec risques)
- Traçabilité des interventions (horodatage, justification du fonctionnement non discriminatoire de l'opérateur)

Il y a également une notion de profil de mobilité : les employés n'utilisent pas les mêmes équipements car les besoins ne sont pas les mêmes pour tous les métiers. Il faut employer le bon outil et pour cela, connaître les lieux d'utilisation et les solutions offertes.

	GPRS/UMTS	*ADSL/RTC*	*Wi-Fi*
Au bureau			☺
A la maison		☺	☺
Chez un client			☺
Sur la route	☺		
Au café/restaurant		☺	☺

Tableau 1: Lieux et mobilité

Dès lors, le lieu et le moyen à utiliser pour accéder à certaines ressources facilitent le choix pour la mise en oeuvre d'une solution.

Toutefois, les ventes d'ordinateurs portables sont passées de 23% en 2003 à 29% en 2004 sur le volume des ventes en micro-informatique [FERO04]. La plupart intègre désormais la norme 802.11 en standard, ce qui favorise l'utilisation des réseaux sans fil. Enfin, le nombre de hotspot augmente très rapidement et les estimations par les grands opérateurs montrent que le marché est porteur.

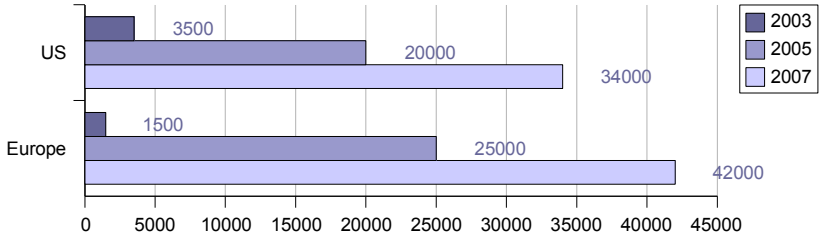


Illustration 4: Nombre de hotspots déployés

2.2.2 Récapitulatif

Cette série de statistiques nous permet de voir que le nomadisme en entreprise touche tout le monde mais que ce sont les fonctions commerciales et dirigeantes qui sont les plus demandeuses.

Les deux tiers des personnes mobiles utilisent un PC portable alors que seulement un tiers emploie un PDA. De plus, 95% des employés ont un téléphone mobile : ce marché semble moins concerner la mobilité informatique mais les nouvelles offres hauts débits (UMTS, 3G...) ainsi que l'évolution technique devraient rapprocher les téléphones et les PDAs et trouver des applications légères compatibles avec les réseaux internet à moyen terme.

Wi-Fi est une certification très employée et utilisable partout (sauf dans les transports) : certains fabriquants ont déjà annoncé des puces spécialisées compatibles 802.11 pour les téléphones mobiles (Samsung, communiqué de presse du 02 décembre 2004). Il est donc prévu un déploiement de cette technologie de manière intensive dans les années à venir (à la fin 2005, l'europe devrait avoir déployé 25000 ASFI).

Cet engouement est toutefois freiné de manière presque égale par le coût... et par la sécurité !

2.3 Répercussions sur la sécurité

La section précédente permet de se rendre compte de la pénétration de la mobilité sur le marché français. Toutefois, 54% des responsables refuse de développer ces réseaux en raison de la sécurité : si celle-ci s'appuyait énormément sur l'accès physique à l'infrastructure, désormais les réseaux sans fil changent la politique des ASSI : autoriser la mobilité des utilisateurs implique généralement l'ouverture des systèmes d'information sur Internet... et cette ouverture augmente le risque de pénétration par des personnes mal intentionnées. Les utilisateurs quand à eux, veulent bénéficier d'un accès à l'intranet en utilisant des supports différents et dès lors, la multiplicité des systèmes d'accès accroît la charge de travail : configurations, maintenances, diagnostics, redondances de matériels, surveillances...

De plus, l'ASSI engage désormais sa responsabilité (en plus de celle de l'entreprise) en cas d'attaque à partir de son réseau : un poste à haut risque et qui implique une très bonne connaissance des failles et des attaques possibles.

Dès lors, l'ASSI dispose de plusieurs méthodes de sécurisation des réseaux et de machines : parmi les plus classiques :

- Identification et authentification (généralement un nom associé à un mot de passe),
- Traçabilité (journaux),
- Gestion des autorisations et des droits,
- Chiffrement des données (cryptage),
- Alertes de sécurité (anti-virus, systèmes d'exploitations et applications),
- Surveillance en temps réels (IDS, scanners, volumétrie...)
- Formation (utilisateurs),
- ....

La sécurité est devenue très importante et elle constitue pour les entreprises l'un des budgets les plus élevés. Cela n'est pas seulement dû à l'émergence des technologies sans fil mais aussi à la croissance du nombre de virus et vers informatique, à l'augmentation du nombre d'équipements en réseau et à la diversité des protocoles permettant l'accès aux systèmes d'informations.

2.3.1 Les attaques classiques

En informatique, il existe de nombreuses attaques possibles : certaines sont basées sur des bugs ou failles des logiciels, d'autres sur l'accès à certaines ressources insuffisamment protégées ou encore sur l'ignorance ou la curiosité des utilisateurs.

2.3.1.1 Attaques externes

Les attaques externes sont les attaques menées depuis l'Internet. Tout réseau connecté à Internet est soumis à de nombreuses attaques qui ont plusieurs objectifs :

- Obtenir des informations sur les serveurs du réseau : la connaissance du système d'exploitation permet d'en connaître les failles officielles et peut-être trouver un serveur qui n'a pas été mis à jour. L'attaque la moins discrète est le balayage de port car des services comme le transfert de fichier (FTP), le terminal distant (Telnet), le service de messagerie (SMTP, POP...) renvoient généralement une chaîne de caractère indiquant la version du service.
- Obtenir un compte sur une machine connectée au réseau : en utilisant une faiblesse du système d'exploitation, un pirate peut se connecter sur une machine et agir par rebond. L'attaque menée vers un réseau sera détectée comme provenant de cette machine mais ce ne sera pas celle du pirate.
- Obtenir un plantage d'un serveur : l'arrêt brutal d'un serveur ne lui permet pas de fournir d'informations sur l'attaquant mais en plus, l'indisponibilité de ce serveur peut entraîner des pertes importantes pour l'entreprise : informations, transactions, ordres, etc. comme l'attaque mené en janvier 2003 sur les serveurs coréens puis américains (13000 guichets de la "Bank of America" ont perdus l'historique de leurs transactions). Les attaques classiques sont le déni de services (DoS ou Deny of Service) ou le remplissage de buffer (buffer overflow) basées sur une faille du système.
- Intercepter et modifier des communications : en bloquant un serveur, le pirate peut introduire à sa place un serveur à lui qui aura presque la même fonction. Toutefois, ce nouveau serveur peut également modifier les messages qui transitent par lui et en changer le contenu. L'intérêt est que le destinataire reçoit d'une machine qu'il croit connaître un message modifié tandis que le pirate dispose de l'information originale. Ce type d'attaque est appelé "man in the middle" (MITM) ou l'homme du milieu.

2.3.1.2 Attaques par ingénierie sociale

Les attaques par ingénierie sociale sont tournées vers les utilisateurs et administrateurs. Plutôt que de tenter une attaque externe, le pirate va tenter d'obtenir l'information par un des employés de la société. Pour cela, il peut se faire passer pour un commercial, un technicien de maintenance, un administrateur du réseau. Il emploiera le téléphone, le courrier, le courrier électronique, voire même le contact direct. Kevin Mitnick un hacker connu a écrit un livre sur ces techniques : L'art de la supercherie. Le phishing[5] est devenu une technique par courrier électronique en affichant un texte demandant de renouveler les mots de passe et un lien connu mais qui pointe en réalité vers une page web d'un serveur pirate : cette dernière est très similaire au site officiel et l'utilisateur saisie les informations demandées en croyant accéder au site officiel. Le pirate dispose alors d'une base de données contenant les comptes et mots de passe de nombreux utilisateurs du service officiel.

5 Contraction de fishing (pécher) et phreaking (pirater les lignes téléphoniques)

2.3.1.3 Attaques par infection

Les attaques par infection concernent les virus, les vers, les spywares[6] et les chevaux de Troie. Ces programmes sont des fichiers contenant du code exécutable (macro VBS pour les fichiers DOC ou XLS par exemple) et qui, lorsque le fichier est ouvert, tente d'infecter le poste de l'utilisateur.

Pour paraître crédible, les virus utilisent généralement le carnet d'adresse de la machine, aussi il n'est pas surprenant de trouver un message d'un ami franco-français qui écrit... en anglais ! Ce devrait être suffisamment surprenant pour ne pas ouvrir la pièce jointe et pourtant de nombreuses personnes se laissent attraper. Le fléau est tel que de nombreux administrateurs ont installés des antivirus sur leurs serveurs de courrier.

Les vers utilisent le réseau via les applications diverses comme les navigateurs, les programmes peer-to-peer, les lecteurs multimédia, les messageries instantanées... ils n'ont pas besoin d'une action de la part de l'utilisateur pour s'activer.

Les chevaux de Troie (par référence au héros mythique Ulysse) est un programme malicieux intégré dans un programme sain. Lorsque le programme sain est lancé, le cheval de Troie est actif et écoute sur un port du système (dans une plage peu utilisée pour éviter un conflit) : il peut alors accepter des commandes en provenance d'un pirate. Le plus célèbre est probablement "Back Orifice" en référence à la suite "Back Office" de Microsoft. Actuellement, une nouvelle menace par cheval de Troie voit le jour avec des programmes capables de simuler l'accord d'un utilisateur lors d'un message provenant d'un pare-feu personnel (CERT – janvier 2005).

Les spywares sont des logiciels espions qui recueillent des informations sur le comportement de l'utilisateur. Certaines données privées sont parfois placées dans des "cookies", de petits fichiers utilisés par les sites web pour mémoriser des données. Une autre utilisation des spywares est l'enregistrement des touches appuyées par l'utilisateur : le pirate est alors en mesure de connaître les mots de passe tapés au clavier. Ces programmes sont aussi appelés "keylogger".

2.3.2 Les attaques sans fil

Les réseaux sans fil ouvrent désormais la voie à de nouvelles attaques : parce que les ondes hertziennes ne sont pas facilement contrôlables dans l'espace, l'implantation d'un équipement réseau sans fil revient à placer un ensemble de prises réseau hors des bureaux.

Deux méthodes existent d'ailleurs pour détecter les réseaux sans fil disponible : le "war-driving" et le "war-shalking" :

2.3.2.1 War-driving

Le war-driving est une technique simple qui consiste à circuler dans les rues et les lieux publics à la recherche d'émetteurs. Un PC portable équipé avec une carte réseau sans fil écoute les différentes fréquences et détecte les caractéristiques des émissions reçues.

2.3.2.2 War-chalking

Le war-chalking est une extension du war-driving. Cette méthode consiste simplement à noter près de l'émetteur (du moins dans sa zone d'émission) ses caractéristiques : est-ce un réseau ouvert, fermé, protégé ? Pour cela, trois symboles sont couramment utilisés (illustration 5).

6 Logiciel-espion

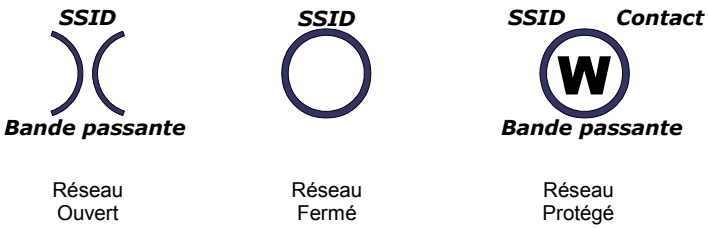


Illustration 5: Symboles utilisés dans le war-chalking

Ces symboles sont tracés à la craie sur un mur, un trottoir. Ceux qui n'en connaissent pas la signification n'y voit qu'un graffiti alors que les hackers y voit une occasion facile de se connecter au réseau. De plus, l'attribution d'adresses IP de manière dynamique facilite la mise en oeuvre d'un équipement sur ce réseau.

Une fois un réseau détecté, les réseaux sans fil sont la cible des attaques précédemment citées mais aussi des suivantes (liées aux techniques de déni de service) :

2.3.2.3 brouillage

Les fréquences employées par les réseaux sans fil peuvent être brouillés et aucune communication ne peut passer. Bien que brutale, cette attaque utilisée de manière ponctuelle peut perturber un réseau sans permettre de trouver facilement la source.

2.3.2.4 arp-poisoning

Ce type d'attaque consiste à répondre plus rapidement que les autres postes à la demande de corrélation entre adresse IP et adresse MAC (arp-who-has) mais en fournissant une fausse adresse MAC. Une méthode dérivée de cette attaque est de remplir les tables ARP des équipements du réseau pour les saturer.

Le résultat rend possible l'usurpation d'une machine par une autre machine hors des locaux de l'entreprise.

2.4 Conclusion

Bien que la mobilité soit un concept possible avant (déplacements chez un client, en réunion ou lors d'un séminaire), les technologies sans fil ont abolies le frein psychologique du réseau fermé, représenté par le câblage. La grande simplicité d'implémentation d'un réseau sans fil attire les décideurs qui voit là, un moyen de suivre au plus près les besoins de leurs clients et diminuer le nombre d'étapes intermédiaires de saisie.

Technologie récente, la mobilité en informatique apporte un confort d'utilisation non négligeable : de nombreux équipements terminaux sont compatibles, peuvent communiquer entre eux et les solutions sont simples à mettre en place. Le déploiement des réseaux sans fil à grande échelle est une réalité incontournable autant en entreprise que chez les particuliers.

Toutefois, cet accroissement de liberté complique la tâche des administrateurs qui définissaient la sécurité de leurs systèmes d'information par rapport à l'accessibilité physique des points de connexions. Les réseaux sans fil rendent ce jugement caduque et implique la recherche de solutions pour parer aux nouvelles menaces dont leur réseau est la proie.

Ainsi ce pose la problématique entre deux objectifs opposés : comment concilier mobilité et sécurité, liberté et contrôle, facilité et contrainte ?

3 CAHIER DES CHARGES

Après avoir décrit la situation du nomadisme et de la sécurité de manière générale, il est maintenant possible de décrire quelles sont les attentes des universités de Grenoble, comment elles déterminent leurs besoins et tentent de résoudre leurs problèmes.

En premier lieu, le fonctionnement du CICG ainsi que sa structure seront expliqués avec comme objectif la compréhension du rôle du CICG entre les différents organismes.

Puis une définition des différents profils utilisés dans les universités et leurs usages associés permettra de connaître le contexte du nomadisme en université.

Enfin, la rédaction d'un cahier des charges et des problèmes liés à l'architecture en place aura pour but de faciliter le travail de recherche et d'étude.

3.1 Définition de l'environnement

Les universités de Grenoble mutualisent un certain nombre de ressources : l'avantage est de diminuer les coûts de gestion, d'exploitation, et d'administration de ces ressources. Dans ce cadre, le Centre Interuniversitaire de Calcul de Grenoble matérialise cette volonté.

3.1.1 Rôles du CICG

Le C.I.C.G. est un service interuniversitaire qui a été crée en 1972 par les établissements d'enseignement supérieur de l'académie de Grenoble.

Depuis fin 1995 les universités, Joseph Fourier, Pierre Mendès-France, Stendhal, de Savoie, et l'Institut National Polytechnique de Grenoble l'ont chargé de deux missions

- l'informatique de gestion qui est assurée par le Département Informatique de Gestion.
- les réseaux informatiques qui est assuré par le Département réseau.

ces deux missions sont définies et réglementées par deux conventions en date du 22 mai 1996 :

- la convention relative à l'organisation de l'informatique de gestion.
- la convention relative à l'activité de réseau informatique.

Il est aussi chargé de la diffusion des logiciels ayant fait l'objet d'accords de diffusion avec le Ministère de l'éducation nationale de l'enseignement supérieur et de la recherche.

- Le C.I.C.G. est administré par un conseil d'administration. Il est dirigé par un Directeur.
- Le C.I.C.G. comprend sous l'autorité du Directeur :
- le Département Informatique de Gestion,
- le Département Réseau,
- l'activité diffusion de logiciels,
- l'administration.

L'organigramme (illustration 6) clarifie la structure du CICG.

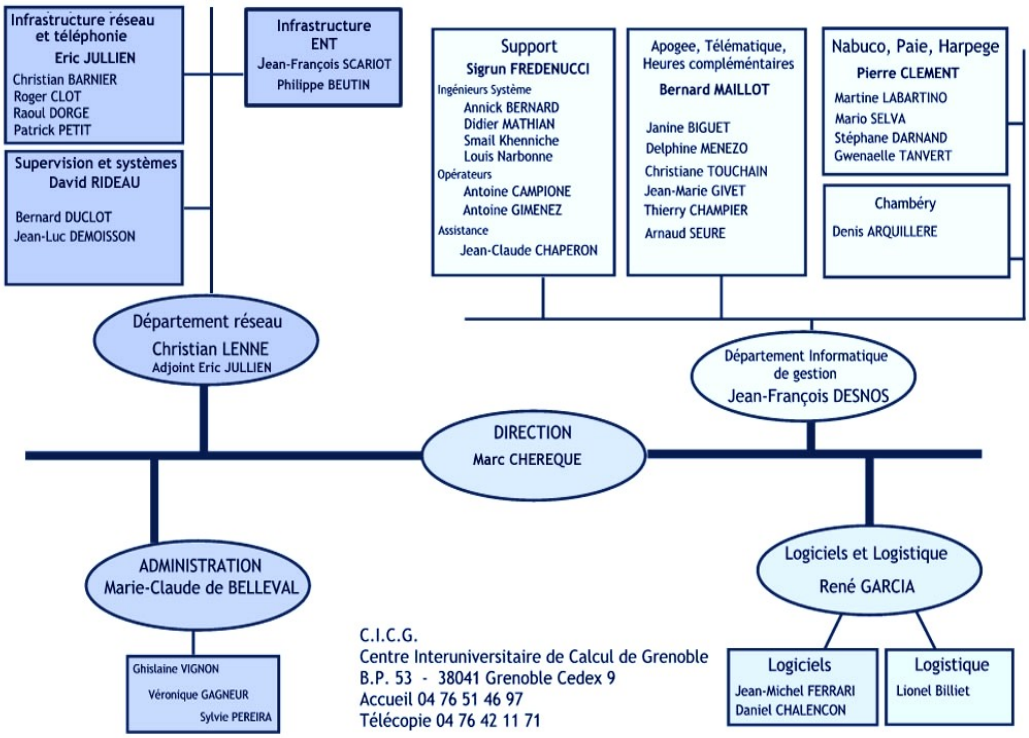


Illustration 6: Organigramme du CICG

3.1.2 Département réseau

Le département réseau du CICG est un service interuniversitaire qui réalise des missions pour le conseil d'administration en accord avec le Comité de Pilotage qui relève des différentes Universités, Scientifique (U1), Sciences Sociales (U2), Lettres (U3) et de l'INPG.

Deux missions principales se dégagent :

- La gestion du réseau interuniversitaire
- La coordination des actions transversales.

Le CICG s'appuie sur le réseau de fibres optiques dont le propriétaire est Metronet mais dont le CICG loue une partie. Il est responsable de l'interconnexion des universités sur ce réseau et de leur raccordement au réseau RENATER, par l'intermédiaire du réseau Tigre.

Illustration 7: Dorsale haut débit Metronet

Toutefois, il est à noter que le CICG n'est pas une entité juridique : ainsi, lors de facturation ou de gestion de budget, le CICG est rattaché à l'université Joseph Fourier.

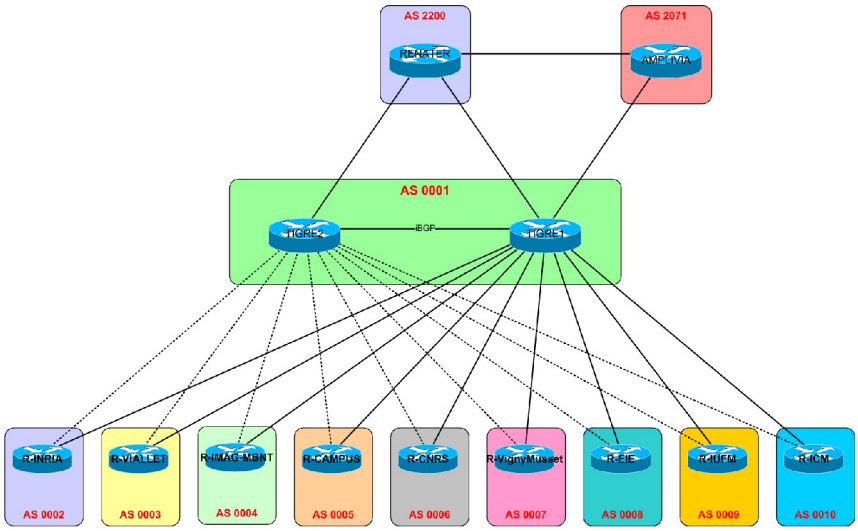


Illustration 8: schéma des réseaux gérés par le CICG

3.1.3 Les différents réseaux

Pour accéder à ses services (messagerie, intranet, web) un utilisateur va utiliser plusieurs réseaux dont les structures sont hiérarchisées.

3.1.3.1 Réseau TIGRE

Le réseau **TIGRE** est le réseau de recherche et d'éducation de Grenoble. Techniquement, il est constitué de deux étoiles routeurs/commutateurs redondants et situées géographiquement au CICG Saint-Martin d'Hères et au centre de Grenoble (Institut National Polytechnique de Grenoble). Le CICG loue les fibres optiques à MetroNet.

Les organismes utilisant ce réseau sont :

- UJF (Université Joseph Fourier, http://www.ujf-grenoble.fr/),
- INPG (Institut National Polytechnique de Grenoble, http://www.inpg.fr/),

- UPMF (Université Pierre Mendès France, http://www.upmf-grenoble.fr/),
- IMAG (Institut d'informatique et Mathématiques Appliquées de Grenoble, http://www.imag.fr/) qui est en fait, une fédération d'unités de recherche du CNRS, de l'UJF, de l'INRIA et de l'INPG.
- CNRS (Centre National de la Recherche Scientifique, http://www.cnrs.fr/),
- INRIA (Institut National de Recherche en Informatique et en Automatique, http://www.inrialpes.fr/).

Ainsi la disponibilité du réseau de type RMU[7] est excellente et permet l'accès à Renater dans les meilleures conditions.

3.1.3.2 Réseau AMPLIVIA

Le réseau **AMPLIVIA** est le successeur du réseau ARAMIS. Il est financé par la région et est ouvert à des " communautés " reconnues de façon autonome sur ce réseau, actuellement : universités et centres de recherche publics de l'académie de Grenoble, universités et centres de recherche publics de l'académie de Lyon, communauté " enseignement scolaire Académie de Grenoble : écoles, collèges, lycées publics et privés sous contrat, organismes publics de l'académie : CIO, CRDP/CDDP, GRETA, IA, etc... communauté " enseignement scolaire Académie de Lyon, communauté " Enseignement agricole ", communauté " formation continue " (CFA...).

3.1.3.3 Réseau RENATER

Le réseau **RENATER**[8] est le réseau national de la recherche et de l'éducation. Le rôle du GIP[9] RENATER, maître d'ouvrage du réseau national, consiste :

- A mettre en œuvre dans le réseau les éléments techniques de sécurité conformes à l'état de l'art, et à en assurer l'exploitation par un opérateur professionnel avec un cahier des charges précis,
- A opérer un des CERT français ; un CERT est une entité d'information technique et opérationnelle sur les actions délictueuses en matières de réseaux et d'équipements informatiques,
- A susciter, chez les organismes et sites connectés, des actions de sensibilisation des responsables et des utilisateurs, ainsi que des actions de mise en œuvre des techniques de sécurisation de leurs réseaux de site et de leurs équipements informatiques (depuis les grands ordinateurs partagés jusqu'aux stations de travail et micro-ordinateurs de chaque utilisateur).

A responsabiliser les acteurs de tous les sites raccordés à RENATER, par l'intermédiaire de la charte de sécurité et de déontologie que le responsable de tout site connecté à RENATER doit signer et respecter.

3.1.3.4 Réseau GEANT

Le réseau **GEANT**[10] est un réseau européen. Il connecte 30 réseaux de recherches et d'éducation (NREN[11]) qui desservent 34 pays. Renater en fait partie.

7 RMU : Réseau Métropolitain Universitaire.
8 RENATER : Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche (http://www.renater.fr/)
9 GIP : Groupement d'Intérêt Public.
10 GEANT : Gigabit European Academic Network (http://www.geant2.net/)
11 NREN : National Research and Education Network.

3.1.3.5 Réseau EDUROAM

Le réseau EDUROAM[12] permet aux utilisateurs des institutions y participant de se connecter en n'importe quel point en utilisant son accréditation habituelle. Il est issue du développement de TERENA[13] (TERENA Mobility).

TERENA est né en 1994, de l'association de RARE[14] et EARN[15]. TERENA est donc une association dont le but est de participer à l'amélioration des réseaux pour la recherche et l'éducation. Pour cela, l'association travaille sur les thèmes suivants :

- Lower Layer Technologies (les techniques de bas niveau employées dans les réseaux),
- Security (la sécurité des systèmes et des réseaux et la coordination entre les différents acteurs. A titre d'exemple, les CSIRT[16])
- Middleware (la "colle" entre l'application et le réseau)
- Mobility (l'outil permettant le nomadisme des étudiants et des chercheurs entre les différents domaines)
- Voice and Video Collaboration (la vidéoconférence, la téléphonie sur IP, les flux audio et vidéo)
- Grid (notamment la modélisation des systèmes de calculs distribués).

Le groupe de travail pour la mobilité (TERENA Task Force) existe depuis janvier 2003 et le projet s'appelle "EduRoam". Ce projet est basé sur une structure hiérarchique de serveurs RADIUS.

3.2 Analyses et classifications

L'analyse des besoins existants permet de déterminer ce qui est nécessaire toutefois, les besoins sont définis par les usages et les usages dépendent des utilisateurs. La taxonomie des utilisateurs, des moyens employés et des ressources utiles est la base de cette section.

3.2.1 Classification des utilisateurs

Dans l'environnement des universités les utilisateurs sont nombreux. En effet, il y a les étudiants, les professeurs, le personnel administratif, le personnel technique, les visiteurs...

- Les étudiants : population très diversifiée en terme de connaissance des outils informatique. Les nombreuses filiales (mathématiques, lettres et langues, droit, économie, techniques, sciences, etc.) et les nombreux cursus (DUT, DEST, licence, maîtrise, ingénieur, etc.) ne permettent pas de déterminer un profil type précis. On peut toutefois dire qu'ils ont un budget limité et qu'ils recherchent activement les solutions gratuites (l'illégalité n'est pas un problème majeur pour eux et c'est dans cette population que les usages des réseaux peer-to-peer est le plus généralisé). Depuis l'offre "un PC portable Wi-Fi pour un euro par jour"[17] les étudiants deviennent très "mobiles".

12 EDUROAM : EDUcation ROAMing (http://www.eduroam.org/)
13 TERENA : Trans-European Research and Education Networking Association
14 RARE : Réseaux Associés pour la Recherche Européenne
15 EARN : European Academic and Research Network
16 CSIRT : Computer Security Incident Response Teams
17 Voir le site http://delegation.internet.gouv.fr/mipe/projet.htm

- Les professeurs : également très diversifiés, les professeurs investissent beaucoup de temps dans l'élaboration de leurs cours. Ils n'ont que rarement un bureau fixe, tout au mieux une salle commune avec des postes non-dédiés. Une partie du travail est effectuée à la maison ou en laboratoire. Ils attendent de la mobilité une simplification de leurs accès et un minimum d'investissement de leur part. La sécurité est essentielle la plupart des professeurs accèdent d'une part aux réseaux pédagogiques (celui des étudiants) et d'autre part aux réseaux des institutions (relevés de notes, dossiers, etc.).
- Le personnel administratif : il gère le bon fonctionnement des universités : gestionnaires, directeurs, secrétaires, ... disposent d'un bureau fixe dans les locaux des universités. Certains disposent même de plusieurs bureaux, en particulier s'ils ont en charge plusieurs bâtiments très distants ou plusieurs fonctions. Ils attendent un réseau fiable et sécurisé et ont accès facilement à un support.
- Le personnel technique : il gère les équipements et les services. Dans cette catégorie se trouve notamment les CRI : c'est généralement ces personnes qui administrent les réseaux et serveurs. Ils sont amenés à utiliser des équipements hétérogènes (Linux ou Windows ou Mac dans différentes versions). Plus compétents techniquement, ils attendent du nomadisme un minimum de travail : moins de support, moins de maintenance et plus de fiabilité. En effet, le support aux étudiants est extrêmement consommateur de ressources.
- Les visiteurs : un commercial, un représentant mais aussi un technicien en maintenance ou tout autre personne nécessitant un accès temporaire et limité au réseau. Dans ce cadre, cette personne peut aussi venir d'une université ou d'un environnement universitaire dans le cadre d'un séminaire, un congrès, une réunion. Ces personnes recherchent principalement un accès à Internet pour accéder à leur messagerie et à leur intranet.

3.2.2 Classification des équipements

L'utilisation d'un seul type d'équipement pour se connecter serait utopique : les offres des constructeurs essayant d'obtenir le plus grand nombre de part de marché rendent les choix des utilisateurs très éclectiques. Il existe plusieurs sortes de matériels et plusieurs systèmes fonctionnant dessus.

Les équipement suivants fournissent une connexion aux réseaux sans fil :

- ordinateur portable : l'équipement en vogue en ce moment, il combine la puissance d'un ordinateur complet (écran haute résolution, clavier, disque-dur et logiciels courants) avec l'encombrement d'un gros classeur. Son autonomie reste malgré tout limitée (environ deux heures) et il est relativement coûteux. Deux grandes catégories se détachent : les machines compatibles et les systèmes Apple. Les machines compatibles peuvent avoir un système exploitation Microsoft Windows (98, Millénium, NT pour les plus anciens ou 2000 et XP pour les appareils supportant les connexions sans fil nativement) ou Linux (Redhat, Mandrake, Debian pour les plus connus mais il en existe des dizaines d'autres).
- PDA : ces petits organiseurs sont pratiques car leur encombrement est réduit tandis que leur autonomie est de plusieurs jours. Toutefois, leur ergonomie est loin d'égaler celle d'un ordinateur portable même s'il intègre des outils compatibles avec les suites bureautiques. Plusieurs systèmes d'exploitation existent : Symbian OS (Sony et Ericsson), Windows Mobile 2003 (Microsoft), Palm OS (Palm), Pocket PC et Linux OS sont les plus connus.

- SmartPhone : entre le téléphone et l'organiseur, le smartphone se veut multi-fonctions. D'ailleurs les utilisateurs ne s'y trompent pas comme en témoigne l'article "PDA en baisse, smartphone en hausse" de Clubic[18]. Il permet de téléphoner et intègre les possibilités d'un PDA pour un encombrement équivalent.

3.2.3 Classification des accès géographiques

Quelque soit le moyen employé, l'utilisateur désire obtenir un service : lire son courrier, accéder à Internet, utiliser les ressources de son intranet, saisir des informations, se synchroniser avec un ensemble d'applications...

Pour lui, le fonctionnement de l'outil utilisé doit être simple et cohérent : l'utilisation à la maison, au bureau, en déplacement ou dans un cybercafé ne devrait pas être différent !

Malgré tout, les différences sont importantes et il convient de les référencer :

	Bureau	Maison	Cybercafé	Déplacement
Lire son courier (webmail)	Facile	Facile	Facile	Facile
Lire son courier (application IMAP/POP)	Facile	Sécurisé	Difficile	Sécurisé
Accéder à Internet	Facile	Facile	Facile	Facile
Accéder aux ressources intranet	Facile	Sécurisé	Difficile	Sécurisé
Utiliser ressources locales (imprimantes...)	Facile	Facile	Facile	Difficile
Utiliser les applications (synchronisation...)	Facile	Sécurisé	Difficile	Difficile

Tableau 2: localisation et usage des services

- Au bureau : tout les services sont facilement accessibles. L'ordinateur appartient à l'entreprise ou à l'université et sont configurés de manière similaire par un service informatique dont la tâche est de veiller à l'homogénéité des équipements et des applications. Les services ne nécessitent que peu d'actions de la part de l'utilisateur pour fonctionner : l'authentification est presque unique.
- A la maison : certains services sont accessibles aisément par le réseau de l'opérateur choisi par l'utilisateur : accès à Internet, utilisation des ressources locales ainsi que la lecture de courrier via un serveur spécialisé (webmail) ! En revanche, il n'est pas possible (si la sécurité est bien assurée) d'utiliser un client IMAP/POP standard pour accéder au serveur de l'entreprise. De même pour accéder aux ressources intranet ou aux applications (calendriers, bases de données, etc.). De plus, le poste employé est généralement l'ordinateur personnel de l'utilisateur (mais qui est souvent utilisé par toute la famille et pour toute sortes d'activités) sur lequel il n'est pas possible de garantir l'intégrité. Toutefois, l'utilisateur possède les droits nécessaires pour installer un logiciel.
- Dans un cybercafé : la problématique est identique à celle du poste à la maison avec une contrainte supplémentaire : les ordinateurs sont en libre service et l'utilisateur n'a généralement pas les droits pour exécuter l'installation d'une application.
- En déplacement : c'est un cas un peu particulier dans lequel l'utilisateur emploie un équipement géré par le service informatique de l'université ou l'entreprise. Le poste est considéré comme sûr, les applications présentes sont celles définies dans la politique du service informatique. En revanche, la fiabilité de la connexion n'est pas garantie !

18 Voir le lien http://www.clubic.com/actualite-20155-pda-en-baisse-smartphone-en-hausse-.html

3.3 Description de l'architecture d'origine

Depuis 2003, le CICG travaillait déjà sur la problématique du nomadisme : ce domaine relativement nouveau était abordé par les pionniers de la mobilité ! Les constructeurs, les utilisateurs et les développeurs ont cherchés des solutions pour résoudre les problèmes au cas par cas ou bien adapter des solutions existantes.

3.3.1 Architecture VPN interuniversitaire

C'est le cas de l'architecture mise en place au premier semestre 2004. Celle-ci s'appuie sur un ensemble de serveur VPN répartis et l'utilisation des technologies basées sur les tunnels IPSec.

Cette solution couvre un ensemble de besoins assez vaste :

- Mobilité depuis les réseaux sans fil Wi-Fi,
- Mobilité depuis la maison avec une liaison ADSL,
- Mobilité depuis un site quelconque à partir d'un PC intégrant le client VPN,
- Sécurité des données transmises ou reçues,
- Authentification forte.

En effet, les contraintes sont peu nombreuses : il suffit d'installer un logiciel tiers (le client VPN) et permettre le dialogue en UDP sur le port 500 pour pouvoir se connecter de manière sûre.

En revanche, il n'est pas possible d'utiliser simultanément deux clients VPN pour encapsuler leur communications : cela se traduit par exemple par un visiteur qui utilise un client VPN pour accéder à son Intranet et qui devrait installer le client VPN Cisco de l'université d'accueil pour sortir du réseau ! Dans ce cas, il ne pourrait pas se connecter.

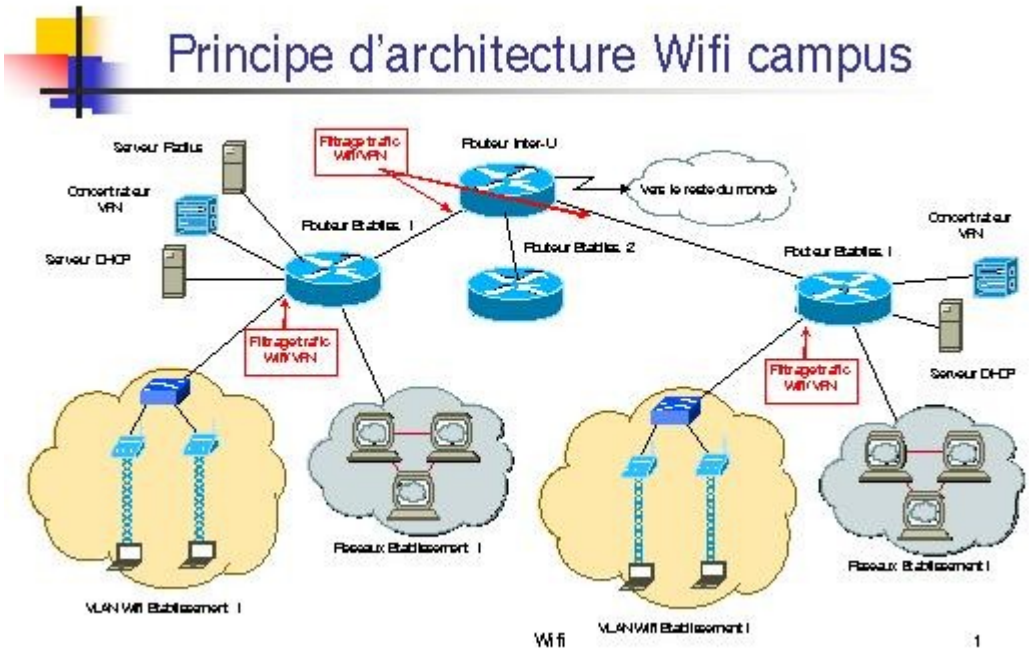


Illustration 9: Architecture Wi-Fi et VPN de Grenoble Universités

3.3.2 Adressage et sécurité

L'architecture sans fil choisie au sein des universités (Illustration 9) utilise massivement les plages d'adresses IP privées (RFC1918). Ces plages ne sont pas routées sur Internet et sont généralement utilisées pour pallier à la pénurie d'adresses IP.

Chaque université dispose d'une plage complète dans la classe A :

- Grenoble1 – 10.1.0.0 / 16
- Grenoble2 – 10.2.0.0 / 16
- Grenoble3 – 10.3.0.0 / 16
- INPG – 10.4.0.0 / 16
- CICG – 10.5.0.0 / 16
- IMAG – 10.6.0.0 / 16

Lorsqu'un utilisateur d'une université veut employer le réseau d'une autre université, il doit quand même pouvoir accéder au serveur VPN de son université. Cela nécessite un routage entre les différents organismes ainsi que l'ouverture de règles de sécurités pour les protocoles spécifiques.

```
Protocole esp vers serveur_VPN
Protocole ahp vers serveur_VPN
Protocole udp sur le port isakmp vers serveur_VPN
```

Mais encore, certaines universités ont des sites déportés dans d'autres villes. Ces sites disposent de la même plage d'adresse de classe A. Dès lors, il est nécessaire de mettre en oeuvre des techniques de tunneling pour masquer la différence de localisation.

3.4 Spécifications des besoins

Bien que les services réseaux soient assurés correctement en terme de nomadisme, l'évolution rapide des technologies et les choix fait par d'autres universités ont amenés le CICG à faire une nouvelle étude.

L'objectif est de fournir un service équivalent ou supérieur a celui déjà en place tout en complétant les défauts inhérent aux systèmes VPN. Pour y parvenir, l'étude des contraintes à été mené pour déterminer le cadre de liberté disponible.

Ensuite, les nouveaux besoins ont été exprimé.

3.4.1 Contraintes

Les contraintes dans un environnement aussi hétérogène impliquent une vue à court et moyen terme. A court terme, la solution ne doit pas tout remettre en question mais au contraire s'intégrer dans le schéma existant. A moyen terme, elle doit pouvoir unifier et réduire les contraintes.

De plus, les contraintes ne sont pas toutes techniques : certaines sont liées à la législation et d'autres sont imposées par le fonctionnement des universités.

3.4.1.1 Contraintes techniques

Le fonctionnement du réseau interuniversitaire implique des contraintes d'ordre technique : il a été choisi de mettre en commun certaines ressources (serveur DNS par exemple) et d'accepter certains modes de fonctionnement (accès VPN par exemple).

Pour pouvoir assurer l'utilisation du réseau avec le maximum de sécurité, un certain nombres de mesures ont été mises en oeuvre :

- Routage contrôlé,
- Règles de filtrages,
- Utilisation de plage d'adresses IP privées.

L'utilisation des VPN Cisco a été rendu possible par l'utilisation de tunnel pour certains sites : la plage privée étant répartie sur plusieurs sites géographiques, c'est le seul moyen de conserver un routage cohérent.

Une autre contrainte technique est liée à l'indépendance des universités entre elles : chacune peut acheter et utiliser le matériel de son choix pour fournir un service. L'hétérogénéité des marques et des équipements est une contrainte pour une solution unifiée : l'utilisation de standards ouverts et pérennes est donc exigé !

Ainsi, la nouvelle solution ne devrait pas compliquer cette situation, au contraire.

3.4.1.2 Contraintes législatives

Le GIP RENATER applique une charte de sécurité et de déontologie dans le but de responsabiliser chaque organisme vis à vis de la communauté. Cette charte est signée par les établissements accédant au réseau Renater.

Elle définie les usages autorisés sur le réseau qui sont "*à des fins professionnelles, à savoir enseignement, recherche, développements techniques, transfert de technologies, diffusion d'informations scientifiques, techniques et culturelles, expérimentations de nouveaux services présentant un caractère d'innovation technique.*".

Le GIP prohibe notamment l'utilisation du réseau à des fins commerciales ou ludiques (jeux en réseaux).

Cette contrainte entraîne le besoin de pouvoir identifier les utilisateurs et connaître leurs paramètres de connexion (adresse IP, date de connexion et durée de connexion). En cas d'alerte en provenance du CERT ou de tout autre organisme, l'établissement doit être capable de déterminer qui est à l'origine du comportement suspect.

3.4.1.3 Contraintes collectives

Le réseau interuniversitaire est constitué de plusieurs universités ayant chacune son service informatique. Ces services appelés CRI[19] ont de nombreuses missions :

- déploiement des usages des Technologies de l'Information et de la Communication,
- assistance aux usagers : étudiants, personnels, enseignants, chercheurs...
- administration, surveillance et exploitation des infrastructures et des services.

Sur Grenoble, chaque université est indépendante des autres et peut donc faire ses propres choix technologiques. Chacune dispose de ses propres ressources, compétences et ressources.

En plus des universités, le réseau interuniversitaire de Grenoble accueille également l'IMAG, le CNRS et l'INRIA, qui sont également autonomes.

Afin de permettre la coordination de projets importants, il existe donc un groupe de coordination : le COR2I[20]. Constitué des directeurs des CRI, il assure le suivi des projets, l'appui des personnels techniques, la validation des recommandations...

19 CRI : Centre de Ressources Informatiques
20 COR2I : Comité Opérationnel des Ressources Informatiques Interuniversitaires

Un groupe de travail technique est également constitué afin de réunir les ressources compétentes dans le domaine abordé dans le projet : généralement, on y trouve une personne de chaque université. Ce groupe de travail se réunit pour mettre en commun les résultats d'expériences, des documentations et tenter de répondre aux problèmes soulevés par le COR2I ou par les utilisateurs.

Ainsi toute solution à déployer devra d'abord recevoir un aval technique par ce groupe de travail : le groupe travaillant sur le nomadisme est connu dans la liste de messagerie "Sans fil Grenoble". Ce groupe a déjà déployé la structure basée sur les concentrateurs VPN Cisco.

3.4.2 besoins

Le monde de l'éducation et de la recherche est par définition ouvert et mutualisé : la mise en commun de ressources par des accords sur des projets attire également les pirates et hackers de tout horizons ! Ils voient dans cet environnement, l'occasion de disposer d'équipements puissants et en nombre suffisant pour faciliter leurs actions peu scrupuleuses (par rebond ou commandes à distance).

La solution déjà en oeuvre (via VPN) est un premiere réponse pour sécuriser les réseaux des universités grenobloises mais elle doit être mise en concurrence avec d'autres solutions qui pourraient être plus adaptées : l'objectif est de fournir une réponse équivalente sinon plus efficace tout en simplifiant les démarches de l'utilisateur. Le VPN est donc le modèle pour la définition des besoins.

Les besoins sont en réalité liés à deux types d'utilisations :

- L'utilisation standard est la situation dans laquelle un visiteur occasionnel ou un utilisateur néophyte se présente sur le campus et désire accéder rapidement à Internet pour lire ses messages ou obtenir un renseignement sur un site web.
- L'utilisation étendue correspond à un utilisateur habitué utilisant le réseau pour accéder à ses ressources privées et à son intranet (en utilisant ses propres applications).

Dans les deux cas, la sécurité du réseau et de ses utilisateurs doit être assurée : d'une part, les attaques menées par une personne ou un groupe de personnes doivent avoir un impact nul ou minimum, d'autre part les attaques virales doivent pouvoir être endiguées.

Enfin, toute connexion doit être identifiable a postériori et tout compte doit être protégé afin de garantir l'authentification (identité juste).

3.4.2.1 Utilisation standard

Ce type d'utilisation est le mode le plus léger. Idéalement, l'utilisateur allume son ordinateur et accède au réseau sans rien avoir à faire. Le minimum de sécurité impose tout de même une authentification pour éviter que le point d'accès ne devienne un ASFI gratuit et surtout sans contrôle (respect de la charte Renater).

L'équipement terminal ne doit pas supporter un téléchargement ou une configuration pour étendre ses capacités. Les différents OS ainsi que les différents logiciels (notamment les différents navigateurs) doivent fonctionner dans ce réseau.

En revanche, il est accepté que les services fournis soient limités et ne permettent pas l'accès à toutes les ressources et protocoles disponibles sur l'intranet.

3.4.2.2 Utilisation étendue

Dans ce mode, la connexion peut être un peu plus lourde : l'objectif étant d'avoir un accès à un nombre de services plus important. L'utilisateur doit avoir les droits nécessaires pour modifier la configuration de son poste. Le téléchargement et l'installation d'une application tierce est possible pour atteindre le niveau de service exigé. En revanche, la protection des données est impérative, en particulier pour les accès à l'intranet.

3.4.2.3 Salubrité des postes

Il est intéressant de pouvoir identifier les postes qui sont infectés par des virus, des vers ou des chevaux de Troies. Il est encore plus intéressant de les empêcher de nuire au réseau, en les plaçant dans une zone de quarantaine ou encore en bloquant les attaques sur le poste.

Les logiciels antivirus et pare-feu représentent une sécurité que tout le monde s'accorde à dire qu'elle est nécessaire. Ces logiciels sont beaucoup plus utiles sur les machines utilisant le système d'exploitation de Microsoft : les fans des OS libres en font leur cheval de bataille. Malheureusement, c'est effectivement vrai comme le montre l'étude de Sophos[21] pour le premier semestre 2005 (le préfixe W32 signifiant Windows 32 bits).

Position	Virus	Pourcentage de signalements
1	W32/Zafi-D	25.3%
2	W32/Netsky-P	17.5%
3	W32/Sober-N	10.3%
4	W32/Zafi-B	4.7%
5	W32/Netsky-D	3.8%
6	W32/Mytob-BE	2.6%
7	W32/Netsky-Z	2.3%
8	W32/Mytob-AS	2.0%
9	W32/Netsky-B	1.9%
10	W32/Sober-K	1.7%
Autres		27.9%

Illustration 10: Statistiques virales du 1er semestre 2005

Cette étude explique brièvement que l'on assiste à une progression géométrique des chevaux de Troies et que si le nombre de virus augmente, le délai d'infection moyen se réduit.

Les postes appartenant aux universités sont désormais équipés d'antivirus et de pare-feu dont les universités ont les licences. En revanche, il est difficile d'obliger un utilisateur à télécharger des logiciels dont il devra acquitter une licence.

Certains produits gratuits existent mais là encore, l'utilisateur peut porter plainte s'il pense que l'installation du logiciel a été préjudiciable sur sa machine.

Cette partie reste toutefois facultative car des contraintes législatives ne permettent pas une liberté suffisante pour faciliter cette lutte. Il est donc demandé de faire un état des lieux des offres permettant de lutter contre ces logiciels néfastes (virus, vers et chevaux de Troies).

3.4.2.4 Résumé des besoins

La recherche d'une solution pour le réseau interuniversitaire doit correpondre à deux types d'utilisation qui répondent aux problématiques suivantes :

- Permettre un accès Internet de manière contrôlé,

21 Étude de juillet 2005, visible en suivant le lien http://www.sophos.fr/pressoffice/pressrel/bilanmi2005.html

- Être indépendant du média employé : Ethernet (802.3) ou sans fil (802.11),
- Permettre le respect de la charte Renater sur laquelle les présidents d'universités se sont engagés (signatures).

Le tableau ci-dessous résume donc les fonctionnalités disponibles en fonction du type de besoin.

	Besoins Standards	Besoins étendues
Authentification à la connexion	✓	✓
Chiffrement de l'authentification	✓	✓
Accès messagerie (webmail)	✓	✓
Journal des connexions (traçabilité)	✓	✓
Accès depuis un AP Wi-Fi	✓	✓
Accès filaire	✓	✓
Accès depuis Internet	×	✓
Accès à l'Intranet	×	✓
Accès multi-services (ports)	×	✓
Chiffrement des communications	×	✓

Tableau 3: Table des fonctionnalités par besoins

De plus, la mutualisation de solutions et les coûts seront également déterminants dans le choix d'une architecture.

4 NORMES ET INFORMATIONS

En premier lieu, les anglo-saxons ne font pas la différence entre norme et standard. Pourtant en France, les deux mots ont une définition légèrement différente.

- Standard : n.m. "anglicisme *signifiant 'type' et provenant de l'ancien français estandard (étandard). Étalon, modèle, type. Conforme à un type de fabrication en série (modèle standard et modèle de luxe)*".
- Norme : n.f. "*du latin norma 'équerre, règle'. Principe ou modèle auquel il faut se conformer. Définition d'un type d'objet ou d'un procédé de fabrication établie en vue de simplifier et d'accroître la production*".

L'utilisation des mots "modèle" et "conforme" dans les deux définitions indique toutefois que l'emploi de l'un à la place de l'autre ne doit pas changer le sens de la phrase ; tout au plus, la norme est la conception intellectuelle tandis que le standard en est le résultat.

Il est donc admis dans ce mémoire que les deux mots sont synonymes et sont employés avec le même sens de "conformité à un modèle".

D'autre part, les technologies ou mécanismes en cours de normalisation sont appelés 'draft' (ébauches) ou projet de normalisation (DIS ou FDIS pour Final Draft International standards). Dans le domaine des télécommunications, on trouve principalement l'ISO[22], l'IEEE[23], l'IETF[24] et l'ITU[25].

Enfin, l'objectif de ce chapitre est de fournir les éléments de base servant à la bonne compréhension des solutions proposées. En effet, les choix techniques d'une architecture sont fondés sur les possibilités des matériels et sur les propriétés des normes employées.

4.1 Introduction

Le nomadisme doit s'appuyer sur les structures et les architectures existantes. Il implique l'utilisation de réseaux et de techniques de transmissions. Par les problèmes qu'il engendre, il est nécessaire d'authentifier la provenance d'un flux et garantir l'intégrité des données transportées.

Avant de rechercher de nouvelles solutions, il est utile de connaître les normes existantes. En effet, les produits du marché (commerciaux ou libres) s'appuient sur ces normes pour répondre aux différents besoins.

Après un centrage sur le type de communication choisit, ce chapitre aborde les standards utilisés sur la plupart des réseaux, puis il montre les standards de communication filaires et sans fil. Ensuite il présente les différentes méthodes assurant la confidentialité et l'intégrité des données sur un réseau. Enfin, il décrit les moyens courants pour authentifier une personne ou une machine.

22 ISO (Organisation Internationale de Normalisation). Ce nom vient du grec *isos* qui signifie *égal* contrairement à l'idée reçue de l'abréviation "International Standards Organisation" (http://www.iso.org/)

23 IEEE (Institute of Electrical and Electronics Engineers) est une association à but non-lucratif constitué de plus de 360 000 membres dans 175 pays, professionnels des technologies.

24 IETF (Internet Engineering Task Force) Communauté internationale ouverte d'opérateurs, chercheurs et ingénieurs dans le domaine des réseaux.

25 ITU (International Telecommunication Union) basé à Genève (Suisse), l'ITU est une organisation des Nations unies dans laquelle les états et le secteur privé coordonnent les réseaux et services mondiaux de télécommunication.

4.2 Nomadisme et mobilité

La mobilité n'implique pas forcément la notion de mouvement mais celle de déplacement : s'il est vrai qu'un téléphone mobile permet de se déplacer pendant une communication, en informatique la mobilité peut aussi indiquer un équipement qui change régulièrement de lieu entre deux communications successives.

Dès lors, bien que certains mécanismes restent propre à la technologie employé, le fonctionnement des réseaux filaires et sans fil présente des similitudes. L'expérience des réseaux fixes est profitable pour les réseaux mobiles : notamment la conservation de protocoles communs pour faciliter les échanges.

Dans ce chapitre nous verrons les standards communs à la technologie filaire et à la technologie sans fil. Ensuite, nous abordons les exceptions et différences pour les réseaux filaires puis les réseaux hertziens (les réseaux optiques ne sont pas abordés) : tout ceci afin de comprendre les interactions et les contraintes dans un réseau de campus.

4.2.1 Modèles de réseaux

La compréhension d'un ensemble de fonctions nécessite généralement son découpage en sous-ensembles. La description précise de chaque sous-ensemble, en fournissant des références communes et des règles devient un modèle ou un standard.

L'ISO est un organisme de normalisation international qui a présenté un modèle de communication en réseau de sept couches. Sans revenir en détail sur le fonctionnement des couches réseaux du modèle OSI[26], il est utile de résumer la fonction de chacune :

Couche	Fonction
7	**Application** (navigateur, messagerie)
6	**Présentation** (données indépendantes de l'OS)
5	**Session** (Établissements de dialogues, gestion des options)
4	**Transport** (Liaison bout en bout, fragmentation et contrôle)
3	**Réseau** (adressage et routage de paquets)
2	**Liaison** (Modulation et synchronisation des transmissions)
1	**Physique** (Support de transmission. Ex. cuivre, ondes,...)

Tableau 4: Le modèle ISO

Ce modèle est une normalisation dont les qualités sont indiscutables mais dont l'implémentation n'a pas connue le succès escompté. En effet, une autre norme, de fait celle-là, s'est répandue avec le protocole TCP/IP[27]. Utilisé à l'origine sur le réseau ARPANet[28], la simplicité de fonctionnement de ce protocole l'a rendu incontournable et actuellement, son successeur (IPv6) n'est pas encore aussi répandu !

26 OSI (Open System Interconnection)
27 TCP/IP (Transmission Control Protocol / Internet Protocol)
28 ARPANet (Advanced Research Projects Agency Network). Projet du DARPA lancé en 1967 et officialisé en 1972.

Illustration 11. : les couches OSI et TCPIP

Sur l'illustration 9, il est facile de voir que les deux modèles n'ont qu'une partie commune au niveau transport et réseau (internet) et que les couches "liaison" et "physique" du modèle ISO sont mélangés sur le modèle TCP-IP. L'application se charge de la présentation et de l'établissement des sessions. Les couches liaison et physique sont plus intimement liées dans TCP/IP. C'est cette couche "accès réseau" qui permet à la couche internet de s'affranchir du média employé pour la connexion.

Le mode de développement de TCP/IP en a fait le protocole officiel d'accès au réseau Internet même si fréquemment, les trames IP sont transportées par des protocoles différents (ATM et Frame Relay par exemple). Tous les systèmes d'exploitation permettant un accès au réseau intègrent la pile TCP/IP : l'utilisation de 'socket' pour programmer des requêtes entres machines rend la vie des programmeurs plus facile et les applications bénéficient de possibilités étendues.

Un autre avantage de ce modèle est que pour une application s'adressant à la couche IP, l'interface matérielle n'est pas connue : modem RTC, modem ADSL, carte ethernet ou carte Wi-Fi... IP s'appuie sur le 'driver' de la carte et sur les normes des couches équivalentes au matériel et au lien.

4.2.2 Normes communes

Les fonctions utilisées par les réseaux de communications sont généralement identiques : de nombreuses analogies avec nos méthodes de communications sont employées pour en permettre une meilleure apréhension.

Les réseaux sans fil qui ont une croissance forte, bénéficient de l'expérience acquise dans le domaine filaire. Le développement de mécanismes étant limité aux contraintes spécifiques de ce type de transmission, l'intégration de ces équipements dans les réseaux filaires existants en est simplifiée. Ainsi, de nombreuses techniques de communication sans fil s'appuient sur les méthodes employées dans les réseaux classiques. Ces derniers étant complètement normés, le développement des réseaux hertziens a également adopté leurs standards de communication pour permettre une simplicité de mise en oeuvre et une grande pénétration du marché.

La plupart des réseaux LAN utilise le protocole TCP/IP, les sections suivantes abordent donc les normes améliorant la qualité des services fournis sur ces réseaux.

4.2.2.1 Norme IEEE 802.1q

Le standard pour les LAN virtuels (vlan ou Virtual LAN) a été définit pour faciliter la gestion des grands réseaux. En effet, plus un réseau contient d'équipements réseaux et plus il y a de collisions : le réseau devient encombré, il y a de nombreuses retransmissions et la bande passante devient quasiment nulle.

La première solution pour segmenter un réseau et d'utiliser un routeur : chaque interface de cet équipement est reliée à un réseau. Le découpage pour déterminer s'il le message doit être transmis par le routeur est fait à l'aide du masque de sous-réseau. Là encore, sans rentrer dans les détails, ce masque permet un découpage logique mais uniquement au niveau des adresses IP (couche réseau du modèle OSI) : si les machines sont sur le même lien physique, la bande passante globale sera partagée par toutes les machines et d'autre part, les paquets de broadcast (c'est à dire destinés à toutes les machines) seront vus par toutes les machines (quelque soit leurs adresses IP).

La seconde solution est d'utiliser un commutateur multi-ports : celui-ci conserve les adresses MAC et le numéro du port où elles sont présentes. Le débit du bus du commutateur étant très largement supérieur au débit de chaque port, on considère que plusieurs machines communiquent simultanément entres-elles. Pour ce faire, le commutateur effectue une communication de port à port. Longtemps considérée comme la solution idéale, le problème des trames de broadcast subsiste encore. De plus, lorsque plusieurs commutateurs sont chaînés, les ports de chaînage deviennent le maillon faible car ils supportent toutes les communications.

La dernière solution s'appuie sur les fonctionnalités des commutateurs pour introduire la notion de LAN virtuel.

Le schéma suivant montre le fonctionnement d'un commutateur supportant les vlans :

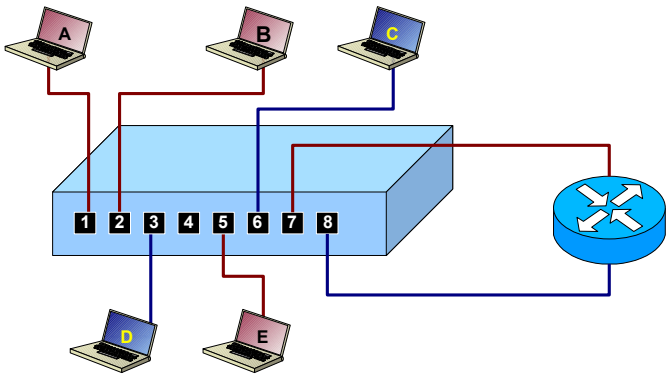


Illustration 12: Fonctionnement des réseaux locaux virtuels

Les machines A, B et E appartiennent à un réseau virtuel "vlan 10" tandis que les machines C et D sont dans le réseau "vlan 20". Le commutateur connaît l'état de chaque port et en particulier à quel LAN virtuel ils appartiennent. Ainsi, pour communiquer de A vers E, le commutateur établit une liaison directe entre le port 1 et 5. En même temps, la machine C peut communiquer vers D, le commutateur instaurant une liaison entre les ports 3 et 6 en parallèle de la première liaison. La différence majeure avec les solutions précédentes est que cette fois, une trame de broadcast sera limité aux seuls ports du vlan définit : dans notre cas, les machines B et E recevront le broadcast en provenance de A mais C et D continueront leur communication sans aucune interruption.

L'intérêt procuré par les vlans est de limiter les trames à un ensemble de machines comme si celles-ci étaient isolées sur un brin physique unique, tout en utilisant la même infrastructure. Les commutateurs permettent de placer une machine sur un brin de manière statique (configuré par un administrateur) ou dynamique (en fonction d'un nom de connexion par exemple).

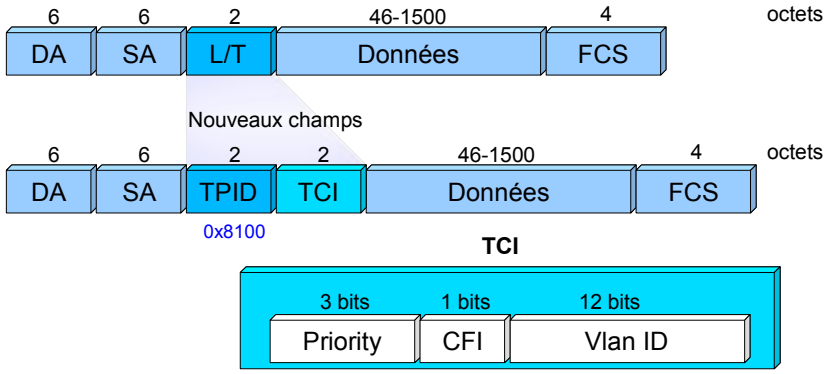


Illustration 13: Insertion champs vlans sur une trame Ethernet

Le "vlan tagging" se situe au niveau 2 des couches ISO : le remplacement du champ L/T (Length/Type) par deux champs TPID (Tag Protocol Identifier) et TCI (Tag Control Information) permet l'utilisation théorique de 4096 vlans et d'une qualité de service (QoS) codée sur 3 bits. Ainsi il y a correspondance entre le niveau trame du réseau Ethernet et la gestion de qualité de service DiffServ et il est possible de réserver la priorité de classe Premium ou EF aux applications de voix et de téléphonie.

L'intérêt de ce protocole dans un environnement nomade est de fournir un accès à un utilisateur mobile entre plusieurs bâtiments. Dans le cas d'un accès filaire, le brassage est fait à distance par l'administrateur du réseau ou mieux, il est fait dynamiquement par le commutateur en fonction de la réponse du serveur d'authentification.

4.2.2.2 Norme IEEE 802.1x

802.1x est un protocole de niveau 2. Il est intimement lié au protocole EAP[29] mais ils n'ont pas les mêmes fonctions. 802.1x comble un manque dans les standards 802 : il a la capacité de n'autoriser que la circulation de trames EAP tant que l'authentification n'a pas été validée. En effet, EAP est un protocole ajouté au protocole PPP mais ce dernier n'a aucune utilité sur les réseaux locaux. Le standard 802.1x est donc utilisé pour ces réseaux.

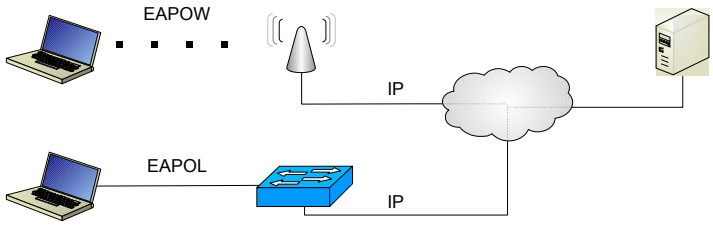


Illustration 14: Le standard 802.1x et ses protocoles

Le protocole d'origine de 802.1x et "EAP encapsulation Over LAN". Ce protocole définit le rôle et le nom des trois intervenants dans la requête EAP :

- le client (ou supplicant) correspond à la machine désirant se connecter sur le réseau,

29 EAP : Extended Authentication Protocol

- le serveur d'authentification (ou authentication server) est l'équipement capable de traiter les requêtes d'authentification et de donner une réponse positive ou négative. On verra plus tard qu'il a souvent d'autres fonctions associées,
- le point d'accès (ou authenticator), parfois appelé PA (ou AP pour Access Point), est l'équipement intermédiaire qui transforme des requêtes provenant d'un protocole de niveau 2 en requêtes IP.

Comme le standard 802.1x se situe dans la couche liaison du modèle OSI, les trames employées utilisent le même entête que les trames des autres protocoles de niveau 2 définis par l'IEEE pour Ethernet, Token-Ring et FDDI :

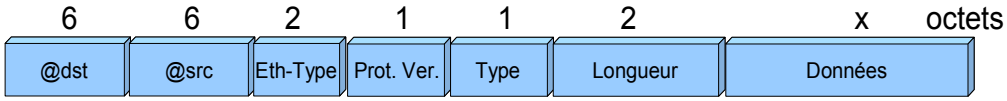


Illustration 15: Trame 802.1x

De manière générique, les 48 premiers bits correspondent à l'adresse MAC du destinataire, les 48 bits suivants correspondent à celle de l'émetteur et le champ "Eth-Type" prend la valeur &h888e qui correspond au protocole EAP.

Le standard 802.1x a été modifié par la suite pour s'adapter aux protocoles des réseaux sans fil : l'utilisation des adresses MAC implique en effet pour ces réseaux que le client et le point d'accès se soient associés pour pouvoir dialoguer. Le protocole ainsi utilisé est appelé EAPOW pour "EAP encapsulation Over Wireless".

La fonction de EAPOL ou EAPOW est de permettre au point d'accès de filtrer toutes les trames provenant d'un client inconnu. Ainsi un client connecté sur un point d'accès (AP) configuré avec du 802.1x ne pourra pas atteindre le réseau avant d'avoir été authentifié. Dans l'illustration 11, le client A ne peut émettre que des trames EAP tandis que le client B qui a été authentifié peut accéder normalement au LAN.

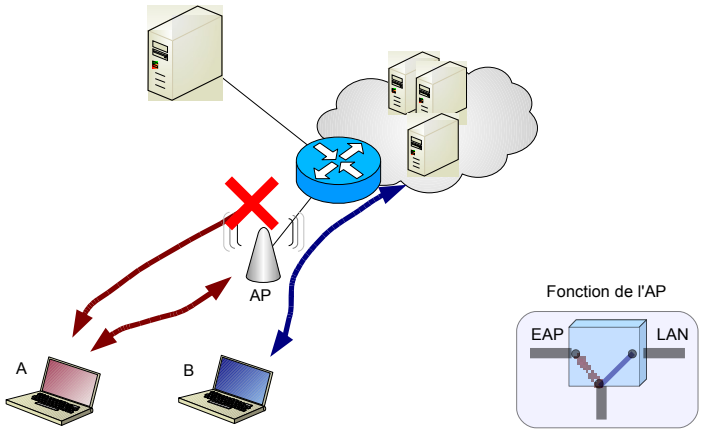


Illustration 16: Fonctionnement du protocole 802.1x

Certains équipements ont toutefois la possibilité de placer un équipement ne sachant pas communiquer en EAP dans un vlan par défaut (dans lequel le client pourra télécharger un client 802.1x par exemple).

Pour remplir sa tâche, le point d'accès utilise en réalité deux piles de communication :

- la première pile qui relie le client et l'AP est EAPOL ou EAPOW. Elle est robuste et empêche les attaques par Déni de Service.

- La deuxième pile qui relie l'AP et le serveur est une pile IP classique : les attributs EAP sont converties en attributs RADIUS puis encapsulés dans des datagramme UDP.

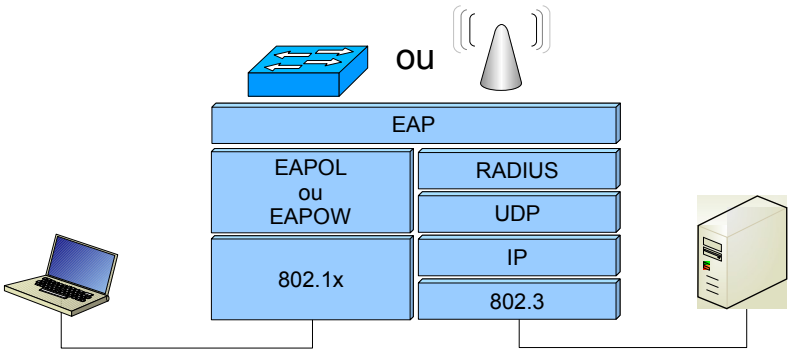


Illustration 17: Les couches EAP

Ce protocole se démocratise rapidement et il est probable que tous les systèmes d'exploitation l'intègre dans les années à venir : sa robustesse et sa simplicité ainsi que sa mise en oeuvre sur plusieurs supports en font un élément idéal pour la sécurité des accès nomade. L'utilisateur n'est plus lié à une prise, un bureau un lieu mais à son système d'authentification.

4.2.3 Normes réseaux filaires

La majorité des communications réseaux passent par une infrastructure filaire : les fibres optiques ou bien les liaisons cuivres sont les médias les plus rapides et les moins sensibles aux perturbations extérieures. Les premiers réseaux comme ARPANET sont nés d'une structure filaire et les protocoles de communications s'appuient sur les caractéristiques propres a ces architectures. Les réseaux sans fil utilisent certaines propriétés des réseaux filaires et à contrario ont dûs trouver d'autres techniques pour adapter leur singularité.

Ce paragraphe présente donc les caractéristiques utilisées sur les réseaux filaires pour permettre ensuite de définir le fonctionnement des réseaux sans fil et leurs différences. Enfin, quelques standards communs sont décris.

4.2.3.1 Réseaux point à point et multipoint

Ces deux modes de fonctionnement sont très différent :

- le mode point à point défini une communication entre deux machines. Il n'y a pas d'intervenant extérieur, mais il faut déjà établir un protocole de communication commun. Les premiers réseaux point à point ont utilisés les ports matériels série (RS-232). En IP, c'est le protocole PPP[30] qui est utilisé.
- Le mode multipoint implique plusieurs machines dans un ensemble de communication "un vers tous" ou "un vers un". Le protocole doit posséder d'autres caractéristiques et en particulier la notion d'adressage. La topologie peut varier mais dans tout les cas, plusieurs machines peuvent communiquer ensemble (et parfois en même temps).

30 PPP : Point to Point Protocol

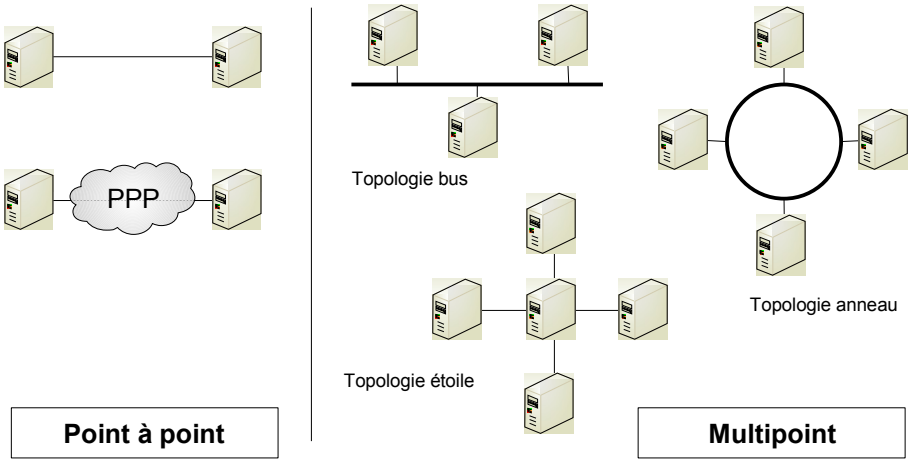


Illustration 18: Les topologies filaires

La topologie en anneau fonctionne sur le principe d'un jeton qui passe de machine en machine. Si le jeton est vide, une machine peut y déposer son message et rendra le jeton vide lorsqu'il aura fait le tour complet.

La topologie bus utilise une technique particulière d'émission et d'écoute simultanée. La machine qui veut émettre un message écoute d'abord si le média est libre. Si c'est le cas, elle émet son message tout en écoutant le média (sur lequel circule son message). Si son message est déformé ou modifié, elle en conclue qu'une autre machine a émis en même temps qu'elle : elle envoie un signal de collision puis s'arrête d'émettre pendant un temps aléatoire.

La topologie en étoile implique le passage par un équipement chargé de gérer les communications. On peut considérer que les commutateurs actuels sont les éléments centraux de cette topologie.

4.2.3.2 IEEE 802.3

Appelé standard *Ethernet*, il fût établit par DEC, Intel et Xerox[31]. Puis l'IEEE a repris cette spécification. Désormais appelé 802.3, ce standard universel spécifie le mode de fonctionnement des réseaux utilisant CSMA/CD[32]. 802.3 désigne également un groupe de travail dont les recherches porte sur les techniques d'accès aléatoire (CSMA). Le standard IEEE 802.3 a donné naissance à la norme ISO 8802.3.

Le standard 802.3x étant relativement récent, les réseaux LAN connectaient plusieurs équipements sur un même brin : il était nécessaire de trouver une méthode de communication permettant à tous d'émettre sans pour autant perturber les transmissions. La méthode des réseaux Ethernet est CSMA/CD.

31 XEROX est le fondateur du standard Ethernet dont les spécifications s'appuient sur celles du réseau Alohanet.
32 CSMA/CD : Carrier Sense Multiple Access / Collision Detect

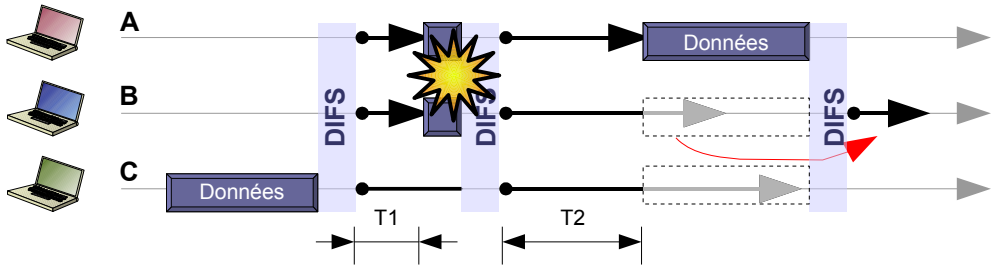


Illustration 19: Mécanisme CSMA/CD

Toutes les stations étant reliées sur un média unique, chacune écoute les transmissions sur celui-ci. A la fin d'un message, un délai d'attente obligatoire est observé par toutes les stations : c'est le DIFS[33]. Une fois le DIFS passé, toutes les stations calculent un délai aléatoire sous la forme d'un compte à rebours. Lorsque le compte à rebours arrive à zéro et qu'aucune communication est en cours, alors la station peut émettre son message. Toutefois, il peut arriver que deux stations décident d'émettre leur message en même temps : dans ce cas, il y a une collision !

Chaque équipement écoutant simultanément, les émetteurs perçoivent la différence entre le message émis et le retour (mélange des deux messages). Ils s'arrêtent donc et attendent un DIFS pour recalculer leur compte à rebours (aussi appelé CW[34] ou "fenêtre de collision"). Toutefois, le nouveau calcul fournira une valeur deux fois plus grande que la précédente : c'est le phénomène de "back-off" ou recul exponentiel. Ce doublement est malgré tout limité à un seuil maximum et dès qu'une trame est émise correctement, la fenêtre reprend sa taille initiale.

4.2.3.3 Les accès via réseau téléphonique

Les réseaux téléphoniques constituent parfois un prolongement du réseau de l'entreprise : la possibilité pour un utilisateur de se connecter depuis sa résidence à son réseau d'entreprise établie les prémisses du travail à distance. Les personnes ayant des astreintes n'ont plus la contrainte de devoir se déplacer pour diagnostiquer un problème ou surveiller un service.

4.2.3.3.a RTC

RTC[35] est le mode de connexion basic via une ligne téléphonique : il utilise la même bande passante que la voix et supporte un débit maximum de 56Kbps en utilisant les standards V.90 et plus récemment V.92. Le protocole PPP est généralement mis en oeuvre sur ce type de liaison.

4.2.3.3.b DSL

DSL[36] est une technologie apportant le haut débit numérique aux entreprises et aux particuliers en utilisant une simple ligne téléphonique. ADSL[37] rend possible l'utilisation d'une ligne téléphonique classique pour transporter des informations numériques à haut débit. Finalisé en 1995 par l'ITU[38] sous le nom barbare G992.1, ce standard permet notamment le transport de données TCP/IP, X.25 et ATM.

33 DIFS : Distributed Inter Frame Space
34 CW : Collision Windows ou fenêtre de collision.
35 RTC : Réseau Téléphonique Commuté
36 DSL (Digital Subscriber Line)
37 ADSL (Asymmetric Digital Subscriber Line)
38 ITU (International Telecommunication Union)

Sur une ligne téléphonique, l'emploi d'un filtre permet en outre d'utiliser simultanément un téléphone analogique pour communiquer (voix ou fax) ce qui rend ce protocole intéressant pour les accès Internet aux particuliers (la plupart des gens ayant une ligne téléphonique à la maison).

4.2.4 Normes réseaux sans fil

L'utilisation de nouvelles technologies a permis de relier des équipements par ondes hertziennes ou par ondes lumineuses. En fonction de la longueur d'une onde (un cycle complet), les propriétés de celle-ci varient : l'oeil capte une plage d'ondes située entre 380 et 780 nm (lumière visible, du violet au rouge). L'oreille est sensible à la plage d'ondes[39] allant de 11 000mm (30 Hz) à 17.2mm (20 kHz).

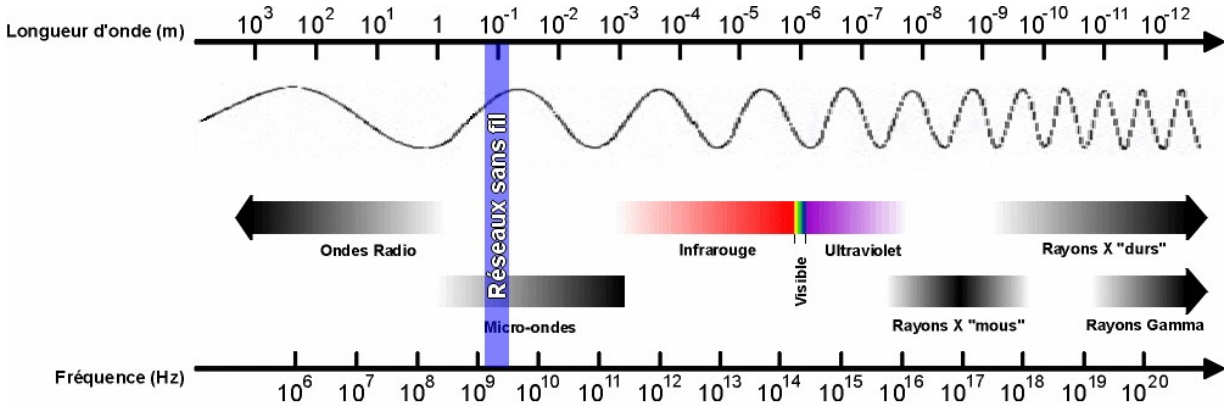


Illustration 20: Spectre de fréquences et longueurs d'ondes

Parmi les longueurs d'ondes présentées dans l'illustration 11, les micro-ondes sont celles qui sont utilisées pour les réseaux sans fil. Leurs propriétés leur permettent de traverser certains obstacles et de ne pas nécessiter une puissance trop élevée pour une quantité de données importante à transmettre.

En effet, la longueur d'onde, la fréquence, le débit et la portée sont intimement liés.

La longueur d'onde et la fréquence sont liés par la formule suivante :

$\lambda = \frac{c}{f}$ où c représente la célérité en mètre par seconde ($m.s^{-1}$), f la fréquence en hertz (Hz) et λ en mètres (m.).

Les autres éléments sont définis par la formule $C = H \times \log_2\left(1 + \frac{Ps}{Pb}\right)$ ou C est la capacité maximale du canal de communication en bits par secondes (bps), H est la largeur de la bande de fréquence employée en Hz, Ps et Pb respectivement la puissance du signal et la puissance du bruit en watts (w).

Afin d'optimiser la transmission d'information, plusieurs techniques sont utilisables dont les modulations radio.

39 Les chiffres données à titre d'exemple sont calculés sur la base d'une vitesse du son à 343 m/s. Voir le site http://www.sengpielaudio.com/calculator-wavelength.htm pour plus d'informations.

4.2.4.1 Modulations et codages

Il existe plusieurs types de modulations pour transporter une information sur les ondes. Ce sont des transformations appliquées sur un signal dit 'porteur' car il sert de référence. A ce signal on ajoute le signal utile (les données). Grâce à ce système, il est possible d'émettre plusieurs signaux utiles dans des gammes de fréquences séparées : les signaux ne se mélangent pas [GERO04].

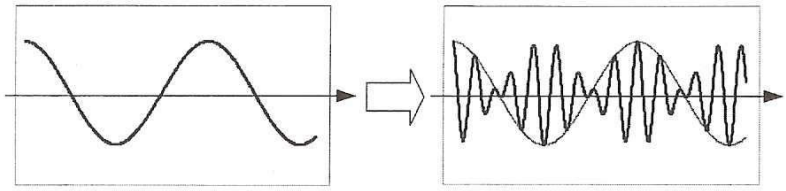


Figure 2.7 — La modulation d'amplitude.

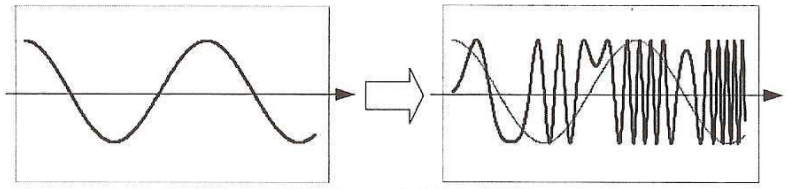


Figure 2.8 — La modulation de fréquence.

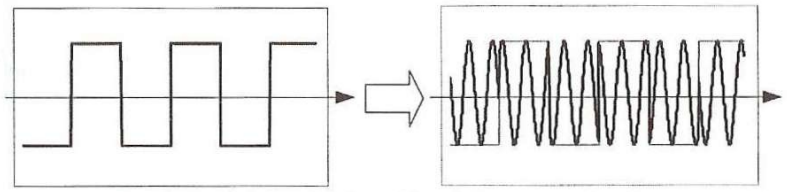


Figure 2.9 — La modulation de phase (plus claire avec un signal source carré).

Illustration 21: Les différentes modulations

4.2.4.1.a Modulation d'amplitude (Amplitude Modulation)

La modulation d'amplitude modifie la puissance d'une fréquence en fonction de l'information. L'avantage est que le récepteur n'écoute qu'une fréquence (largeur de bande extrêmement réduite) mais l'inconvénient est que les données faibles sont mélangés avec le bruit puisque leur valeur est proche de zéro.

4.2.4.1.b Modulation de fréquence (Frequency Modulation)

Plus efficace que la première méthode, elle consiste à moduler la fréquence du signal en fonction de la donnée à transmettre. L'amplitude reste constante, ce qui est son principal avantage en revanche le récepteur doit écouter une largeur de bande plus importante. Cette méthode est utilisée avec les radios FM

4.2.4.1.c Modulation de phase (Phase Modulation)

La modulation de phase s'applique particulièrement bien sur un signal carré. A chaque fois qu'il y a un changement d'information, on change la phase du signal. Le récepteur compare le signal reçu avec une porteuse de fréquence identique et la soustraction des signaux permet de retrouver le signal source.

Dans un environnement numérique, ces techniques sont utilisées sous les noms d'ASK (Amplitude Shifting Key), FSK (Frequency Shifting Key) et PSK (Phase Key Shifting).

Il existe une petite variation pour la modulation de phase qui est plus facile à mettre en oeuvre pour la synchronisation entre l'émetteur et le récepteur : la modulation différentielle. Au lieu de comparer deux signaux et de choisir l'information en phase (0) ou en opposition de phase (1), c'est le changement de phase qui devient important : pas de changement de phase (0) ou changement de phase (1). Cette modulation est appelée DPSK pour Differential PSK.

4.2.4.1.d Les symboles

Le raisonnement utilisé pour la modulation de phase à deux états peut-être étendu à quatre états (0°, 90°, 180° et 270°) ou plus. Chaque phase peut alors représenté un ensemble de bits (00, 01, 10 et 11) appelé symbole et ainsi, sur un cycle du signal porteur il est possible de transporter beaucoup plus d'informations. En utilisant la technique QPSK (Quadrature PSK) ou 4PSK, il est possible de doubler ou quadrupler le débit de données. Appliquée avec une modulation d'amplitude ayant plusieurs niveaux (et donc plusieurs symboles) on obtient des débits très importants seulement limités par le rapport signal/bruit : ce rapport varie fortement en fonction de la... distance.

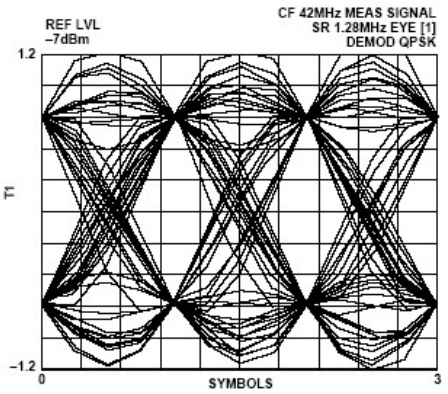


Figure 16. QPSK Modulation

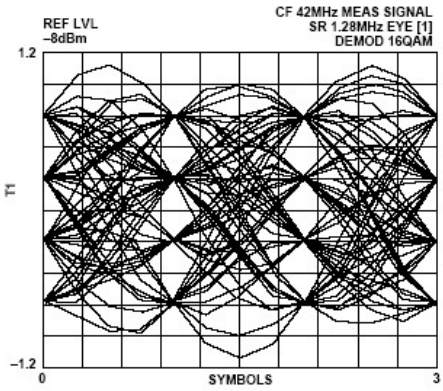


Figure 18. 16-QAM Modulation

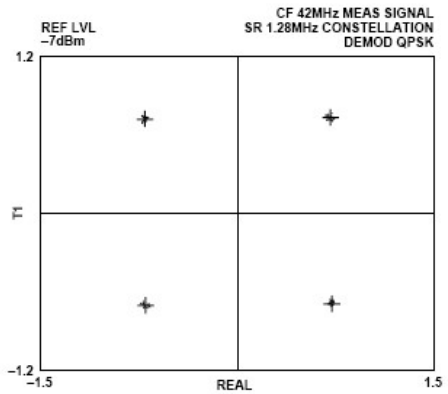


Figure 17. QPSK Modulation

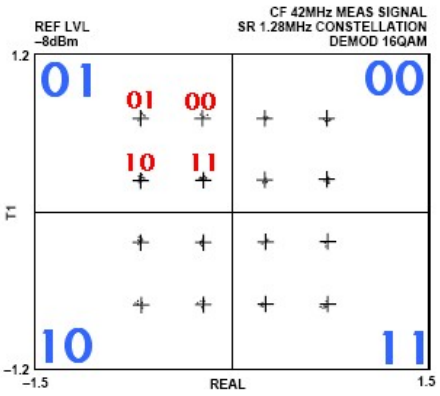


Figure 19. 16-QAM Modulation

Illustration 22: Extrait d'un datasheet d'un composant électronique

L'illustration 21 [ANDI99] matérialise le fonctionnement de la modulation de phase associée à la modulation d'amplitude : ainsi le point le plus haut à gauche aura comme symbole la valeur binaire 0101 (5 en décimal) dans le mode QAM alors qu'il ne pourra prendre qu'une valeur codé sur 2 bits en QPSK.

4.2.4.2 Distances et interférences

Plus la distance sera élevée, plus le rapport signal/bruit sera faible : la modulation d'amplitude – qui est la plus sensible par ses propriétés à ce rapport – sera la première modulation inutilisée sur de grandes distances.

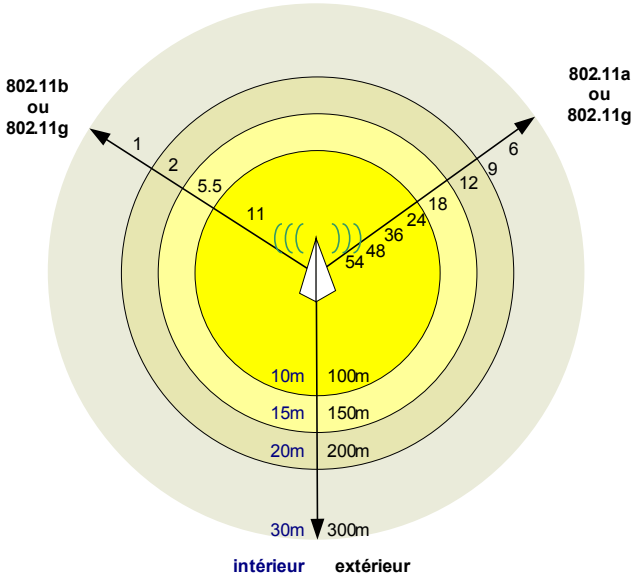


Illustration 23: débits en fonction de la distance en 802.11

4.2.4.2.a Distances

L'illustration 4.5 [GERO04] met en évidence le principe décrit ci-dessus : plus la distance est courte et moins il y a de perte dans le signal utile. L'émetteur et le récepteur s'accordent sur les méthodes de modulation à employer en fonction de la force du signal reçu, ce qui détermine le débit maximum théorique.

Cet exemple concerne le standard 802.11 qui est abordé en détail un peu plus loin.

4.2.4.2.b interférences

C'est bien sur le cas idéal car les ondes voient leurs caractéristiques modifiées par l'environnement ambiant : les murs, les arbres, la pluie, les grillages sont autant d'éléments passifs perturbants.

Ainsi, la partie transmission et réception doit être soigné (qualité des antennes) et l'environnement doit être pris en compte. La qualité du signal est classé de la manière suivante [MAPU04]:

Rapport signal/bruit	État du signal
50	Excellent
40	Très bon
30	Bon
20	Moyen
10	Faible

Tableau 5: Echelle de qualité de signal

En effet, si la distance joue un rôle important, l'environnement modifie également de manière importante la propagation des ondes : réflexion, diffusion, diffraction, réfraction et absorption sont autant d'obstacles.

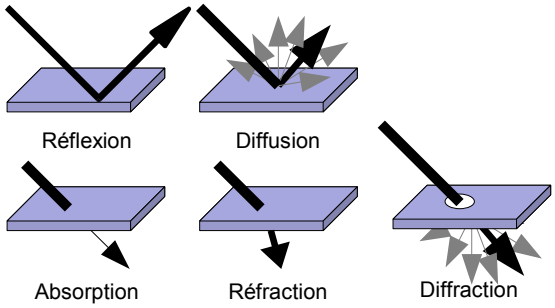


Illustration 24: les différentes perturbations des ondes

Ces phénomènes physiques peuvent en effet, perturber l'onde principale (qui atteint le récepteur de manière directe) en arrivant avec un léger délai de retard sur l'antenne du récepteur.

Bien sur, d'autres éléments actifs perturbent également la bonne propagation des ondes : four à micro-ondes, alarmes volumétriques, radars, antennes "pirates", etc. émettent dans la bande de fréquence utilisé par de nombreux systèmes de communications.

4.2.4.3 Étalement de spectre

Afin de compenser les problèmes de perturbations, il existe plusieurs solutions dont les familles les plus connues sont FHSS[40] et DSSS[41]. Ces deux techniques impliquent toutefois que l'émetteur et le récepteur soient synchronisés sur une même séquence de code.

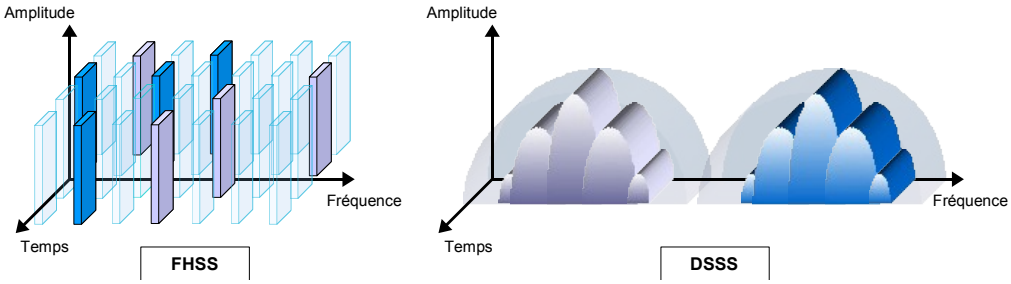


Illustration 25: étalement de spectre

4.2.4.3.a FHSS

FHSS découpe les informations à transmettre dans le temps. Après un temps défini, il y a changement de fréquence (signal porteur). La bande de fréquence employée est la plus étroite possible. Le changement de fréquence (et le choix de la nouvelle fréquence) est lié à un code

4.2.4.3.b DSSS

DSSS utilise un code de taille supérieur (N bits) à l'information à envoyer, qui module cette dernière. Il est nécessaire d'étendre la bande passante pour transmettre les nouvelles données. L'annexe 7.2 présente un schéma exact de l'onde générée par l'étalement de fréquence DSSS.

40 FHSS (Frequency Hopping Spread Spectrum) : étalement de spectre à saut de fréquence.
41 DSSS (Direct Sequence Spread Spectrum) : étalement de spectre à séquence directe)

4.2.4.4 Les réseaux sans fil 802.11

S'appuyant sur les différents éléments cités précédemment, plusieurs standards de réseaux sans fil existent. Les grandes familles diffèrent par leurs débits et la distance maximum d'utilisation, comme le montre la figure suivante [PUJO05].

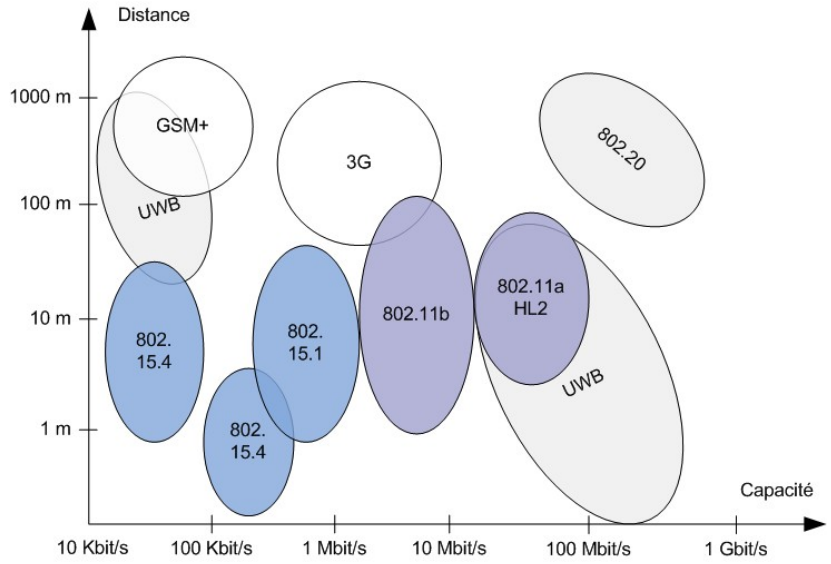


Illustration 26: Les différentes familles de réseaux sans fil

Les standards utilisés par la téléphonie classique comme DECT, GSM, GPRS, UMTS et 3G ne sont pas abordés dans ce rapport, le sujet étant étroitement lié à l'informatique et aux réseaux IP.

En revanche, les standards 802 définis pas l'IEEE sont très utilisés pour le transport de données informatique : les normes 802.11, 802.15 et 802.16 sont les plus connues du public et des administrateurs réseaux.

Les différents groupes de travail de l'IEEE 802 qui travaillent sur les réseaux sans fil n'onte pas les mêmes objectifs. C'est pourquoi on trouve plusieurs normes différentes dont les caractéristiques se complètent.

Ainsi les normes 802.11 (surnommée "Wi-Fi"), 802.15 (appelée "BlueTooth") et 802.16 (baptisée "Wi-Max") ont chacune un champ d'application particulier.

- 802.11 est orienté LAN : les débits varient entre 1 Mbps et 54 Mbps et la portée est comprise entre quelques mètres en intérieur, jusqu'à plusieurs dizaines de mètres en extérieur (variables en fonction de la distance et des perturbations).
- 802.15 est utilisé pour relier des équipements de proximité entre eux : appareils photos, souris et clavier sans fil. Il s'agit donc de picot-réseaux.
- 802.16 vise les réseaux MAN haut débit : il pourrait même compléter l'ADSL dans certaines zones.

La seule norme qui sera décrite dans ce rapport est 802.11 car ses spécifications la rendent incontournable pour les réseaux locaux de demain...

4.2.4.4.a Généralités sur le 802.11

Ce groupe travaille sur le standard le plus connu car sa pénétration du marché des entreprises et des particuliers est très forte. Ces principaux avantages sont la portée importante et le débit équivalent ou supérieur à une liaison ADSL. De nombreux équipements pour les particuliers accouplent un liaison ADSL, des liaisons Ethernet et une interface Wi-Fi : pas besoin de refaire le câblage de la maison pour naviguer sur Internet. Pour les entreprises, les équipements sont interopérables et permettent d'équiper en réseaux des bâtiments existants pour un coût bien inférieur à l'implantation d'un réseau filaire dans ceux-ci.

Les abus de langage de la presse décrivent souvent des "équipements Wi-Fi" ou "équipements à la norme Wi-Fi" alors que Wi-Fi désigne plutôt la certification de compatibilité des-dits équipements aux standards 802.11.

Illustration 27: logo de certification Wi-Fi

D'autre part, pour endiguer la pénétration des termes anglo-saxons, l'académie française a créer l'acronyme ASFI[42] qui signifie "Accès Sans Fil à Internet". Il est donc utile de rappeler que la mise en oeuvre d'un équipement Wi-Fi pour accéder à Internet n'est pas un accès Wi-Fi mais un ASFI (remplace également le terme anglais "hotspot").

Les équipements certifiés Wi-Fi doivent préciser les normes supportés : 802.11a, 802.11b et/ou 802.11g pour les transmissions et depuis juin 2004, 802.11i pour la sécurisation.

En effet, le groupe 802.11 travaille sur de nombreux amendements :

Amendement	Description	Status
802.11a	Définition d'une nouvelle couche physique : jusqu'à 54 Mbps (U-NII)	Finalisé
802.11b	Définition d'une nouvelle couche physique : jusqu'à 11 Mbps (ISM)	Finalisé
802.11c	Incorporation des fonctionnalités de 802.11d	Finalisé
802.11d	Travaux sur la couche physique permettant l'utilisation dans d'autre pays du standard 802.11	Finalisé
802.11e	Travaux sur la QoS (Qualité de Service)	En cours
802.11f	Définition de l'interopérabilité entre point d'accès par le protocole de gestion des handovers IAPP (Inter-Access Point Protocol)	En cours
802.11g	Définition d'une nouvelle couche physique : jusqu'à 54 Mbps (ISM)	Finalisé
802.11h	Harmonisation de 802.11a avec la réglementation européenne	En cours
802.11i	Amélioration des mécanismes de sécurité	Finalisé
802.11j	Harmonisation de 802.11a avec la réglementation Japonaise	En cours
802.11k	Fonctionnalité facilitant la localisation et la configuration des terminaux grâce aux informations radios (RRM : Radio ressource Measuremnt)	En cours
802.11m	Amélioration du standard 802.11 et des amendements finalisés	En cours
802.11n	Définition d'une nouvelle couche physique : débit de 100 Mbps	En cours

Tableau 6: les amendements du standard 802.11

La Wi-Fi alliance[43] s'appuie sur ces standards pour proposer la certification d'équipements réseaux sans fil. Bien que tous ces équipements répondent aux spécifications 802.11,

42 ASFI : Accès Sans Fil à Internet

43 Wi-Fi alliance : Wireless-Fidelity alliance (http://www.wi-fi.org/). C'est une association industrielle à but non-lucratif de plus de 200 membres dont l'objectif est de promouvoir le WLAN (réseaux locaux sans fil). La Wi-Fi alliance a un programme de certification s'appuyant sur les spécifications du groupe 802.11.

4.2.4.4.b Les spécifications de fréquences du standard 802.11

Les spécifications de transmissions 802.11 se place dans les couches physique et liaison du modèle OSI. La couche physique utilise quatre modes de transmissions :

- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)
- IR (Infra-Rouge)
- OFDM (Orthogonal Frequency Division Multiplexing)

Le mode infra-rouge est moins connu car il s'appuie sur les ondes lumineuses dont la portée et les contraintes (émetteur visible par le destinaire) l'ont rendu caduque par les modes utilisant les ondes radios. Son utilisation reste cantonnée à quelques domaines spécifiques.

Le tableau ci-après résume les différences entre les 3 méthodes de transmissions des équipements certifiés Wi-Fi.

	802.11a	802.11b	802.11g
Débit maximum	54 Mbps	11 Mbps	54 Mbps
Méthode employée	FHSS	DSSS	DSSS/OFDM
Bande de fréquence	5.725 - 5.850 Ghz	2.4 - 2.4835Ghz	2.4 - 2.4835Ghz
Largeur total de bande	125 Mhz	83 Mhz	83 Mhz
Nombre de canaux	79	14	14
Largeur d'un canal	1 Mhz	5 Mhz	5 Mhz
Nombre de bandes sans chevauchement	8	3	3

Tableau 7: Les principales différences de transmission 802.11

Comme on peut le constater, 802.11b et 802.11g sont très proches et 802.11g est même entièrement compatible avec 802.11b. En revanche, 802.11a utilise une modulation et une bande de fréquence différente et ne peut donc pas communiquer avec des équipements 802.11b/g.

D'autre part, les fréquences employés par ces équipements font l'objet d'une régulation par l'ART[44]. En premier lieu, les fréquences employées font parties de la bande ISM[45]. La puissance d'émission des équipements est soigneusement limité en fonction de la fréquence et s'il s'agit d'une émission en extérieure ou en intérieure (voir annexe 7.2)

Les équipements 802.11b et 802.11g utilisent une gamme de 13 fréquences en europe (voir annexe 7.2), il est donc possible d'étendre la zone de couverture du réseau. Toutefois, les fréquences concommitantes se chevauchement.

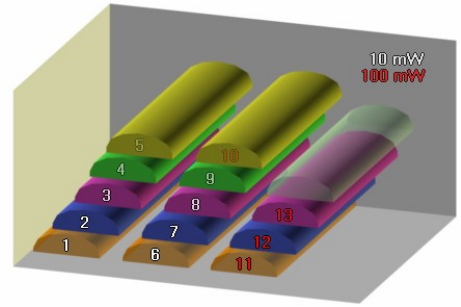


Illustration 28: Chevauchement des fréquences en 802.11b/g

44 ART : Autorité de Régulation des Telecoms (http://www.art-telecom.fr/). Aussi appelé ARCEP (Autorité de Régulation des Communications et les Postes), c'est une autorité administrative indépendante créée par la loi du 26 juillet 1996 pour l'ouverture du secteur des télécommunications.

45 ISM : Industrial, Scientific and Medical.

Dès lors, le déploiement d'un ensemble de points d'accès doit éviter ces recouvrements sinon la qualité des signaux sera perturber : il faut établir une cartographie des locaux et choisir un ensemble de canaux (1-6-11, 2-7-12, 3-8-13 ou encore 4-9 ou 5-10).

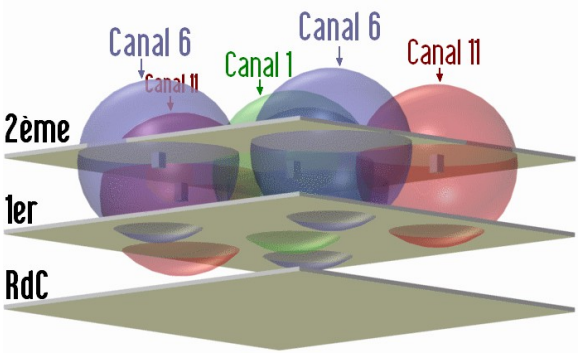


Illustration 29: Exemple de répartition de canaux

4.2.4.4.c Le fonctionnement du standard 802.11

La couche liaison de données est toutefois divisé en deux sous-couches :

- La couche 802.2 LLC est identique à celle utilisé sur les réseaux Ethernet. Il est donc possible de relier un réseau WLAN sur tout réseau local respectant les standards de l'IEEE.
- La couche MAC 802.11 : spécifique au standard 802.11, elle ressemble a la couche MAC du standard 802.3 pour la partie écoute de la porteuse avant émission (fonction CSMA).

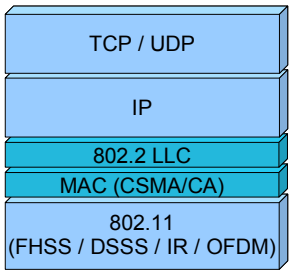


Illustration 30: Les couches du standard 802.11

L'association des équipements entre eux permet de créer des structures aux propriétés bien définies :

- Mode Ad-Hoc : non sécurisées, l'association à ce type de réseau est très facile. En revanche, c'est un mode souple pour échanger des fichiers entre deux machines. Un ensemble de machine dialoguant dans ce mode forme un IBSS[46]. Ce mode est à bannir en entreprise.
- Mode infrastructure : ce mode implique que toute communication passe par un point d'accès. Ce type de structure peut être ouvert ou nécessiter une authentification. Le cas le plus simple est appelé BSS et n'implique qu'un point d'accès isolé. Lorsque les points d'accès peuvent dialoguer ensemble (par le LAN ou via une connexion , l'architecture ainsi formée est appelée ESS[47].

46 IBSS : Independant Basic Service Set.
47 ESS : Extended Service Set

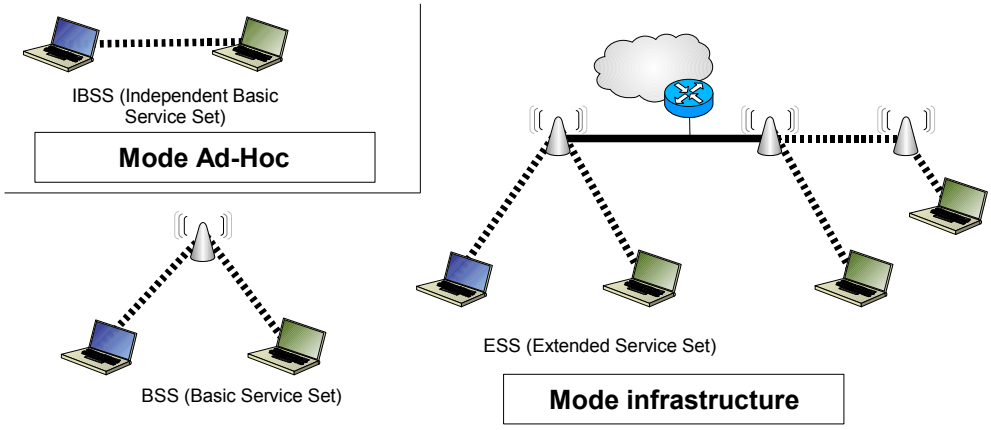


Illustration 31: Les différents modes de connexion 802.11

En terme de sécurité, il est important d'utiliser un mode infrastructure mais il faut également prévoir la sécurisation des communications entre point d'accès. En effet, une attaque propre à la structure choisie (AP en mode répéteur reliés par un commutateur commun) peut conduire à ce que deux terminaux puissent communiquer entre eux directement. Il faut donc activer les fonctions de protection prévue à cet effet (illustration X).

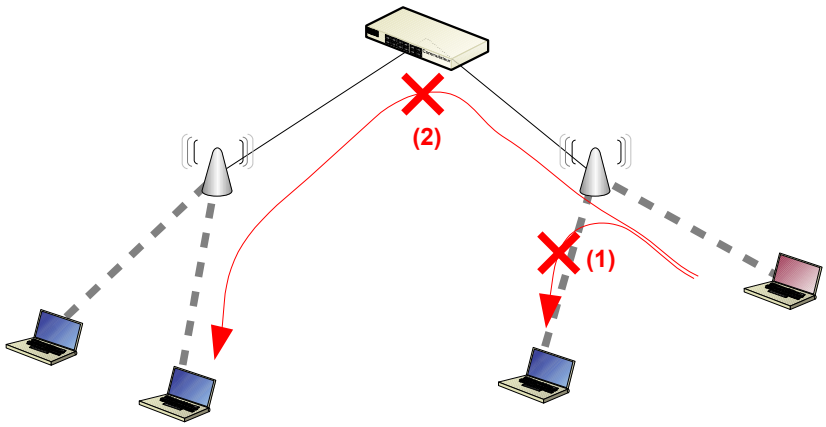


Illustration 32: Protection de communication entre les points d'accès

Dans un environnement ou plusieurs points d'accès ayant le même SSID[48] couvrent le lieu où se trouve l'utilisateur, c'est la machine de se dernier qui choisit sur lequel elle va se connecter. De la même manière, si le signal de son AP devient trop faible, elle peut décider d'en changer : pour cela, elle émet en premier une trame de dé-association à destination de l'AP d'origine. Ensuite elle émet une requête de ré-association au nouvel AP : cette requête contient l'identité de l'ancien point d'accès : ceci permet aux deux AP de se mettre en relation pour se transmettre des informations et éventuellement les paquets en attentes. Ce mécanisme est appelé "handover". Dans ce cas, la machine ne change pas d'adresse IP et l'opération dure moins d'une demi-seconde.

48 SSID : Service Set Identifier (en réalité, il faudrait parler d'ESSID).

Un autre cas est celui d'une machine changeant de réseau et d'adresse IP : ce cas est bien plus complexe puisqu'il nécessite que les équipements de niveau 3 communiquent ensemble, gèrent des files d'attentes et soient capables de traiter les ré-associations très rapidement. De plus, la qualité de service (QoS) et la voix sur IP (VoIP) impliquent un flux constant ce qui pose des problèmes pour des délais de ré-association supérieur à une dizaine de millisecondes. Ce mécanisme est appelé "roaming" (bien qu'un handover soit également nécessaire).

Enfin, les communications sur les réseaux 802.11 sont gérées avec un protocole basé sur CSMA. Toutefois, ici il n'est pas possible de détecter les collisions car la réception des signaux dépend de la puissance et de la distance des émetteurs. Il est alors facilement imaginable que deux stations hors de portée l'une de l'autre émettent en même temps vers le point d'accès commun.

C'est donc le protocole CSMA/CA[49] qui est employé. Il existe plusieurs modes de fonctionnement mais le mode DCF[50] est le plus classique (par opposition au mode PCF[51] dans lequel l'AP donne un temps de parole à chaque station de manière cyclique, à la manière d'un anneau à jeton).

Le fonctionnement du mode DCF est expliqué ci-dessous :

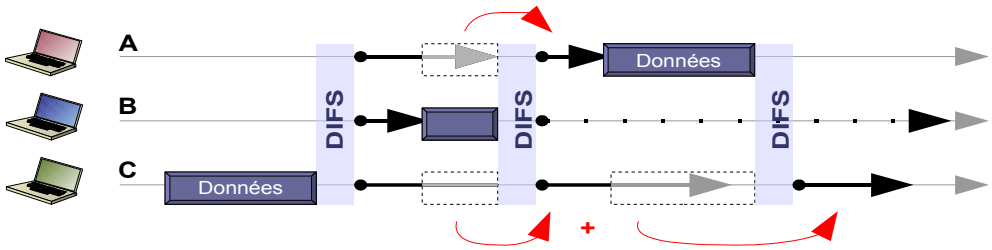


Illustration 33: Fonctionnement de CSMA/CA

Chaque équipement attend après un silence, un délai fixe appelé DIFS[52]. Une fois ce délai passé, chaque station va créer un compte à rebours d'un délai aléatoire dont la taille maximum est appelée CW (Collision Windows). Le premier équipement dont le compteur atteint zéro émet une trame RTS[53] (qui indique entre autre, puis attend un délai fixe SIFS[54] (bien plus court que le DIFS) : ainsi aucune station ne peut émettre dans cet intervalle mais assure à l'émetteur qu'il n'y a pas de collision. La station attend alors une trame CTS[55] de la part du récepteur pour pouvoir émettre ses données.

Deux remarques viennent s'ajouter sur la stratégie des modes de CSMA/CA :

- Afin de permettre aux stations ne pratiquant pas le mode PCF de pouvoir communiquer, la norme 802.11 impose que ce mode soit toujours alterné avec le mode DCF.
- Pour les données de petites tailles (généralement inférieures à 1000 octets), le standard 802.11 accepte que ces données soit transmise dans la trame RTS.

49 CSMA/CA : Carrier Sense Multiple Access / Collision Avoidance
50 DCF : Distributed Coordination Function. Mode du CSMA/CA.
51 PCF : Point Coordination Function. Mode du CSMA/CA de type Contention Free (libre de toute dispute)
52 DIFS : Distributed Inter Frame Space
53 RTS : Request To Send
54 SIFS : Short Inter Frame Space
55 CTS : Clear To Send

Une attention particulière doit donc être apportée sur les associations de clients sur un même point d'accès. En effet, l'utilisation de machines utilisant le même standard mais à des distances différentes peut faire chuter dramatiquement les débits notamment lors de l'utilisation du mode DCF.

Le tableau suivant [IMAG01] fait apparaître une faiblesse du standard 802.11b (en mode DCF), confirmé par une équipe de l'INRIA [INRIA03] :

Host rates	Measured Throughput
11 Mbps – **11** Mbps	**5.5** Mbps
11 Mbps – **1** Mbps	**0.84** Mbps

Tableau 8: Débits contatés avec deux stations 802.11b (source IMAG-LSR)

Le mode PCF est un mode basé sur le partage de temps et constitue donc une solution possible. Toutefois, afin de permettre aux équipements n'ayant pas ce mode implenté dans leurs circuits, la norme 802.11 requiert de faire de l'alternance DCF/PCF (durant le mode PCF, les stations ne sachant faire que du DCF ne peuvent communiquer).

4.3 Sécurité

Le fait de pouvoir transmettre un message de manière sécurisé a été mis en exergue par les militaires. Le premier à avoir codé des messages serait Jules César avec un décalage de lettre dans les mots. Plus tard, lors de la seconde guerre mondiale les allemands eurent l'avantage pendant une longue période grâce à leur machine "enigma"[56] : une sorte de machine à écrire où chaque appui sur une lettre fait tourner un rotor sur lequel se trouve des lettres. Équipée de trois rotors (le second rotor tourne d'un cran lorsque le premier rotor fait un tour complet) cette machine sera finalement copiée par les forces alliés. Les mathématiciens ont pus matérialiser de nombreuses propriétés de leur science.

En terme de sécurité, cinq types de services sont définit :

- Confidentialité : la sécurité doit assurer la protection des données et assurer que celles-ci ne puissent pas être vues par des personnes non-autorisées,
- Authentification : ce service permet d'assurer que l'identité d'une entité n'a pas été usurpée.
- Intégrité : ce service s'appuie sur les deux services précédent pour garantir que les données émises par un utilisateur authentifié non pas été compromises.
- Non-répudiation : ce mécanisme fonctionne un peu comme une lettre avec accusé de réception et permet de garantir que des données émises par un utilisateur authentifié ont été reçues par le destinataire sans avoir été altérées.
- Autorisation : le contrôle des accès aux données et aux ressources par des personnes ayant les droits nécessaires est garantie.

Ces cinq services utilisent généralement des mécanismes de chiffrement qui permettent de masquer les informations sensibles. La bonne compréhension des méthodes de chiffrement est nécessaire : les mécanismes permettant l'authentification s'appuient totalement sur leurs propriétés. De plus, les réseaux privés virtuels qui sont incontournables en matière de sécurité des réseaux, utilisent les mécanismes de chiffrement et d'authentification.

56 Voir le site http://lwh.free.fr/pages/algo/crypto/enigma.htm

4.3.1 Chiffrement

Il existe deux familles d'algorithmes de chiffrement : symétrique (dit à clé secrète) et asymétrique (dit à clé publique)

4.3.1.1 algorithmes à chiffrement symétrique

Les algorithmes à chiffrement symétrique sont généralement plus rapide mais moins sûrs car ils sont réversibles. La même clé est utilisée pour coder et décoder le message. Ainsi, ces algorithmes imposent que la clé soit connue par l'émetteur et le destinataire ce qui pose un problème pour la transmission de cette clé de manière sécurisée. Appartiennent à cette famille les algorithmes AES, DESX, RC4, Triple DES.

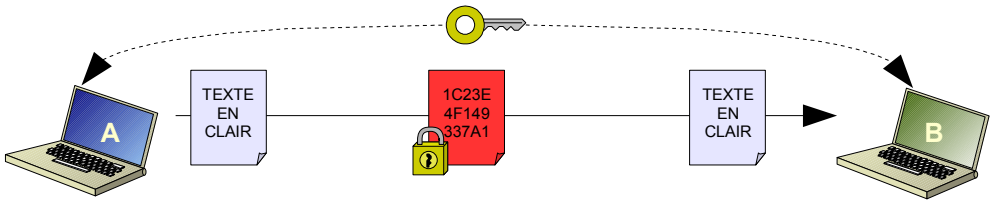


Illustration 34: Fonctionnement d'un algorithme de chiffrement symétrique

4.3.1.1.a RC4

RC4 (Ron's Code, du nom du concepteur Ron Rivest) a été créé en 1987. Cet algorithme de type symétrique est aussi un algorithme de chiffrement de flux (stream-cipher) ce qui l'a rendu populaire dans les équipements réseaux. La clé peut avoir une taille variable mais à cause des lois d'exportation, elle a souvent une longueur de 40 bits.

Elle sert à générer une table d'état de 256 bits qui sera employée pour générer une suite de d'octets pseudo-aléatoire. Cette suite, combinée par un OU exclusif (XOR) au flux de données aura pour résultat un flux chiffré. Cette méthode le rend dix fois plus rapide que l'algorithme DES.

4.3.1.1.b DES

DES (Data Encryption Standard) a été adopté en 1978 par le NBS[57] (devenu depuis, NIST[58]). Cet algorithme est basé sur le travail d'IBM (algorithme 'Lucifer') et modifié par la NSA[59]. DES (aussi connu sous le nom de DEA ou norme ANSI X3.92) répond aux critères suivants [WEB002]:

- ayant un haut niveau de sécurité lié à une clé de petite taille servant au chiffrement et au déchiffrement
- compréhensible
- ne devant pas dépendre de la confidentialité de l'algorithme
- adaptable et économique
- efficace et exportable

C'est un algorithme de type symétrique et de chiffrement par bloc. DES utilise une clé de 64 bits dont 8 sont utilisés pour les tests de parité (intégrité de la clé). Il emploie des fonctions de combinaison, substitution et permutation dans un ensemble de 'rondes' (boucles itératives).

57 **NBS** : National Bureau of Standards
58 **NIST** : National Institute of Standards and Technology
59 **NSA** : National Security Agency

Bien que très robuste en son temps, une évolution fût nécessaire : le 3DES (triple DES ou ANSI X9.52). Elle consiste à enchaîner trois fois l'algorithme DES comme indiqué ci-dessous :

$$\mathbf{3DES = DES \rightarrow DES^{-1} \rightarrow DES}$$

Bien sûr, dans ce mode de fonctionnement on utilise deux clés différentes pour éviter que les opérations **DES** → **DES**$^{-1}$ ne s'annulent.

Toutefois, le triple DES est désormais considéré comme n'étant plus assez fiable (sensible aux attaques par dictionnaire multiples, sa résistance est équivalente à 2^{113} possibilités, c'est à dire environ $2x2^{56}$)

4.3.1.1.c AES-Rijndael

AES (Advanced Encryption Standard) a été instigué par le NIST en 1997 pour succéder à DES. L'algorithme Rijndael (des belges Vincent Rijmen et Joan Daemen) a été choisi en 2000. AES répond aux critères suivants :

- Standard libre de droit et sans brevet,
- Algorithme de type symétrique,
- Algorithme de chiffrement par bloc,
- Supporte différentes longueur de clé et longueur de bloc (128-128, 192-128 et 256-128)

Toutefois, les points fort d'AES sont qu'il ne nécessite pas une puissance de calcul trop importante, ne consomme pas beaucoup de mémoire et son implémentation est vraiment aisée.

Il utilise des fonctions de substitution, de permutation, de combinaison linéaire et d'algèbre booléenne (OU exclusif). Grâce à cela, il est beaucoup plus résistant que DES ou 3DES aux attaques par dictionnaire (sa résistance est directement proportionnelle à la longueur de la clé soit 2^{128} possibilités dans la forme minimum de l'algorithme).

Une information plus complète sur le fonctionnement des algorithmes et les attaques par dictionnaires de 3DES et AES se trouve sur le site www.securiteinfo.com[60].

4.3.1.2 Algorithmes à chiffrement asymétrique

Par opposition, les algorithmes à chiffrement asymétrique sont moins rapide mais ils disposent d'un avantage non-négligeable : ils fonctionnent avec deux clés appelées "clé publique" et "clé privée". La clé publique est fournie au destinataire afin qu'il puisse coder un message que seul l'émetteur de la clé pourra lire à l'aide de sa clé privée.

La deuxième propriété utile de ses mécanismes est qu'un message chiffré à l'aide de la clé privée sera déchiffrable avec une des clés publiques générées par l'algorithme.

Le mécanisme de chiffrement le plus connu dans cette catégorie est RSA.

60 http://www.securiteinfo.com/crypto/aes.shtml

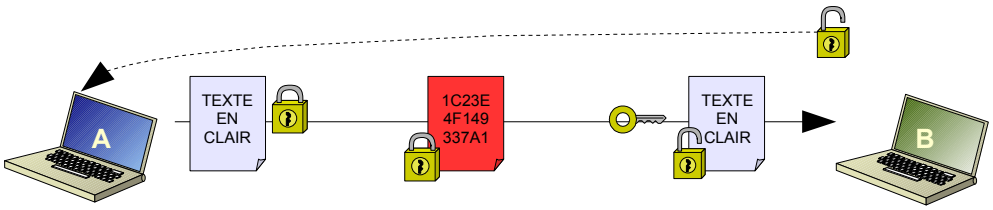


Illustration 35: Fonctionnement d'un algorithme de chiffrement asymétrique

Le schéma ci-dessus est une métaphore : le futur destinataire (B) fournit un cadenas dont lui seul a la clé. L'émetteur (A) utilise le cadenas pour verrouiller le message en clair et l'envoie au destinataire. Même en cas d'interception de la clé publique, un pirate ne peut pas décoder le message. La clé privée n'est jamais transmise évitant ainsi d'être compromise.

4.3.1.3 fonctions de hachage et de signature

4.3.1.3.a Fonction de hachage

Les algorithmes employés dans une fonction de hachage ne sont pas réversibles, c'est ce qui fait leur force. Toutefois, puisque le message original ne peut pas être retrouvé par qui que ce soit à partir du résultat, ces algorithmes sont généralement utilisés conjointement à d'autres méthodes de chiffrement.

Leur intérêt est qu'ils sont capable de garantir l'intégrité des données contenues dans un message à la condition que pendant son transport, ce dernier soit chiffré (de préférence avec un algorithme à clé publique).

En effet, si le mécanisme ne permet pas la modification du message sans fournir un résultat différent, rien n'empêche une personne malveillance de modifier le message puis de générer une clé de hachage en utilisant le bon algorithme.

Le schéma suivant montre un exemple d'application de ces systèmes de codage.

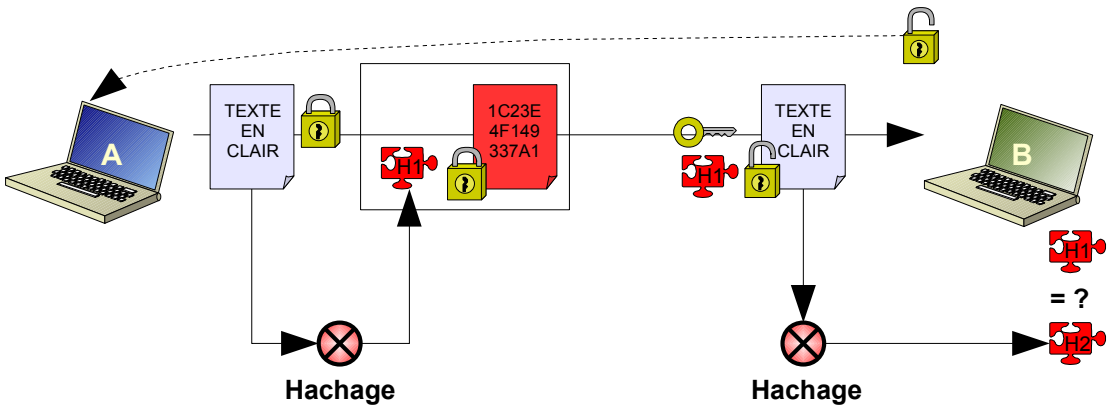


Illustration 36: Fonctionnement d'un mécanisme de hachage

- L'émetteur A hache le message en clair : il obtient une empreinte H1,
- il code ensuite le message et ajoute l'empreinte,
- le récepteur B décode le message : il hache ensuite le message décodé, avec la même fonction de hachage (et obtient H2),

- il compare H1 et H2. En cas d'inégalité, le message est considéré comme ayant été altéré.

La fonction de hachage (parfois appelée fonction de condensation) permet d'obtenir un condensé ou une empreinte d'un message ou d'un fichier. Certains sites web fournissent des programmes en téléchargement et fournissent une empreinte pour que l'utilisateur puisse s'assurer avoir copié le programme original (sans code ajouté).

Les algorithme les plus utilisés sont MD5 (Message Digest 5) qui créé une empreinte sur 128 bits et SHA-1 qui créé une empreinte de 160 bits. La taille des empreintes est importante car la protection offre 2^n possibilités mais en revanche, le message haché n'a pas de taille fixe et il existe forcément un message qui donne une empreinte identique à d'autres messages : on appelle cela une collision. Le théorème des anniversaires prouve qu'il faut $2^{n/2}$ essais pour trouver une collision au hasard. Bien sûr, il faudrait que le texte soit cohérent pour que le récepteur puisse être abusé : recevoir un message intègre contenant une suite de lettres ou de mots incohérent risque d'éveiller les soupçons !

Toutefois, rien ne permet d'assurer à l'utilisateur que le message ou le fichier n'a pas été intercepté puis re-émis (la clé de hachage pouvant être refaite par le pirate). Il faut alors utiliser une méthode d'authentification forte : la signature électronique.

4.3.1.3.b Fonction de signature électronique

La fonction de signature électronique se base sur la propriété des algorithmes à chiffrement asymétrique suivante : ils sont capables de générer plusieurs clés publiques pour une seule clé privé mais toutes ces clés sont capables de déchiffrer un message codé avec la clé privé. Ainsi le possesseur d'une clé privée ne peut l'employer pour transmettre des messages confidentiels car n'importe quelle personne peut se procurer une clé publique et le déchiffrer. Cette faiblesse est pourtant un avantage dans le cas de la signature électronique.

Elle permet en effet d'assurer au destinataire que l'information a été chiffrée uniquement par le possesseur de la clé privé : la clé publique ne peut décoder que les messages correspondants à l'émetteur de cette clé, c'est à dire l'utilisateur de la clé privée.

4.3.2 Authentification, Autorisation et accounting

L'authentification s'appuie sur les méthodes de chiffrement précédemment citées : celle-ci n'étant testée que périodiquement, elle emploie généralement un chiffrement asymétrique. Elle est majoritairement basé sur un ensemble 'nom d'utilisateur / mot de passe' : la biométrie commence à faire son apparition (en particulier, les systèmes basés sur l'empreinte digitale) mais sa mise en oeuvre reste surtout médiatique. Dans les cas sensibles, il est plus fréquent de voir des systèmes utilisant des cartes à puce ou intégrant un mécanisme d'OTP[61] mais aussi des systèmes utilisant des certificats.

Le déploiement de ces solutions est généralement rendu nécessaire pour sécuriser les accès au réseau mais aussi aux différents services dont les données sont critiques (messageries, bases de données, comptabilités, laboratoires de recherches...) ce qui rend l'administration des authentifications et autorisations difficiles. Nous verrons dont qu'il existe des systèmes capables de simplifier cette gestion et enfin des structures dédiées pour le contrôle général des accès.

4.3.2.1 Différentes méthodes d'authentification

Pour pouvoir être authentifier, il faut pouvoir fournir une preuve de son identité : cette preuve peut prendre plusieurs formes mais est basée sur la propriété d'unicité lié à l'utilisateur. Il doit être le seul (avec le système) à connaître cette preuve. Pour cela il existe de nombreuses méthodes dont les principales sont décrites ci-dessous.

61 **OTP** : One Time Password

4.3.2.1.a Mot de passe

Actuellement, tout utilisateurs d'une machine en réseau doit gérer plusieurs mots de passe : les employés d'une entreprise sur un LAN mais aussi les particuliers à la maison en RTC ou ADSL. Il est admis qu'un mot de passe inférieur à 8 caractères et n'incluant pas de chiffres ou de symboles n'offre qu'une protection limite : il n'est donc pas rare que les systèmes de sécurité lors de la création du mot de passe appliquent ces règles pour l'accepter. De plus, il est fortement recommandé de changer régulièrement ceux-ci.

L'utilisateur doit alors mémoriser plusieurs mots de passe et surtout le système auquel il est associé : qui n'a jamais tapé plusieurs mot de passe (compliqués) à la suite pour trouver celui qui fonctionne ?

4.3.2.1.b One Time Password

Le système de mot de passe à usage unique (plus connu par l'abréviation OTP) est une méthode efficace contre le piratage : le mot de passe n'est utilisé qu'une seule fois. En général, une application (comme s/key par exemple) demande le mot de passe de l'utilisateur et calcule (en fonction d'un nombre pseudo-aléatoire) une clé (s/key fournit une suite de 6 mots anglais).

Lors de l'authentification sur un système, il sufft de saisir le mot de passe dans l'application qui retourne la clé et de copier cette clé dans la demande de mot de passe du système (compatible avec l'authentification OTP).

Des petits gadgets électroniques dotés d'un afficheur peuvent servir pour générer des mots de passe à usage unique (Token Card).

4.3.2.1.c Biométrie

Très médiatisé (récemment, l'aéroport de Roissy) la biométrie se base sur un trait unique de la morphologie humaine : empreinte digitale, iris de l'oeil, empreinte rétinienne, empreinte vocale, signature dynamique...

Le système le plus vulgarisé est probablement l'empreinte digitale (il existe un accessoire qui utilise le port USB pour un prix inférieur à 60€) mais ces technologies restent difficiles à déployer : les lecteurs nécessitent un calibrage et une rigueur importante sans parler que le corps humain est soumis à de nombreuses variations (par exemple, une coupure sur un doigt sale rend la prise d'empreinte difficile et le capteur sera salit). Certaines technologies sont jugées trop intrusive (empreinte rétinienne nécessitant l'utilisation d'un rayon lumineux pour éclairer le fond de l'oeil).

4.3.2.1.d Carte à puce

La carte à puce a connue un développement très important par sa facilité de fabrication et sa difficulté à être copiée. Créée par deux ingénieurs français (Roland Moreno et Michel Ugon), à la fin des années 1970, les cartes de paiement utilisent toutes une puce qui intègre un certificat numérique : l'utilisateur fournit son code à la puce qui le vérifie et qui envoie au terminal de paiement si le code est bon (le terminal n'a donc pas connaissance du code). Dans le cas d'un montant élevé, le terminal du magasin requiert une authentification forte en mettant en relation la puce et la banque. La banque envoie un challenge que la puce calcule à l'aide d'algorithmes de chiffrement (3DES) et de la clé secrète (partie illisible de la carte par le terminal mais connue du centre bancaire) let quelle retourne à la banque (via le terminal) [WEB003]

4.3.2.1.e Single Sign On

Le mécanisme d'une seule signature permet de n'authentifier qu'une fois un utilisateur sur un seul système. Les autres systèmes désirant l'authentification de celui-ci recevront un ticket en provenance du premier système et dans lequel ils auront confiance. Bien entendu, tout les éléments de la chaîne doivent utiliser le même standard.

4.3.2.2 Architecture AAA

Les systèmes dit "AAA"[62] sont très utilisés dans le domaine des télécommunications. L'authentification est déjà relativement complexe à mettre en oeuvre mais il a déjà été dit, elle permet de fournir un accès à un ensemble de ressources et de services. Cette gestion reste simple sur un réseau unique mais devient critique sur un ensemble de réseaux différents. Le cas typique en télécommunication est celui des opérateurs (FAI) : ils ne peuvent pas couvrir l'ensemble du territoire avec leur propre infrastructure et doivent passer des accords avec d'autres fournisseurs. Toutefois, l'utilisateur final doit être authentifié par son fournisseur tout en se connectant sur les équipements d'un autre fournisseur.

Pour cela, il existe deux fonctionnement possibles :

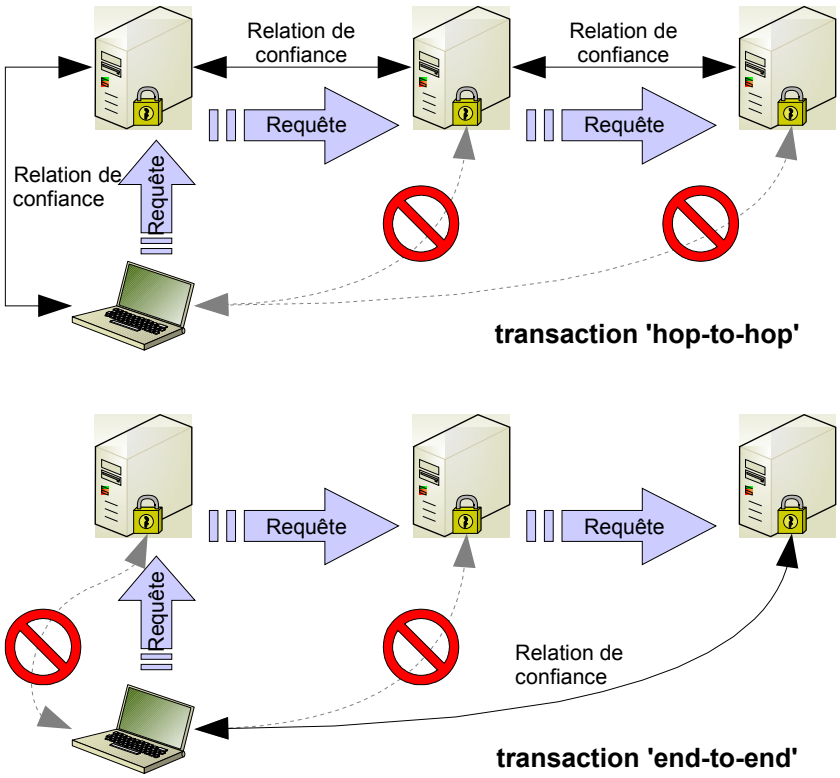


Illustration 37: Les deux modèles d'architecture AAA

- Dans le cas d'une transaction 'hop-to-hop' (point à point), chaque serveur connait et fait confiance à ses voisins déclarés. L'utilisateur final ne dialogue qu'avec le serveur local. Dans ce modèle, les relations de confiance ne sont pas transitive ce qui implique qu'aucun serveur ne peut "court-circuiter" un élément de la chaîne.
- Dans le cas d'une transaction de bout en bout, la relation de confiance n'existe qu'entre l'utilisateur et son serveur final. Les autres serveurs ne font que transmettre la requête initiale. Ce modèle est utilisé par les systèmes basés sur les certificats.

62 **AAA** : Authentification, Autorisation and Accounting

Le protocole RADIUS[63] (rfc 2865) sur lequel s'appuie de nombreux systèmes AAA permet en effet de transporter des informations concernant l'authentification mais aussi les services autorisés et les données de comptabilité pour une éventuelle facturation.

RADIUS utilise le protocole de transport UDP pour communiquer ses requêtes. Celles-ci peuvent transiter via plusieurs serveurs car il utilise le modèle point-à-point.

RADIUS présente toutefois des faiblesses qu'il convient de bien connaître. La liste ci-dessous énumère les principales [HASS02]:

- en terme de sécurité, lorsqu'une requête est émise, elle peut passer par plusieurs serveurs relais : ainsi chaque serveur voit passer la requête complète. Cela signifie que si la sécurité d'un seul serveur est compromise, toutes les authentifications transitant par lui seront compromises,
- les spécifications du protocole n'impose pas que les ressources allouées lors de l'authentification puissent être modifiées après l'authentification. Dès lors, une suspension de compte ne sera prise en compte qu'à la prochaine authentification de l'utilisateur et ce dernier peut ne pas se déconnecter...
- étant un protocole 'stateless" (sans mémorisation), il est impossible de garder une trace des sessions précédentes dans les nouvelles. Cela complique donc la gestion des ressources et des sessions.
- Enfin, RADIUS supporte mal d'être utilisé dans des systèmes à grande échelle et peut aboutir à des problèmes de performances ou pire, des pertes de données. L'IESG[64] explique même en en-tête de la RFC que c'est parce que RADIUS ne gère pas les contrôles de congestion, et qu'il est conseillé de suivre le groupe AAA de l'IETF sur la progression d'un successeur.

RADIUS, AAA, TACACS, LDAP... OTP (One Time Password), SSO (Single Sign On), Diameter

PAM (Pluggable Authentication Modules) de l'OSF (maintenant Opengroup)

http://www.hsc.fr/ressources/articles/dsi-auth/index.html.fr

Radius, Ldap, EAP (eap-md5, eap-tls, eap-ttls, eap-peap, eap-fast), AAA, certificats, PKI

4.3.2.3 Structure d'authorité de certification

Avant de décrire l'architecture et l'utilisation d'une Infrastructure de Gestion de Clés (IGC) ou en anglais "Public Key Infrastructure" (PKI), nous allons voir l'utilité de cette structure.

Pour résoudre les problèmes d'authentifications multiples et valider la distribution des clés publiques, une idée simple est de fournir un objet contenant des informations précises, secrètes et inviolables. Dans un système normalisé, cet objet représente une identité : il est donc unique, compatible avec le système et valide. Cet objet est un certificat.

63 **RADIUS** : Remote Authentication Dial In User Service
64 **IESG** : Internet Engineering Steering Group

Les certificats sont utilisés couramment sur Internet, dans tout les systèmes proposant des pages web sécurisées : le protocole HTTPS est en fait un protocole HTTP auquel on a ajouté une sécurisation SSL[65]. Lapparition d'un cadenas dans la barre d'état des navigateur (IE, Firefox, Opera, Maxthon, etc.) indique qu'une échange SSL est en cours avec un site de confiance.

D'autre utilisation de certificat existent mais le point commun est la confiance donnée à un organisme de certification.

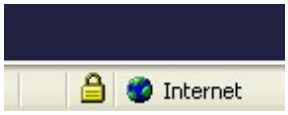


Illustration 38: symbole cadenas pour le protocole HTTPS

En effet, un certificat est délivré par entité digne de confiance : l'autorité de certification. Celle-ci est reconnue par une communauté d'utilisateur et délivre des certificats uniques ainsi que les listes de révocation.

Un certificat contient les données suivantes :

- Numéro de version,
- Numéro de série unique (délivré par l'autorité de certification),
- algorithme de signature (un algorithme asymétrique et un algorithme de hachage),
- Nom de l'émetteur du certificat (DN à la norme X.500),
- Période de validité,
- Nom du propriétaire du certificat (celui qui possède la clé privée),
- Clé publique du propriétaire (peut-être utilisé par un destinataire pour renvoyer des données chiffrées, lisibles uniquement par le propriétaire du certificat),
- La signature de l'autorité de certification.

L'IETF définit une PKI comme un ensemble de moyens matériels, de logiciels, de composants cryptographiques, mis en oeuvre par des personnes, combinés par de spolitiques, des pratiques et des procédures requises, qui permettent de créer, gérer, conserver, distribuer et révoquer des certificats basés sur la cryptographie asymétrique [MISC13].

Certificats, PKI, révocation...

DER (Definite Encoding Rules) est utilisé pour encoder des certificats X509 en notation ASN.1 (Abstract Syntax Notation). Les extensions habituelles sont .der, .cer, .crt et .cert.

PEM (Privacy Enhanced Mail) peut contenir des clés privées, des clés publiques et des certificats X509. Le format PEM est du DER encodé en base64 et auquel est ajouté un entête en ASCII. Les extensions sont .pem, .cer, crt, .cert.

PFX est l'ancêtre de PKCS#12 et est une spécification de Microsoft désormais caduque. L'extension est .pfx et il y a parfois confusion sur les systèmes Microsoft qui donnent cette extension aux fichiers PKCS#12.

Le système PKCS de RSA

65 **SSL** : Socket Secure Layer

4.3.3 Tunnels et Réseaux Virtuels Privés

4.3.3.1 SSL (Secure Socket Layer)

SSL est un VPN de niveau 7 (application).

SSL (3DES 168b + SHA-1 = USA, RC4 128b + MD5, DES 56b + SHA-1)
http://www.salemioche.com/doc/ssl3.php

SSH (3DES, Blowfish, AES)

4.3.3.2 IPSec (Internet Protocol Secure)

IPSec (Internet Protocol Secure) est le protocole de sécurisation des communications qui s'appuie sur le protocole IP. Si ce protocole est optionnel en IPv4, il est intégré en standard dans le protocole IPv6. Il est présent au niveau 3 du modèle OSI.

IPSec est employé de deux manière :

- mode transport : dans ce mode, les trames sont limités entre serveurs ou de serveurs à clients (et vice-versa). Ce mode ne peut pas être routé.
- Mode tunnel : c'est le mode le plus répandu. Il permet de franchir plusieurs réseaux tout en garantissant la sécurité des trames encapsulées.

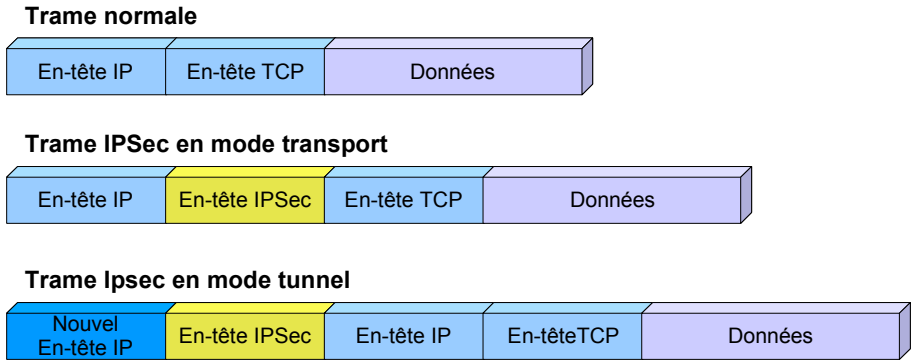


Illustration 39: Les modes transport et tunnel d'IPSec

Alors que le mode transport se contente d'insérer un champ IPSec entre l'en-tête IP et l'en-tête TCP, le mode tunnel encapsule toute la trame d'origine dans une nouvelle trame IP (incluant également un en-tête IPSec).

IPSec est basé sur deux protocoles pour la sécurisation des flux : AH[66] et ESP[67]. Ils utilisent tout les deux des méthodes de chiffrement, toutefois AH ne garantit pas la confidentialité des trames (aucun chiffrement sur le message original n'est fait). [COCO03]

4.3.3.2.a AH (Authentication Header)

AH est spécialisé dans l'authentification et utilise pour cela des mécanismes de hachage (RFC2402). A ces mécanismes, il est possible d'associer des algorithmes asymétriques pour créer une signature électronique (HMAC-MD5 et HMAC-SHA-1).

66 **AH** : Authentication Header
67 **ESP** : Encapsulating Security Payload

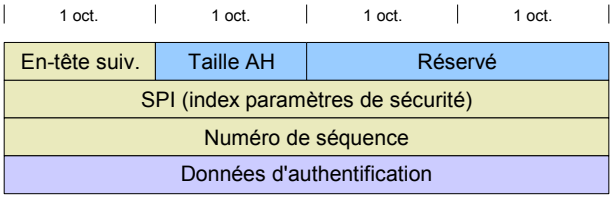


Illustration 40: Structure de l'en-tête AH

- Le champ "En-tête suiv." indique le numéro du protocole IP protégé. Il est égal à 6 pour UDP, 17 pour TCP et 4 pour IP (voir "Protocol numbers sur le site de l'IANA[68]).
- Le champ "SPI (index paramètres de sécurité)" est un numéro qui va identifier l'association de sécurité pour cette trame dans la base de données des associations de sécurité (SAD).
- "numéro de séquence" ce numéro de séquence permet d'éviter les attaques par rejeu.
- Le champ "Données d'authentification" est le résultat du mécanisme d'authentification sur toute la trame (sauf les champs variables comme le champ TTL par exemple).

4.3.3.2.b ESP (Encapsulating Security Paiload)

Ce protocole garantit l'intégrité, l'authentification mais aussi la confidentialité de chaque trame (RFC2406). Il utilise le contrôle d'intégrité (hachage) et le chiffrement des échanges.

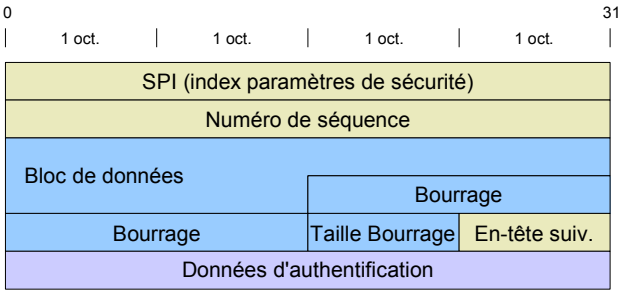


Illustration 41: Structure de l'en-tête ESP

On retrouve les champs "En-tête suiv.", "SPI" et "Numéro de séquence" de la structure d'en-tête du protocole AH. On trouve également deux champ nouveaux :

- Le champ "Bloc de données" contient les données à protéger (c'est à dire uniquement les données de la trame d'origine dans le mode transport ou toute la trame dans le mode tunnel).
- Le champ "Bourrage" qui assure l'alignement des champs "Taille Bourrage" et "En-tête suiv." sur les deux octets de poids fort et qui est également nécessaire lors de l'emploi d'un algorithme de chiffrement par bloc (bloc-cipher).
- Le champ "Données d'authentification" est le résultat du mécanisme d'authentification sur toute la trame après l'en-tête ESP (donc légèrement du protocole AH).

68 **IANA** : Internet Assigned Numbers Authority (http://www.iana.org/assignments/protocol-numbers)

Au niveau de l'authentification, IPSec peut employer HMAC-MD5 ou bien HMAC-SHA-1. Pour la partie chiffrement, il peut s'appuyer sur 3DES-168, CAST-128, DES, Blowfish et AES. Le choix de ces deux paramètres est fait à l'aide du protocole IKE[69] : ce protocole permet l'échange de clé de manière automatique, en utilisant les SA (Security Associations). Une association de Sécurité est un ensemble de données pour caractériser l'échange des données. L'ensemble des SA est contenu dans une SAD (Security Association Database) et chaque SA contient généralement les adresses IP source et destination, un nom au format X.500 ou DNS, le protocole (UDP et TCP principalement) et les ports source et destination.

4.3.3.3 PPTP (Point to Point Tunneling Protocol)

PPTP est un VPN de couche 2 : cela lui procure un avantage important sur les VPN de niveau 3 ! en effet, PPTP peut transporter d'autre protocole que TCP/IP (IPX, NetBEUI, etc.). Toutefois, cet avantage est parfois visible comme étant un inconvénient.

En effet, les VPN sont souvent utilisés pour transmettre des données IP mais le niveau de fonctionnement de PPTP ne permet pas le routage : ainsi, toute les données sont d'abord envoyées vers le serveurs VPN-PPTP, même s'il s'agit d'un trafic à destination d'Internet.

Il résulte alors un volume de trafic plus important avec PPTP qu'avec IPSec. D'autre part, PPTP ne fonctionne qu'avec un algorithme de chiffrement RC4 à 128 bits : cela reste suffisant pour la sécurité même si l'implémentation de ce mécanisme a été rendu impopulaire par les réseaux sans fil.

4.3.3.4 EAP

EAP (Extensible Authentication Protocol) est une extension du protocole PPP. PPP est un protocole de niveau 2 essentiellement prévu pour transporter des trames IP. EAP est dédié à l'authentification et il supporte de nombreuses méthodes comme Kerberos, TLS, MS-CHAP, MD5,...

Son fonctionnement rend possible l'ajout de nouvelles méthodes de manière simple. Seul le champ du paquet EAP appelé 'type' et codé sur un octet limite l'ensemble des mécanismes à un peu moins de 256 valeurs.

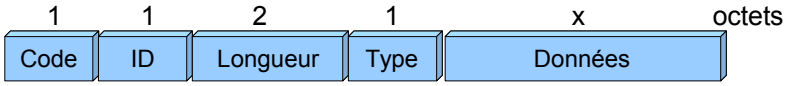


Illustration 42: Format de trame EAP

Le champ 'Code' n'a que quatre valeurs possibles : Request, Response, Success et Failure.

L'intérêt d'EAP est de fournir une couche standard pour les mécanismes d'authentifications. Grâce au standard 802.1x, EAP n'est plus lié au protocole PPP et peut être utilisé sur n'importe quelle interface utilisant un standard de l'IEEE. Il permet les échanges des requêtes nécessaires pour authentifier un équipement et/ou un utilisateur tout en isolant parfaitement le réseau LAN des attaques classiques par déni de service.

Il existe plusieurs mécanismes d'authentification EAP. Le tableau ci-dessous montre pour les plus connus ainsi que leurs points forts et leurs points faibles.

69 IKE : Internet Key Exchange.

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Authentification serveur	-	Hashage mot de passe	Certificat Clé publique	Certificat Clé publique	Certificat Clé publique
Authentification client	Hashage mot de passe	Hashage mot de passe	Clé publique Certificat, puce…	CHAP, PAP, EAP MS-CHAP (v2)	EAP, MS-CHAP (v2) Clé publique
Distribution dynamique des clés	non	oui	oui	oui	oui
Certificat client obligatoire	non	non	oui	non	non
Risques sécurité	Vol de session Attaque dictionnaire Attaque MiM	Attaque dictionnaire	Obtention ID client	Attaque MiM	Attaque MiM

Tableau 9: Points forts des différents algorithmes utilisés avec EAP

- EAP-MD5 n'est pas recommandé (et peu utilisé) car il ne gère pas la distribution de clé dynamique WEP et car les échanges ne sont pas chiffrés : le challenge circule en clair puis chiffré par le client ce qui le rend sensible aux attaques par dictionnaire ou attaques brutes.
- EAP-LEAP est une méthode développée par Cisco mais dont la faiblesse a rapidement été découverte. En plus d'être une solution propriétaire, elle s'appuie sur le hashage MS-CHAPv1 (vulnérable) et le login de l'utilisateur circule en clair. Les échanges ne sont pas chiffrés.
- EAP-TLS est la méthode la plus sûre. En effet, le serveur et le client échangent leurs certificats et leurs clés publiques : seul le destinataire peut décoder le message avec sa clé publique. Sa seule faiblesse est le vol de certificat (et de la clé privée associée) mais la mise en oeuvre d'une IGC pour gérer autant de certificats peut dissuader de nombreux administrateur.
- EAP-TTLS simplifie un peu la méthode précédente. Seul le serveur envoie son certificat, le client utilisant cette clé publique pour coder le challenge. Cette méthode n'est sensible qu'à une attaque de type "Man in the middle". L'établissement d'un tunnel pour transmettre la véritable identité de l'utilisateur et son mot de passe rend l'écoute inutile.
- EAP-PEAP ressemble à EAP-TTLS avec pour seule différence que EAP-PEAP encapsule les données à échanger dans le tunnel dans des trames EAP tandis que TTLS utilise les pairs "attribut-valeur" (AVP) encapsulés dans des trames EAP-TTLS.
- EAP-FAST est censé être plus facile à mettre en oeuvre mais son fonctionnement ressemble à TLS. Cisco déclare qu'il est aussi sur que EAP-PEAP et aussi simple à mettre en oeuvre que EAP-LEAP (et bien sûr très rapide pour l'authentification, d'où son nom). EAP-FAST utilise un PAC[70] à la place d'un certificat mais pour être aussi sûr que EAP-PEAP, il faut certifier ce PAC... à l'aide d'un certificat ! Cette méthode ne sera pas décrite plus en avant à cause de son coté propriétaire (Cisco).

Afin de bien comprendre les phases d'authentifications du protocole EAP, la méthode EAP-TLS et EAP-TTLS sont décrites plus bas : se sont les deux méthodes les plus universelles (fonctionnent aussi bien sur tout systèmes d'exploitation, contrirement à EAP-LEAP, EAP-FAST et EAP-PEAP).

4.3.3.4.a EAP-TLS

EAP-TLS est le mode le plus sûr puisqu'il fonctionne sur le principe de l'échange de certificats. La figure ci-dessous montre les échanges entre le client (supplicant), le point d'accès (authenticator) et le serveur d'authentification.

70 **PAC** : Protected Access Credential

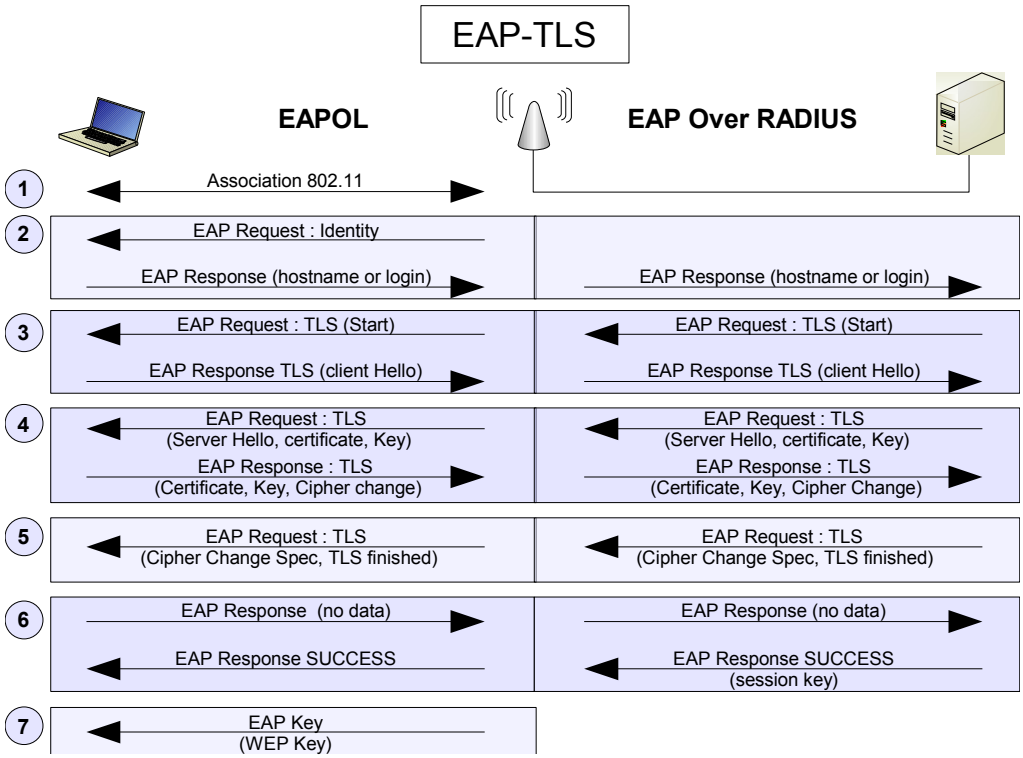


Illustration 43: Authentification EAP-TLS

1. Association du client au point d'accès (AP). En détectant le SSID d'un point d'accès le client demande à s'associer au réseau (équivalent de l'activation d'un port en 802.3).
2. Le point d'accès envoie des requêtes d'identité. Certains points d'accès ne recevant pas de réponse de la part du client ont la possibilité de les placer dans un vlan défini par l'administrateur. Si le client intègre le protocole EAP, il répond au point d'accès par une identité passé en clair et le type d'EAP utilisé (TLS). L'AP est en mesure de transmettre une requête au serveur d'authentification contenant les données fournies par le client.
3. Le serveur transmet une requête TLS à l'AP qui agit comme intermédiaire. A aucun moment le client ne dialogue avec le serveur ! L'AP émet une requête vers le client qui doit répondre par une réponse "client hello".
4. Le serveur envoie alors son certificat qui permet au client de chiffrer un challenge que seul le serveur sera capable de décoder (voir chapitre précédent). Il en profite pour fournir les spécifications de chiffrement qu'il peut utiliser et bien sûr son certificat à lui.
5. Le serveur répond alors et termine l'échange TLS.
6. Le client valide le protocole d'échange choisit et attend la réponse du serveur (toujours via l'AP). Toutefois, ce dernier message concerne aussi le point d'accès qui va utiliser la clé de session pour générer une nouvelle clé WEP.
7. Le point d'accès envoie la clé WEP au client.

4.3.3.4.b EAP-TTLS et EAP-PEAP

C'est deux méthodes sont un peu moins simple à mettre en oeuvre, toutefois la sécurité est très élevée également.

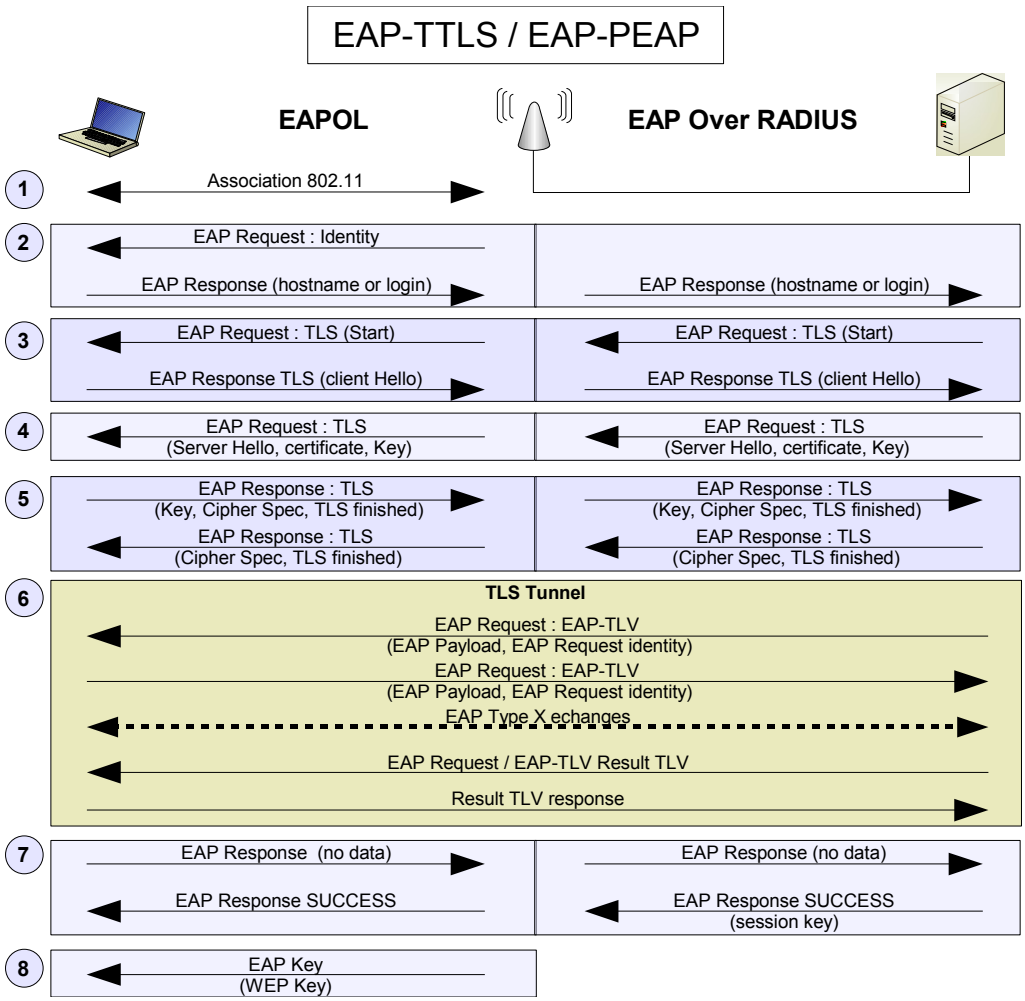


Illustration 44: Authentification EAP-TTLS

Avec cette méthode, les points 1 à 4 sont similaires à EAP-TLS. Toutefois, le point 5 entraine les changements suivants :

5. Le client n'ayant pas de certificat renvoie le challenge chiffré avec le certificat du serveur et indique quel mode de chiffrement il supporte. Le serveur répond et dans ce cas là, il confirme l'ouverture d'un tunnel.
6. Les requêtes suivantes transitent alors dans le tunnel : le point d'accès relaie toujours les trames mais n'interprète plus les requêtes. Le serveur demande alors l'identité réelle du client dans une requête TLV[71]. Après quelques échanges, le client fournit au serveur son mot de passe (en utilisant PAP ou MS-CHAPv2 selon la méthode choisie au départ). Le serveur est désormais en possession de tous les éléments pour statuer sur l'authenticité de l'identité du client.
7. Le client valide le protocole d'échange choisit et attend la réponse du serveur (toujours via l'AP). Toutefois, ce dernier message concerne aussi le point d'accès qui va utiliser la clé de session pour générer une nouvelle clé WEP.
8. Le point d'accès envoie la clé WEP au client.

71 **TLV** : Type, Length, Value

4.3.3.5 VLAN

Les vlans peuvent être considérés comme des Réseaux Virtuels Privés mais appliqués aux réseaux locaux. Le standard 802.1q normalise les mécanismes capables de gérer la diffusion sélective des données. Il s'agit d'une méthode de gestion des flux de niveau 2 du modèle OSI.

5 SOLUTIONS ET DÉPLOIEMENT

L'étude des différents protocoles et standards facilite maintenant le choix et la mise en oeuvre d'une solution au sein du CICG et sa généralisation au niveau du réseau interuniversitaire.

En premier lieu, l'accès à l'infrastructure doit se faire de manière nominative : un compte anonyme ne doit pas pouvoir utiliser le réseau interuniversitaire pour agir à l'encontre de la charte Renater. Cet accès implique donc le déploiement d'un serveur d'authentification. De plus, il doit être possible de retrouver à partir d'une adresse IP à quel service et quel personne utilise un poste corrompu ou dont le comportement est illégal. Il est dont nécessaire de choisir un système compatible avec une architecture AAA.

En premier lieu, l'objectif de permettre à un utilisateur d'accéder à Internet de manière sécurisée implique l'utilisation d'un standard de chiffrement entre son application ou sa machine et le point d'accès. Le réseau physique est jugé suffisamment sûr grâce à l'accès sécurisé du bâtiment, la segmentation en vlans et à l'implémentation de règles de filtrage. La politique de sécurité est donc suffisante pour considérer que le réseau filaire est sain.

5.1.1 Solution de base

Cette solution ne doit nécessiter que peu d'action de la part de l'utilisateur. Les tunnels nécessitant l'installation d'un logiciel sur le poste des utilisateurs, c'est la solution du portail captif qui est retenue. Cette solution présente les avantages suivants :

- compatible avec tous les équipements utilisant le protocole TCP/IP,
- elle ne nécessite aucun droit particulier sur le poste de travail,
- elle est capable d'utiliser un système d'authentification évolué (RADIUS),
- aucune action technique n'est demandée à l'utilisateur final,
- la sécurité est basée sur les failles du portail et non pas sur le poste de l'utilisateur.

Cette solution permet donc aux utilisateurs de se connecter de manière ouverte sur un des réseaux des universités de Grenoble et d'utiliser un navigateur internet pour accéder librement aux sites web, aux services webmail (messagerie par interface web). En revanche, les protocoles employés sont restreints

5.1.2 Solution étendue

Cette solution implique l'installation d'un logiciel sur le poste de l'utilisateur. Il est donc nécessaire que celui-ci donne son accord et en accepte les risques (toute installation de logiciel peut entraîner un dysfonctionnement de la machine). De plus, il doit avoir les privilèges nécessaires à l'installation du logiciel.

Cette solution reste tout de même la plus intéressante :

- chiffrement des données lors des communications,
- limitations moindres sur les protocoles employés,
- fonctionnement "universel" des solutions utilisant le protocole 802.1x,
- utilisation de méthodes d'authentification fortes,
- indépendance vis à vis du réseau d'accès pour les solutions VPN.

Cette solution moins souple à priori reste une solution très intéressante pour les véritables nomades : le téléchargement d'une application avant de pouvoir utiliser de manière sécurisée le réseau n'est un frein que la première fois ! Les connexions suivantes sont beaucoup moins pénibles (le logiciel client étant déjà installé et configuré).

5.1.3 Tronc commun au deux solutions

Dans les deux solutions, il y a la mise en oeuvre d'un serveur d'authentification. Cette solution est d'autant plus logique qu'elle est interopérable : il est ainsi possible à chaque université d'alimenter sa propre base d'utilisateurs et de gérer leurs autorisations. Les serveurs d'authentification sont capables de se mettre en relation pour accepter ou non un utilisateur sur le réseau, quelque soit sa provenance.

Cette propriété est essentielle et nous verrons qu'elle est obligatoire dans le cadre de la mobilité sur les réseaux européens.

5.2 Authentification

Les systèmes d'authentification sont nombreux. Les systèmes compatibles avec une véritable architecture AAA ne sont pas aussi nombreux : les besoins définis dans le cahier des charges impliquent de trouver une solution permettant de gérer l'authenticité d'une identité mais surtout de pouvoir l'identifier sur le réseau. La plupart des applications permettant l'accès à un réseau utilisent le protocole RADIUS pour interroger un serveur AAA.

Nous avons donc cherché les produits pouvant répondre à nos besoins puis nous avons mis en oeuvre la solution retenue.

5.2.1 Présentation

Les solutions suivantes répondent à l'architecture AAA : toute sont capables d'authentifier un utilisateur et de gérer la trace de sa connexion.

5.2.1.1 Steel Belted Radius (Funk Software Inc.)

Cette solution commerciale est développée par la société Funk Software inc. Basée aux États-Unis, elle a été créée par Paul FUNK en 1982. D'abord orientée dans les développements sur Lotus 1-2-3, elle amorce son intégration des réseaux en 1992 avec un logiciel de télémaintenance (Proxy Remote Control). Elle est désormais spécialisée dans les systèmes d'authentification et la mobilité.

Steel Belted Radius s'adresse aux entreprises comme aux fournisseurs d'accès Internet avec deux offres distinctes : SBR/enterprise et SBR/Service Provider Edition. La version Steel Belted Radius Enterprise coûte environ $3200 ce qui n'est pas négligeable.

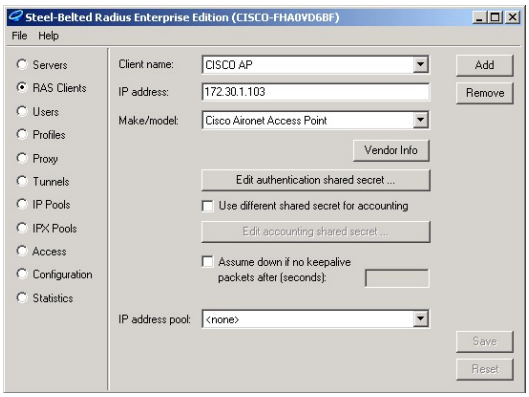


Illustration 45: interface de Steel Belted Radius

5.2.1.2 Microsoft IAS (Microsoft)

Microsoft Internet Authentication Server est une solution interessante pour les administrateurs ayant des serveurs Microsoft. Ce module est en effet inclut de manière standard à partir de Windows 2000 serveur.

Pour les versions Windows NT, il faut récupérer un pack additionnel qui contient IAS et d'autres programmes.

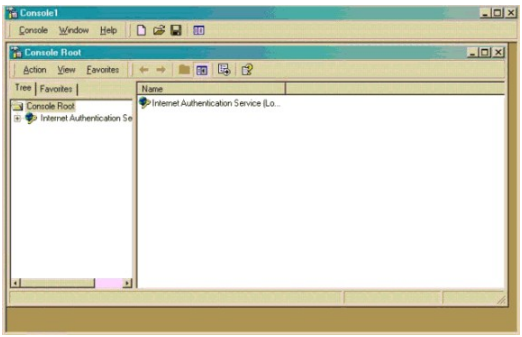


Illustration 46: Interface d'IAS de Microsoft

5.2.1.3 Radiator (OSC)

Le groupe "Open System Consultants" est une société créée en 1991 et établie à Gold Coast et Melbourne, en Australie. Ils proposent des solutions pour les fournisseurs d'accès et particulièrement le produit Radiator, développé en Perl.

Radiator supporte plus de 60 méthodes d'authentification (LDAP, PAM, iPass, bases de données, fichiers à plat, ...) et propose un fonctionnement d'échange de trames entres relais RADIUS (proxy) sécurisé : RadSec (IANA, port 2083).

Le prix de cette solution n'est pas prohibitif et est adapté aux différents besoins (tarif un serveur : 600€, pour 2 à 7 serveur : 1800€, Entreprise Pack (infini) : 5100€).

La configuration utilise des fichiers au format texte (comme dans l'exemple ci-dessous).

```
<Client www-proxy.open.com.au>
    Secret            mysecret
    Identifier        www-proxy
</Client>
# www-proxy
<Handler Client-Identifier=www-proxy>
    <AuthBy FILE>
        Filename      %D/www-proxy-users
    </AuthBy>
</Handler>
```

5.2.1.4 FreeRADIUS (Alan DEKOK)

FreeRADIUS est une application AAA libre (open-source) et gratuite. Malgré cela, ses possibilités sont très étendus et il est le seul logiciel capable de soutenir la comparaison face aux applications commerciales.

Historiquement, FreeRADIUS est basé sur les sources de Cistron RADIUS qui n'est désormais plus développé.

Des solutions gratuites, il est le plus aboutit et son évolution est régulière (XTRadius n'évolue plus depuis mars 2002 et OpenRADIUS ne permet pas l'utilisation de mécanismes EAP).

IBM a même une page dédiée à la configuration de FreeRADIUS sur son site (http://www-128.ibm.com/developerworks/library/l-radius/).

5.2.2 Déploiement dans la solution

Le choix effectué au CICG est FreeRADIUS : sa gratuité n'entraîne pas de limitations en fonction du nombre de licence. Il est fournit sous forme de paquetage sous différents Linux, il a une "mailing-list" très active et est déjà employé dans certaines universités et au CICG.

En revanche, il la documentation reste succincte et s'adresse à un public avertit. De plus, la configuration se fait par plusieurs fichiers texte, ce qui ne simplifie pas la compréhension de premier abord.

Les fonctionnalités retenues sont :

- Authentification directe dans le fichier "users" de FreeRADIUS,
- Authentification sur un serveur LDAP,
- Compatibilité avec les mécanismes EAP pour l'authentification forte,
- Utilisation d'une base MySQL pour l'archivage des authentifications,
- Possibilités de relayage de trames RADIUS,
- Utilisation des paires d'attribut-valeur à destination des équipements NAS[72].

5.2.3 Installation de base

Après avoir téléchargé l'archive du programme, l'installation commence par une phase de compilation. Si le choix du répertoire des fichiers de configuration se fait facilement, l'emplacement des fichiers utiles (exécutables, documentations, dictionnaires...) nécessite une action dans le fichier 'configure', avant la compilation.

La documentation est vraiment succinte et il n'existe qu'un livre sur RADIUS. Deux chapitres sont dédiés au fonctionnement de FreeRADIUS, toutefois, les explications restent superficielles sur les possibilités de l'application. La documentation la plus complète se trouve dans les commentaires (très nombreux) des fichiers de configurations.

Malgré tout, la lisibilité de l'ensemble reste relativement complexe et même l'abonnement à la liste des utilisateurs de FreeRADIUS ne facilite pas sa mise en oeuvre. Un seul livre parle de FreeRADIUS mais c'est notamment pour expliquer le protocole RADIUS...

L'architecture de FreeRADIUS et son synoptique ont été testés pendant plusieurs semaines :

72 NAS : Network Access Server

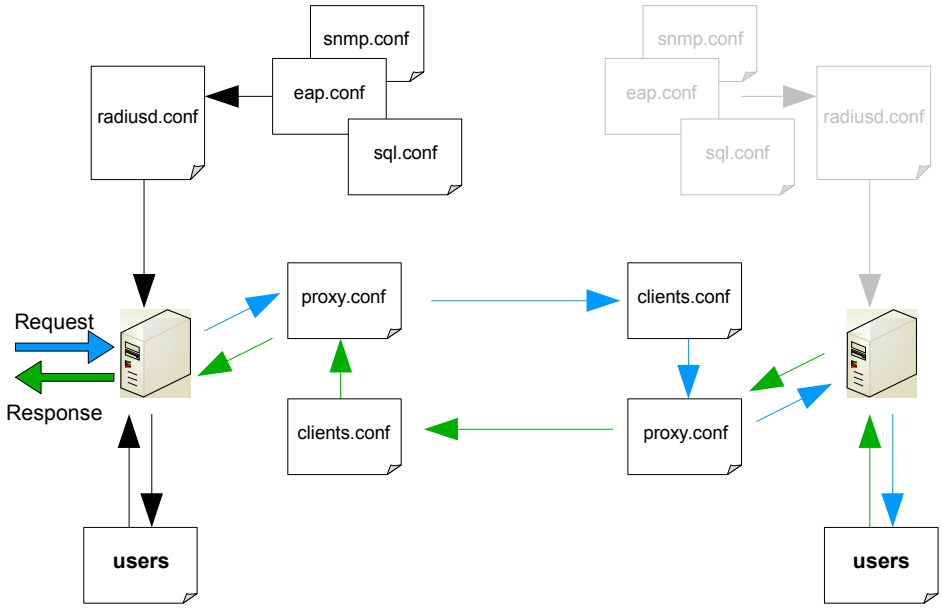


Illustration 47: synoptique de fonctionnement FreeRADIUS

L'illustration ci-dessus est le résultat des différents essais : une fois compris, la configuration de FreeRADIUS et le relayage de trames d'authentification deviennent simples !

Toutefois, l'utilisation de FreeRADIUS nous a contraint à utiliser une base de données (MySQL) et un script Perl pour pouvoir correler les utilisateurs et les adresses IP.

5.2.4 configuration EAP-TTLS

Certificats, fichier eap.conf.

Accounting

Proxyfication

Radius

5.3 Portails captifs

Les seules solutions permettant d'accéder à Internet sans installation de codes sur le poste de l'utilisateur sont les portails captifs. Ce terme est l'association du mot 'portail' (dans le sens d'ouverture vers l'extérieur) et de l'adjectif 'captif' (dont le sens correspond au contrôle de la liberté).

Les portails captifs permettent donc un accès contrôlé à Internet. Pour cela, ils utilisent généralement les applications déjà présentent sur les ordinateurs et PDA multimédia : les navigateurs. Les applications utilisant les protocoles HTTP et HTTPS sont désormais massivement présentes dans tous les systèmes d'exploitation et les serveurs HTTP et HTTPS sont faciles à mettre en oeuvre.

Le principe général est donc de bloquer l'accès vers l'Internet tant que l'utilisateur ne s'est pas authentifié par l'intermédiaire d'une page web. Une fois authentifié – et durant toute la session – le poste de l'utilisateur sera autorisé à sortir du réseau local.

5.3.1 M0n0wall et pfSense

M0n0wall[73] est un projet gratuit (mais pas open-source) basé sur un ensemble d'outils disponibles sous FreeBSD. La philosophie de ce produit est une simplicité extrême : le système démarre sur un CDRom "bootable" et enregistre sa configuration sur une disquette. Il remplace un routeur, dont les caractéristiques obligent à être authentifié pour pouvoir accéder à Internet.

L'autre outil – pfSense[74] – est une version dérivée de m0n0wall : gratuit également, il n'utilise pas les mêmes outils. La principale différence est l'utilisation de FreeBSD 4 pour m0n0wall tandis que pfSense utilise FreeBSD 5. Les fonctionnalités restent similaires...

5.3.1.1 Installation et configuration

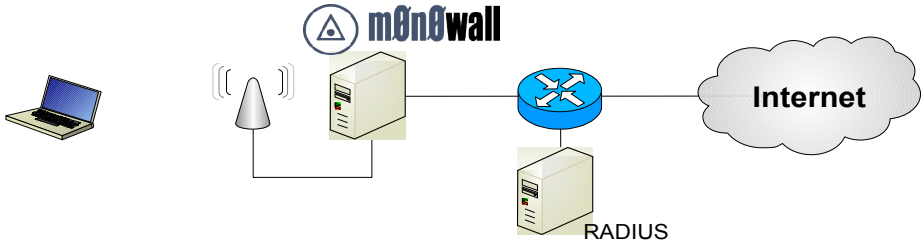


Illustration 48: architecture typique m0n0wall

L'architecture testée est simple avec deux interfaces : une interface connectée sur le point d'accès sans fil, l'autre branchée sur Internet.

Après avoir téléchargé l'image ISO de l'application depuis Internet et enregistré celle-ci sur un CD, nous utilisons une machine de test avec deux cartes réseaux. Le PC amorce le démarrage sur le CD sous FreeBSD. Toutefois, lors de la première configuration l'une des cartes n'est pas reconnue : après un deuxième démarrage avec deux cartes réseaux 3Com, plus aucun problème. La configuration sur la machine elle-même (en utilisant son écran et son clavier) se limite à la configuration des adresses IP et masques réseaux des cartes.

Ensuite, la configuration se fait à distance par l'interface web : http://m0n0wall.grenet.fr/

73 http://www.m0n0.ch/wall/
74 http://www.pfsense.com/

L'interface et claire et agréable à utiliser, les fonctionnalités sont nombreuses. De plus, m0n0wall propose également des fonctionnalités VPN (IPsec et PPTP).

5.3.1.2 Les avantages

La solution m0n0wall est intéressante et probablement une des plus sûre :

- démarrage sur un CDRom (pas de modification possible mais sauvegarde de la configuration sur disquette),
- administration par une interface web très claire,
- filtrage très précis par utilisateur,
- filtrage complet permettant l'utilisation de nombreux services ou applications (filtrage sur socket avec numéros de ports),
- authentification par session https (à partir de la version 1.2 beta 7),
- logs du firewall.

5.3.1.3 Les inconvénients

Il existe tout de même des inconvénients incontournables ne permettant pas un déploiement immédiat :

- nombreux bugs rencontrés sur les versions 1.2b7 et 1.2b8, notamment quelques plantages,
- la fermeture de session https (authentification) ne ferme pas les filtres : il y a possibilité d'usurpation d'une machine autorisée (bug),
- le filtrage est basé sur l'adresse physique (adresse MAC), ce qui ne permet pas un déploiement mutualisé,
- dans la configuration utilisée au CICG, l'accès à l'interface d'administration se fait par l'interface connectée sur le réseau privée (coté réseau sans fil).

La solution m0n0wall n'est donc pas immédiatement utilisable : outre le fait de devoir attendre une version stable, le filtrage sur une adresse physique ne permet pas de placer m0n0wall comme portail captif mutualisé au niveau des routeurs d'entrées de l'interuniversité.

5.3.2 Talweg

Talweg est un projet développé par le CRIUM (CRI de l'Université de Metz). La version testée est 0.2 ce qui témoigne de la jeunesse du produit, toutefois, ses qualités sont indéniables et sont mode de fonctionnement très sécurisé : Talweg agit comme un portail captif mais encapsule toutes les trames émises par le client dans une session SSL. Ainsi, tout le trafic est protégé.

5.3.2.1 Installation et configuration

Pour pouvoir utiliser Talweg dans un contexte mutualisé, une modification de routage est appliquée sur le(s) routeur(s) concerné(s) afin d'envoyer toutes les trames HTTP et HTTPS en provenance des réseaux sans fil, vers le portail captif (policy routing).

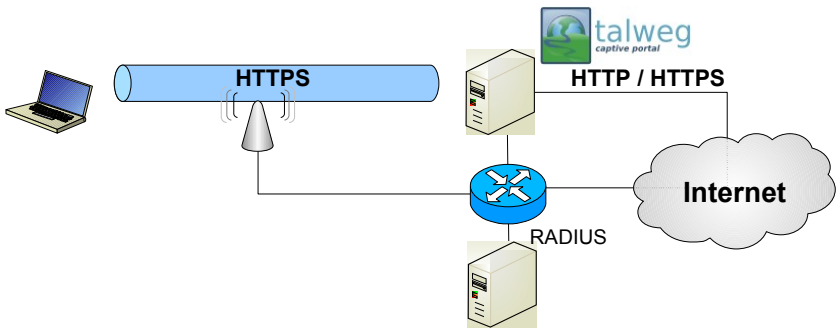


Illustration 49: architecture Talweg

Après avoir téléchargé l'application et décompressé celle-ci sur un linux, il faut éditer les fichiers avec un éditeur de texte. C'est moins convivial que m0n0wall mais le manuel en ligne est bien fait et les opérations bien décrites.

Edition du fichier /etc/modutils/aliases pour définir les cartes réseaux, puis édition du fichier /etc/network/interfaces pour créer les interfaces virtuelles :

```
#--- begin to add ---
# interface de la passerelle : router.talweg.loc
auto eth1
iface eth1 inet static
```

```
        address 10.13.0.1
        netmask 255.255.0.0
        network 10.13.0.0
        broadcast 10.13.255.255

# interface de redirection : redirect.talweg.loc
auto eth1:0
iface eth1:0 inet static
        address 10.13.0.2
        netmask 255.255.0.0
        network 10.13.0.0
        broadcast 10.13.255.255

# interface du proxy : proxy.talweg.loc
auto eth1:1
iface eth1:1 inet static
        address 10.13.0.3
        netmask 255.255.0.0
        network 10.13.0.0
        broadcast 10.13.255.255

# interface de l'authentification : auth.talweg.loc
auto eth1:2
iface eth1:2 inet static
        address 10.13.0.4
        netmask 255.255.0.0
        network 10.13.0.0
        broadcast 10.13.255.255

#interface du serveur www (https) local : www.talweg.loc
auto eth1:3
iface eth1:3 inet static
        address 10.13.0.5
        netmask 255.255.0.0
        network 10.13.0.0
        broadcast 10.13.255.255
#--- end of add ---
```

En fonctionnement, Talweg est très impressionant. En tapant n'importe quel url (ou en cliquant sur n'importe quel lien) dans un navigateur, Talweg intercepte la requête. Si l'utilisateur n'est pas encore authentifié, un formulaire s'affiche (après acceptation du certificat du serveur si ce dernier n'est pas certifié par une autorité de confiance dans la liste du navigateur) demandant un login et un mot de passe.

Ensuite, tout les liens sont automatiquement ré-écrit par Talweg.

Illustration 50: exemple de ré-écriture de liens sous Talweg

Dès la fermeture du navigateur, la session SSL est cassée, il est ainsi impossible pour une personne malveillante de récupérer la session d'un utilisateur précédemment connecté sur le poste.

5.3.2.2 Les avantages

Bien que le produit soit très récent et que le CRIUM n'ait pas beaucoup de temps pour le développer, les points suivants de Talweg nous ont séduits :

- Authentification sécurisé,
- Communication entre le serveur et le client chiffrée (tunnel SSL),

- logs très précis,
- utilisation des 'favoris' ou de liens par copier/coller possible.

5.3.2.3 Les inconvénients

En revanche, un seul point négatif restent encore à améliorer pour en faire la solution idéale :

- mauvaise compatibilité avec les active X, certains scripts et les liens relatifs.

Cela n'est pas rédibitoire mais n'est pas une solution à moyen terme en l'état. Nous avons donc pris contact avec le CRIUM pour les informer de notre constat et nous attendons une correction de leur part.

5.3.3 Squid

SQUID est un système de relayage de requêtes HTTP et HTTPS. Il est facilement mutualisable (c'est même son principal intérêt) mais n'a aucune capacité d'authentification ni de chiffrement.

Cette solution a rapidement été rejeté.

5.4 Réseaux Virtuels Privés

Les réseaux virtuels privés (RVP ou VPN en anglais) connaissent un essor important depuis l'arrivée du haut débit : toute personne

5.4.1 VPN Cisco 3030

Cette solution existe déjà sur le campus. Elle est basée sur le concentrateur VPN 3030 de Cisco.

5.4.2 VPN SSL F5 Networks

[pourquoi acheter un boitier F5 alors que ça existe déjà]

5.4.3 Solution WPA

La solution WPA s'appuie sur la solution EAP. Cette solution s'applique exclusivement sur les réseaux sans fil car elle contient à la fois une méthode d'authentification forte (EAP) et le chiffrement des données (RC4+TKIP ou AES+CCMP).

Cette solution est très robuste et simple à mettre en oeuvre. Le système d'authentification utilisant le protocole RADIUS, l'utilisation d'un serveur FreeRADIUS déjà en place ne demande qu'un minimum de modification de celui-ci.

Les points d'accès sans fil utilisés par les universités sont des CISCO AP-1100.

EAP est une norme : EAP-MD5, EAP-LEAP, EAP-PEAP, EAP-TLS, EAP-TTLS et EAP-FAST.

5.5 Gestion du projet

Le travail effectué pendant un an correspond à plusieurs sous-projets ou plusieurs étapes. Les méthodes vues lors de la formation d'ingénieur CNAM s'appliquent de manière naturelle mais n'ont pas été formalisées sous forme de document. Les différentes approches concernant le développement du projet, son organisation et les méthodes de communications employées sont donc décrites ici.

5.5.1 Développement

La plupart des projets utilisent une gestion de planning avec une représentation en diagramme de Gantt. Cette représentation très pratique permet de gérer le temps et les ressources pour accomplir un projet dans un temps défini. Toutefois, cette méthode a rapidement été abandonnée par son manque de souplesse : d'une part il n'y a qu'une seule ressource à gérer et d'autre part la création des sous-étapes n'est pas aisée.

Dans ce type de projet, une représentation par un diagramme de Gantt n'est pas approprié : il faut parfois ajouter des sous-étapes pour déterminer si une fonction doit être ajoutée. Certaines solutions sont apparues au cours du projet (validation WPA2 en juin 2004 mais premier produits permettant de l'utiliser sur le client comme le point d'accès : mai 2005 pour le patch Microsoft).

La gestion de projet par diagramme de Gantt n'a donc pas été utilisée.

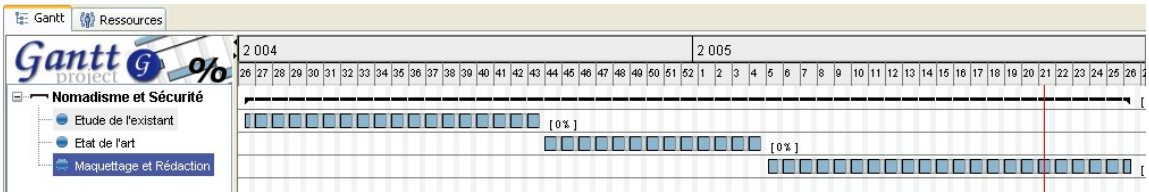


Illustration 51: Gestion de projet par diagramme de Gantt

En revanche, pour permettre la bonne réalisation du projet, il a été choisi un ensemble d'applications et de méthodes différents.

La représentation du travail effectué dans le temps est relativement simple : le rythme n'est pas linéaire et devient de plus en plus rapide, au fur et à mesure que les concepts sont intégrés. Alors qu'au début il a fallu intégrer de nombreuses notions, la fin du projet est surtout ralentit par des problèmes techniques.

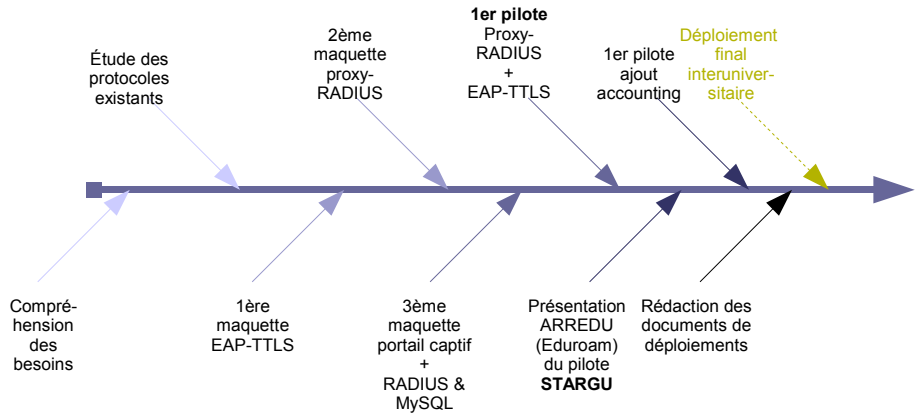


Illustration 52: Progression du travail dans le temps

Le mode de développement correspond à un ensemble de cycles itératifs :

- Plannification des fonctionnalités (thèmes à aborder, méthodes, documentation...),
- Actions menées (recherches, installation, configuration),
- Tests sur l'état du projet (différentes maquettes, validation des fonctions mises en oeuvre),
- Améliorations et ajouts (réunions, points hebdomadaires, présentation aux personnes engagées sur le projet)

Cela ressemble au cycle de la roue de Deming (Plan, Do, Check, Act) mais dont la durée est beaucoup plus courte et certains cycles dépassent la simple amélioration.

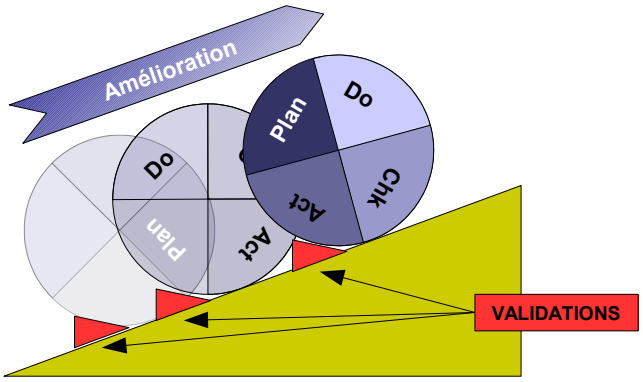


Illustration 53: Cycle de la roue de Deming

5.5.2 Organisation

La maîtrise du sujet nécessitant l'intégration de nombreuses connaissances, l'utilisation d'un outil d'organisation d'idées a permis de ne perdre aucune piste ou possibilité.

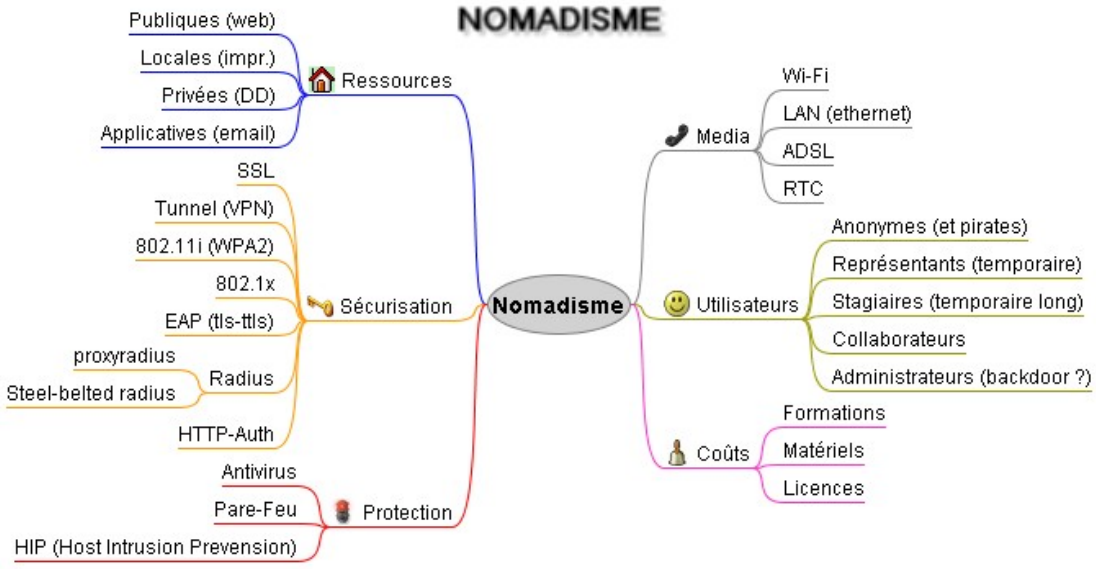


Illustration 54: Organisation d'idées...

L'utilisation de cet outil très visuel permet d'organiser et ré-organiser facilement les thèmes (branches principales) et les idées (feuilles). Le graphe ci-dessus montre la structure au début du projet : on constate que certaines notions ne sont pas encore connues correctement (mauvaise position dans l'arbre) mais que d'un seul coup d'oeil tout les thèmes sont abordés.

Il est alors simple d'ajouter, déplacer et supprimer une feuille afin de conserver une vue globale du projet.

5.5.3 Communication

Deux types de communication ont été utilisés sur le projet : une communication interne avec les personnes faisant parties du projet (mon tuteur Eric JULLIEN ainsi que Patrick PETIT) et une communication externe dans laquelle nous représentons le groupement interuniversitaire de Grenoble (au niveau des universités mais aussi national).

5.5.3.1 Communication interne

Outre les classiques réunions bi-hebdomadaires dans lesquelles sont définies les tâches accomplies et les points à aborder, un BLOG a été utilisé pour faciliter les échanges avec le responsable du projet.

Cet outil a les avantages suivants :

- Accessible en ligne à plusieurs personnes (protection par mot de passe malgré tout),
- Organisation des billets publiés par date et par thème,
- Recherche par mots-clés,
- Ajout de commentaires possibles par les lecteurs,
- Accès asynchrone aux informations (plus souple que la messagerie)

Ainsi un BLOG permet un suivi de projet de manière simple puisqu'il s'agit d'un "journal de bord" : l'état d'avancement est décrit au jour le jour et peut être suivi et commenté par les décideurs. Il peut y avoir plusieurs billets dans une même journée et la recherche par mots-clés permet de retrouver rapidement une information utile.

Le BLOG a été employé pour suivre l'évolution du projet en temps réel tout en gardant un historique des points techniques. Cet outil se révèle beaucoup plus pratique qu'un cahier car il permet de structurer l'information et s'intègre dans une politique "zéro papier".

Un exemple de présentation est fournit ci-dessous :

Illustration 55: Exemple de "weblog" employé pour le projet STAR

5.5.3.2 Communication externe

Le déploiement du projet STAR a aboutit à une communication écrite et une présentation le vendredi 1er juillet. Afin que le projet puisse prendre essor, un document écrit d'une vingtaine de pages a été rédigé pour décrire comment mettre en oeuvre l'authentification interuniversitaire : l'architecture générale, les applications utilisées, les configurations ainsi que les scripts facilitant sa mise en oeuvre ont été fournis à cette occasion.

La présentation des différentes solutions testées a été soutenue par une démonstration de toutes les solutions fonctionnelles jugées acceptables (VPN, m0n0wall, talweg, WPA et WPA2) avec notamment l'utilisation de l'authentification répartie (l'UPMF utilise également un RADIUS pour l'authentification).

Le projet du CRU appelé ARREDU a débuté en mars 2005. Correspondant au travaux effectués sur Grenoble pour le projet STAR, nous y avons pris part. Dès lors, nous avons présenté une dizaine de transparents au personnes inscrites à la première réunion (14 juin 2005).

Une autre communication importante basé sur ce travail a été acceptée pour le JRES 2005. Cette manifestation bi-annuelle *contribue au déploiement et à l'essor des nouvelles technologies pour l'information et la communication*. Notre résumé sur notre activité a été retenu, un article a été rendu (septembre 2005) et la présentation correspondante est datée du 6 décembre 2005.

5.5.4 Architecture finale déployée

Le projet a duré un an : durant cette année, de nombreuses expérimentations et quelques tâtonnements ont été nécessaires pour valider une architecture répondant aux attentes des différentes parties.

Finalement, pour les universités de Grenoble, les moyens à mettre en oeuvre ne sont pas énormes : deux vlans sont nécessaires, les serveurs d'authentification RADIUS existent déjà chez certaines, sinon un simple PC sous linux suffit. La mise à jour des points d'accès Cisco AP1100 permet l'utilisation de multiples SSID simultanément et l'utilisation du nouveau standard WPA2 (tout en conservant une compatibilité avec WPA). Les clients 802.1x sont de plus en plus nombreux (nous avons utilisé SecureW2 mais de nombreux fabricants en fournissent un avec leurs cartes). Cette solution ne bloque pas l'utilisation d'un client VPN, même si le rendement en terme de débit est un peu moins bon (chiffrement IPSec dans un tunnel RC4/TKIP ou AES/CCMP), ce qui permet à un visiteur d'accéder via sont client VPN à son intranet tout en étant authentifié sur le réseau interuniversitaire. De plus, cette solution s'intègre parfaitement dans les méthodes choisies par EduRoam et matérialisées par ARREDU.

Enfin, l'utilisation d'un portail captif mutualisé permet d'utiliser un vlan sans client particulier tout en permettant l'accès à certaines ressources sur Internet. Simple et rapide à utiliser, cette solution complète parfaitement les solutions précédentes.

Dans tout les cas, l'utilisation d'un serveur VPN reste justifié car c'est la seule solution capable de fournir un accès à l'intranet à partir de n'importe quel lieu.

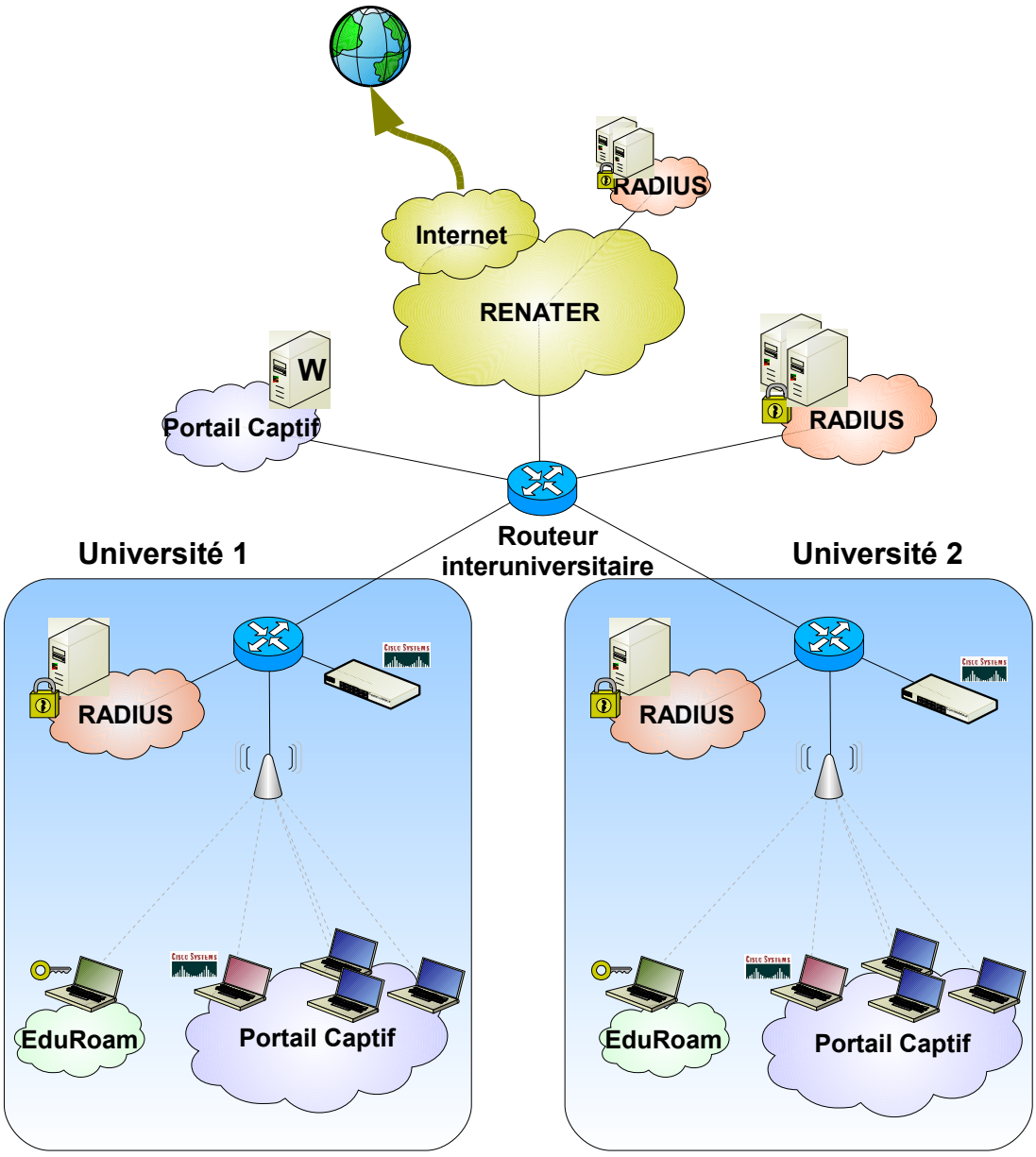


Illustration 56: Architecture finale

Cette architecture permet de garder l'existant tout en apportant la souplesse des nouvelles solutions. Pour parvenir à cette organisation, nous avons dû utiliser une approche par enrichissement afin de valider chaque nouveau point et intégrer de nouvelles notions. Plusieurs maquettes ont été employées et plusieurs configuration ont été essayées.

5.6 Perspectives et projections

Les ouvertures : Ipv6, redondance et partage de charge, Diameter, exploitation des paires attribut-valeur, snmp, VoIP, QoS

Ce projet permet désormais une ouverture plus grande et une flexibilité plus importante. L'architecture ainsi constituée reste robuste face aux attaques extérieures. Toutefois, le manque de temps et l'augmentation de connaissances soulèvent quelques questions qui restent en suspend :

- A court terme, il reste à vérifier le fonctionnement de la redondance de serveur RADIUS ainsi que la répartition de charge. FreeRADIUS permet d'utiliser ces deux fonctions mais elles n'ont pas été testées complètement. L'ajout d'une supervision SNMP est également réalisable facilement mais il reste à déterminer les indicateurs utiles.
- A moyen terme, il serait intéressant d'utiliser les paires d'attribut-valeur que peuvent transporter les serveurs RADIUS aux équipements terminaux. Une application typique est le filtrage par protocole en fonction de l'utilisateur (le filtrage par IP étant plus difficile à gérer car l'architecture ne permet pas de déterminer l'adresse IP de l'utilisateur à l'avance. Cette limitation pourrait disparaître avec l'arrivée d'IPv6). Il y a également une problématique sur l'utilisation d'un agent de salubrité qui pourrait s'insérer entre la saisie de l'utilisateur et l'envoie de l'authentification au point d'accès (et également lors des ré-associations).
- A long terme, la mise en oeuvre de la qualité de service (QoS) devrait permettre l'utilisation d'application comme la voix sur IP. D'autre part, RADIUS connaît certaines limitations de charges que son successeur – diameter – devrait faire disparaître. Toutefois, Diameter n'est pour le moment qu'un 'draft' à l'IEEE, même si un projet open-source[75] existe déjà sur Internet.

75 http://www.diameter.org/

6 CONCLUSION

L'étude s'est donc terminée par un déploiement de solutions fonctionnelles. Toutefois, cela n'est pas une réponse satisfaisante car la problématique est plutôt déplacée que résolue : en effet, l'authentification répartie met en oeuvre une politique de confiance entre établissements mais le cadre reste le réseau de la recherche et de l'éducation et notamment, les établissements ayant adhérés au projet ARREDU. Hors de ce périmètre, les autres universités ou bien les visiteurs extérieurs ne peuvent pas être authentifiés et restent des cas particuliers.

Les limites ont été repoussées, étendues au confins de l'europe mais elles sont toujours là !

6.1 Projections

Pour résoudre la problématique, il faudrait un système mondial unifié, il faudrait que chaque individu soit reconnu de manière unique, il faudrait un monde dont la science-fiction nous brosse un portrait révoltant. La coopération des différents pays au projet EduRoam est positive mais il reste à inventer une politique de fonctionnement internationale dans laquelle un nomade puisse traverser un pays virtuel, un domaine informatique sans rester bloqué aux frontières.

Malheureusement, les exemples de la vie réelle montrent que la solution idéale n'existe pas et que cette gestion reste totalement arbitraire.

Microsoft a fait figure de Big Brother avec sont système d'authentification Passport mais déjà d'autres sociétés tentent de créer un standard pour demain : Liberty Alliance, fondé par Sun, IBM, Nokia et HP entres-autres devrait être une solution d'identification alternative basée sur des standards ouverts.

Ce marché sera certainement le défi des années à venir

6.2 Conclusion personnelle

Cette année de travail fût pour moi l'occasion d'accroître mes connaissances et d'apprendre à travailler. L'évolution de mon raisonnement depuis le début de mes études au CNAM n'a cessé d'évoluer et me permet aujourd'hui d'apréhender de nouvelles tâches et de nouveaux projets

7 ANNEXES

7.1 Les groupes de travail de l'IEEE

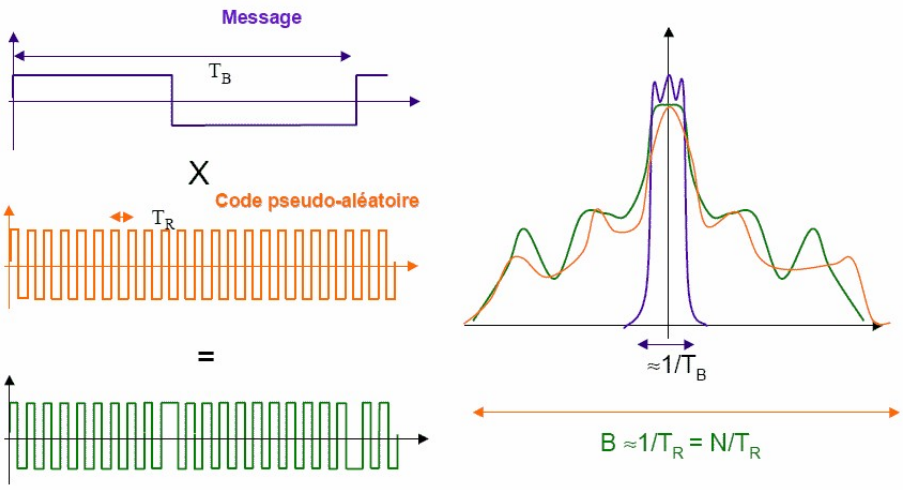
Nom groupe	*Description*
802.1	Higher Layer LAN Protocols Working Group / Link Security Executive Committee Study Group (active)
802.2	Logical Link Control Working Group (inactive)
802.3	Ethernet Working Group (active)
802.4	Token Bus Working Group (disbanded)
802.5	Token Ring Working Group (inactive)
802.6	Metropolitan Area Network Working Group (disbanded)
802.7	Broadband TAG (disbanded)
802.8	Fiber Optic TAG (disbanded)
802.9	Isochronous LAN Working Group (disbanded)
802.10	Security Working Group (disbanded)
802.11	Wireless LAN Working Group (active)
802.12	Demand Priority Working Group (inactive)
802.13	-
802.14	Cable Modem Working Group (Temporarily housed off-site) (disbanded)
802.15	Wireless Personal Area Network (WPAN) Working Group (active)
802.16	Broadband Wireless Access Working Group (active)
802.17	Resilient Packet Ring Working Group (active)
802.18	Radio Regulatory TAG (active)
802.19	Coexistence TAG (active)
802.20	Mobile Broadband Wireless Access (MBWA) Working Group (active)
802.21	Media Independent Handoff Working Group (active)
802.22	Wireless Regional Area Networks (active)

7.2 Valeurs de fréquences et puissance d'émission

Numéro de Canal	Fréquences en MHz	Intérieur	Extérieur
1 2 3 4 5 6 7 8 9	2412 2417 2422 2427 2432 2437 2442 2447 2452	100 mW	100 mW
10 11 12 13	2457 2462 2467 2472	100 mW	10 mW 100 mW*

- avec accord de la Défense ou bien départements de la Guadeloupe, Martinique, St-Pierre et Miquelon et Mayotte.

7.3 Caractéristique de la modulation DSSS



7.4 Différences et similitudes entre protocoles VPN

	PPTP	*L2F*	*L2TP/IPSec*	*IPSec transport*	*IPSec tunnel*
Le FAI doit s'impliquer dans la négociation du RPV	NON	OUI	Au choix	NON	NON
Protocole d'encapsulation	GRE	Protocoles orientés paquets (X.25, IP, ATM, Frame relay)	Protocoles orientés paquets (X.25, IP, ATM, Frame relay)	IP (ESP/AH)	IP (ESP/AH)
Peut encapsuler autre chose que de l'IP	**OUI**	**OUI**	**OUI**	NON	Standard en cours
Authentification de l'utilisateur	OUI via PPP	OUI via PPP	OUI via PPP	Standard en cours	Standard en cours
Authentification des machines	OUI en attribuant un compte utilisateur à la machine	**OUI**	**OUI**	**OUI**	**OUI**
Confidentialité (cryptage)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
Intégrité	NON	NON	**OUI**	**OUI**	**OUI**
Support du NAT-T (NAT traversal)	OUI	OUI	Standard en cours	Standard en cours	Standard en cours
Adapté pour les RPV End-2-LAN	OUI	Moyen	OUI	NON	
Adapté pour les RPV Lan-2-LAN	Moyen	OUI	OUI	NON	OUI

Tableau extrait du livre "Les VPN" [COCO03]

INDEX LEXICAL

A

AAA.....
accounting..... 4, 49
Accounting.....3, 4, 65
authentification....4, 8, 18, 22, 29, 30, 31, 42, 45, 49, 50, 51, 52, 54, 55, 56, 57, 58, 61, 62, 63, 64, 65, 67, 68, 69, 70, 74, 75, 77, 78
Authentification. 3, 4, 5, 6, 19, 45, 49, 62, 64, 69, 80
autorisation..... 4, 8, 49, 62
Autorisation.....3, 4, 45, 49
radius.....63
Radius.....5, 6, 52, 62, 63, 65
RADIUS.... 2, 5, 6, 16, 31, 52, 61, 62, 63, 64, 65, 70, 74, 75, 77, 82

E

ethernet.....27
Ethernet. 6, 24, 29, 30, 32, 40, 42, 79

N

Normalisation.....
IEEE..4, 5, 25, 28, 29, 30, 32, 39, 42, 56, 77, 79
iso..... 29
ISO.....7, 25, 26, 27, 29, 32, 66
Norme IEEE.....28, 29
Normes.....
IEEE.....25, 32
IETF..... 25
ISO.....25, 27, 29, 32
ITU..... 25, 33
Norme IEEE.....28

P

Protocoles.....
eap.....52
EAP.....52, 56
EAPOL.....30
TCP/IP..... 26, 27, 33, 56, 61
VPN.....
eap.....52, 65
EAP.... 4, 5, 6, 7, 29, 30, 31, 52, 56, 57, 58, 59, 63, 64, 65, 70

S

Sécurité.....
Protocoles.....
eap.....52
EAP..... 52, 56, 70
SSL..... 54, 70
VPN..... 54, 56, 70
Standards.....
Norme IEEE 802.1x.....29
802.11...4, 6, 7, 8, 24, 37, 39, 40, 41, 42, 44, 45, 79, 82
802.1x.....4, 6, 29, 30, 56, 61, 75

V

VPN..... 3, 5, 6, 19, 20, 21, 22, 54, 56, 61, 67, 70, 74, 75, 80, 82
IPsec.....67
IPSec..... 4, 6, 19, 54, 56, 75, 80
L2TP..... 80
PPTP..... 4, 56, 67, 80
ssl..... 54
SSL.....4, 5, 53, 54, 68, 69, 70

W

WPA..5, 70, 71, 74, 75, 79, 82

BIBLIOGRAPHIE

Cryptologie et sécurité sur PC - cryptographie, stéganographie, espionnage, règles de sécurités.

[LIBL04] **Eric Tschiembler (coord.)** Livre blanc - La mobilité en entreprise (2004) EBG ISBN :

[FERO04] **Frédéric ROMBAULT** Hot spots Wi-Wi : usages - moyens - Stratégies (livre blanc) (07/11/2003) EBG ISBN :

[GERO04] **Aurélien GERON** Wi-Fi déploiement et sécurité (le WPA et la norme 802.11i) (2004) DUNOD ISBN : 2 10 048433 8

[ANDI99] Programmable Digital QPSK/16-QAM modulator AD9853 (01/1999) Analog Devices ISBN : -

[MAPU04] **Males, Pujeolle** Pratique Wi-Fi (2004) Eyrolles ISBN :

[PUJO05] **Guy Pujolle** Les Réseaux (2005) Eyrolles ISBN : 2 212114370

J. Antonio García-Macías, Franck Rousseau, Gilles Berger-Sabbatel,Leyla Toumi, Andrzej Duda Quality of Service and Mobility for the Wireless Internet [2001]

Performance Analysis of Finite Load Sources in802.11b Multirate Environments Performance Analysis of Finite Load Sources in802.11b Multirate Environments [juillet 2003]

Frédéric Bayart La sécurité des cartes bancaires

[HASS02] **Jonathan HASSELL** RADIUS (Octobre 2002) O'REILLY ISBN : 0-596-00322-6

Florence NAMBOT Principes fondamentaux de la PKI [06/2004]

[COCO03] **R. & E. CORVOLAN et Y. Le CORVIC** Les VPN (2003) DUNOD ISBN : 2 10 006632 3