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 15 décembre 2005

JURY

Présidente : Mme Véronique Donzeau-Gouge

Membres : M. Eric Gressier
M. Jean-Pierre Giraudin
M. André Plisson
M. Andrzej Duda
M. Eric Jullien

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 15 décembre 2005

Stage réalisé au sein du Département Réseau de la
Direction des Systèmes d'Information de Grenoble Université
sous la responsabilité de
Mr JULLIEN Eric, responsable adjoint du Département Réseau.

Mes remerciements :

Durant ce stage, j'ai pu évoluer dans un environnement très instructif et dont le cadre ouvert m'a permis d'obtenir tous les renseignements et toute l'aide dont j'avais besoin. Cette année de travail au sein du CICG restera une expérience très bénéfique pour moi.

Je tiens à remercier particulièrement :

- Le CNAM qui facilite l'acquisition de compétences et permet à de nombreuses personnes engagées en entreprise de poursuivre leurs études.
- Christian LENNE qui m'a accueilli dans son département et auquel je suis reconnaissant d'un sujet passionnant au sein du CICG.
- Éric JULLIEN, qui s'est beaucoup investi dans son rôle de tuteur, et dont les suggestions, les conseils et le positivisme m'ont beaucoup aidé.
- 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, Philippe BEUTIN et David RIDEAU).
- Les membres du jury qui consacrent une grande partie de leur temps aux auditeurs du CNAM, notamment pour les épreuves de mémoire et de probatoire.
- Ma femme Béatrice pour m'avoir motivé à continuer mon cursus ingénieur puis à m'avoir encouragé dans les moments difficiles ainsi que mes fils qui m'ont permis de relativiser les problèmes : je leur dédie ce mémoire.
- Les différentes communautés "Wi-Fi Grenoble", "Wi-Fi CRU", "ARREDU", "FreeRADIUS" et en particulier Rok PAPEZ du réseau slovène ARNES pour son aide précieuse dans le projet de connexion au réseau EDURoam.
- Les développeurs "Open Office" pour les différentes aides et améliorations d'applications sur la version beta (dont certaines corrections ont été spécialement intégrées dans la roadmap 2.0 pour moi !).

TABLE DES MATIÈRES

1 INTRODUCTION....1

2 NOTIONS FONDAMENTALES....3
2.1 Définitions....3
2.1.1 Définitions liées au nomadisme....3
2.1.1.1 Nomadisme....4
2.1.1.2 Itinérance (roaming)....4
2.1.1.3 Mobilité....4
2.1.1.4 Handover....4
2.1.1.5 ASFI....4
2.1.1.6 Wi-Fi....5
2.1.2 Définitions liées à la sécurité....5
2.1.2.1 Sécurité....5
2.1.2.2 Identification....5
2.1.2.3 Authentification (authentication)....5
2.1.2.4 Autorisation....6
2.1.2.5 Accounting....6
2.1.2.6 Cryptologie....6
2.2 Constats sur le nomadisme informatique....7
2.2.1 Statistiques et évolutions....7
2.2.2 Récapitulatif....9
2.3 Répercussions sur la sécurité....10
2.3.1 Attaques des réseaux classiques....11
2.3.1.1 Attaques externes....11
2.3.1.2 Attaques par ingénierie sociale....11
2.3.1.3 Attaques par infection....12
2.3.2 Attaques des réseaux sans fil....12
2.3.2.1 War-driving....12
2.3.2.2 War-chalking....13
2.3.2.3 Brouillage....13
2.3.2.4 Arp-poisoning....13
2.4 Conclusion....13

3 CAHIER DES CHARGES....15
3.1 Définition de l'environnement....15
3.1.1 Rôles du CICG....15
3.1.2 Département réseau....16
3.1.3 Présentations des réseaux déployés....17
3.1.3.1 Réseau TIGRE....17
3.1.3.2 Réseau AMPLIVIA....18
3.1.3.3 Réseau RENATER....18
3.1.3.4 Réseau GEANT....19
3.1.3.5 Réseaux relationnels....20
3.1.3.5.a TERENA....20
3.1.3.5.b EDUROAM....20
3.2 Analyses et classifications....21
3.2.1 Classification des utilisateurs....21
3.2.2 Classification des équipements....22
3.2.3 Classification des accès géographiques....23
3.2.4 Conclusion des analyses....24
3.3 Description de l'architecture d'origine....24
3.3.1 Architecture VPN interuniversitaire....24

3.3.2 Fonctionnement de l'architecture....25
3.4 Spécifications des besoins....26
3.4.1 Description des contraintes....27
3.4.1.1 Contraintes techniques....27
3.4.1.1.a Contraintes de la solution VPN....27
3.4.1.1.b Contraintes de l'architecture réseau....27
3.4.1.2 Contraintes législatives....28
3.4.1.3 Contraintes collectives....28
3.4.2 Description des besoins....29
3.4.2.1 Utilisation "simplifiée"....30
3.4.2.2 Utilisation "étendue"....30
3.4.2.3 Salubrité des postes....30
3.4.2.4 Résumé des besoins....31

4 NORMES ET INFORMATIONS....33
4.1 Nomadisme et mobilité....33
4.1.1 Modèles de réseaux....33
4.1.2 Normes communes....35
4.1.2.1 Norme IEEE 802.1q....35
4.1.2.2 Norme IEEE 802.1x....36
4.1.3 Normes réseaux filaires....38
4.1.3.1 Réseaux point-à-point et multipoint....38
4.1.3.2 Ethernet....39
4.1.3.3 Accès via réseau téléphonique....40
4.1.3.3.a RTC....40
4.1.3.3.b DSL....40
4.1.4 Normes réseaux sans fil....41
4.1.4.1 Modulations et codages....41
4.1.4.1.a Modulation d'amplitude (Amplitude Modulation)....42
4.1.4.1.b Modulation de fréquence (Frequency Modulation)....42
4.1.4.1.c Modulation de phase (Phase Modulation)....42
4.1.4.1.d Modulations et symboles....43
4.1.4.2 Distances et interférences....43
4.1.4.2.a Distances....44
4.1.4.2.b Interférences....44
4.1.4.3 Etalement de spectre....45
4.1.4.3.a FHSS....45
4.1.4.3.b DSSS....45
4.1.4.4 Réseaux sans fil 802.11....46
4.1.4.4.a Généralités sur le standard 802.11....47
4.1.4.4.b Spécifications du standard 802.11....47
4.1.4.4.c Fonctionnement du standard 802.11....49
4.2 Sécurité....52
4.2.1 Chiffrement....53
4.2.1.1 Algorithmes à chiffrement symétrique....53
4.2.1.1.a RC4....53
4.2.1.1.b DES....53
4.2.1.1.c AES-Rijndael....54
4.2.1.2 Algorithmes à chiffrement asymétrique....54
4.2.1.3 Fonctions de hachage et de signature....55
4.2.1.3.a Fonction de hachage....55
4.2.1.3.b Fonction de signature électronique....56
4.2.2 Authentification, Autorisation et accounting....56
4.2.2.1 Différentes méthodes d'authentification....56
4.2.2.1.a Mot de passe....57
4.2.2.1.b One Time Password....57
4.2.2.1.c Biométrie....57

4.2.2.1.d Carte à puce....57
4.2.2.1.e Single Sign On....58
4.2.2.2 Autorisation et traces (AAA)....58
4.2.2.2.a Architecture AAA....58
4.2.2.2.b Gestion de droits et journalisation....59
4.2.2.2.c RADIUS....59
4.2.2.3 Structure d'autorité de certification....60
4.2.3 Tunnels et Réseaux Virtuels Privés....62
4.2.3.1 SSL, TLS et SSH (Secure SHell)....62
4.2.3.1.a SSL/TLS....62
4.2.3.1.b SSH....62
4.2.3.2 IPSec (Internet Protocol Secure)....63
4.2.3.2.a AH (Authentication Header)....64
4.2.3.2.b ESP (Encapsulating Security Paiload)....64
4.2.3.2.c Fonctionnement d'IPSec....64
4.2.3.3 PPTP (Point to Point Tunneling Protocol)....65
4.2.3.4 EAP....65
4.2.3.4.a EAP-TLS....67
4.2.3.4.b EAP-TTLS et EAP-PEAP....68

5 SOLUTIONS ET DÉPLOIEMENT....71
5.1 Les éléments de réponse....71
5.1.1 Solution "simplifiée" sans configuration cliente....71
5.1.2 Solution "étendue" avec installation d'un logiciel tiers....71
5.1.3 Elément commun aux deux solutions....72
5.2 Services d'authentification....72
5.2.1 Evaluation de solutions....72
5.2.1.1 Steel Belted Radius (Funk Software Inc.)....72
5.2.1.2 Microsoft IAS (Microsoft)....73
5.2.1.3 Radiator (OSC)....73
5.2.1.4 FreeRADIUS (Alan DEKOK)....74
5.2.1.5 Résumé des solutions évaluées....74
5.2.2 Choix de la solution....74
5.2.3 Installation et configuration d'un serveur FreeRADIUS....75
5.2.3.1 Installation de base....75
5.2.3.1.a Utilisation de SSH....75
5.2.3.1.b Installation de FreeRADIUS....76
5.2.3.2 Configuration de base....76
5.2.3.3 Configuration avancée....77
5.3 Portails captifs....79
5.3.1 Squid et fonction de routage politique....79
5.3.1.1.a SQUID....80
5.3.1.1.b Routage politique....80
5.3.1.2 Avantages....80
5.3.1.3 Inconvénients....80
5.3.1.4 Conclusion sur SQUID et sur le routage politique....80
5.3.2 M0n0wall et pfSense....81
5.3.2.1 Installation et configuration....81
5.3.2.2 Avantages....82
5.3.2.3 Inconvénients....83
5.3.2.4 Conclusion sur m0n0wall....83
5.3.3 Talweg....83
5.3.3.1 Installation et configuration....84
5.3.3.2 Avantages....85
5.3.3.3 Inconvénients....85
5.3.3.4 Conclusion sur Talweg....85
5.3.4 Conclusion....85

5.4 Réseaux Virtuels Privés....86
5.4.1 VPN + Portail SSL F5 Networks....87
5.4.1.1 Installation et configuration....87
5.4.1.2 Avantages....88
5.4.1.3 Inconvénients....88
5.4.1.4 Conclusion sur un VPN F5 Networks....89
5.4.2 VPN + Portail Cisco 3030....89
5.4.2.1 Avantages....90
5.4.2.2 Inconvénients....90
5.4.2.3 Conclusion sur un VPN Cisco 3030....90
5.4.3 Solution WPA....90
5.4.3.1 Partie client (supplicant)....91
5.4.3.2 Partie point d'accès (authenticator)....92
5.4.3.3 Partie serveur....93
5.4.3.4 Avantages....95
5.4.3.5 Inconvénients....95
5.4.3.6 Résumé et conclusion sur WPA....96
5.4.4 Architecture finale déployée....96
5.4.4.1 Capacités de l'architecture....96
5.4.4.2 Intégration des différentes solutions....97
5.5 Salubrité de poste....99
5.5.1 Objectifs....99
5.5.2 Moyens....99
5.5.3 Problèmes rencontrés....100
5.6 Gestion du projet....100
5.6.1 Déroulement du projet....100
5.6.2 Organisation des idées....101
5.6.3 Communication....102
5.6.3.1 Communication interne....102
5.6.3.2 Communication externe....103

6 CONCLUSION ET PERSPECTIVES....105
6.1 Pérennité de la solution VPN....105
6.2 Validité des solutions déployées....105
6.3 Perspectives émergeantes....105
6.3.1 Perspectives sur l'authentification....105
6.3.2 Perspectives sur la protection....106
6.3.3 Perspectives sur les autorisations....106
6.4 Projections....107

7 ANNEXES....109
7.1 Les standards PKCS....109
7.2 Les groupes de travail de l'IEEE....110
7.3 Valeurs de fréquences et puissance d'émission....110
7.4 Principe de l'étalement de spectre....111
7.5 Différences et similitudes entre protocoles VPN....111
7.6 Script d'accounting....112
7.7 Extraits de la notice de configuration du réseau STAR....117

8 ACRONYMES....119

9 INDEX LEXICAL....121

10 BIBLIOGRAPHIE....123

INDEX DES ILLUSTRATIONS

Illustration 1: Répartition des fonctions mobiles en entreprise....7
Illustration 2: Équipement des personnes mobiles en entreprise (2004)....8
Illustration 3: Principaux freins au développement des réseaux mobiles....8
Illustration 4: Nombre de "hotspots" déployés....9
Illustration 5: Symboles utilisés dans le war-chalking....13
Illustration 6: Organigramme du CICG....16
Illustration 7: Logo du CICG et nouveau logo DSIGU....16
Illustration 8: Dorsale haut débit Metronet....17
Illustration 9: Schéma logique du réseau TIGRE....18
Illustration 10: Le réseau Renater....19
Illustration 11: Étendue du réseau relationnel EDURoam (27 juillet 2005)....21
Illustration 12: Architecture Wi-Fi et VPN de Grenoble Universités....25
Illustration 13: Les tunnels interuniversitaires....26
Illustration 14: Statistiques virales du 1er semestre 2005....31
Illustration 15: Les couches OSI et TCP/IP....34
Illustration 16: Fonctionnement des réseaux locaux virtuels....35
Illustration 17: Insertion champs VLAN dans une trame Ethernet....36
Illustration 18: Fonctionnement du protocole 802.1x....37
Illustration 19: Le standard 802.1x et ses protocoles....37
Illustration 20: Trame 802.1x....37
Illustration 21: Les couches EAP....38
Illustration 22: Les topologies filaires....39
Illustration 23: Mécanisme CSMA/CD....40
Illustration 24: Spectre de fréquences et longueurs d'ondes....41
Illustration 25: Les différentes modulations....42
Illustration 26: Extrait d'un datasheet d'un composant électronique....43
Illustration 27: Débits en fonction de la distance en 802.11....44
Illustration 28: Les différentes perturbations des ondes....45
Illustration 29: Étalement de spectre....45
Illustration 30: Les différentes familles de réseaux sans fil....46
Illustration 31: Logo Wi-Fi, BlueTooth et Wi-Max....46
Illustration 32: Chevauchement des fréquences en 802.11b/g....48
Illustration 33: Exemple de répartition de canaux....49
Illustration 34: Les couches du standard 802.11....49
Illustration 35: Les différents modes de connexion 802.11....50
Illustration 36: Protection de communication entre les points d'accès....50
Illustration 37: Problème de détection de collision en 802.11....51
Illustration 38: Fonctionnement de CSMA/CA....51
Illustration 39: Fonctionnement d'un algorithme de chiffrement symétrique....53
Illustration 40: Fonctionnement d'un algorithme de chiffrement asymétrique....55
Illustration 41: Fonctionnement d'un mécanisme de hachage....55
Illustration 42: Les deux modèles d'architecture AAA....58
Illustration 43: Symbole cadenas pour le protocole HTTPS (navigateur IE 6)....60
Illustration 44: Structure typique d'une IGC (cf. www.securiteinfo.com)....61
Illustration 45: Redirection de ports avec SSH....63
Illustration 46: Les modes transport et tunnel d'IPSec....63
Illustration 47: Structure de l'en-tête AH....64
Illustration 48: Structure de l'en-tête ESP....64
Illustration 49: VPN PPTP....65
Illustration 50: VPN IPsec....65
Illustration 51: Format de trame EAP....65

Illustration 52: Authentification EAP-TLS..... 67
Illustration 53: Authentification EAP-TTLS..... 68
Illustration 54: Interface de Steel Belted Radius..... 73
Illustration 55: Interface d'IAS de Microsoft..... 73
Illustration 56: PuTTY, interface de configuration/connexion..... 76
Illustration 57: Synoptique de fonctionnement FreeRADIUS..... 77
Illustration 58: Logo du projet STAR..... 78
Illustration 59: Extrait d'une présentation du système STAR..... 79
Illustration 60: Fonctionnement du routage politique (policy routing)..... 80
Illustration 61: Architecture typique m0n0wall..... 81
Illustration 62: M0n0wall, panneau de configuration..... 82
Illustration 63: Architecture Talweg..... 83
Illustration 64: Exemple de ré-écriture de liens sous Talweg..... 84
Illustration 65: VPN IPSec et VPN SSL..... 86
Illustration 66: Firepass, interface de configuration..... 87
Illustration 67: Portail utilisateur sur Firepass 1000..... 88
Illustration 68: Cisco VPN 3030, interface de configuration..... 89
Illustration 69: Première maquette : tests EAP-TTLS..... 91
Illustration 70: SecureW2, interface de configuration..... 91
Illustration 71: SecureW2, interface de connexion..... 91
Illustration 72: Configuration des éléments de la chaîne EAP-TTLS..... 92
Illustration 73: Cisco AP-1100, interface web de configuration..... 93
Illustration 74: Principe de fonctionnement du script Perl..... 94
Illustration 75: Résultats visibles dans la table 'ACCOUNTING'..... 95
Illustration 76: Architecture STAR interuniversitaire finale..... 98
Illustration 77: Progression du travail dans le temps..... 100
Illustration 78: Gestion de projet par diagramme de Gantt..... 101
Illustration 79: Cycle de la roue de Deming..... 101
Illustration 80: Organisation d'idées... le projet au début de l'étude..... 102
Illustration 81: Exemple de "weblog" employé pour le projet STAR..... 104
Illustration 82: Principe de l'étalement de spectre..... 113

INDEX DES TABLES

Tableau 1: Lieux et mobilité..... 9
Tableau 2: Localisation et usage des services..... 23
Tableau 3: Profils type de l'ensemble des utilisateurs..... 24
Tableau 4: Table des fonctionnalités par besoins..... 32
Tableau 5: Le modèle ISO..... 34
Tableau 6: Echelle de qualité de signal..... 44
Tableau 7: Les amendements du standard 802.11..... 47
Tableau 8: Les principales différences de transmission 802.11..... 48
Tableau 9: Débits constatés avec deux stations 802.11b (source IMAG-LSR)..... 52
Tableau 10: Points forts des différents algorithmes utilisés avec EAP..... 66
Tableau 11: Tableau résumant les différentes solutions évaluées..... 74
Tableau 12: Tableau comparatif des solutions portails captifs..... 85
Tableau 13: Tableau récapitulatif de l'architecture mixte..... 97
Tableau 14: Les standards PKCS..... 111
Tableau 15: Les groupes de travail de l'IEEE 802..... 112
Tableau 16: Fréquences et puissances d'émission 802.11..... 112
Tableau 17: Les différents protocoles VPN (niveau 2 et 3)..... 113

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'a pas été facile de déterminer si c'est la technique qui a fait progresser les méthodes de travail, l'inverse ou les deux à la fois. 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 19 000 tubes représentent l'ère préhistorique de cette planète virtuelle 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 où les contrats d'embauche précisent que le lieu de travail est une région voire même un pays, la technologie devient un moyen de garder un lien, une attache avec ses proches : train à grande vitesse, téléphone mobile, courrier électronique, vidéo-conférence...

Cette technologie nous rend aussi esclave du temps et du travail : envoi de rapports depuis la maison, saisie de commandes et consultation des stocks en temps réel pour garantir un délai aux clients, supervision permanente de structures (astreintes)... telles sont les contre-parties que la technologie mobile apporte à l'Homme itinérant.

Désormais dans l'ère des services, l'Homme sédentaire de l'ère industrielle – devenu une sorte de "cro-magnon" – a fait place à un homo-sapiens capable de se déplacer, de voyager, de parcourir des distances importantes tout en restant en liaison permanente avec son entourage.

Dans ce cadre, ce mémoire a pour objectif de mieux comprendre ce qu'est le nomadisme en informatique et de trouver des solutions aux problèmes de sécurité que l'itinérance implique dans un contexte interuniversitaire.

Pour cela, la première partie s'attache à décrire les notions essentielles à la compréhension de cette évolution, le vocabulaire employé et ses répercussions.

La seconde partie définit le cadre de travail et les spécifications propres aux universités de Grenoble.

Ensuite, nous présentons les normes techniques existantes sur lesquelles s'appuient les communications mobiles et les sécurités associées.

Enfin la recherche et la mise en œuvre des solutions testées dans le cadre du CICG sont détaillées. Le déploiement de l'architecture finalement adoptée au sein du réseau interuniversitaire est décrite et justifiée.

1 ENIAC : Electronic Numerical Integrator and Computer, premier ordinateur au monde fonctionnant à lampes et conçu en 1946, il pèse 30 tonnes pour une surface occupée de 72m².

2 NOTIONS FONDAMENTALES

L'informatique est passée d'un modèle centralisé (entre 1950 et 1975) à un modèle réparti (à partir de 1974 avec l'arrivée d'Apple). C'est toutefois un nouveau modèle qui existe aujourd'hui avec la mobilité.

En effet, si les téléphones cellulaires ont ouvert la voie avec la transmission de paroles, c'est la transmission des données et des services associés qui développe la mobilité informatique :

- géolocalisations et téléguidages en temps réel,
- réservations d'hôtels ou de transports "en ligne"[2],
- transactions boursières à toute heure et en tout lieu,
- météorologie, ventes en ligne, gestion de stocks en direct,
- travaux collaboratifs, ENT[3], calendriers partagés...

Les déplacements représentent un temps considérable souvent perdu sur de longs trajets (avion, bateau, train) et les réunions ne permettent pas toujours le partage immédiat d'informations.

Rendre les équipements informatiques capables de fonctionner lors de déplacements comme s'ils étaient reliés en permanence au réseau de l'entreprise est un défi technique dont l'aboutissement se traduit par un gain de performance.

La technologie est heureusement là pour répondre à ce défi : toutefois, l'évolution rapide des besoins et la résolution des problèmes de manière ponctuelle conduisent les fabricants à créer de nouveaux concepts et de nouveaux termes. Parfois il s'agit simplement de la déviation d'un terme connu, d'autres fois c'est l'utilisation de termes anglais.

Ce chapitre a pour objectif de clarifier le domaine du nomadisme et de la sécurité afin que les lecteurs aient la même vision quelques soient leurs domaines de travail (télécommunications ou réseaux par exemple). Après la description de plusieurs termes utiles, nous verrons qui sont les utilisateurs nomades et nous proposons un classement basé sur les usages des outils nomades et finalement mettons en exergue quels sont les blocages à l'expansion du nomadisme informatique.

2.1 Définitions

En informatique, les termes sont souvent utilisés par abus de langage. De nombreux articles emploient des mots dont la signification n'est pas exacte voire complètement fausse. Généralement, les abréviations les plus connues sont anglaises mais certains documents utilisent l'abréviation française ce qui peut porter à confusion : un RVP signifie un "point de rendez-vous" chez les anglo-saxons mais un "réseau privé virtuel" en France. De plus, les interprétations des termes ne sont parfois pas identiques. Cette section a pour objet de définir les termes et abréviations employés dans ce mémoire et détailler les abus de langage qui sont parfois utilisés.

2.1.1 Définitions liées au nomadisme

Cette section couvre les termes utilisés dans ce rapport avec les définitions originales et celles redéfinies par les utilisateurs, concernant les technologies sans fil.

2 Lorsqu'on est connecté à un réseau.
3 ENT : Environnement Numérique de Travail.

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*". Il est vrai que la population active est souvent amenée dans le cadre du travail à se déplacer pour toutes sortes de motifs qui seront énumérés plus loin.

Dans ce rapport, le terme nomadisme définit le mode de vie des personnes qui lors de leurs déplacements, doivent impérativement se connecter à un réseau informatique. Il englobe les notions d'itinérance et de mobilité.

2.1.1.2 Itinérance (roaming)

Traduction du mot anglais "roaming", le terme "itinérance" n'existe pas dans les dictionnaires français 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*".

Toutefois, dans sa partie télécommunication, le grand dictionnaire terminologique de l'Office Québécois de la langue française[4] définit l'itinérance comme 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.*".

Par conséquent, l'itinérance est employée 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

Si en téléphonie, le terme itinérance est plus facilement utilisé, en informatique et réseau c'est le terme mobilité qui est le plus fréquemment employé. On rencontre ce terme en entreprise dans l'expression "mobilité géographique", qui traduit la capacité de changer de lieu de travail tout en restant dans la même société.

Dans ce mémoire "mobilité" est utilisé comme étant *la capacité d'un équipement de changer de réseau dans l'espace, dans le temps ou les deux en même temps*. Cela signifie qu'un système dispose d'une autonomie complète lui permettant de choisir et de se connecter sur un réseau puis de pouvoir atteindre des services utiles à l'utilisateur.

2.1.1.4 Handover

Ce terme anglais se traduit par "relais" ou "cession" en français. C'est le mécanisme permettant à un équipement de choisir son point de rattachement dans un même réseau pour effectuer ses communications, en fonction de paramètres tels que la qualité de réception. Cette fonction est capitale dans les réseaux sans fil.

2.1.1.5 ASFI

Pour endiguer la pénétration des termes anglo-saxons, l'Académie française a créé l'acronyme ASFI[5] qui signifie "Accès Sans Fil à Internet". Il est donc utile de rappeler que la mise en œuvre d'un équipement compatible Wi-Fi pour accéder à Internet n'est pas un accès Wi-Fi mais un ASFI : cet acronyme remplace également le terme anglais "hotspot".

4 http://www.granddictionnaire.com/
5 ASFI : Accès Sans Fil à Internet.

2.1.1.6 Wi-Fi[6]

Cet acronyme anglais est la contraction de "Wireless Fidelity", un clin d'œil aux équipements musicaux qualifiés de haute fidélité, en anglais Hi-Fi (High Fidelity).

Les abus de langage de la presse parlent souvent des "connexions Wi-Fi", des "équipements Wi-Fi" ou "équipements à la norme Wi-Fi" alors que Wi-Fi désigne la compatibilité des-dits équipements de différentes marques à quelques standards de la famille 802.11 : c'est une certification commerciale.

2.1.2 Définitions liées à la sécurité

Les définitions concernant la sécurité des systèmes informatiques constituent cette section : les enjeux de cette sécurité sont très importants et il n'est pas surprenant de trouver du vocabulaire généralement cantoné aux séries policières.

2.1.2.1 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 de tous les organismes communicant par réseaux. Désormais une fonction dédiée à la sécurité des systèmes d'information existe : ASSI[7] ou RSSI[8].

2.1.2.2 Identification

L'identité est un ensemble d'éléments qui permettent de reconnaître un individu (ex: Jean Dupont), une entité ou bien une marque. Toutefois, une identité peut être copiée et les contre-façons existent.

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

2.1.2.3 Authentification (authentication)

Pour s'assurer qu'un identifiant soit bien présenté par l'identité (l'utilisateur) qu'il représente, il faut authentifier ce dernier.

L'authentification est le procédé permettant à un individu ou une entité de prouver son identité : la photo sur 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.

6 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 à un programme de certification s'appuyant sur les spécifications du groupe 802.11.
7 ASSI : Agent de Sécurité des Systèmes d'Information.
8 RSSI : Responsable Sécurité des Systèmes d'Information.

2.1.2.4 Autorisation

Pour utiliser les ressources d'un environnement sécurisé, il est nécessaire d'avoir une ou plusieurs autorisations. 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 se connecter. De plus, les accès aux ressources impliquent des droits attribués de manière individuelle d'une part, et par l'appartenance à des groupes, d'autre part.

2.1.2.5 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 et l'entreprise étant responsables des fautes commises à partir de leur réseau, il leur est nécessaire de pouvoir déterminer avec précision qui l'utilise et à quel moment.

2.1.2.6 Cryptologie

La cryptologie est la science des écritures secrètes et des messages chiffrés. Elle comprend la cryptographie et la cryptanalyse. 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*"[9].

Cette science emploie un vocabulaire souvent mal utilisé et dont les anglicismes sont venus remplacer les termes français. La liste ci-dessous redonne la définition exacte de ces mots et entre parenthèses, leur équivalent anglais [WEB001].

- Cryptographie (cryptography) : du grec *kruptos*, caché, et *graphein*, écrire. Science du chiffrement.
- Cryptanalyse (Cryptanalysis) : Art de déchiffrer les messages codés (sans obtenir par voie officielle les mécanismes ou les codes utilisés).
- 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) : message codé résultant du chiffrement.
- Texte en clair (Plaintext) : message original.
- Challenge (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 limitée est un challenge.

9 Article 28 de la loi 90-1170 du 29 décembre 1990 modifiée

2.2 Constats sur le nomadisme informatique

Le vocabulaire étant acquis, nous allons présenter le concept de nomadisme informatique et les problèmes qu'il pose. Dans la théorie, le nomadisme informatique consiste simplement à supprimer les contraintes géographiques d'accès aux réseaux. Dans les faits, il faut des investissements conséquents et une modification profonde des méthodes de travail des entreprises et organismes publics pour obtenir des résultats intéressants. Nous allons donc nous attarder sur les statistiques existantes pour comprendre pour qui et pourquoi la mobilité se développe et quels sont ses freins.

2.2.1 Statistiques et évolutions

La mobilité touche de plus en plus de personnes en entreprise. Les populations 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*) [LIBL04] :

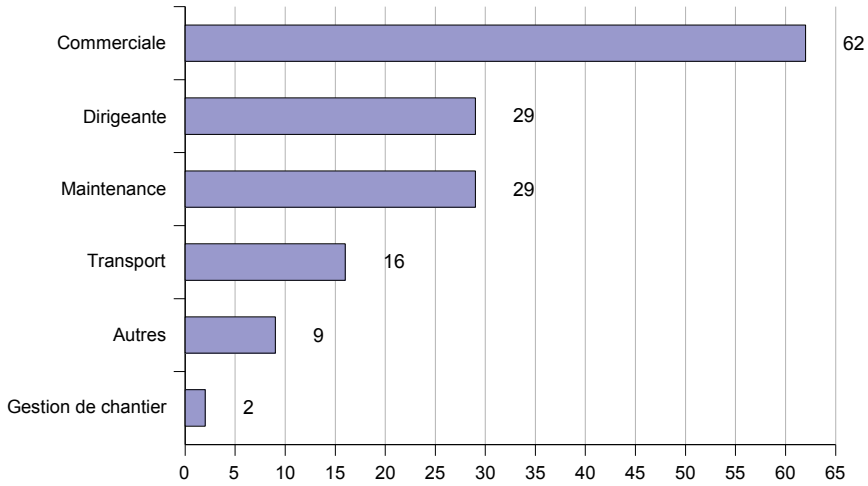


Illustration 1: Répartition des fonctions mobiles en entreprise

Cette évolution est liée à l'accroissement de productivité des individus ce qui entraîne de nouvelles demandes. Ces demandes 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... il est intéressant de constater que la notion de mobilité est plutôt associée aux téléphones mobiles, comme le montre le tableau suivant.

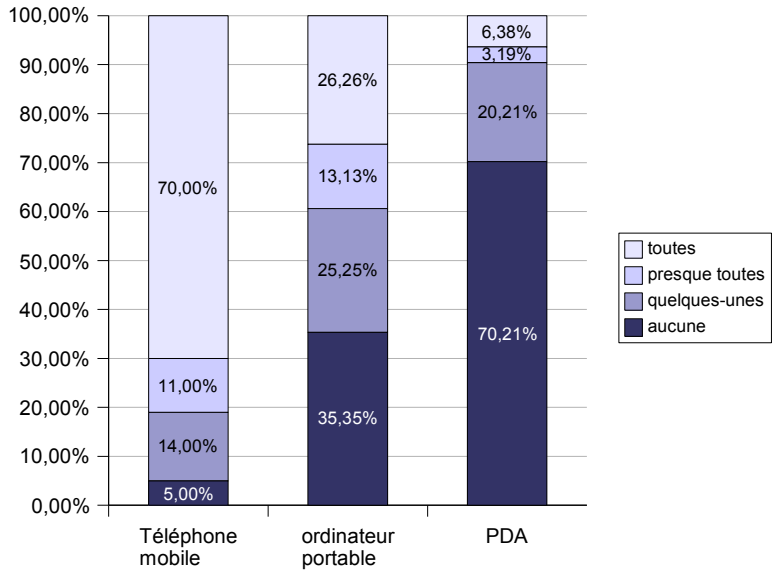


Illustration 2: Équipement des personnes mobiles en entreprise (2004)

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 œuvre sont les arguments les plus bloquants, comme le montre l'illustration suivante :

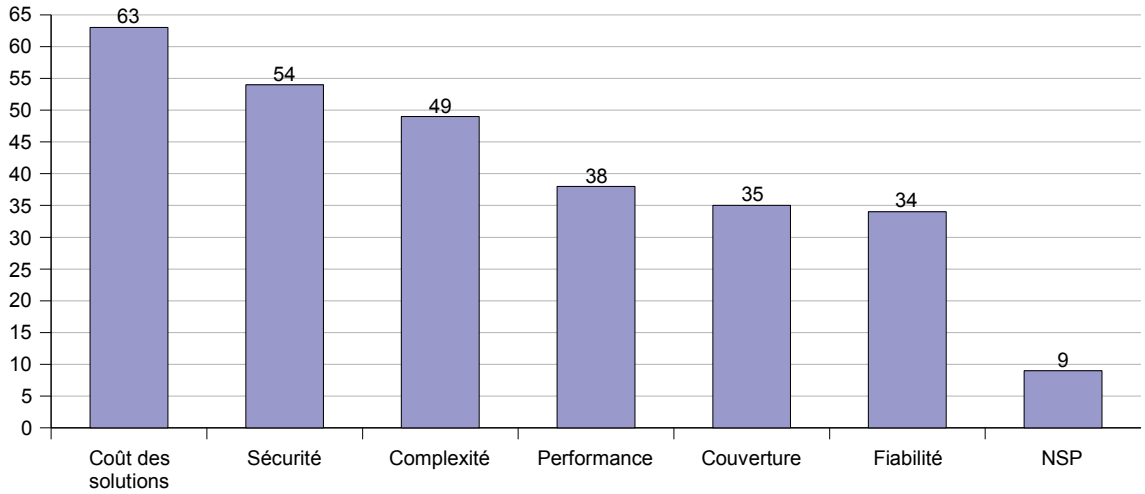


Illustration 3: Principaux freins au développement des réseaux mobiles

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

Pourtant, 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 (mises à jour régulières et plus fréquentes, diminution des doubles saisies, plus d'informations collectées, informations plus précises),
- productivité (diminution des coûts administratifs, ordonnancement plus efficace, outillages et pièces corrects diminuant le nombre des interventions nécessitant une deuxième visite, re-planification dynamique),

- accès à l'information sur site (accès direct aux informations pertinentes et à jour), moindre dépendance vis-à-vis des processus papiers (brochures et nouveautés catalogues),
- pilotage de la performance (suivi des niveaux de services, assistance et retour d'informations individualisés, clôtures d'interventions plus précises),
- 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 existe également un 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*	*802.11*
Au bureau	☺		☺
A la maison	☺	☺	☺
Chez un client	☺		☺
Sur la route	☺		
A l'hôtel/au 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 œuvre d'une solution nomade.

D'ailleurs, 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 de ces terminaux intègrent désormais la norme 802.11 en standard, ce qui favorise l'expansion des réseaux sans fil. Enfin, le nombre d'ASFI augmente très rapidement et les estimations par les grands opérateurs montrent que le marché est porteur.

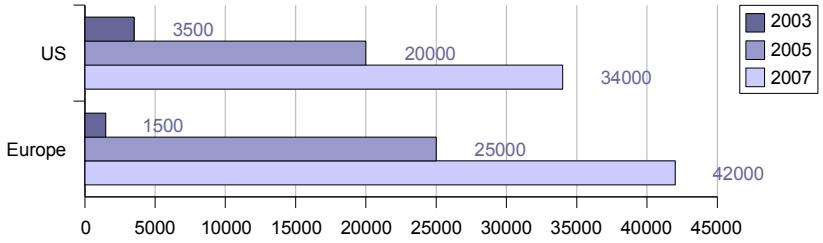


Illustration 4: Nombre de "hotspots" déployés

2.2.2 Récapitulatif

Cette série de statistiques essentiellement françaises 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 des PC portables alors que seulement un tiers emploie des PDA. Mais encore, 95% des employés ont un téléphone mobile : ce marché touchait moins le nomadisme informatique mais les nouvelles offres hauts débits (UMTS, 3G...) ainsi que les évolutions techniques (autonomie accrue, taille réduite) devraient rapprocher les téléphones et les PDA et fournir des applications légères compatibles avec les réseaux internet à moyen terme.

Les réseaux 802.11 sont très employés et utilisables presque partout (des difficultés subsistent dans les déplacements rapides) : certains fabriquants ont déjà annoncé des puces spécialisées compatibles 802.11 pour les téléphones mobiles[10]. 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 à part 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 refusent de développer ces réseaux en raison de la sécurité : si celle-ci s'appuyait énormément sur l'accès physique à l'infrastructure, les réseaux sans fil changent désormais la politique des ASSI : autoriser la mobilité des utilisateurs implique généralement l'ouverture des systèmes d'information hors des locaux de l'entreprise... et cette ouverture augmente le risque de pénétration par des personnes mal intentionnées. Les utilisateurs quant 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, supports, diagnostics, redondances de matériels, surveillances...

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

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

- Authentification (généralement un identifiant associé à un mot de passe),
- Traçabilité (journaux),
- Gestion des autorisations et des droits (individuels ou de groupes),
- Chiffrement et intégrité des données (cryptages et signatures électroniques),
- Alerte de sécurité (anti-virus, systèmes d'exploitation et applications),
- Surveillance en temps réels (IDS, scanners, volumétrie...)
- Mise à jour des failles logicielles (téléchargement de patchs),
- Filtrage par systèmes antivirus et pare-feu des virus, chevaux de Troie et trames mal-formées,
- Formation (utilisateurs),

10 Samsung, communiqué de presse du 02 décembre 2004

- ....

La sécurité est devenue très importante et elle constitue l'un des budgets les plus élevés pour les entreprises. Cela n'est pas seulement dû à l'émergence des technologies sans fil mais aussi à la croissance des nombres de virus et vers informatiques, 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 Attaques des réseaux 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 elle est facilement repérable. Elle est intéressante pour le pirate car des services comme le transfert de fichier (FTP), le terminal distant (Telnet), le service de messagerie (SMTP, POP...) renvoient généralement une chaîne de caractères indiquant le nom et la version de l'application gérant ces ports.
- 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 d'une machine corrompue mais ce ne sera pas celle du pirate.
- Obtenir un plantage d'un serveur : l'arrêt brutal d'un serveur ne permet pas d'obtenir d'informations sur l'attaquant, par contre, l'indisponibilité de ce serveur peut entraîner des pertes importantes pour l'entreprise : informations, transactions, ordres, etc., comme l'attaque menée en janvier 2003 sur les serveurs coréens puis américains (13000 guichets de la "Bank of America" ont perdu 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). Elles sont basées sur les failles des systèmes visés.
- Intercepter et modifier des communications : en bloquant un serveur, le pirate peut introduire à sa place un serveur 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 [MITN04] sur ces techniques. Le phishing[11] est d'ailleurs devenu une technique très en vogue par courrier électronique en affichant un message demandant de renouveler les mots

11 Contraction de fishing (pêcher) et phreaking (pirater les lignes téléphoniques)

de passe d'un compte chez un organisme connu. Le lien affiché pointe en réalité vers une page web d'un serveur pirate imitant la mise en page du site officiel et l'utilisateur confiant saisit les informations demandées en croyant être sur le site officiel. Même si le message ne touche qu'une partie de la population, le pirate dispose alors d'une base de données contenant les identifiants et mots de passe de nombreux utilisateurs du service officiel (généralement, ce sont les banques qui sont le plus visées).

2.3.1.3 Attaques par infection

Les attaques par infection concernent les virus, les vers, les spywares[12] et les chevaux de Troie. Ce 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'adresses 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 généralisent le déploiement 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.

Un cheval 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 s'active 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 valider un message d'alerte 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 Attaques des réseaux sans fil

Les réseaux sans fil sont sensibles aux attaques précédentes comme les autres réseaux mais ils ouvrent également la voie à de nouvelles attaques : parce que les ondes hertziennes ne sont pas facilement contrôlables, la mauvaise implantation d'un point d'accès réseau sans fil revient à placer des prises réseaux hors des locaux.

Deux méthodes existent pour détecter des réseaux sans fil et permettre leur écoute : 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 informations reçues.

12 Logiciel-espion

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).

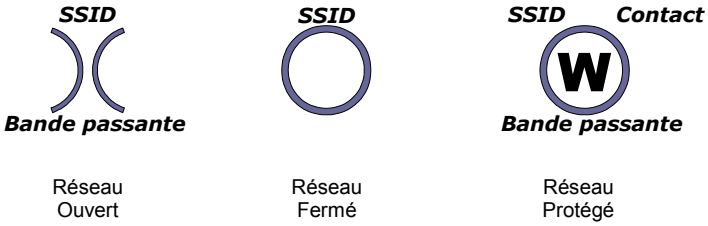


Illustration 5: Symboles utilisés dans le war-chalking

Ceux qui n'en connaissent pas la signification n'y voit qu'un graffiti alors que les hackers y voit une occasion de se connecter au réseau. De plus, l'attribution d'adresses IP de manière dynamique facilite la mise en œuvre d'un équipement sur ce réseau.

Une fois détectés, 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 brouillées afin qu'aucune communication ne puisse passer. Bien que brutale, cette attaque utilisée de manière ponctuelle et irrégulière perturbe un réseau sans permettre de trouver facilement l'origine.

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 existant depuis de nombreuses années (déplacements chez un client, en réunion ou lors d'un séminaire), les technologies sans fil ont aboli le frein psychologique du réseau fermé, représenté par le câblage. La grande simplicité d'implémentation d'un réseau sans fil attire les décideurs qui voient là, un moyen de suivre au plus près les besoins de leurs clients et diminuer les étapes intermédiaires de saisie.

Issus d'une technologie récente, ces réseaux apportent en effet, 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 entreprises que chez les particuliers.

Toutefois, cet accroissement de liberté complique la tâche des administrateurs qui définissaient la sécurité de leurs systèmes d'information en fonction de l'accessibilité physique des points de connexions. Les réseaux sans fil mettent en évidence ce jugement erroné et imposent la recherche de solutions pour parer aux nouvelles menaces dont les réseaux sont la proie.

Ainsi se pose la problématique entre deux objectifs opposés : comment concilier mobilité et sécurité, liberté et contrôle, simplicité 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 déterminer quelles sont les attentes des universités de Grenoble et comment elles souhaitent résoudre les problèmes liés à l'utilisation de ces technologies sans fil.

En premier lieu, la structure du CICG ainsi que son fonctionnement sont expliqués avec comme objectif la compréhension des différents rôles du CICG au niveau local, régional et national.

Puis une définition des différents profils d'utilisateurs présents dans les universités et des usages du réseau permettra de connaître le contexte du nomadisme en université.

Enfin, la rédaction d'un cahier des charges et l'énumération des contraintes liées à l'architecture en place auront 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 CICG est un service interuniversitaire qui a été créé en 1972 par les établissements d'enseignement supérieur de l'académie de Grenoble et dont l'activité tournait autour des supercalculateurs et du calcul scientifique.

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,
- la gestion des 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.

Le CICG 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.

Il est administré par un conseil d'administration et dirigé par un Directeur. Sous l'autorité de ce dernier, se trouvent :

- le Département Informatique de Gestion (DIG),
- le Département Réseau (DR),
- l'activité diffusion de logiciels,
- l'administration.

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

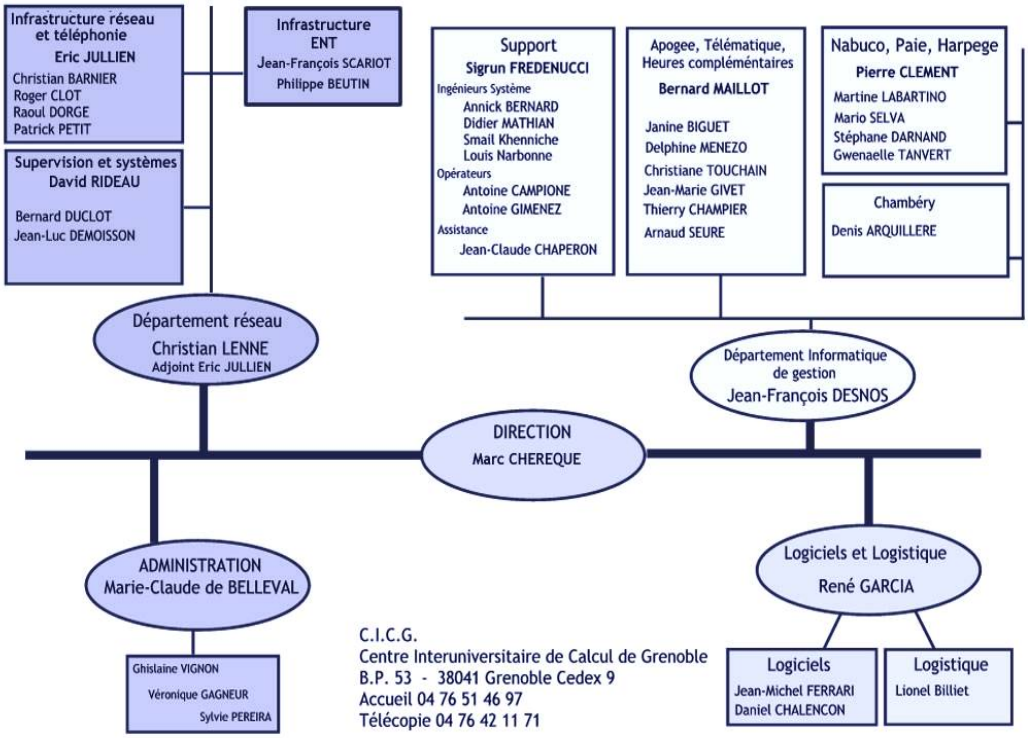


Illustration 6: Organigramme du CICG

Très récemment, le nom du CICG et son logo ont été modifiés pour se rapprocher de ses missions contemporaines : il est devenu DSIGU[13].

Illustration 7: Logo du CICG et nouveau logo DSIGU

Toutefois, à l'heure de l'écriture de ces pages, la redéfinition de ses missions est en cours mais n'est pas terminée.

3.1.2 Département réseau

Le département réseau du CICG au sein duquel s'est déroulé notre stage, 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.

Le Département Réseau a deux missions principales :

- La gestion de différents réseaux, dont le réseau interuniversitaire,
- La coordination d'actions transversales.

13 Direction des Systèmes d'Information de Grenoble Universités

3.1.3 Présentations des réseaux déployés

Pour accéder à ses services (messagerie, intranet, web) un utilisateur va utiliser plusieurs niveaux de réseaux dont les structures sont hiérarchisées. Le CICG intervient dans ces structures qui sont expliquées dans cette section.

3.1.3.1 Réseau TIGRE

Le réseau **TIGRE**[14] est le réseau MAN[15] enseignement supérieur et recherche de l'Académie de Grenoble. Techniquement, il est constitué de deux étoiles (routeurs/commutateurs) dont les cœurs redondants sont situés géographiquement au CICG (à Saint-Martin d'Hères) et à l'INPG (au centre de Grenoble). Sur cette partie, le CICG – opérateur du réseau – loue les fibres optiques à MetroNet.

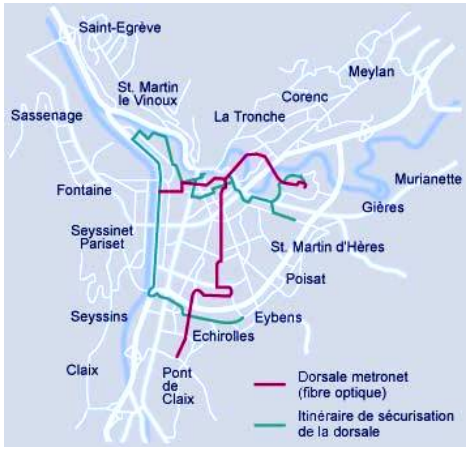


Illustration 8: Dorsale haut débit Metronet

Les organismes utilisant ce réseau sont :

- UJF (Université Joseph Fourier, http://www.ujf-grenoble.fr/) aussi appelée U1,
- UPMF (Université Pierre Mendès France, http://www.upmf-grenoble.fr/) ou U2,
- Université Stendhal (Université Stendhal, http://www.u-grenoble3.fr/) surnommée U3,
- INPG (Institut National Polytechnique de Grenoble, http://www.inpg.fr/) dit U4,
- 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/),
- ESRF (European Synchrotron Radiation Facility, http://www.esrf.fr/) ,
- ILL (Institut Laue-Langevin, http://www.ill.fr/),
- EMBL (European Molecular Biology Laboratory, http://www.embl-grenoble.fr/ et http://www.embl.org/),
- IUFM (Institut Universitaire de Formation des Maîtres, http://www.grenoble.iufm.fr/),
- CROUS (Centre Régional des Oeuvres Universitaires et Scolaires , http://www.crous-grenoble.fr/).

14 TIGRE : Toile Informatique de GREnoble
15 Metropolitan Area Network

Le bon fonctionnement du réseau repose sur une architecture logique redondante des liens et équipements formant les cœurs du réseau via un routage dynamique BGP : ainsi la disponibilité du réseau de type RMU[16] est excellente et permet l'accès à Renater dans les meilleures conditions (forte bande passante et fiabilité).

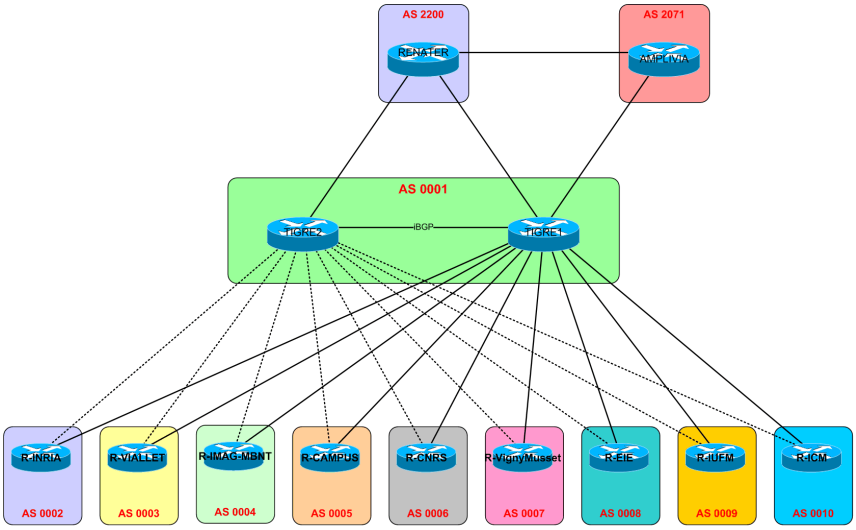


Illustration 9: Schéma logique du réseau TIGRE

Le CICG est donc responsable de l'exploitation et de l'évolution du réseau TIGRE, un rôle crucial puisqu'il a en charge les demandes d'agréments Renater, le routage et le filtrage, la gestion des alertes, la maintenance des équipements et l'évolution du réseau tout en garantissant un accès fiable et rapide aux ressources.

3.1.3.2 Réseau AMPLIVIA

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

Dans ce cadre, le CICG joue un rôle d'interface (mandatée par les sites universitaires) à la jonction des différents points d'accès entre ce réseau et les sites universitaires de la région.

3.1.3.3 Réseau RENATER

Le réseau **RENATER**[17] est le réseau national de la recherche et de l'éducation. Il relie plus de 600 sites (universités et organismes de recherche) et la troisième génération (Renater 3) est actuellement en exploitation tandis que la quatrième – annoncée par le ministre délégué à l'Enseignement supérieur et à la Recherche en juin 2005 – est en cours de déploiement.

Renater permet également l'accès vers l'Internet français (via SFINX), l'Internet international, les réseaux de l'Asie pacifique, les DOM-TOM et les réseaux de l'éducation et de la recherche européens et américains.

16 RMU : Réseau Métropolitain Universitaire

17 RENATER : Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche (http://www.renater.fr/)

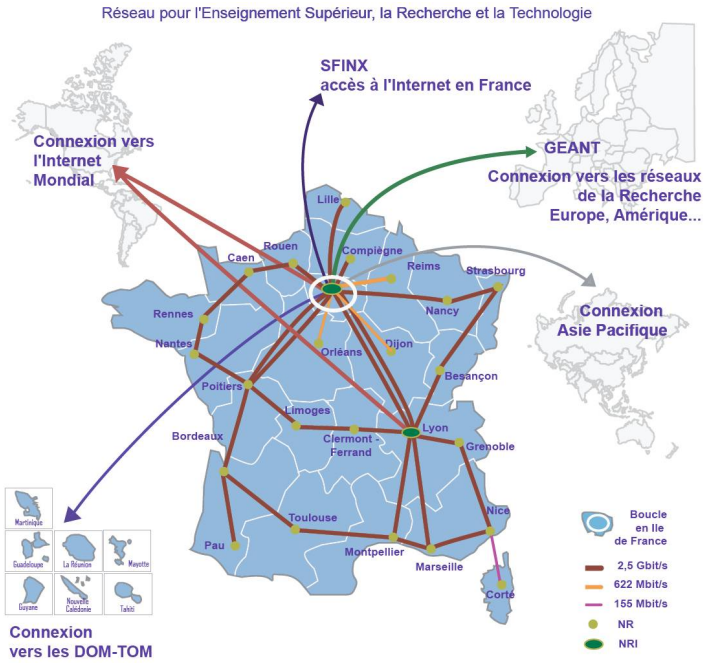


Illustration 10: Le réseau Renater

Le rôle du GIP[18] RENATER, maître d'ouvrage du réseau national, consiste :

- à 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,
- à opérer un des CERT[19] français ; un CERT est une entité d'information technique et opérationnelle sur les actions délictueuses en matière de réseaux et d'équipements informatiques (à ne pas confondre avec le CERTA[20]),
- à 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),
- à 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 (et théoriquement tout utilisateur) connecté à RENATER doit signer et respecter.

Là encore, le rôle du CICG est fondamental puisqu'il est l'interlocuteur unique entre le réseau national Renater et les membres du réseau TIGRE.

3.1.3.4 Réseau GEANT

Le réseau **GEANT**[21] est un réseau européen. Il connecte 30 réseaux de recherche et d'éducation (NREN[22]) qui desservent 34 pays. Renater en fait partie pour la France.

18 GIP : Groupement d'Intérêt Public.
19 CERT : Computer Emergency Response Team
20 CERTA : Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques. Il est rattaché à la DCSSI (http://www.ssi.gouv.fr/)
21 GEANT : Gigabit European Academic Network (http://www.geant2.net/)
22 NREN : National Research and Education Network.

En plus de fournir une plateforme IPv4 à très haut débit (certaines connexions atteignent 10Gbps), d'autres services sont disponibles pour répondre à la demandes des chercheurs : IPv6, multicast, VPN. De plus, GEANT améliore l'interconnexion avec les autres réseaux mondiaux (Amérique du nord, zone Asie-Pacifique, l'Amérique du Sud et les pays méditerranéens).

3.1.3.5 Réseaux relationnels

Ces réseaux s'appuient sur les réseaux d'infrastructures nationaux (comme Renater) et sur le réseau Européen GÉANT. Ce sont plutôt des groupes d'expérimentation travaillant de manière indépendante sur des thèmes communs.

3.1.3.5.a TERENA

TERENA est né en 1994, de l'association de RARE[23] et EARN[24]. 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[25]),
- Middleware (la couche interdépentante 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 CICG, par son rôle, est impliqué dans la plupart de ces groupes de travail et participe aux projets nationaux, parfois de manière "moteur". Travaillant sur des projets prestigieux comme la mobilité, IPv6, la voix sur IP, la qualité de service, la vidéoconférence... le CICG est bien placé pour avoir un rôle de conseil auprès des universités et des autres partenaires. Il pilote donc également les groupes de travail pour le déploiement de ces technologies dans les facultés et universités de Grenoble.

3.1.3.5.b EDUROAM

Le réseau EDUROAM[26] permet aux utilisateurs des institutions participantes de se connecter en n'importe quel point en utilisant son accréditation habituelle. Il est issu du développement d'un groupe de travail de TERENA[27] (TERENA Mobility).

Ce groupe existe depuis janvier 2003 et le projet s'appelle "EDURoam". Ce projet est basé sur une structure hiérarchique de serveurs RADIUS.

La politique d'EDURoam n'est pas figée sur les moyens techniques à mettre en œuvre, l'objectif étant de faciliter le nomadisme entre les pays ayant rejoint le groupe de travail. Il n'y a donc aucune solution pré-établie ce qui permet une certaine autonomie de travail pour chaque pays et favorise l'expérimentation.

23 RARE : Réseaux Associés pour la Recherche Européenne
24 EARN : European Academic and Research Network
25 CSIRT : Computer Security Incident Response Team
26 EDUROAM : EDUcation ROAMing (http://www.eduroam.org/)
27 TERENA : Trans-European Research and Education Networking Association

La carte suivante montre les pays adhérents.

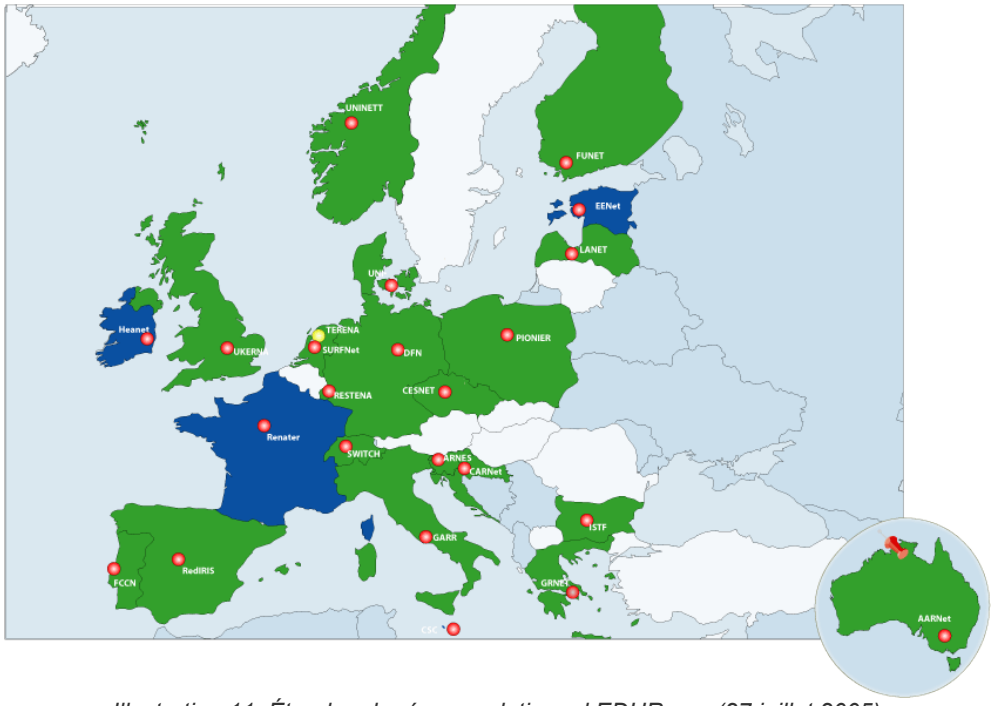


Illustration 11: Étendue du réseau relationnel EDURoam (27 juillet 2005)

Les pays ayant déjà mis en production une solution compatible avec EDURoam sont représentés en vert tandis que les pays en cours de déploiement sont affichés en bleu.

3.2 Analyses et classifications

Maintenant que les rôles du CICG sont définis et que l'imbrication des différents réseaux utilisés est connue, il est temps de s'intéresser aux raisons de l'existence de ces réseaux : les utilisateurs et leurs besoins. La taxonomie des utilisateurs, des moyens employés et des ressources utiles est la base de cette section qui va permettre d'analyser les besoins, de définir les usages et de mettre en évidence les contraintes actuelles.

3.2.1 Classification des utilisateurs

Dans l'environnement des universités les différentes catégories d'utilisateurs sont nombreuses. En effet, il y a les étudiants, les enseignants, le personnel administratif et technique, les visiteurs...

- Les étudiants : population très diversifiée en terme de connaissance des outils informatiques, on peut distinguer les novices pour lesquels l'ordinateur est une boîte noire permettant d'effectuer un travail et ceux qui sont capables de modifier la configuration de leurs machines. A part ce critère, les nombreuses UFR[28] (littéraires, économiques, techniques, scientifiques, etc.) et les nombreux cursus (DUT, DEST, master, etc.) ne permettent pas de déterminer un profil type précis. On peut toutefois ajouter qu'ils ont un budget limité et qu'ils se sentent peu "concernés" par les risques liés au piratage (multimédias, serveurs, services...). Depuis l'offre "un PC portable Wi-Fi pour un euro par jour"[29] les étudiants deviennent la population "mobile" par excellence.

28 UFR : Unité de Formation et de Recherche
29 Voir le site http://delegation.internet.gouv.fr/mipe/projet.htm

- Les enseignants : également très diversifiés, ils ont 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 sont amenés à accéder à plusieurs réseaux (réseaux pédagogiques pour les formations des étudiants, réseaux administratifs pour les dossiers administratifs, ...) et – dans le cadre de travaux – intégrer un laboratoire ou une autre université. Ils sont considérés comme personnels permanents et comme pour les étudiants leur niveau de connaissances en informatique est variable.
- Les membres du personnel : ils gèrent le bon fonctionnement des universités (gestionnaires, directeurs, secrétaires, ...) disposent d'un bureau fixe dans les locaux des universités. Dans cette catégorie se trouve également les CRI[30] qui administrent les réseaux et serveurs. Ici encore, une personne peut être rattachée à un autre organisme que celui pour qui elle travaille régulièrement. Il n'y a pas de profil type déterminé et si le personnel technique est plus disposé à maîtriser l'outil informatique, le personnel administratif est en revanche plus exigeant sur l'ergonomie de celui-ci.
- 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. Elles 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 parts 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 fixe : ce sont les équipement que l'on retrouve à la maison, dans les salles de cours, les cybercafés et de nombreux autres lieux encore. Incontournables, il ne sont pas forcément synonymes de mobilité dans le sens de déplacement mais leur présence en tout lieu dans le monde permet d'en faire un point d'accès au réseau Internet (modem RTC, ADSL, RNIS ou autres liaisons).
- 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 onéreux.
- 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 des ordinateurs portables même s'ils intègrent 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[31]. Il permet de téléphoner et intègre les possibilités d'un PDA pour un encombrement équivalent.

30 CRI : Centre de Ressources Informatiques
31 Voir le lien http://www.clubic.com/actualite-20155-pda-en-baisse-smartphone-en-hausse-.html

Les équipements les plus utilisés sont les ordinateurs fixes et portables pour lesquels il faut encore dissocier les systèmes d'exploitation. Deux grandes catégories se détachent : les machines compatibles IBM et les systèmes Apple.

Les machines compatibles peuvent avoir un système d'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).

Les machines Apple ont un système d'exploitation propriétaire mais les dernières versions (à partir de MAC OS/X) utilisent un noyau Unix pour fonctionner (proche de Linux).

3.2.3 Classification des accès géographiques

Quelque soit l'équipement 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 d'un intranet	Facile	Sécurisé	Difficile	Sécurisé
Utiliser les ressources locales (imprimantes...)	Facile	Facile	Facile	Difficile
Utiliser les applications (synchronisation...)	Facile	Sécurisé	Difficile	Difficile

** en utilisant un FAI*

Tableau 2: Localisation et usage des services

- Au bureau : tous les services sont facilement accessibles. Les difficultés de connexion sont masquées parce que les ordinateurs appartiennent à l'entreprise ou à l'université et sont configurés de manière standard par un service informatique dont la tâche est de veiller à l'homogénéité des équipements et des applications. L'authentification est généralement unique pour permettre l'accès à l'ensemble des ressources.
- A la maison (via FAI) : 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 ! En revanche, il n'est pas possible d'utiliser un client IMAP/POP standard pour accéder au serveur de l'entreprise (si la sécurité est bien assurée) : 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 (souvent utilisé par toute la famille et pour toutes sortes d'activités) sur lequel il n'est pas possible de garantir l'intégrité et la salubrité (spywares et virus). Toutefois, l'utilisateur possède les droits nécessaires pour installer un logiciel.
- A la maison (via une connexion directe) : dans ce cas, l'utilisateur se retrouve dans la même configuration qu'au bureau et c'est son entreprise ou établissement qui joue le rôle de fournisseur d'accès. Ce cas est toutefois en forte diminution à cause des coûts de communications et de l'utilisation souvent détournée de cet accès aux ressources professionnelles pour des besoins personnels.
- 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 suffisants pour installer une application personnelle.

- 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 d'accueil. Le poste est considéré comme sûr, les applications présentes sont celles définies dans la politique du service informatique. Elle peut nécessiter la création d'un compte temporaire sur le site d'accueil. En revanche, la sécurité de la communication n'est pas garantie !

3.2.4 Conclusion des analyses

L'ensemble des analyses précédentes fait apparaître des informations essentielles sur les utilisateurs, les usages et la mobilité. Malgré les nombreux types d'utilisateurs, il n'y a que quatre possibilités vraiment différentiables : les utilisateurs permanents, les visiteurs, ainsi que les personnes novices (ou sans droits d'administration) et les personnes exigeantes (capables d'installer et configurer un équipement informatique). Les capacités de ces utilisateurs sont résumées dans le tableau ci-dessous.

	Novices	Exigeantes
Permanents	Simplifié	Étendu
Visiteurs	Simplifié	Étendu

Tableau 3: Profils type de l'ensemble des utilisateurs

Quelque soit le profil de l'utilisateur, l'analyse met en évidence une grande diversité d'équipements gérant les réseaux sans fil. Toutefois, la grande majorité des utilisateurs se sert d'un ordinateur compatible IBM ou Apple. On s'aperçoit alors que seuls trois systèmes d'exploitation émergent : Microsoft Windows, MAC OS et Linux. Ils constituent la majorité des équipements mobiles.

Enfin, bien que l'UMTS/GPRS soit une solution universelle pour se connecter à un réseau, son coût et son débit la limitent à la téléphonie et aux services associés. Ainsi, pour accéder à son intranet, il ne reste que deux possibilités : la connexion depuis l'extérieur par l'Internet (RTC ou ADSL) ou l'utilisation du réseau interne (prises réseaux ou points d'accès sans fil).

3.3 Description de l'architecture d'origine

Depuis 2003, le CICG travaillait déjà sur la problématique du nomadisme : ce domaine relativement nouveau a été abordé par les pionniers de la mobilité ! Les constructeurs, les utilisateurs et les développeurs ont cherché des solutions pour résoudre les problèmes au cas par cas ou bien ont adapté des solutions existantes. Ainsi les universités grenobloises se sont dotées d'un système permettant le nomadisme dans leur domaine géographique.

3.3.1 Architecture VPN interuniversitaire

Mise en place au premier semestre 2004, cette architecture s'appuie sur un ensemble de concentrateurs VPN (Cisco) répartis et sur l'utilisation des technologies basées sur les tunnels IPSec. De plus, un ensemble de points d'accès réseau sans fil est réparti dans chaque université : grâce à ces réseaux, les utilisateurs ne sont plus dépendants des prises disponibles pour se connecter.

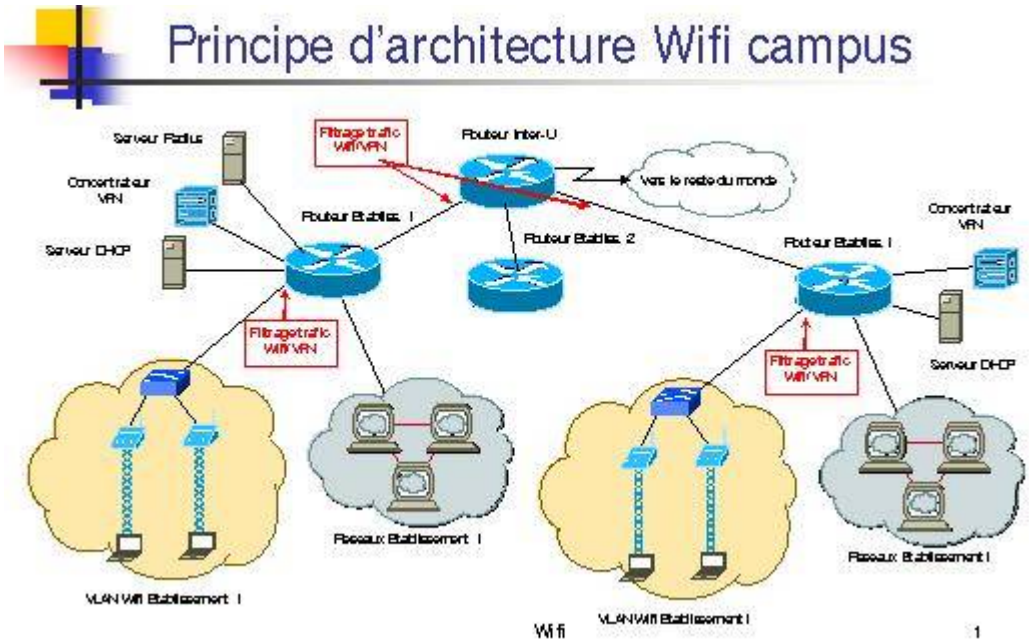


Illustration 12: Architecture Wi-Fi et VPN de Grenoble Universités

Cette solution couvre un ensemble de besoins assez vaste :

- Mobilité depuis les réseaux sans fil des universités,
- 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.

L'utilisation de l'infrastructure demande quelques modifications de l'équipement client :

- il faut un pilote (driver) et une carte à la norme 802.11b ou 802.11g pour pouvoir se connecter sur le réseau sans fil le plus proche. L'interface est configurée par le serveur DHCP de la zone (adresse IP locale, masque de sous-réseau, adresse de la passerelle et des serveurs DNS),
- il faut installer un logiciel tiers (le client VPN) et permettre le dialogue en UDP sur le port 500 pour pouvoir se connecter de manière sûre au concentrateur VPN. Celui-ci fait office de système d'authentification et de routeur lorsque l'utilisateur est correctement connecté.

3.3.2 Fonctionnement de l'architecture

L'architecture des réseaux sans fil choisie au sein des universités (Illustration 12) utilise massivement les plages d'adresses IP privées (RFC 1918). 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
- Univ. Savoie – 10.7.0.0 / 16
- CNRS – 10.8.0.0 / 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 sécurité 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 œuvre des techniques de "tunneling" pour masquer la différence de localisation.

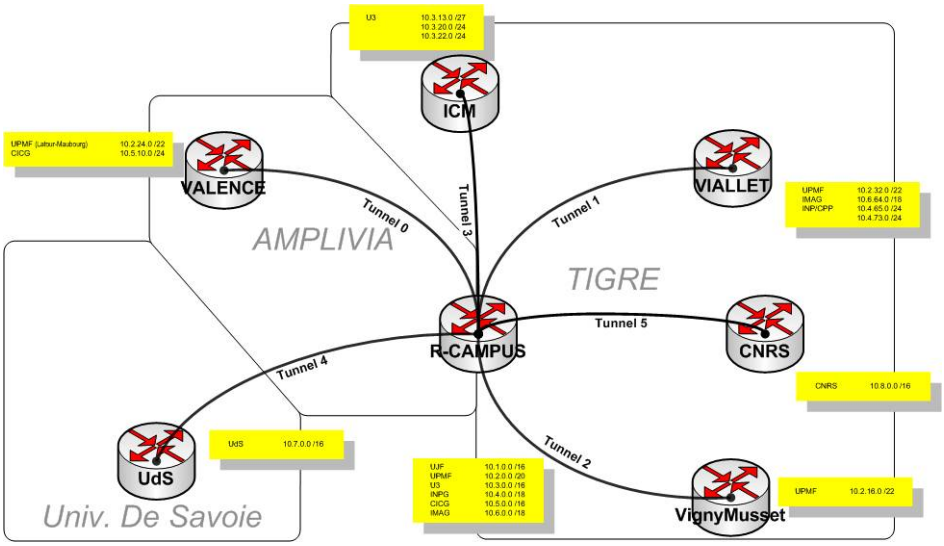


Illustration 13: Les tunnels interuniversitaires

Ces plages d'adresses privées ne permettent pas d'accéder à Internet. Toutefois il est possible de récupérer le client VPN Cisco sur un serveur web dédié[32] ainsi que la configuration. Le site explique comment installer et faire fonctionner le client.

Une fois le client VPN lancé sur la machine, une authentification est faite (l'utilisateur saisit son identifiant et le mot de passe associé) puis une interface réseau virtuelle prend les paramètres fournis par le serveur d'authentification : une adresse IP publique est allouée à chaque personne. Cette adresse est unique et permanente ce qui permet de filtrer les zones accessibles par celle-ci.

3.4 Spécifications des besoins

Bien que le nomadisme soit assuré correctement au sein des universités de Grenoble, l'évolution rapide des technologies et les choix faits par d'autres universités en France ont amené le CICG à faire une nouvelle étude.

32 Lien du serveur dédié : https://nomadisme.grenet.fr/

L'objectif est de fournir un service équivalent ou supérieur à celui déjà en place tout en complétant les défauts inhérents aux systèmes VPN. Pour y parvenir, l'étude des contraintes a été menée pour déterminer le cadre de liberté disponible. Ensuite, les nouveaux besoins ont été exprimés, notamment sur la simplicité d'utilisation, la généralisation à l'ensemble des universités et l'amélioration des services.

3.4.1 Description des contraintes

Les contraintes dans un environnement aussi hétérogène impliquent une vue à court et moyen terme : à 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 les unifier et les réduire.

De plus, les contraintes ne sont pas toutes d'ordre technique : 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 techniques. D'une part, il y a celles liées à la solution VPN, d'autre part il y a celles imposées par l'architecture des réseaux employés.

3.4.1.1.a Contraintes de la solution VPN

Les contraintes de la solution en place sont liées au matériel :

- les concentrateurs Cisco VPN3030 sont limités en puissance de traitement ce qui limite le nombre de connexions simultanées sur chaque site,
- le client VPN Cisco ne peut être installé que par une personne ayant les droits d'administration sur le poste client,
- il n'existe pas de client VPN Cisco pour tous les équipements (actuellement le client n'existe que pour Microsoft Windows, Linux, MAC et Pocket PC),
- il n'est pas possible d'imbriquer deux tunnels VPN sur un même poste à cause du protocole employé par le produit Cisco (IPSec),
- il est obligatoire que chaque utilisateur ait une adresse IP publique unique et fixe pour que le concentrateur VPN puisse fournir un accès à l'intranet et Internet,
- la configuration du client peut rebuter un utilisateur débutant et l'utilisation d'un profil de connexion diffère selon le type d'accès (réseau interne sans fil ou réseau Internet).

Cette solution très efficace n'est pas intuitive pour tout le monde. Elle requiert l'utilisation de plusieurs profils et l'installation d'un logiciel sur le poste de l'utilisateur. Cela n'est pas un problème pour un nombre limité d'utilisateurs mais devient critique lorsqu'il s'agit de dizaines de milliers d'étudiants.

3.4.1.1.b Contraintes de l'architecture réseau

L'utilisation de plages d'adresses particulières pour les accès via les réseaux sans fil et la structure des réseaux universitaires génèrent les contraintes ci-dessous :

- il est nécessaire de router les adresses des réseaux sans fil dans tout le réseau TIGRE,
- il est également nécessaire de filtrer les flux provenant de ces adresses au strict minimum (client VPN),

- il faut protéger les réseaux sans fil des personnes extérieures tout en laissant l'accès libre au serveur fournissant les informations et le programme client VPN,
- il est nécessaire d'activer des tunnels entre plusieurs sites géographiques appartenant à un même domaine pour partager la plage d'adresses privées qui lui est affectée.

Les équipements utilisés dans la solution existante s'adaptent à ces spécifications incontournables mais il faut en permanence actualiser les informations et communiquer les changements dans l'architecture à tous les membres du réseau interuniversitaire.

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 l'ensemble de la communauté. Cette charte est signée par les présidents des établissements utilisant le réseau Renater.

Elle définit 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, téléchargement de musiques en peer-to-peer, etc.).

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 à qui appartient l'adresse IP doit être capable de déterminer qui est à l'origine du comportement suspect.

Une autre contrainte plus législative vient également appuyer cette nécessité d'identifier les flux et informations impliquant les établissements : la LCEN[33]. Cette loi institue notamment les points suivants :

- elle propose une définition claire de la notion de communication et de commerce par voie électronique ;
- elle impose la participation des hébergeurs et des fournisseurs d'accès à la lutte contre les contenus illicites : la loi définit un corps de mesures réglementaires ;
- elle définit l'équilibre entre les droits de l'expression et les droits de la personne, en modernisant notamment le régime de délit de presse ;
- elle précise l'ensemble des dispositions rattachées à l'utilisation et le développement d'Internet dans la sphère publique.

Des informations plus précises peuvent être trouvées sur le site du gouvernement[34] mais l'essentiel est de pouvoir déterminer à tout moment la provenance d'un flux ou d'une infraction et d'agir conformément au texte de la LCEN.

3.4.1.3 Contraintes collectives

Le réseau interuniversitaire est constitué de plusieurs universités ayant chacune leurs services informatiques (CRI). Ceux-ci 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.

33 LCEN : Loi sur la Confiance en l'Économie Numérique (loi n° 2004-575 définitivement adoptée par les parlementaires et parue au JO n° 143 du 22 juin 2004)

34 http://www.internet.gouv.fr/rubrique.php3?id_rubrique=336

Sur Grenoble, chaque université est indépendante des autres et peut donc faire ses propres choix technologiques. Chacune dispose de ses propres ressources, compétences et budgets. Une partie des contraintes techniques est issue des choix réalisés par chaque établissement.

Afin de permettre la coordination de projets importants et limiter les nouvelles contraintes, il existe des groupes de coordination dont le COR2I[35]. Constitué des directeurs des CRI, il assure le suivi des projets, l'appui des personnels techniques, la validation des recommandations au niveau interuniversitaire...

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. Il existe plusieurs groupes correspondants aux différents projets ou thèmes abordés par le COR2I : celui travaillant sur le nomadisme est inscrit dans la liste de messagerie sous le nom "Sans fil Grenoble" (wifi-grenoble@ujf-grenoble.fr). C'est ce groupe qui a imaginé et déployé la structure basée sur les concentrateurs VPN Cisco.

3.4.2 Description des 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 tous 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 actuellement en exploitation est une première réponse pour sécuriser les réseaux des universités grenobloises. Sa pertinence doit toutefois être ré-évaluée avec d'autres solutions nouvelles qui pourraient être plus adaptées : le modèle VPN est donc la référence pour la définition des besoins.

L'étude menée à la section 3.2 met en évidence 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 et/ou exigeant 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 à posteriori et tout compte utilisateur doit être protégé afin de garantir l'authentification (identité juste).

En fonction du mode d'utilisation, nous pouvons déterminer les besoins correspondants qui vont permettre la recherche d'une architecture générale répondant à ces demandes.

35 COR2I : Comité Opérationnel des Ressources Informatiques Interuniversitaires

3.4.2.1 Utilisation "simplifiée"

Ce type d'utilisation est le mode le plus léger, sans configuration. 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 nécessiter 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. En résumé :

- accès sans installation de programme ni configuration (côté client),
- accès à Internet après un mécanisme d'authentification,
- compatible avec la majorité des équipements (notamment ceux énoncés dans la section 3.2.4),
- limitation acceptable des services accessibles (services minimaux : web et web sécurisé),
- traçabilité des connexions,
- utilisation intuitive et simple.

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.

- Accès à quasiment tous les services et toutes les applications intranet,
- Sécurisation des flux quelque soit le média employé (Internet ou ASFI de l'établissement),
- Accès après Authentification,
- Traçabilité des connexions,
- Installation de programmes ou applications autorisées.

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 Troie. 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 les systèmes d'exploitation de Microsoft réputés peu sécurisés : les adeptes des OS libres en font leur cheval de bataille. Malheureusement, c'est effectivement vrai comme le montre l'étude de Sophos[36] pour le premier semestre 2005 (le préfixe W32 signifiant Windows 32 bits).

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

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 14: Statistiques virales du 1er semestre 2005

Cette étude explique brièvement que l'on assiste à une progression de plus en plus rapide des chevaux de Troie et que si le nombre de virus augmente, le délai d'infection moyen quant à lui 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 sur son poste personnel et dont il devra acquitter une licence.

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

Cette partie est facultative bien que de nombreuses alertes remontées par le CERT aient pour origine des machines infectées. La priorité est donnée aux méthodes de connexion : si elles intègrent des mécanismes de salubrité, c'est un plus...

3.4.2.4 Résumé des besoins

La recherche d'une solution pour le réseau interuniversitaire doit correspondre à deux types d'utilisation (simplifié et étendu) qui doivent répondre aux problématiques suivantes :

- Permettre un accès contrôlé au réseau (traces),
- Permettre une indépendance maximum par rapport au 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),
- Permettre de déterminer la pertinence de la solution VPN actuellement en place par rapport à d'autres solutions.

Le tableau ci-après (tableau 4) résume donc les fonctionnalités disponibles en fonction du type de besoin.

	Besoins Standards	Besoins étendus
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 4: Table des fonctionnalités par besoins

De plus, la capacité de mutualiser les solutions et les coûts sont également déterminants dans le choix d'une architecture. Les choix doivent se porter au maximum sur les solutions s'appuyant sur les normes établies : ceci afin de garantir une évolution ouverte et de ne pas rendre les universités dépendantes d'une solution trop propriétaire.

4 NORMES ET INFORMATIONS

De nombreuses sociétés développent des solutions pour les problèmes de tous les jours. L'informatique étant une science permettant d'éviter les travaux répétitifs, les informaticiens ont mis en commun certaines solutions et établi des normes. Ces normes sont nombreuses et il existe donc plusieurs organismes pour les gérer. Dans le domaine des télécommunications, on trouve principalement l'ISO[37], l'IEEE[38], l'IETF[39] et l'ITU[40].

Avant de rechercher de nouvelles solutions, il est utile de connaître les normes utilisées dans les produits susceptibles de répondre au cahier des charges. En effet, pour être le plus ouvert possible, le nomadisme doit s'appuyer sur des réseaux et des techniques de transmission normalisées. Toutefois, les problèmes de sécurité qu'engendre la mobilité rendent obligatoire l'authentification et le chiffrement des données transportées. Ces mécanismes doivent être eux aussi standardisés.

Voilà pourquoi ce chapitre aborde les standards utilisés dans la plupart des réseaux, puis il reprend les standards de communication filaire et sans fil. Ensuite, il présente les différentes méthodes assurant la protection et l'intégrité des données sur un réseau. Enfin, il décrit les moyens courants pour authentifier une personne ou une machine.

4.1 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 employée, 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 étudierons les standards communs à la technologie filaire et à la technologie sans fil. Ensuite, nous aborderons les différences afin de comprendre les interactions et les contraintes dans un réseau de campus.

4.1.1 Modèles de réseaux

La compréhension d'une fonction complexe nécessite généralement son découpage en sous-ensembles. La description précise de chaque sous-ensemble fournit des règles et des références communes.

L'ISO est un organisme de normalisation international qui a présenté un modèle de communication en réseau de sept couches appelé OSI[41]. Sans revenir en détail sur le fonctionnement de chaque couche, il est utile de résumer la fonction de chacune (tableau 5) :

37 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/)

38 IEEE : Institute of Electrical and Electronics Engineers. C'est une association à but non-lucratif constituée de plus de 360 000 membres dans 175 pays, professionnels des technologies.

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

40 ITU : International Telecommunication Union. Basée 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.

41 OSI :Open System Interconnection

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 5: Le modèle ISO

Ce modèle est une normalisation dont les qualités sont indiscutables mais dont l'implémentation n'a pas connue le succès escompté. Au contraire, le protocole TCP/IP[42] s'est répandu dans le monde entier. Utilisé à l'origine sur le réseau ARPANet[43], sa simplicité de fonctionnement l'a rendu incontournable.

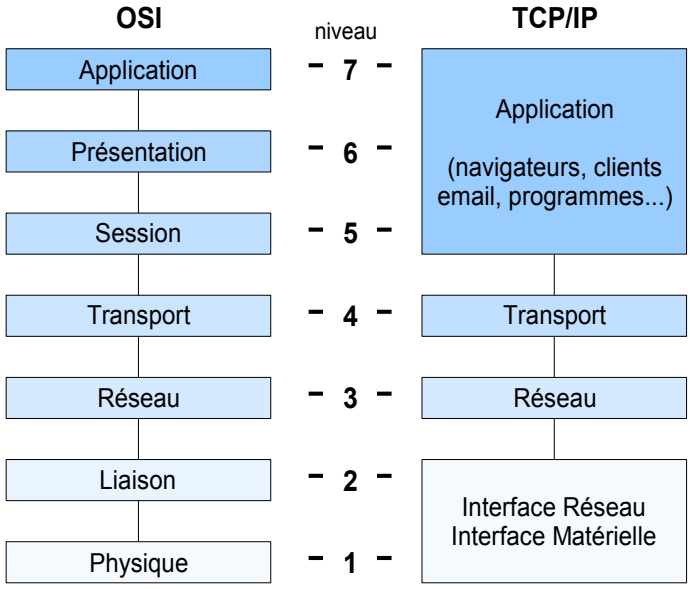


Illustration 15: Les couches OSI et TCP/IP

Sur l'illustration 15 [JLMO97], il est facile de voir que les deux modèles n'ont qu'une partie commune au niveau transport et réseau alors que les couches "liaison" (niveau 2) et "physique" (niveau 1) du modèle OSI sont mélangées sur le modèle TCP/IP. L'application se charge de la présentation et de l'établissement des sessions. L'intérêt de ces modèles en couches est que chaque couche est indépendante des autres : ainsi dans TCP/IP, le protocole IP (couche 3) est indépendant du matériel et média employé.

Le mode de développement de TCP/IP en a fait le protocole officiel d'accès au réseau Internet et aux réseaux locaux. Tous les systèmes d'exploitation permettant un accès réseau intègrent une pile TCP/IP : l'avantage de ce modèle est l'utilisation de 'socket' pour dialoguer entre machines ce qui permet aux programmeurs de ne pas avoir à gérer l'adressage ou le routage des messages dans leurs applications, ni même la retransmission de ceux-ci en cas d'erreur.

42 TCP/IP : Transmission Control Protocol / Internet Protocol
43 ARPANet : Advanced Research Projects Agency Network. Projet du DARPA lancé en 1967 et officialisé en 1972.

4.1.2 Normes communes

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

Les réseaux sans fil qui connaissent une croissance forte, bénéficient de l'expérience acquise dans le domaine filaire. L'intégration de ces équipements dans les réseaux filaires existants en est simplifiée. Les réseaux hertziens ont adopté les standards de communication des réseaux filaires pour améliorer la compatibilité et permettre une grande pénétration du marché à moindre coût.

4.1.2.1 Norme IEEE 802.1q

Le standard pour les LAN virtuels (VLAN ou Virtual LAN) a été défini 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 les débits diminuent.

La première solution pour segmenter un réseau est d'utiliser un routeur : chaque interface de cet équipement est reliée à un réseau différent. Pour déterminer si un message doit être retransmis d'une interface à une autre, le routeur utilise un masque de sous-réseau. Cette solution est coûteuse et prend du temps (le routeur doit traiter les trames de niveau 3).

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 bus du commutateur ayant un débit très largement supérieur au débit de chaque port, les machines semblent communiquer simultanément entre-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.

Toutefois, La solution la plus intéressante 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 VLAN :

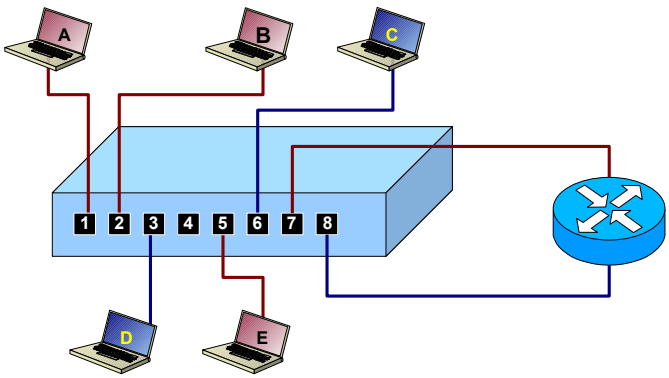


Illustration 16: Fonctionnement des réseaux locaux virtuels

Les machines A, B et E appartiennent à un même réseau virtuel (VLAN 10) tandis que les machines C et D sont dans un autre réseau virtuel (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 limitée aux seuls ports du VLAN défini : 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 VLAN 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 réseau virtuel de manière statique (configuré par un administrateur) ou dynamique (en fonction d'un nom de connexion par exemple).

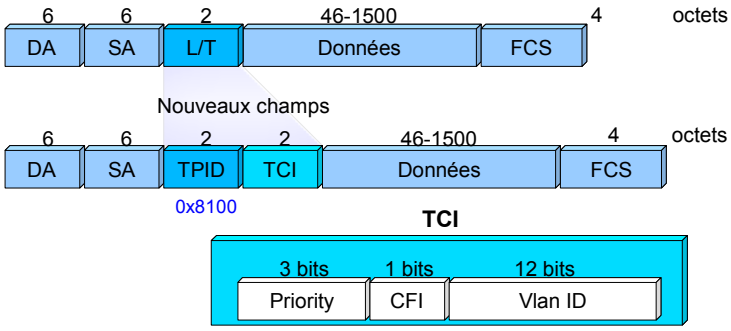


Illustration 17: Insertion champs VLAN dans une trame Ethernet

Pour ce faire, les commutateurs utilisent le "VLAN tagging" sur les trames de la couche deux du modèle OSI : 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 VLAN et de gérer en plus une qualité de service (QoS) codée sur 3 bits.

En effet, un autre avantage de 802.1q est d'être compatible avec la gestion de qualité de service du modèle DiffServ[44] et ainsi permettre l'utilisation des classes Premium (ou EF) aux applications de voix et de téléphonie : cette gestion de QoS est supérieure à la gestion TOS[45] d'origine.

Dans un environnement nomade, l'intérêt de ce standard est de fournir un accès à un utilisateur mobile entre plusieurs bâtiments : chaque commutateur connaît l'ensemble des VLAN du réseau et peut y placer un équipement client quelque soit sa localisation.

4.1.2.2 Norme IEEE 802.1x

802.1x est un protocole normalisé de niveau 2 intimement lié au protocole EAP[46] décrit plus loin. EAP est un ensemble de mécanismes d'authentification intégré au protocole PPP : le standard 802.1x étend donc l'utilisation d'EAP aux réseaux multipoints, notamment en bloquant tout trafic tant que l'authentification n'est pas acceptée sur le réseau.

Le protocole à l'origine de 802.1x est "EAP encapsulation Over LAN". Il implique l'intervention de trois acteurs :

- le client (ou supplicant) qui correspond à la machine désirant se connecter sur le réseau,
- le serveur d'authentification (ou authentication server) qui est l'équipement capable de traiter les requêtes d'authentification et de donner une réponse positive ou négative. Nous verrons plus tard qu'il a souvent d'autres fonctions associées,

44 DiffServ : Differentiated Services. RFC 2474 (Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers) et RFC 2475 (An Architecture for Differentiated Service).
45 TOS : Type Of Service. RFC 795 (Service mappings).
46 EAP : Extended Authentication Protocol.

- le point d'accès (ou authenticator), aussi appelé PA (ou AP pour Access Point), qui est l'équipement intermédiaire qui transforme des requêtes provenant du protocole 802.1x niveau 2) en requêtes IP (niveau 3).

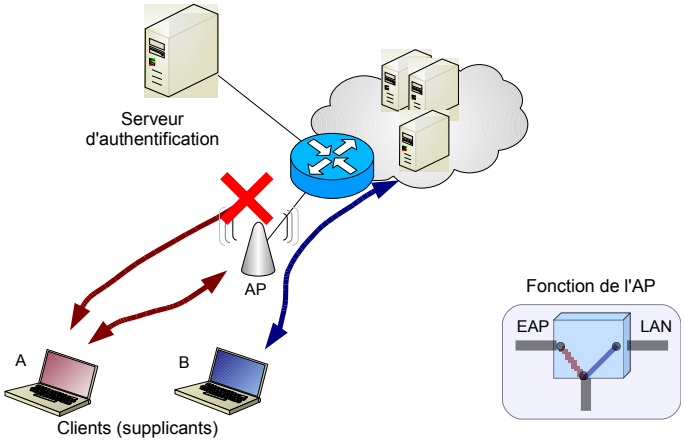


Illustration 18: Fonctionnement du protocole 802.1x

Par la suite, le standard 802.1x a été modifié pour s'adapter au protocole des réseaux sans fil 802.11 : en effet, le client et le point d'accès doivent d'abord être associés (équivalent de la couche physique) pour pouvoir utiliser des adresses MAC. Le protocole ainsi utilisé est appelé EAPOW pour "EAP encapsulation Over Wireless".

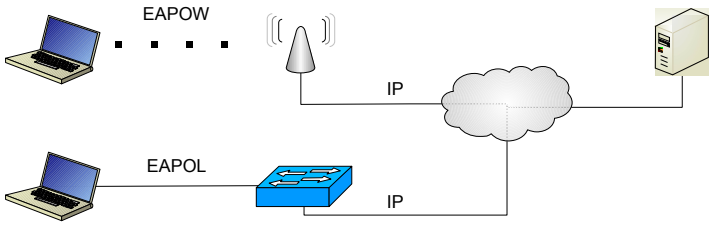


Illustration 19: Le standard 802.1x et ses protocoles

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 20, le client A ne peut émettre que des trames EAP tandis que le client B qui a été authentifié peut accéder normalement au LAN.

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 20) :

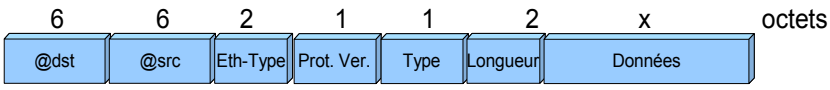


Illustration 20: Trame 802.1x

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.

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 convertis en attributs RADIUS puis encapsulés dans des datagrammes UDP.

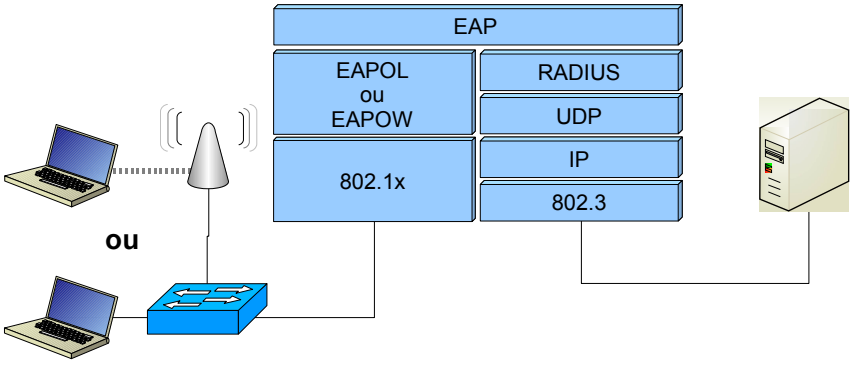


Illustration 21: Les couches EAP

Il est à noter que certains commutateurs et points d'accès ont la possibilité de placer un équipement ne sachant pas communiquer en EAP dans un VLAN défini (dans lequel le client pourra télécharger un client 802.1x par exemple).

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

4.1.3 Normes réseaux filaires

Les premiers réseaux comme ARPANET sont nés d'une structure filaire et les protocoles de communication s'appuient sur les caractéristiques propres à ces architectures. Les réseaux sans fil utilisent certaines propriétés des réseaux filaires mais ont dû trouver d'autres techniques pour adapter leur singularité.

Ce paragraphe présente donc les caractéristiques utilisées sur les réseaux filaires puis définit ensuite le fonctionnement des réseaux sans fil et leurs différences.

4.1.3.1 Réseaux point-à-point et multipoint

Ces deux modes de fonctionnement sont très différents :

- le mode point-à-point définit 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 utilisé les ports matériels série (RS-232). En IP, c'est le protocole PPP[47] qui est utilisé.
- Le mode multipoint implique plusieurs machines dans un ensemble de communication "un vers tous" ou "un vers un". Le protocole peut posséder d'autres caractéristiques et en particulier la notion d'adressage. La topologie peut varier mais dans tous les cas, plusieurs machines peuvent communiquer ensemble (et parfois en même temps).

47 PPP : Point to Point Protocol.

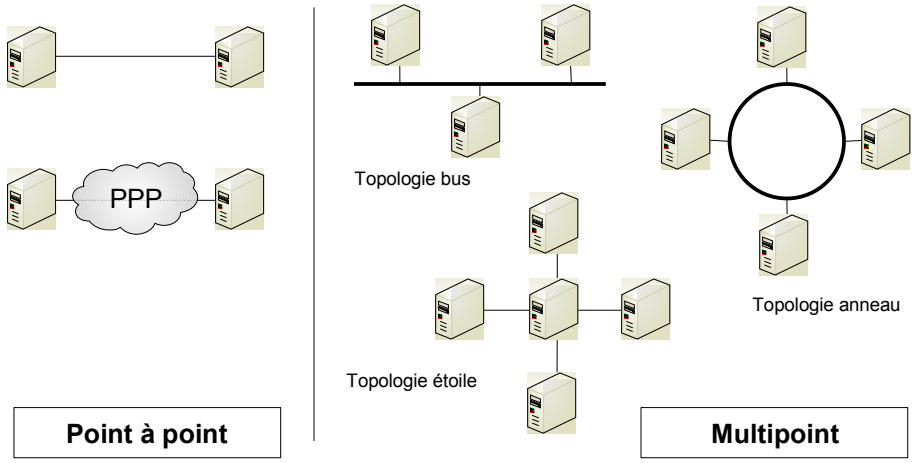


Illustration 22: Les topologies filaires

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 le remplir en y déposant son message et elle le videra 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 puis elle émet son message tout en écoutant le média (sur lequel circule son message). S'il y a une collision les machines émettrices s'arrêtent pendant un temps aléatoire.

La topologie en étoile implique le passage par un équipement capable de gérer les communications. Actuellement, les commutateurs sont les éléments centraux de cette topologie.

4.1.3.2 Ethernet

Connu sous les termes "standard *Ethernet"*, il fût établi par DEC, Intel et Xerox[48] à la fin des années 70, puis l'IEEE a repris cette spécification : désormais appelé 802.3, ce standard universel spécifie le mode de fonctionnement des réseaux utilisant CSMA/CD[49]. 802.3 désigne également un groupe de travail dont les recherches portent sur les techniques d'accès aléatoire (CSMA). Le standard IEEE 802.3 a donné naissance à la norme ISO 8802.3.

Les réseaux LAN connectent plusieurs équipements sur un même brin physique : il est nécessaire de trouver une méthode de communication permettant à tous d'émettre sans pour autant perturber les transmissions. La méthode employée dans les réseaux Ethernet est CSMA/CD. Elle est particulièrement adaptée aux réseaux cuivres et son fonctionnement est expliqué ci-après.

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

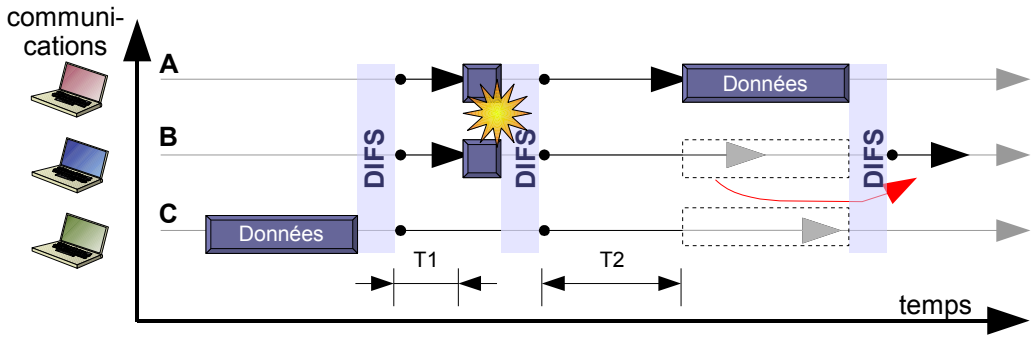


Illustration 23: Mécanisme CSMA/CD

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[50]. 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 n'est en cours, alors la station peut émettre son message. Toutefois, il peut arriver que deux stations décident d'émettre en même temps : dans ce cas, il y a une collision (illustration 23) !

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 délai DIFS pour recalculer leur compte à rebours (aussi appelé CW[51] 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.

4.1.3.3 Accès via réseau téléphonique

Les réseaux téléphoniques constituent parfois un prolongement du réseau de l'entreprise : un utilisateur peut se connecter depuis sa résidence à son réseau d'entreprise pour faire du travail à distance. Les personnes ayant des astreintes n'ont plus la contrainte de devoir se déplacer systématiquement pour diagnostiquer un problème ou surveiller un service. Ce type d'accès connaît une forte croissance avec l'arrivée de l'ADSL.

4.1.3.3.a RTC

RTC[52] 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 œuvre sur ce type de liaison. Il n'est pas possible de téléphoner en même temps que l'ordinateur est connecté.

4.1.3.3.b DSL

DSL[53] est une technologie apportant le haut débit numérique aux entreprises et aux particuliers. Via une simple ligne téléphonique, ADSL[54] permet de transporter des informations numériques à haut débit. De plus, l'emploi d'un filtre sur la prise téléphonique permet de conserver un téléphone analogique pour communiquer tout en étant simultanément connecté au réseau Internet.

50 DIFS : Distributed Inter Frame Space.
51 CW : Collision Windows ou fenêtre de collision.
52 RTC : Réseau Téléphonique Commuté.
53 DSL : Digital Subscriber Line.
54 ADSL : Asymetric Digital Subscriber Line.

Finalisé en 1995 par l'ITU sous le nom barbare G992.1, ce standard permet notamment le transport de données TCP/IP, X.25 et ATM.

4.1.4 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 sa longueur d'onde (un cycle complet), les propriétés de celle-ci varient : l'œil 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[55] allant de 11 000mm (30 Hz) à 17.2mm (20 kHz).

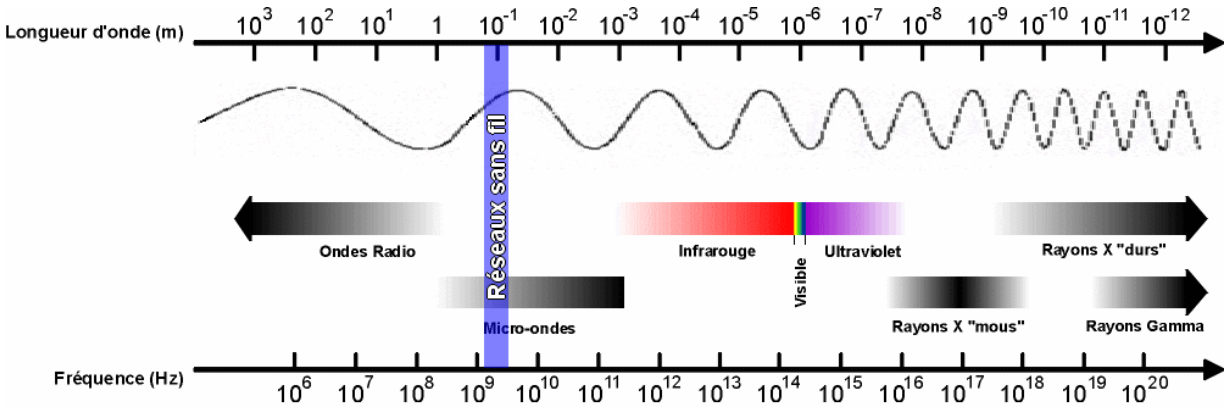


Illustration 24: Spectre de fréquences et longueurs d'ondes

Parmi les longueurs d'ondes présentées dans l'Illustration 24, 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 transmettre une quantité importante de données.

En effet, la longueur d'onde, la puissance, le débit et la portée sont étroitement liés. La longueur d'onde et la fréquence sont liées 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 seconde (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'informations, plusieurs techniques sont utilisables et notamment les modulations et les codages.

4.1.4.1 Modulations et codages

Il existe plusieurs types de modulation 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].

55 Les chiffres donnés 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.

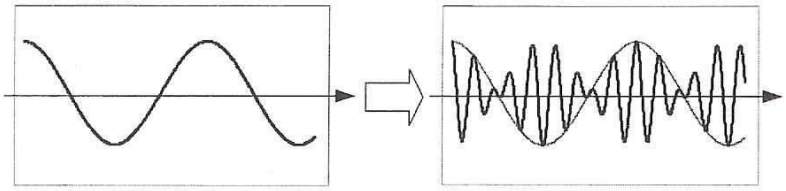


Figure 2.7 — La modulation d'amplitude.

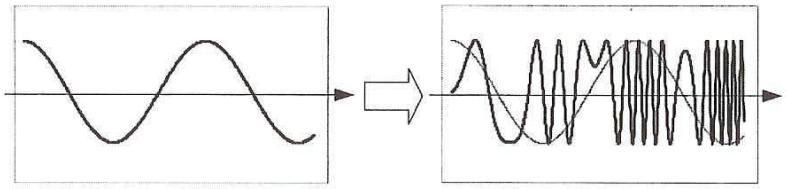


Figure 2.8 — La modulation de fréquence.

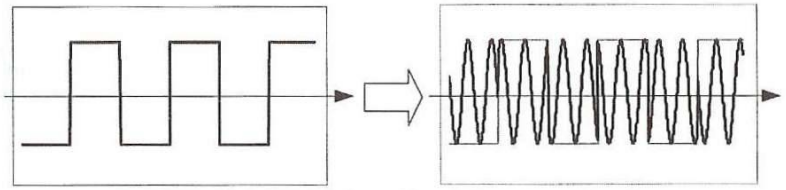


Figure 2.9 — La modulation de phase (plus claire avec un signal source carré).

Illustration 25: Les différentes modulations

Dans un environnement numérique, ces techniques sont utilisées sous les noms d'ASK[56] pour la modulation d'amplitude, FSK[57] pour la modulation de fréquence et PSK[58] pour la modulation de phase.

4.1.4.1.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 de faible puissance sont mélangées avec le bruit puisque leur valeur est proche de zéro.

4.1.4.1.b Modulation de fréquence (Frequency Modulation)

Plus efficace que la première méthode, la modulation de fréquence 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 pour les radios FM.

4.1.4.1.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.

Il existe une petite variation pour la modulation de phase qui est plus facile à mettre en œuvre pour la synchronisation entre l'émetteur et le récepteur : la modulation différentielle.

56 ASK : Amplitude Shifting Key.
57 FSK : Frequency Shifting Key.
58 PSK : Phase Key Shifting.

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.

4.1.4.1.d Modulations et 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 représenter un ensemble de bits (00, 01, 10 et 11) appelés symboles 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 dont la seule limite est le rapport signal/bruit : en effet, ce rapport varie fortement en fonction... de la distance.

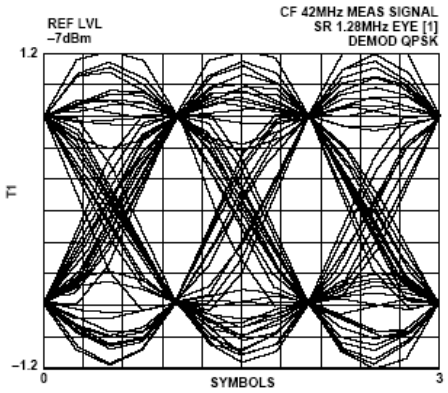


Figure 16. QPSK Modulation

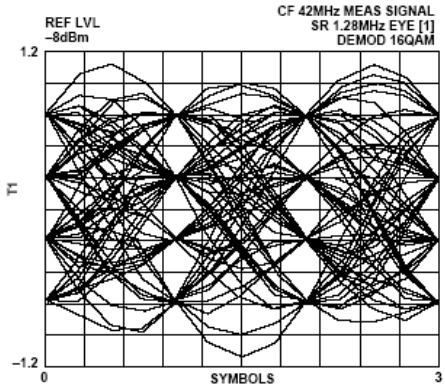


Figure 18. 16-QAM Modulation

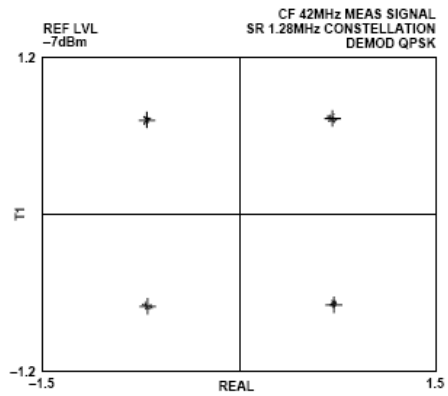


Figure 17. QPSK Modulation

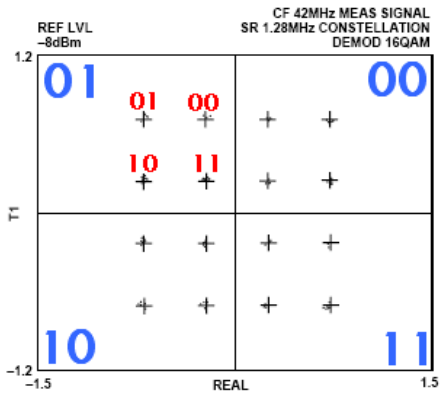


Figure 19. 16-QAM Modulation

Illustration 26: Extrait d'un datasheet d'un composant électronique

L'illustration 26 [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 (diagramme de droite) alors qu'il ne pourra prendre qu'une valeur codée sur 2 bits en QPSK (diagramme de gauche).

4.1.4.2 Distances et interférences

La puissance d'un signal émis est limitée à des normes strictes. Le débit varie donc en fonction de la distance (plus elle est élevée, plus le rapport signal/bruit est faible) et en fonction des interférences.

4.1.4.2.a Distances

L'illustration 27 [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 puissance du signal reçu, ce qui détermine le débit maximum théorique.

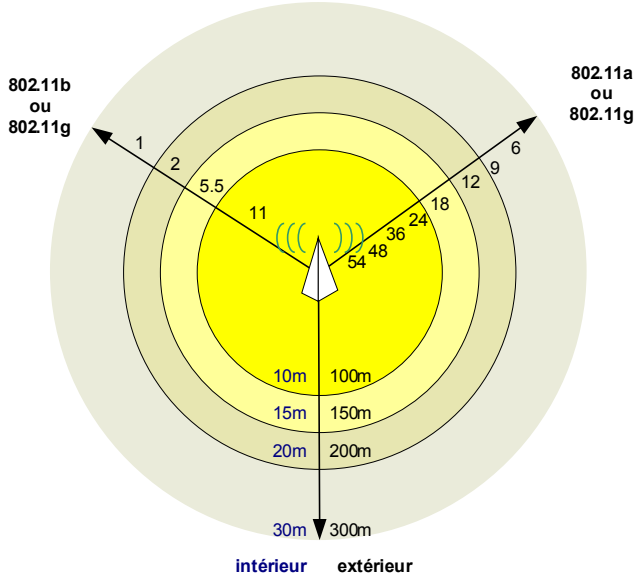


Illustration 27: Débits en fonction de la distance en 802.11

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

4.1.4.2.b Interférences

Le cas ci-dessus est bien sûr 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.

Pour chaque débit, la qualité du signal est classée de la manière suivante [MAPU04]:

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

Tableau 6: 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.

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.

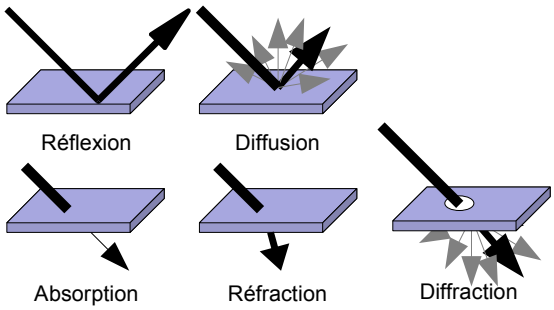


Illustration 28: Les différentes perturbations des ondes

Evidemment, 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 fréquences utilisée par de nombreux systèmes de communication.

4.1.4.3 Etalement de spectre

Afin de compenser les problèmes de perturbation, il existe plusieurs solutions dont les familles les plus connues sont FHSS[59] et DSSS[60]. Ces deux techniques impliquent toutefois que l'émetteur et le récepteur soient synchronisés sur une même séquence de code.

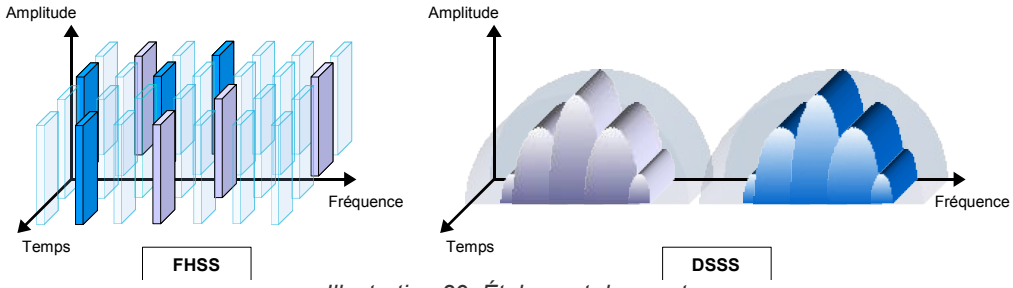


Illustration 29: Étalement de spectre

4.1.4.3.a FHSS

Le principe de FHSS est de changer la fréquence du signal porteur régulièrement. Ainsi, les informations à transmettre sont découpées dans le temps et dans les fréquences, d'où le nom de cette technique dite à "saut de fréquence". Chaque bande de fréquence employée est la plus étroite possible (illustration 29). Le choix de la fréquence suivante est lié à un code partagé entre l'émetteur et le récepteur et qui correspond à un canal de communication. Si une fréquence est parasitée, seule une petite partie de l'information sera retransmise.

4.1.4.3.b DSSS

DSSS en revanche utilise une bande de fréquence beaucoup plus large pour un même canal car le signal utile est étalé par un code qui module l'information à envoyer. Ce code de plusieurs bits toujours identiques module chaque bit de données. C'est pourquoi Il est nécessaire d'étendre la bande passante pour transmettre les données : l'intérêt de cette technique est qu'elle est peu sensible au bruit (sur l'ensemble de la bande occupée) et aux parasites sur une fréquence étroite car le signal utile est répété sur plusieurs harmoniques. L'annexe 7.4 présente la forme d'onde exact générée par l'étalement de fréquence DSSS.

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

4.1.4.4 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].

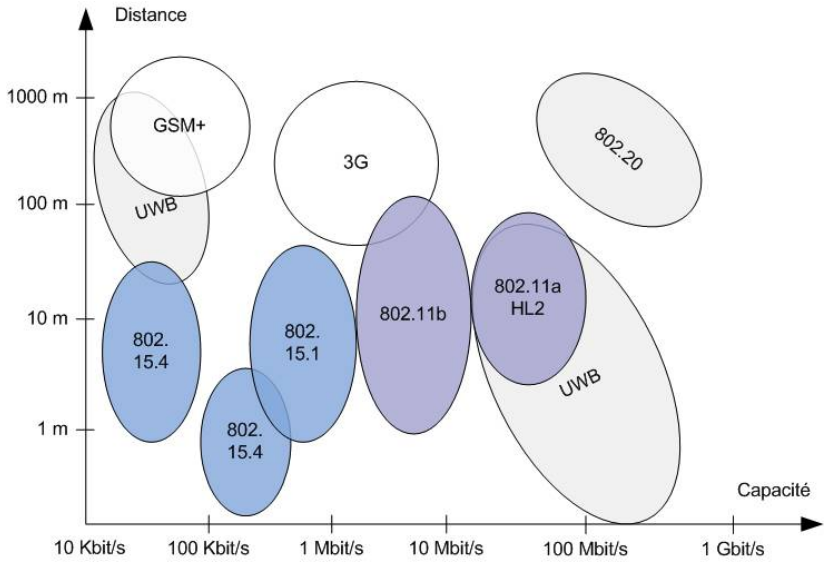


Illustration 30: Les différentes familles de réseaux sans fil

Les standards utilisés par la téléphonie classique comme DECT, GSM, GPRS, UMTS et 3G ne sont pas abordés dans ce rapport, le sujet traitant essentiellement des réseaux IP.

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

Illustration 31: Logo Wi-Fi, BlueTooth et Wi-Max

Les différents groupes de travail de l'IEEE 802 qui œuvrent sur les réseaux sans fil n'ont pas les mêmes objectifs. C'est pourquoi on trouve plusieurs normes différentes dont les caractéristiques se complètent. Ainsi les normes 802.11, 802.15 et 802.16 ont chacune un champ d'application particulier :

- 802.11 est orientée 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). Elle est communément appelée "Wi-Fi" (à tort).
- 802.15 est utilisée pour relier des équipements de proximité entre eux : appareils photos, souris et claviers sans fil. Il s'agit donc de pico-réseaux. Là encore l'appellation commerciale "BlueTooth" est plus connue.
- 802.16 vise les réseaux MAN haut débit : il pourrait même compléter l'ADSL dans certaines zones. Son appellation commerciale est "Wi-Max"

Seule la norme 802.11 est décrite dans ce rapport car ses spécifications la rendent incontournable pour les réseaux locaux sans fil de demain (WLAN[61])...

61 WLAN : Wireless Local Area Network (réseau local sans fil).

4.1.4.4.a Généralités sur le standard 802.11

Ce groupe travaille sur le standard 802.11 qui est le plus connu car sa pénétration du marché des entreprises et des particuliers est très forte. Ses principaux avantages sont la portée importante et le débit équivalent ou supérieur à une liaison ADSL. De nombreux équipements pour les particuliers associent une liaison ADSL, des prises 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 équipements certifiés Wi-Fi doivent préciser les normes supportées : 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 7: Les amendements du standard 802.11

La Wi-Fi alliance s'appuie sur ces standards pour proposer la certification d'équipements réseaux sans fil.

4.1.4.4.b Spécifications du standard 802.11

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

- 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 destinataire) l'ont rendu caduque par les modes utilisant les ondes radios.

Le tableau ci-après résume les différences entre les 3 méthodes de transmission 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 8: 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 ainsi qu'une bande de fréquence différente et ne peut donc pas communiquer directement avec des équipements 802.11b/g.

D'autre part, les fréquences employées par ces équipements font l'objet d'une régulation par l'ART[62]. En premier lieu, les fréquences employées font parties de la bande ISM[63]. La puissance d'émission des équipements est soigneusement limitée en fonction du lieu d'utilisation (intérieur ou extérieur) et de la fréquence (voir annexe 7.2)

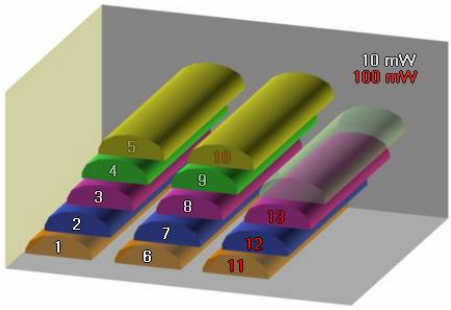


Illustration 32: Chevauchement des fréquences en 802.11b/g

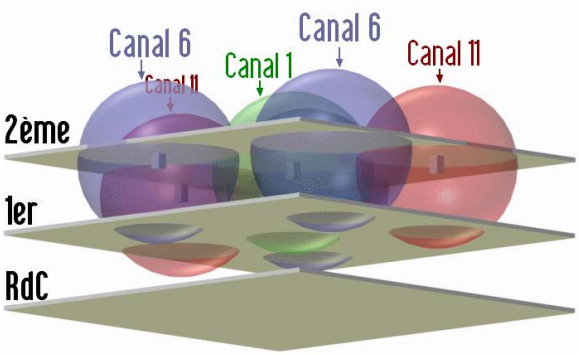
Les équipements 802.11b et 802.11g utilisent une gamme de 13 canaux en Europe (il existe d'autres gammes en Amérique et au Japon). Pour permettre l'extension de la zone de couverture du réseau tout en évitant que les signaux ne s'annulent, il est obligatoire de choisir des canaux suffisamment éloignés dans les fréquences. Malheureusement, les canaux concomitants se chevauchent comme l'illustre la figure ci-dessous.

Dès lors, le déploiement d'un ensemble de points d'accès doit éviter ces recouvrements sinon la qualité des signaux sera perturbée : 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) générant le minimum de perturbation.

En effet, une propriété importante des ondes est qu'elles se déplacent dans tous les sens (sauf en utilisant une antenne directionnelle). Il faut donc prendre en compte l'espace dans ses trois dimensions comme le montre l'illustration 33.

62 ART : Autorité de Régulation des Telecoms (http://www.art-telecom.fr/). Désormais appelée 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. Lorsque le Parlement adopte la Loi relative à la régulation des activités postales (JO du 21 mai 2005) l'ART devient alors l'ARCEP.

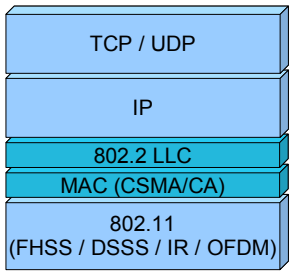
63 ISM : Industrial, Scientific and Medical.



4.1.4.4.c Fonctionnement du standard 802.11

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

- La couche 802.2 LLC est identique à celle utilisée sur les réseaux Ethernet. Il est donc possible de relier un réseau WLAN[64] sur tout réseau local respectant les standards de l'IEEE.
- La couche MAC 802.11 : spécifique au standard 802.11, elle ressemble à la couche MAC du standard 802.3 pour la partie écoute de la porteuse avant émission (fonction CSMA).



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

- Mode ad hoc : non sécurisé, l'association à ce type de réseau est très facile. C'est un mode souple pour échanger des fichiers entre deux machines. Un ensemble de machines dialoguant dans ce mode forme un IBSS[65]. Toutefois, ce mode est à bannir en entreprise car trop accessible.
- 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[66] et n'implique qu'un point d'accès isolé. Lorsque les points d'accès peuvent dialoguer ensemble (par le LAN ou via une connexion sans fil), l'architecture ainsi formée est appelée ESS[67].

64 WLAN : Wireless LAN. Réseau local sans fil.
65 IBSS : Independant Basic Service Set.
66 BSS : Basic Service Set.
67 ESS : Extended Service Set

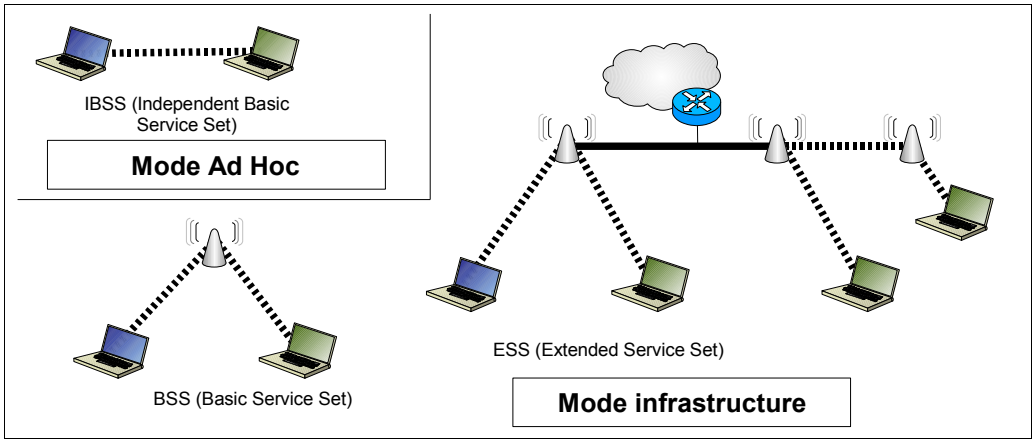


Illustration 35: Les différents modes de connexion 802.11

En terme de sécurité, il est important d'utiliser un mode infrastructure mais il faut également prévoir la sécurisation des communications entre points d'accès. En effet, une attaque propre à la structure choisie (AP en mode répéteur relié par un commutateur commun) peut conduire à ce que deux terminaux puissent communiquer entre eux directement. Il faut donc activer les fonctions de protection prévues à cet effet (illustration 36).

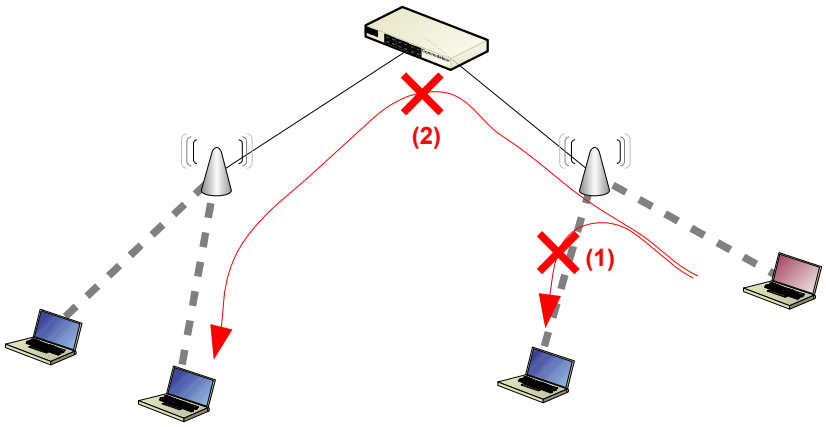


Illustration 36: Protection de communication entre les points d'accès

Lorsque plusieurs points d'accès ayant le même SSID[68] couvrent le lieu où se trouve l'utilisateur, c'est la machine de celui-ci qui choisit sur quel AP elle va se connecter et si le rapport signal/bruit de son AP devient trop faible, d'en changer. C'est un "handover".

Toutefois la norme 802.11 n'intègre pas un "handover" identique à celui des réseaux téléphoniques mobiles : en réalité, une trame de dé-association est d'abord émise à destination de l'AP d'origine. Ensuite une requête de ré-association est envoyée au nouvel AP : elle contient l'identité de l'ancien point d'accès, permettant ainsi aux deux AP de se mettre en relation pour se transmettre des informations et éventuellement les paquets en attente. Ce mécanisme de "handover" dure moins d'une demi-seconde et dans ce cas, la machine ne change pas d'adresse IP (en téléphonie mobile, il n'y a pas de dé-association tant que la ré-association n'est pas faite).

Le mécanisme appelé "roaming" est quant à lui plus complexe car il implique que la machine puisse changer d'adresse IP en changeant de réseau, ce qui est plus long.

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

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. Le cas de la "station cachée" correspond à deux stations hors de portée l'une de l'autre qui émettent en même temps vers le point d'accès commun : aucun des émetteurs ne peut détecter la collision.

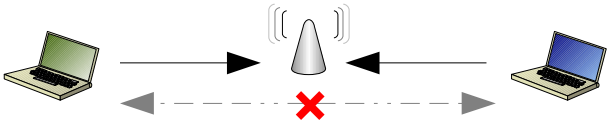


Illustration 37: Problème de détection de collision en 802.11

C'est donc le protocole CSMA/CA[69] qui est employé [MAPU04]. Il existe plusieurs modes de fonctionnement mais le mode DCF[70] est le plus classique (par opposition au mode PCF[71] 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 :

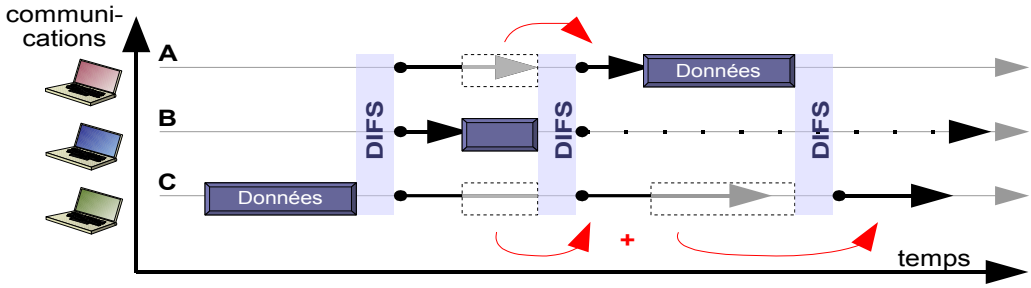


Illustration 38: Fonctionnement de CSMA/CA

Chaque équipement attend après un silence, un délai fixe appelé DIFS[72]. 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[73] puis attend un délai fixe SIFS[74] (bien plus court que le DIFS, ce délai n'est utilisable que par le destinataire du CTS[75]) : 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 de la part du récepteur pour pouvoir émettre ses données.

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

- Pour les données de petites tailles (généralement inférieures à 1000 octets), le standard 802.11 accepte qu'elles soient transmises dans la trame RTS.
- Le mode PCF a été défini dès le début du standard 802.11 (1997) mais les premiers équipements qui implémentent ce mode existent depuis 2002 seulement. De plus, il n'est pas obligatoire et ne fait pas parti des tests de certification Wi-Fi [GERO04].
- Pour que les stations ne pratiquant pas le mode PCF puissent communiquer, la norme 802.11 impose que ce mode soit toujours alterné avec le mode DCF.

69 CSMA/CA : Carrier Sense Multiple Access / Collision Avoidance.
70 DCF : Distributed Coordination Function. Mode du CSMA/CA.
71 PCF : Point Coordination Function. Mode du CSMA/CA de type Contention Free (libre de toute dispute).
72 DIFS : Distributed Inter Frame Space.
73 RTS : Request To Send.
74 SIFS : Short Inter Frame Space.
75 CTS : Clear To Send.

Une attention particulière doit donc être apportée sur les connexions de clients sur un même point d'accès. En effet, l'association de machines utilisant le même standard mais à des distances différentes peut faire chuter dramatiquement les débits notamment pendant les phases en mode DCF qui ne répartit pas équitablement les temps de communication.

Le tableau suivant [IMAG01] fait apparaître une faiblesse du standard 802.11b (en mode DCF), confirmée 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 9: Débits constatés 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, il n'est pas toujours correctement implémenté. Il vaut mieux lui préférer la norme 802.11e qui reprend et améliore les deux modes DCF et PCF (qui deviennent EDCF et EPCF ou HCF[76]) et permet de gérer la qualité de service.

4.2 Sécurité

Le fait de pouvoir transmettre un message de manière sécurisée a été mis en exergue par les militaires. Le premier a avoir codé des messages serait Jules César avec un décalage de lettres 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"[77] : 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 alliées.

Loin de ces points d'histoire, la sécurité informatique est définie par cinq types de service :

- Confidentialité : la sécurité doit assurer la protection des données et assurer que celles-ci ne puissent pas être lues 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 points précédents pour garantir que les données émises par un utilisateur authentifié n'ont 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 garanti.

Ces cinq services utilisent généralement des propriétés mathématiques permettant le chiffrement et ainsi masquer les informations sensibles. La bonne compréhension des méthodes de chiffrement est nécessaire car 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 également les mécanismes de chiffrement et d'authentification.

76 HCF : Hybrid Coordination Function
77 Voir le site http://lwh.free.fr/pages/algo/crypto/enigma.htm

4.2.1 Chiffrement

Il existe deux familles d'algorithmes de chiffrement : les algorithmes symétriques (dits à clé secrète) et les algorithmes asymétriques (dits à clé publique).

4.2.1.1 Algorithmes à chiffrement symétrique

Les algorithmes à chiffrement symétrique sont généralement plus rapides 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. Les algorithmes RC4, DES et Triple DES, AES appartiennent à cette famille.

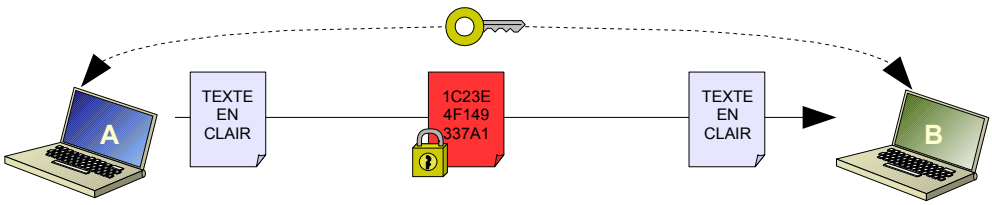


Illustration 39: Fonctionnement d'un algorithme de chiffrement symétrique

4.2.1.1.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 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. Toutefois, une mauvaise implémentation de cet algorithme peut l'affaiblir : c'est le cas du protocole de sécurité WEP[78]. Une valeur de clé commençant par "00 00 FD" à 14% de chance de produire une sortie commençant par "00 00". Ce sont des clés faibles.

4.2.1.1.b DES

DES (Data Encryption Standard) a été adopté en 1978 par le NBS[79] (devenu depuis, NIST[80]). Cet algorithme est basé sur le travail d'IBM (algorithme 'Lucifer') et modifié par la NSA[81]. DES (aussi connu sous le nom de DEA ou norme ANSI X3.92) répond aux critères suivants [WEB002]:

- haut niveau de sécurité lié à une clé de petite taille servant au chiffrement et au déchiffrement,
- compréhensible,
- indépendant de la confidentialité de l'algorithme,
- adaptable et économique,
- efficace et exportable.

78 WEP : Wired Equivalent Privacy.
79 NBS : National Bureau of Standards.
80 NIST : National Institute of Standards and Technology.
81 NSA : National Security Agency.

C'est un algorithme de type symétrique et de chiffrement par bloc (bloc cipher). 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). Il existe seulement 4 clés faibles connues, ce qui permet de les éviter.

Bien que très robuste en son temps, une évolution a été nécessaire et a donné naissance au 3DES (triple DES ou ANSI X9.52). La méthode 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 : mais la résistance reste faible pour les deux premiers chiffrements, de l'ordre de 2^{57} et c'est le troisième qui va rendre l'ensemble robuste.

Toutefois, le triple DES est désormais considéré comme n'étant plus assez fiable : sa résistance est équivalente à 2^{112} possibilités au lieu de 2^{168}, à cause de sa sensibilité au mode d'attaque "rencontre au milieu"[82] et malgré une clé finale de 3x56 bits (168 bits).

4.2.1.1.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 longueurs de clé et longueurs 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 pour chiffrer, ne consomme pas beaucoup de mémoire et son implémentation est vraiment aisée. On le trouve désormais dans les équipements supportant la norme 802.11i.

Il utilise des fonctions de substitution, de permutation, de combinaison linéaire et d'algèbre booléenne (OU exclusif). 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 des attaques par dictionnaires de 3DES et AES se trouve sur le site www.securiteinfo.com[83].

4.2.1.2 Algorithmes à chiffrement asymétrique

Par opposition, les algorithmes à chiffrement asymétrique sont moins rapides mais ils disposent d'un avantage important : 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 ces algorithmes 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.

82 http://fr.wikipedia.org/wiki/Cryptanalyse#Attaque_par_rencontre_au_milieu
83 http://www.securiteinfo.com/crypto/aes.shtml

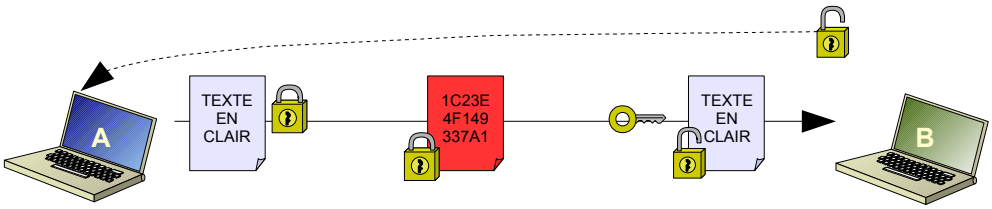


Illustration 40: Fonctionnement d'un algorithme de chiffrement asymétrique

Le schéma ci-dessus est une métaphore : le destinataire (B) fournit un cadenas (clé publique) 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 car la clé privée n'est jamais transmise évitant ainsi d'être compromise.

4.2.1.3 Fonctions de hachage et de signature

4.2.1.3.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 à partir du résultat, ces algorithmes sont généralement utilisés conjointement à d'autres méthodes de chiffrement ou bien en système de contrôle (un peu plus efficace que le traditionnel CRC[84]).

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 également l'empreinte pour que l'utilisateur puisse s'assurer avoir copié le programme original (sans code ajouté).

L'intérêt de ces mécanismes est que, utilisés conjointement à un mécanisme de chiffrement, ils sont capables de garantir l'intégrité des données contenues dans un message. En effet, si le hachage ne permet pas la modification du message sans fournir un résultat différent, rien n'empêche une personne malveillante de générer une nouvelle clé de hachage.

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

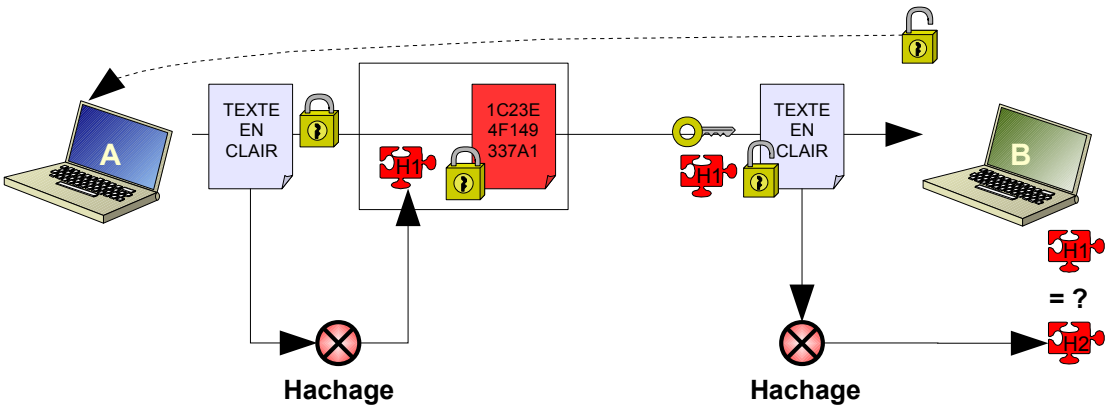


Illustration 41: Fonctionnement d'un mécanisme de hachage

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

84 CRC : Cyclic Redundancy Check. Contrôle de redondance cyclique.

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

Les algorithmes les plus utilisés sont MD5 (Message Digest 5) qui crée une empreinte sur 128 bits et SHA-1 qui crée une empreinte de 160 bits. La taille des empreintes est importante car la protection offre 2^n possibilités. En revanche, le message haché n'a pas de taille fixe et comme il existe une infinité de messages possibles, 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 message pirate soit cohérent pour que le récepteur puisse être abusé : recevoir un message intègre contenant une suite de lettres ou de mots incohérents 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 retransmis (la clé de hachage pouvant être refaite par le pirate). Il faut alors utiliser une méthode d'authentification forte : la signature électronique.

4.2.1.3.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 de multiples clés publiques pour une seule clé privée et chacune est capable de déchiffrer un message codé avec la clé privée. 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 les déchiffrer. Cette faiblesse devient pourtant un avantage pour la signature électronique.

Elle assure en effet au destinataire que l'information a été chiffrée uniquement par le possesseur de la clé privée : 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.

4.2.2 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 (plus long en terme de calcul qu'un chiffrement symétrique). Elle est majoritairement basée 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 œuvre 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[85] mais aussi des systèmes utilisant des certificats.

Le déploiement de ces solutions est généralement rendu nécessaire pour sécuriser les accès aux réseaux et aux différents services dont les données sont critiques (messageries, bases de données, serveurs critiques, comptabilités, laboratoires de recherche...) cela rend l'administration des authentifications et autorisations difficile. Toutefois, il existe des systèmes et des structures capables de simplifier cette gestion de contrôle des accès.

4.2.2.1 Différentes méthodes d'authentification

Pour être authentifié, il faut pouvoir fournir une preuve de son identité : cette preuve peut prendre plusieurs formes mais est basée sur la propriété d'unicité liée 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.

85 OTP : One Time Password.

4.2.2.1.a Mot de passe

Actuellement, tout utilisateur 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 (pour l'accès par un FAI[86] en RTC ou ADSL par exemple). 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 limitée : il n'est donc pas rare que les systèmes de sécurité appliquent des règles pour en vérifier la validité. De plus, il est fortement recommandé de les changer régulièrement.

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

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

Lors de l'authentification sur un système, il suffit 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).

L'avantage de l'authentification par mot de passe unique est que le mot de passe transitant sur le réseau ne fonctionne qu'une fois ce qui rend inutile l'écoute et la récupération.

4.2.2.1.c Biométrie

Très médiatisée (cf. l'information à l'aéroport de Roissy[87]) la biométrie se base sur un trait unique de la morphologie humaine : empreinte digitale, iris de l'œil, 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). Certaines technologies sont jugées trop intrusives (empreinte rétinienne nécessitant l'utilisation d'un rayon lumineux pour éclairer le fond de l'œil).

4.2.2.1.d Carte à puce

La carte à puce a connu 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 le résultat de la comparaison (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 mais connue du centre bancaire) et qu'elle retourne à la banque (via le terminal) [WEB003]

86 FAI : Fournisseur d'Accès Internet.

87 Article : http://www.01net.com/editorial/279577/identite-electronique/la-biometrie-debarque-a-l-aeroport-de-roissy/ (01Net du 30/05/2005)

4.2.2.1.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 en lequel ils ont confiance. Bien entendu, tous les éléments de la chaîne doivent utiliser le même standard.

4.2.2.2 Autorisation et traces (AAA)

Les systèmes dit "AAA"[88] sont capables de gérer l'authentification mais aussi les autorisations et les traces des utilisateurs. Ils sont très utilisés dans le domaine des télécommunications. L'authentification est relativement complexe à mettre en œuvre mais elle permet de donner l'accès à un ensemble de ressources et de services. Même si cette gestion reste simple sur un réseau unique, elle devient critique sur un ensemble de réseaux gérés par différents organismes. Le cas typique en télécommunication est celui des opérateurs (FAI) : ils ne peuvent pas couvrir l'ensemble du territoire avec leur propre infrastructure (POP[89]) et doivent passer des accords avec d'autres fournisseurs. L'utilisateur doit être authentifié par son fournisseur tout en se connectant sur l'équipement d'un autre fournisseur.

4.2.2.2.a Architecture AAA

Pour cela, il existe deux fonctionnements possibles :

- Dans le cas d'une transaction 'hop-to-hop' (point-à-point), chaque serveur connaît 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 transitives ce qui implique qu'aucun serveur ne puisse "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.

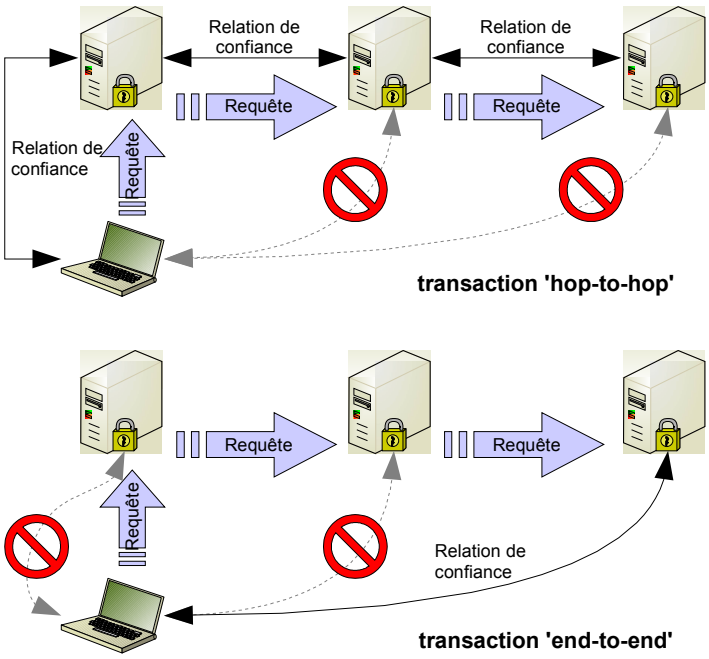


Illustration 42: Les deux modèles d'architecture AAA

88 AAA : Authentification, Autorisation and Accounting.
89 POP : Point Of Presence.

4.2.2.2.b Gestion de droits et journalisation

Une fois l'authentification effectuée, l'utilisateur se voit affecter des droits. De plus, pour des questions de répartition de coûts, la durée de la connexion ou de la session est consignée dans un journal : c'est l'accounting ou la comptabilisation. Ces deux fonctions font parties intégrantes des systèmes AAA :

- les autorisations sont centralisées sur le serveur AAA, ainsi tout accès à un service ou un serveur sera identique quelque soit la localisation,
- la comptabilisation (traçage) permet la facturation des services utilisés. De plus, une utilisation frauduleuse du réseau ne reste pas anonyme.

Toutefois, dans le cas où un utilisateur accède à un point d'accès ne supportant pas les services requis, il est possible de refuser l'ouverture de la session afin de ne pas facturer le client pour un service qu'il n'a pas eu. C'est pourquoi les systèmes AAA peuvent échanger des informations lors des requêtes d'authentification. Le protocole le plus répandu capable de supporter ces fonctionnalités est RADIUS.

4.2.2.2.c RADIUS

Le protocole RADIUS[90] (RFC 2138 et RFC 2139) 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". Il présente donc des faiblesses qu'il convient de bien connaître. La liste ci-dessous énumère les principales faiblesses [HASS02] :

- En terme de sécurité, les requêtes émises peuvent transiter par plusieurs serveurs relais et chaque serveur voit passer la requête complète. Ce mode point-à-point pour les serveurs RADIUS rend ce protocole vulnérable à certaines attaques (RFC 2607[91]).
- Les spécifications du protocole n'imposent 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 d'état), 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 performance ou pire, des pertes de données. L'IESG[92] explique même en en-tête de la RFC que c'est parce que RADIUS ne gère pas les contrôles de congestion, et conseille de suivre le groupe AAA de l'IETF sur la progression d'un successeur.

RADIUS n'est pas idéal mais est pour le moment la seule norme existante : le protocole DIAMETER (qui est une refonte de RADIUS) n'est qu'au stade embryonnaire et les autres protocoles (comme TACACS+) sont des solutions propriétaires.

90 RADIUS : Remote Authentication Dial In User Service.
91 RFC 2607 : http://www.faqs.org/rfcs/rfc2607.html
92 IESG : Internet Engineering Steering Group.

4.2.2.3 Structure d'autorité de certification

Pour résoudre les problèmes d'authentifications multiples et valider la distribution des clés publiques, une idée simple est de fournir un objet normalisé contenant des informations précises, secrètes et inviolables. Cet objet est un certificat et représente une identité unique. Pour les gérer, il existe un modèle de structure assez répandu abordé ici.

Avant de décrire l'architecture d'une Infrastructure de Gestion de Clés (IGC) ou en anglais "Public Key Infrastructure" (PKI), nous allons voir l'utilité de cette structure. Le rôle d'une IGC est de garantir à tout instant que l'identité présentée dans un certificat est bien valide et reconnue. En accordant sa confiance à une IGC, un organisme accepte tous les certificats gérés par cette IGC. Elle est donc un élément déterminant de la sécurité d'un organisme.

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[93]. L'apparition d'un cadenas dans la barre d'état des navigateurs (IE, Firefox, Opera, Maxthon, etc.) indique qu'un échange SSL est en cours avec un site de confiance.

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

Illustration 43: Symbole cadenas pour le protocole HTTPS (navigateur IE 6)

En effet, un certificat est délivré par une entité digne de confiance : l'autorité de certification. Celle-ci est reconnue par une communauté d'utilisateurs 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 utilisée par un destinataire pour renvoyer des données chiffrées, lisibles uniquement par le propriétaire du certificat),
- signature de l'autorité de certification.

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

Une structure générique (mais pas complète) est présentée dans l'illustration ci-dessous :

93 SSL : Socket Secure Layer.

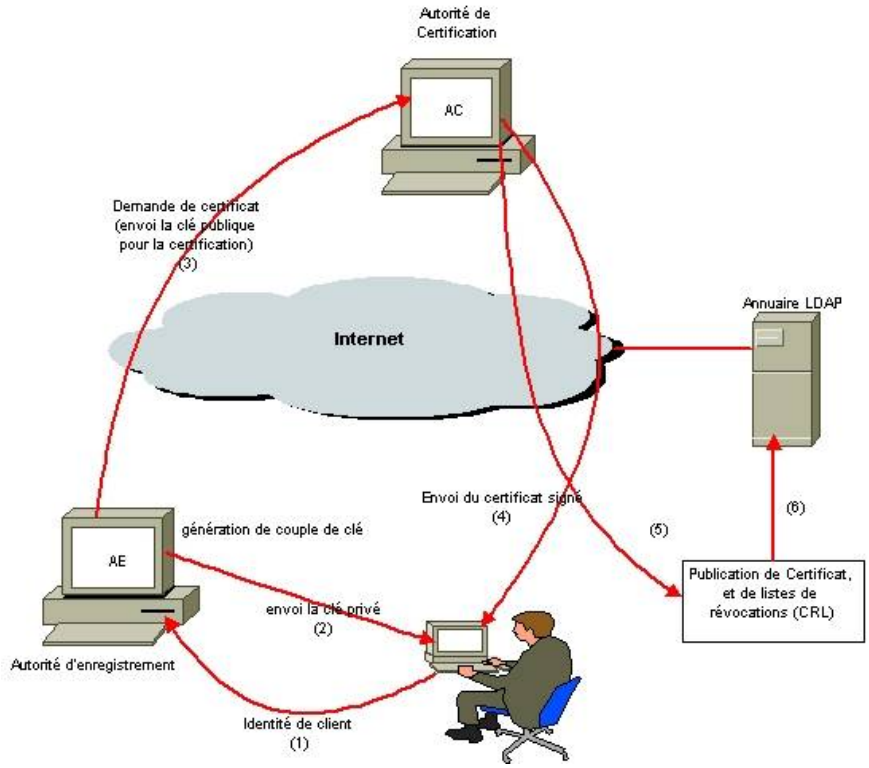


Illustration 44: Structure typique d'une IGC (cf. www.securiteinfo.com)

L'IETF définit – pour une IGC complète – 5 entités distinctes dont les noms et les rôles sont :

- L'Autorité de Certification (AC ou CA) qui a pour mission de signer les demandes de certificat[94] et de signer les listes de révocation[95], cette autorité est la plus critique.
- L'Autorité d'Enregistrement (AE ou RA) qui a pour mission de générer les demandes de certificat, et d'effectuer les vérifications d'usage sur l'identité de l'utilisateur final (les certificats numériques doivent être nominatifs et uniques pour l'ensemble de l'IGC).
- L'Autorité de Dépôt (Repository) qui a pour mission de stocker les certificats numériques ainsi que les listes de révocation.
- L'Autorité de Séquestre (AS ou KE pour Key Escrow), qui a un rôle particulier. En effet lorsqu'on génère des certificats de chiffrement, on a l'obligation légale de fournir aux autorités un moyen de déchiffrer les données chiffrées pour un utilisateur de la PKI. C'est là qu'intervient le Séquestre, cette entité a pour mission de stocker de façon sécurisée les clés de chiffrement qui ont été générées par la PKI, pour pouvoir les restaurer le cas échéant.
- L'Entité Finale (EE) est optionnelle, cette entité est en charge d'enregistrer les nouveaux utilisateurs finaux.

Les systèmes techniques des IGC s'appuient généralement sur le standard PKCS[96] qui est composé de 15 standards décrits en annexe.

La mise en œuvre d'une IGC est un projet important dans une organisation car il dépasse le cadre technique des projets classiques : il implique une gestion administrative, une politique de certification et un cadre d'assurance qualité... peu d'entreprises ou d'organismes ont franchi le pas pour le moment ! [MISC13]

94 CSR : Certificate Signing Request.
95 CRL : Certificate Revocation List..
96 PKCS : Public Key Cryptography Standards.

4.2.3 Tunnels et Réseaux Virtuels Privés

Plusieurs méthodes de transport sécurisé de données existent, chacune ayant ses avantages et inconvénients. Les plus connues sont SSL, IPSec et désormais WPA. Elles sont parfois complémentaires et utilisent toutes au minimum un mécanisme d'authentification et un mécanisme de chiffrement tels que décrits dans le chapitre précédent. Abordons maintenant leurs implémentations les plus connues.

4.2.3.1 SSL, TLS et SSH (Secure SHell)

SSL[97] et SSH[98] sont deux protocoles différents mais leur abréviation se ressemblant, nous avons choisi de les traiter ensemble pour éviter les confusions plus tard. TLS[99], dont l'abréviation est totalement différente est en revanche un synonyme de SSL.

4.2.3.1.a SSL/TLS

SSL est un protocole de sécurisation inventé en 1994 par Netscape Communication. Repris par l'IETF, son nom est devenu TLS (RFC 2246). Son application la plus connue est la sécurisation de sites web. Il est pourtant utilisé pour sécuriser d'autres protocoles : HTTPS (443), NNTPS (563), LDAPS (636), FTPS(989 pour les données, 990 pour le contrôle), TELNETS (992), IMAPS (993), POP3S (995).

SSL est un VPN de niveau 4 (Transport) ce qui limite sa souplesse aux applications le gérant [MISC10] contrairement à d'autres VPN de niveau 3 qui s'appuient sur le réseau (niveau 3). Il utilise généralement les combinaisons de mécanismes de chiffrement et d'authentification suivants :

- chiffrement : 3DES, FORTEZZA, IDEA, RC4, DES (le nombre de bits employés dépend de la législation locale),
- intégrité : MD5 (16 bits) et SHA-1 (20 bits),
- authentification : certificats X.509 et mécanisme MAC[100] (fonction HMAC, RFC 2104).

SSL/TLS est donc capable de générer un tunnel pour faire transiter de l'information.

4.2.3.1.b SSH

SSH a été mis au point en 1995 par le Finlandais Tatu Ylönen. Il fonctionne de la même manière que SSL/TLS en créant un tunnel IP (protocole TCP, port 22). Il est toutefois plus utilisé en remplacement de programme d'accès à distance à un système tel que Telnet, rsh, rlogin et rexec : ces programmes transmettent les données de l'utilisateur en clair sur le réseau ce qui rend le système vulnérable à de simples "écoutes" pirates.

Les différences notables entre SSL et SSH sont les suivantes :

- SSL ne nécessite pas d'authentification côté serveur : une connexion peut être anonyme. Sous SSH, cela n'est pas autorisé.
- SSL ne propose qu'un mécanisme d'échange de clés publiques pour l'authentification tandis que SSH propose de nombreuses autres options.
- SSL n'est utile qu'en cas d'échange entre deux applications tandis que SSH crée un tunnel qui peut rester ouvert même si aucune donnée n'est transmise.

97 SSL : Secure Socket Layer.
98 SSH : Secure SHell.
99 TLS : Transport Layer Security.
100 MAC : Messages Authentication Codes.

De manière concrète, SSH utilise les mêmes mécanismes de chiffrement que les autres VPN : IDEA, DES, 3DES, RC4, Blowfish... mais les mécanismes d'authentification peuvent être propriétaires (certificat, mot de passe, etc.).

SSH est également employé pour faire de la redirection de port pour sécuriser des flux qui ne le sont pas à l'origine. Le schéma ci-après permet de comprendre pourquoi SSH peut néanmoins poser des problèmes de sécurité : l'ouverture du seul port TCP 22 ouvre de nombreuses possibilités...

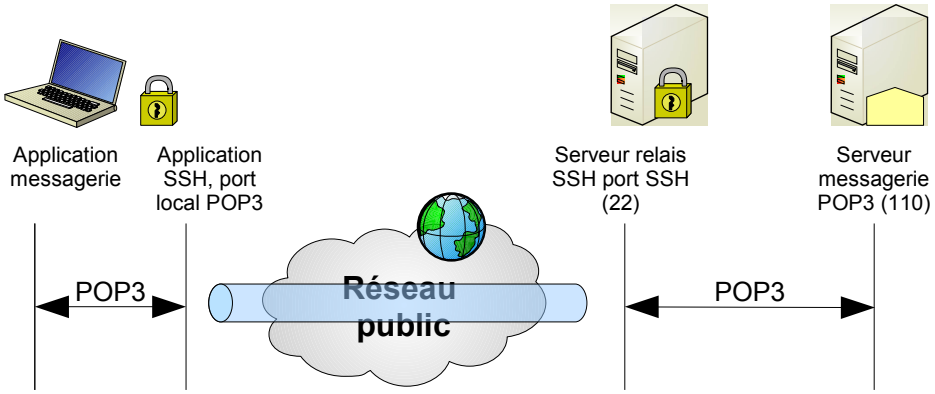


Illustration 45: Redirection de ports avec SSH

Toutefois, l'utilisation de SSH se généralise sur les systèmes d'exploitation comme Linux, ce qui sécurise grandement ces systèmes.

4.2.3.2 IPSec (Internet Protocol Secure)

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

IPSec est employé de deux manières :

- mode transport : dans ce mode, les trames sont limitées 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.

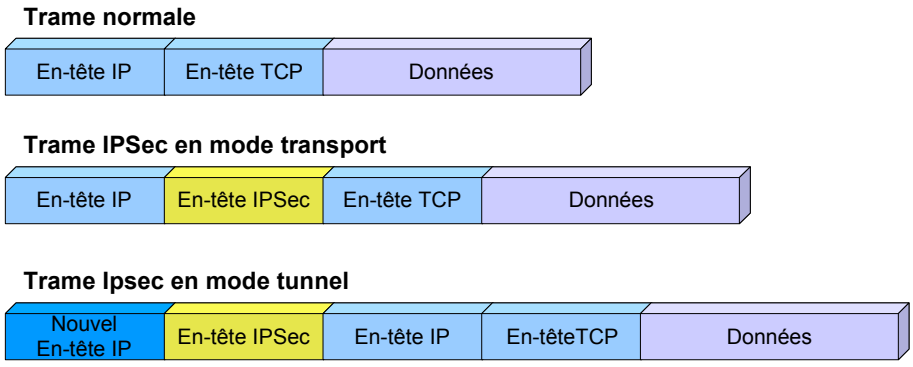


Illustration 46: Les modes transport et tunnel d'IPSec

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[101] et ESP[102]. Ils utilisent tous 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]

4.2.3.2.a AH (Authentication Header)

AH est spécialisé dans l'authentification (mais ne garantit pas l'intégrité des données) et utilise pour cela des mécanismes de hachage (RFC2402).

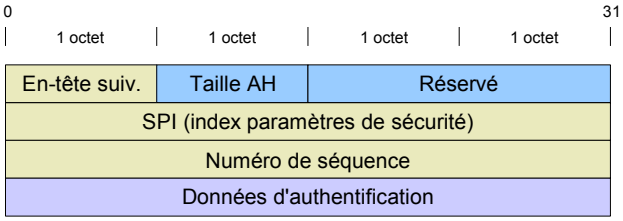


Illustration 47: Structure de l'en-tête AH

La structure AH permet d'éviter le "rejeu" de séquences (grâce aux numéros de séquence) et le champ 'en-tête suivant' permet de connaître le numéro du protocole protégé (valeur conforme au "Protocol numbers" sur le site de l'IANA[103]).

4.2.3.2.b ESP (Encapsulating Security Paiload)

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

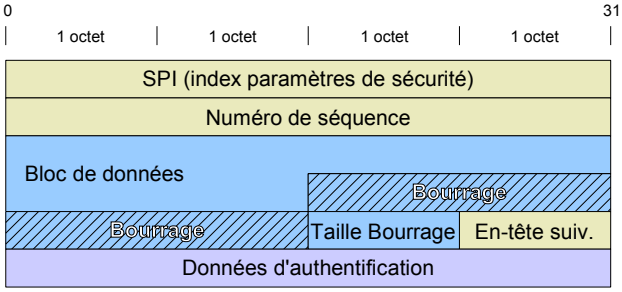


Illustration 48: Structure de l'en-tête ESP

On retrouve les champs "En-tête suivant", "SPI" et "Numéro de séquence" de la structure d'en-tête du protocole AH. Le bloc de données correspond aux données à protéger (confidentialité) avec des champs de "bourrage" (remplissage ou "padding" en anglais) pour permettre l'utilisation d'algorithmes de chiffrement par bloc.

4.2.3.2.c Fonctionnement d'IPSec

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.

101 AH : Authentication Header.
102 ESP : Encapsulating Security Payload.
103 IANA : Internet Assigned Numbers Authority (http://www.iana.org/assignments/protocol-numbers)

Le choix de ces deux paramètres est fait dynamiquement à l'aide du protocole IKE[104] (RFC 2409) : ce protocole permet l'échange de clé de manière automatique via le protocole UDP (port 500), en utilisant les SA (Security Associations).

IPSec est principalement utilisé en mode tunnel car il permet le chiffrement des données et l'utilisation de réseaux non sécurisés pour la transmission.

4.2.3.3 PPTP (Point to Point Tunneling Protocol)

PPTP est un VPN de couche 2 : d'un côté cela lui procure un avantage important sur les VPN de niveau 3 car il peut transporter d'autres protocoles que TCP/IP (IPX, NetBEUI, etc.).

D'un autre côté le niveau de fonctionnement de PPTP ne permet pas le routage : ainsi, toutes les données sont d'abord envoyées vers le serveur VPN-PPTP, même s'il s'agit d'un trafic à destination d'Internet.

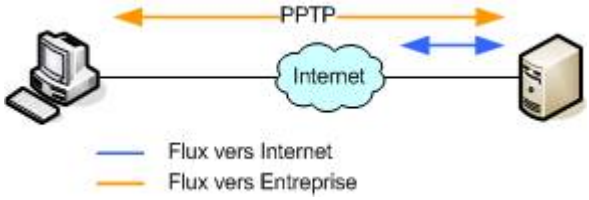


Illustration 49: VPN PPTP

Il résulte alors un volume de trafic plus important avec PPTP qu'avec IPSec qui est capable de router correctement les trames en fonction de leur destination (split tunneling).

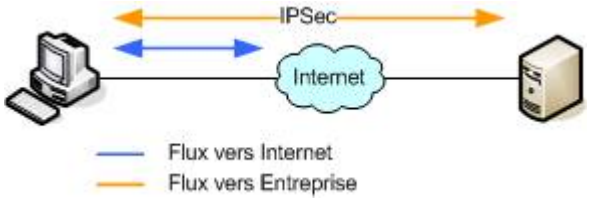


Illustration 50: VPN IPsec

D'autre part, PPTP ne fonctionne qu'avec un algorithme de chiffrement RC4 à 128 bits. Mais si une mauvaise implémentation de ce mécanisme a rendu impopulaire la sécurité des réseaux sans fil, cela n'est pas le cas dans PPTP.

4.2.3.4 EAP

EAP (Extensible Authentication Protocol) est une extension du protocole PPP (protocole de niveau 2 transportant 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.

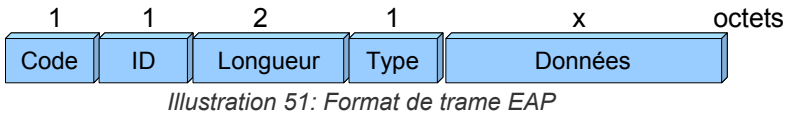


Illustration 51: Format de trame EAP

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

104 IKE : Internet Key Exchange.

L'intérêt d'EAP est de fournir une couche standard pour les mécanismes d'authentification. 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, notamment 802.3 et 802.11. 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 [WEB005] montre les plus connus ainsi que leurs points forts et leurs points faibles.

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Authentification serveur	-	Hachage mot de passe	Certificat Clé publique	Certificat Clé publique	Certificat Clé publique
Authentification client	Hachage mot de passe	Hachage 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 10: Points forts des différents algorithmes utilisés avec EAP

- EAP-MD5 n'est pas recommandé (et peu utilisé) car les échanges ne sont pas chiffrés : le challenge circule sur le réseau en clair puis chiffré par le client ce qui le rend sensible aux attaques par dictionnaire ou attaques brutes. De plus, il ne gère pas la distribution de clé dynamique WEP.
- 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 hachage 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). En contre-partie, la mise en œuvre d'une IGC pour gérer autant de certificats (un par client et par serveur) peut dissuader de nombreux administrateurs.
- 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 des trames EAP tandis que TTLS utilise les paires "attribut-valeur" (AVP) encapsulées dans des trames EAP-TTLS.
- EAP-FAST est déclaré par Cisco comme aussi sûr que EAP-PEAP et aussi simple à mettre en œuvre que EAP-LEAP (et très rapide pour l'authentification, d'où son nom). Pour cela, EAP-FAST utilise un PAC[105] à la place d'un certificat mais pour être aussi fiable que EAP-PEAP, il faut certifier ce PAC... à l'aide d'un certificat ! Cette méthode ne sera pas décrite plus en avant il s'agit d'une solution propriétaire (Cisco).

Afin de bien comprendre les phases d'authentification 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 tous les systèmes d'exploitation, contrairement à EAP-LEAP et EAP-FAST).

105 PAC : Protected Access Credential.

4.2.3.4.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.

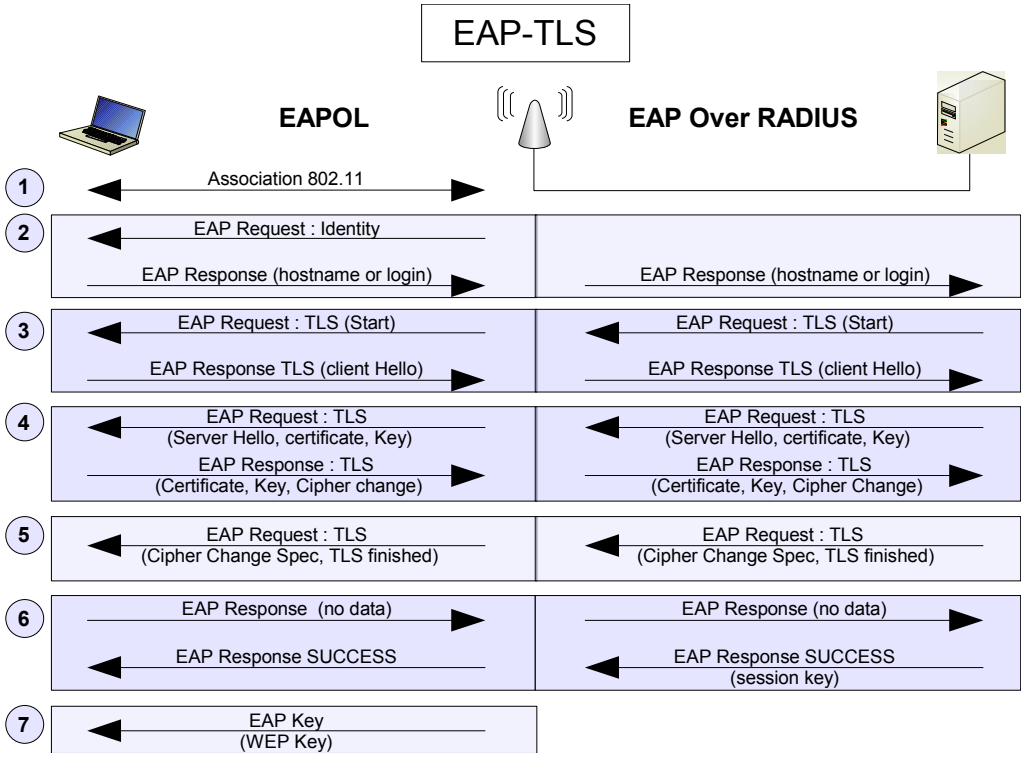


Illustration 52: Authentification EAP-TLS

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 passée en clair (mais pas forcément l'identité réelle) 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 propre certificat.
5. Le serveur répond alors et termine l'échange TLS.
6. Le client valide le protocole d'échange choisi 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.

4.2.3.4.b EAP-TTLS et EAP-PEAP

Ces deux méthodes (très similaires) sont un peu moins simples à mettre en œuvre, toutefois la sécurité reste également très élevée.

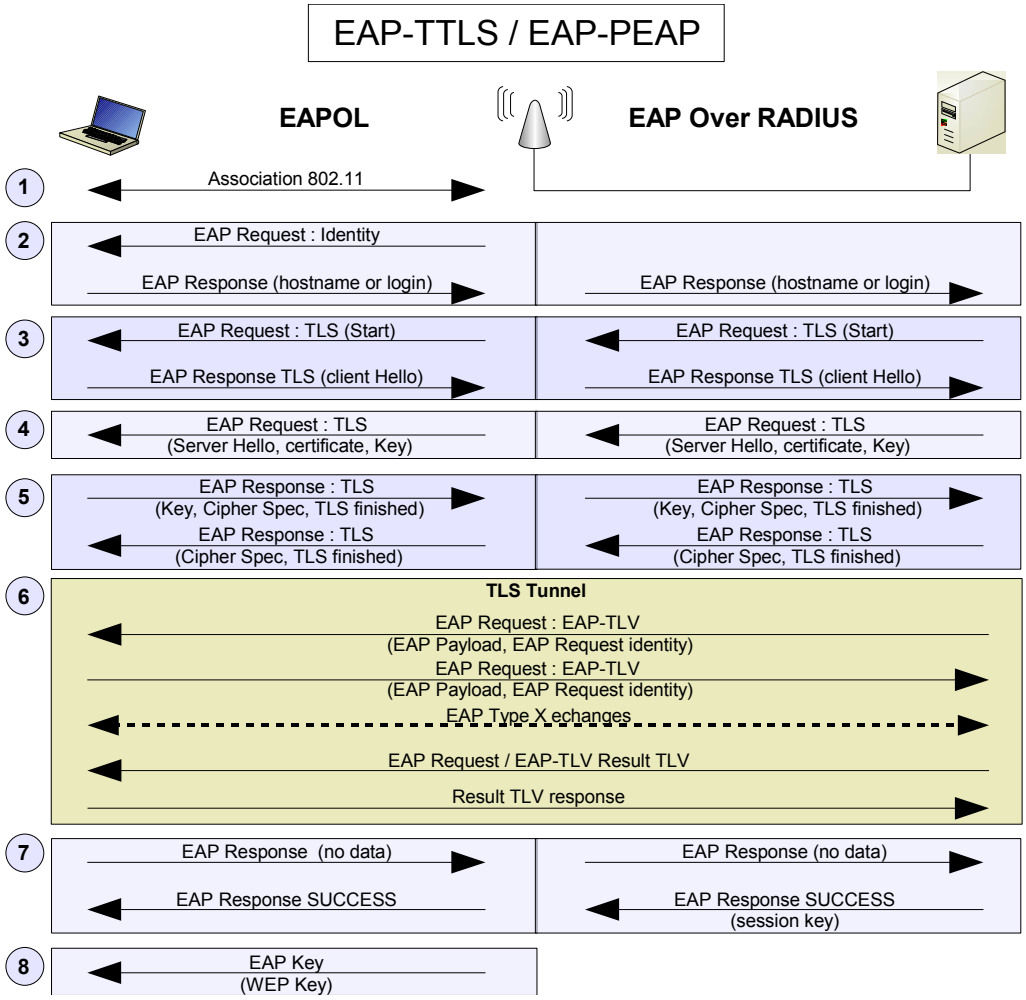


Illustration 53: Authentification EAP-TTLS

Avec cette méthode, les points 1 à 4 sont similaires à EAP-TLS. Toutefois, le point 5 entraîne 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 en confirmant 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[106] pour TTLS). Après quelques échanges, le client fournit au serveur son mot de passe (en utilisant PAP ou MS-CHAPv2 selon la méthode EAP 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 choisi 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.

106 TLV : Type, Length, Value

EAP est un mécanisme très robuste d'authentification qui est supporté nativement par les équipements réseaux utilisant les normes 802.3 et 802.11. Sur les réseaux sans fil, il permet de contourner les faiblesses du protocole WEP en fournissant un vecteur d'initialisation lors de l'ouverture de session.

EAP n'est pas lié au chiffrement ce qui rend son utilisation possible en WPA (RC4+TKIP) ou WPA2 (AES).

5 SOLUTIONS ET DÉPLOIEMENT

L'étude des différents protocoles et standards que nous avons réalisée dans le chapitre précédent, facilite maintenant le choix et la mise en œuvre d'une solution au sein du CICG et sa généralisation au niveau du réseau interuniversitaire grenoblois.

5.1 Les éléments de réponse

Tout d'abord, l'accès à l'infrastructure doit se faire de manière nominative : un utilisateur 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 quelle personne utilise un poste corrompu ou dont le comportement est illégal. Il est dont nécessaire de choisir un système compatible avec une architecture AAA.

Ensuite, permettre à un utilisateur d'accéder à ses ressources de manière sécurisée implique l'utilisation d'un standard de chiffrement entre son application ou sa machine et le point d'accès. Le réseau filaire est jugé suffisamment sûr grâce à l'accès sécurisé du bâtiment, la segmentation en VLAN et surtout à l'implémentation de règles de filtrage. Les efforts sont donc concentrés sur les réseaux sans fil dont le mécanisme WEP s'avère insuffisant en l'état.

Nous rappelons que le cahier des charges met en évidence d'une part le besoin d'une solution simple, d'autre part le besoin d'une solution performante et évoluée : nous allons donc sélectionner puis comparer les produits pour finalement les déployer dans le réseau interuniversitaire.

5.1.1 Solution "simplifiée" sans configuration cliente

Cette solution ne doit nécessiter que peu d'actions de la part de l'utilisateur : se sont les solutions de portails captifs qui sont retenues car elles ne nécessitent aucune configuration sur les équipements des utilisateurs. Elles présentent les avantages suivants :

- elles sont compatibles avec tous les équipements utilisant le protocole TCP/IP,
- elles ne nécessitent aucun droit particulier sur le poste de travail,
- elles sont capables d'utiliser un système d'authentification évolué (RADIUS),
- aucune action technique n'est demandée à l'utilisateur final,
- la sécurité et les mises à jour concernent uniquement le serveur supportant le portail.

Cette solution doit donc permettre aux utilisateurs de se connecter aux réseaux des universités de Grenoble en utilisant un navigateur internet pour accéder – après authentification – aux sites web, aux services webmail (messagerie par interface web) et éventuellement à d'autres services.

5.1.2 Solution "étendue" avec installation d'un logiciel tiers

Cette solution implique l'installation d'un logiciel sur le poste de l'utilisateur. C'est le cas des solutions mettant en œuvre les VPN. Pour permettre cette installation, les utilisateurs doivent donner leur accord et accepter les risques (toute installation de logiciel peut entraîner un dysfonctionnement de la machine) mais ils doivent également avoir les privilèges nécessaires sur leurs équipements.

Ces solutions sont plus intéressantes que les portails captifs car elles fournissent des services supérieurs :

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

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

5.1.3 Elément commun aux deux solutions

Dans les deux solutions, la mise en œuvre d'un serveur d'authentification est conseillée sinon nécessaire. Cette solution est d'autant plus logique qu'elle est interopérable : il est ainsi possible pour chaque université d'alimenter sa propre base d'utilisateurs et de gérer sa politique de sécurité (gestion des droits et autorisations). Les serveurs d'authentification sont capables de se mettre en relations pour accepter ou non un utilisateur sur le réseau, quelque soit sa provenance.

Cette propriété est essentielle dans un cadre de nomadisme étendu et nous verrons qu'elle est obligatoire dans le cadre de la mobilité sur les réseaux européens d'EDURoam. Le système d'authentification est donc la charnière de cette étude.

5.2 Services d'authentification

Les systèmes d'authentification sont nombreux. Les systèmes compatibles avec une véritable architecture AAA sont moins 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 gérer sa reconnaissance sur l'ensemble du réseau interuniversitaire. 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 œuvre la solution retenue.

5.2.1 Evaluation de solutions

Les solutions suivantes répondent à l'architecture AAA. Toutes les solutions évaluées 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 – qui est celle qui nous intéresse – coûte environ $3200 : un prix trop élevé dans notre contexte universitaire.

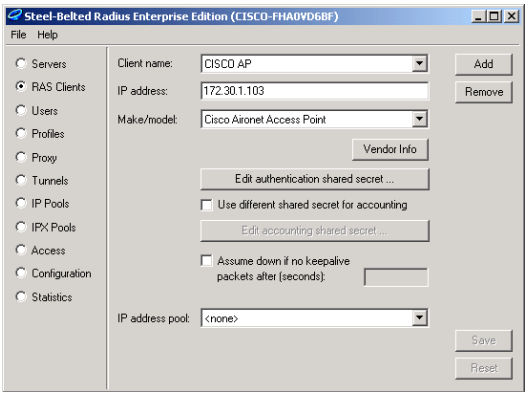


Illustration 54: Interface de Steel Belted Radius

5.2.1.2 Microsoft IAS (Microsoft)

Microsoft Internet Authentication Server est une solution intéressante pour les administrateurs ayant des serveurs Microsoft. Ce module est en effet inclu 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. Microsoft propose sa vision de l'authentification mais l'application n'est pas aussi complète que les autres produits (notamment absence d'authentification de type EAP-TTLS).

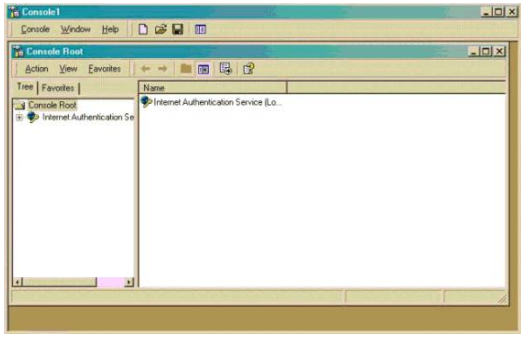


Illustration 55: Interface d'IAS de Microsoft

5.2.1.3 Radiator (OSC)

Le groupe "Open System Consultants" est une société créée en 1991. Ce groupe établi à Gold Coast et Melbourne, en Australie, propose 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 mécanisme sécurisé d'échange de trames entre relais RADIUS (proxy) : RadSec (IANA, port 2083) qui est une solution propriétaire.

Le prix de ce produit n'est pas prohibitif et est adapté aux différents besoins (tarif pour un serveur : 600€, pour 2 à 7 serveurs : 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>
```

Malheureusement, cette solution développée en langage Perl pose le problème de la performance (Perl étant un langage interprété et non pas compilé).

5.2.1.4 FreeRADIUS (Alan DEKOK)

FreeRADIUS est une application AAA libre (open-source) et gratuite. Malgré cela, ses possibilités sont très étendues 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.

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

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

5.2.1.5 Résumé des solutions évaluées

Les critères de sélection qui sont liés au cahier des charges (le coût, la capacité en charge, les fonctionnalités et l'ergonomie) sont résumés dans le tableau ci-dessous.

	Steel Belted (Funk Soft.)	IAS (Microsoft)	Radiator (OSC)	FreeRADIUS (A. DEKOK)
Prix	$$$	0*	$	0
Capacités	+	+	-	+
Fonctionnalités	+	-	+	+
Ergonomie	+	+	-	-

** à condition d'avoir une licence pour un serveur Windows 2000 au minimum*

Tableau 11: Tableau résumant les différentes solutions évaluées

La synthèse de ce tableau correspond à l'utilisation d'un système AAA dans notre environnement et il ne s'agit nullement de juger de la pertinence de ces produits dans un autre cadre que le nôtre.

5.2.2 Choix de la solution

La comparaison des solutions évaluées est résumée dans le tableau 11. Le choix effectué au CICG est FreeRADIUS car cette application présente les avantages suivants :

- sa gratuité n'entraîne pas de limitation en fonction du nombre de licence,
- elle est écrite en C ce qui permet un fonctionnement rapide,
- elle est fournie sous forme de paquetage sous différents Linux et a une "mailing-list" très active,
- elle est déjà employée au CICG et dans certaines universités ce qui réduit son délai de prise en main.

Cependant elle présente également quelques inconvénients :

- sa documentation reste succincte et s'adresse à un public averti,

- sa configuration se fait par l'intermédiaire de plusieurs fichiers texte, ce qui rend son approche difficile et peu intuitive.

Les fonctionnalités retenues pour nos besoins sont :

- authentification directe dans le fichier "users" de FreeRADIUS,
- authentification via un serveur LDAP,
- compatibilité avec les mécanismes EAP pour l'authentification forte (EAP-TLS, EAP-TTLS et EAP-PEAP),
- utilisation possible d'une base de données pour la journalisation (MySQL),
- possibilités de relayer des trames RADIUS (mode proxy),
- utilisation des paires d'attribut-valeur (AVP) à destination des équipements NAS[107].

5.2.3 Installation et configuration d'un serveur FreeRADIUS

La documentation est succincte et je n'ai trouvé qu'un livre sur RADIUS. Deux chapitres sont dédiés au fonctionnement de FreeRADIUS, toutefois, les explications restent superficielles sur les possibilités étendues de l'application. La documentation la plus complète se trouve dans les commentaires (très nombreux) des fichiers de configuration ou dans les archives de la liste de diffusion (freeradius-users@lists.freeradius.org).

Nous avons testé l'architecture de FreeRADIUS pendant plusieurs semaines. Au démarrage du démon "radiusd" les fichiers sont lus et chargés en mémoire. Cela explique pourquoi il faut redémarrer le démon après chaque modification.

5.2.3.1 Installation de base

Le serveur d'authentification est constitué d'un PC utilisant un système d'exploitation Redhat 9 (http://www.redhat.com/) : l'utilisation de paquetages (package en anglais) est simple grâce à l'utilitaire "rpm".

5.2.3.1.a Utilisation de SSH

Les systèmes Linux encouragent l'utilisation du protocole SSH pour se connecter à distance en mode console : cette sécurisation a rendu nécessaire l'utilisation des programmes gratuits TeraTerm de Ayera (http://www.ayera.com/teraterm/) et PuTTY de Simon Tatham (http://www.putty.nl/) qui permettent de faire du SSH ou du telnet. PuTTY ne permet pas la communication sur un port série mais n'a pas besoin d'installation pour fonctionner puisqu'il s'agit d'un simple exécutable. Ces deux programmes ont été utilisés pour les accès distants aux serveurs RedHat en SSH, mais aussi au routeur de la maquette et aux points d'accès Cisco.

Cette sécurité contribue à rendre les serveurs plus fiables et moins vulnérables aux attaques sur le réseau.

107 NAS : Network Access Server.

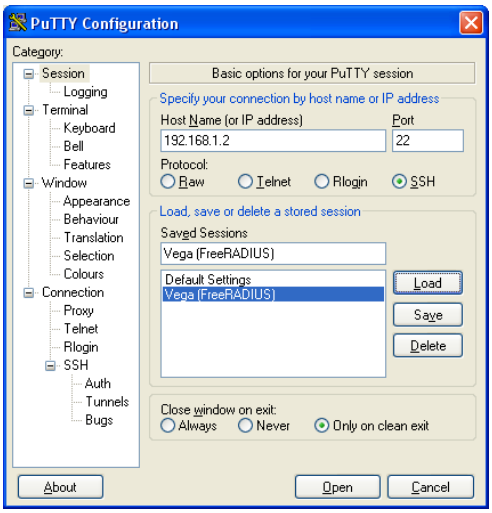


Illustration 56: PuTTY, interface de configuration/connexion

5.2.3.1.b Installation de FreeRADIUS

Après avoir installé Linux Redhat 9 et les paquetages utiles pour la maquette (DHCP, MySQL, environnement de développement incluant le compilateur gcc, etc.) nous avons téléchargé la dernière version du programme FreeRADIUS (version 1.0.1) car le paquetage FreeRADIUS est une version trop ancienne et dans laquelle l'utilisation d'EAP n'est pas suffisamment claire. 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.

```
tar zxvf freeradius-1.0.4.tar.gz
cd freeradius-1.0.4
./configure --ac_prefix=/usr/local/freeradius
make
make install
```

S'il n'y a aucun message d'erreur à la compilation, la configuration de FreeRADIUS peut commencer. Sinon, il ne faut pas oublier de faire un **`make clean`** avant de recommencer une compilation.

5.2.3.2 Configuration de base

Dans une configuration basique, les fichiers "radiusd.conf" et "users" sont les seuls fichiers à modifier.

Le fichier "radiusd.conf" est largement commenté (c'est pourquoi il vaut mieux faire une sauvegarde de l'original avant de le modifier) seules quelques lignes méritent une attention particulière :

```
...
# permet de démarrer RADIUS avec des droits restreints (sécurité)
user = radius
group = radius
...
# ne pas logguer les passwords sinon en cas d'attaque, la liste est en
# clair dans les logs de RADIUS :)
log_auth = yes
log_auth_badpass = no
log_auth_goodpass = no
```

En revanche le fichier "users" présente surtout des exemples mais sa syntaxe et ses attributs sont peu expliqués. Ce fichier permet pourtant de consulter des annuaires LDAP, des bases SQL, le fichier utilisateur du système (/etc/passwd) et sa propre liste d'utilisateurs. Il permet également de comparer des attributs fournis par un système demandant une authentification (PPP, Frame-User, etc.) et de créer ou modifier ces attributs.

```
# Permet de récupérer le nom utilisé à l'intérieur du tunnel EAP
DEFAULT         Freeradius-Proxied-To == 127.0.0.1
                User-Name = `%{User-Name}`,
                Fall-Through = Yes

# Il n'est pas nécessaire de spécifier le type d'authentification
# pour EAP (Auth-Type :=EAP). FreeRADIUS le gère parfaitement seul.
Anonymous       Auth-Type := EAP
eric            Auth-Type := LDAP
david           Auth-Type := local, User-Password == "mot_de_passe"
franck          Auth-Type := system, Huntgroup-Name == "unixgroup"
...
```

Après avoir vérifié le bon fonctionnement du serveur RADIUS en mode déboguage (commande radiusd -X) nous avons fait évoluer le serveur plusieurs fois, jusqu'à obtenir une configuration finale beaucoup plus complète.

5.2.3.3 Configuration avancée

La solution finalement déployée s'appuie sur plusieurs serveurs RADIUS et met en œuvre les fonctions suivantes : authentification EAP, authentification répartie, redondance de serveur et gestion des traces de connexions.

Le synoptique décrit dans l'illustration suivante a été réalisé pendant l'exploitation de plusieurs serveurs RADIUS : il permet de comprendre les interactions entre les différents fichiers de configuration pour déployer les fonctions ci-dessus avec – au minimum – deux serveurs.

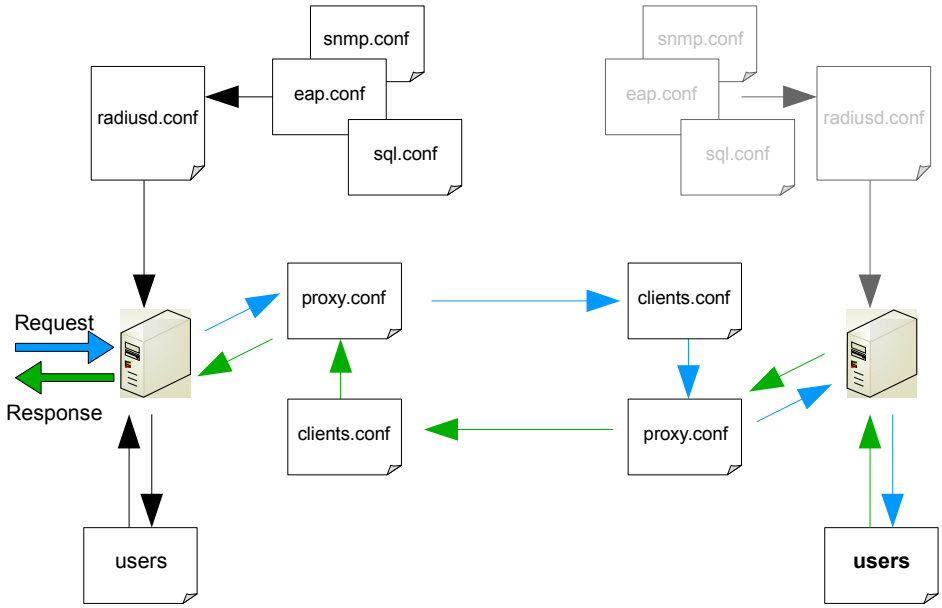


Illustration 57: Synoptique de fonctionnement FreeRADIUS

Lors des premiers tests, un deuxième serveur a été configuré dans la maquette, mais ensuite, nous avons intégré les serveurs RADIUS en production au CICG et à l'UPMF. Cette étape importante a marqué le début de l'authentification répartie avec traces.

Pour cela, quelques développements ont été nécessaires ainsi que des modifications majeures dans les fichiers de FreeRADIUS :

- ajout d'un script Perl pour pouvoir corréler les utilisateurs et les adresses IP : ce script nous oblige à utiliser une base MySQL pour récupérer les paramètres de connexion des utilisateurs (heure et durée de connexion, NAS ayant servi pour les transactions, adresse MAC du supplicant, ID de session...) : nous avons donc modifié le fichier "sql.conf",
- modification des fichiers "eap.conf" et "users" pour permettre au serveur RADIUS de reconnaître les mécanismes d'authentification EAP et de pouvoir fournir son certificat au supplicant,
- création d'une IGC factice pour générer des certificats serveurs nécessaires au fonctionnement d'EAP en mode TLS, TTLS ou PEAP. Pour cela nous avons utilisé le logiciel OpenSSL (plus tard nous avons utilisé l'IGC du CNRS pour produire des certificats officiels),
- mise à jour des fichiers "clients.conf" et "proxy.conf" pour activer l'authentification répartie sur plusieurs serveurs RADIUS (en fonction du "realm", c'est-à-dire du nom de domaine). En revanche, le fichier "eap.conf" ne varie pas car lors d'une authentification distante, seul le serveur final doit connaître le mode d'authentification choisi, les autres relayant simplement la requête EAP dans son intégralité.

Il est à noter que les paires "attribut-valeur" ne sont pas encore utilisées car il faut définir une politique commune d'utilisation et que les tests avec les équipements de la maquette n'ont pas été concluants. Seuls les traces, le mode relais et l'authentification EAP ont été validés.

Les serveurs RADIUS ainsi déployés ont donné naissance au projet interuniversitaire STAR : Système Transversal d'Authentification Répartie.

Illustration 58: Logo du projet STAR

Ce système permet aux personnels et enseignants des différentes universités grenobloises de s'authentifier et d'être reconnus dans n'importe quelle université appartenant au groupement interuniversitaire. La structure finale s'intègre dans le projet national ARREDU et européen EDURoam.

L'illustration montre l'architecture finale STAR ainsi que son fonctionnement lors d'une authentification distante.

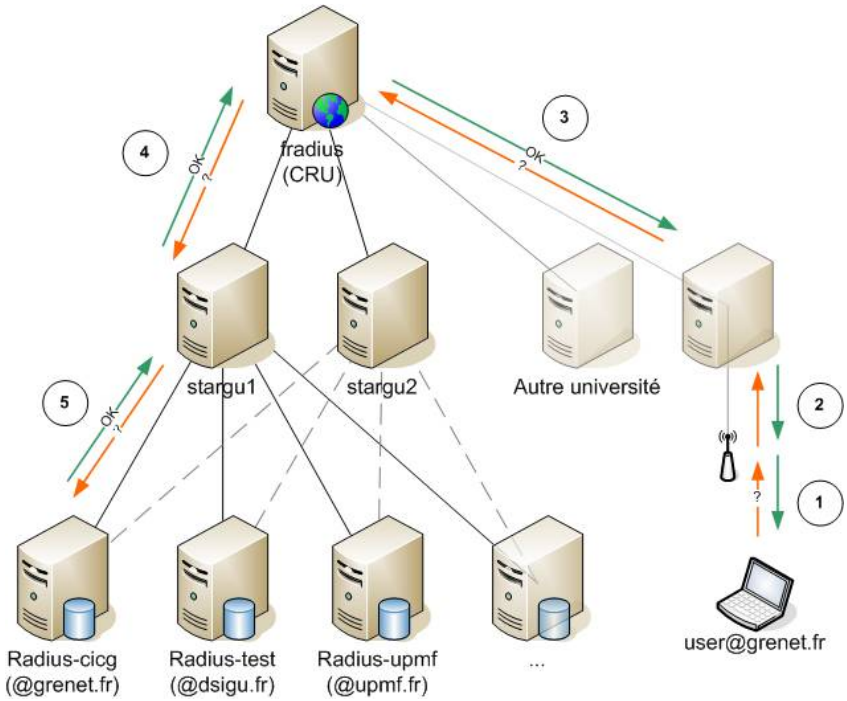


Illustration 59: Extrait d'une présentation du système STAR

Le système d'authentification étant opérationnel, nous avons donc étendu la maquette en intégrant un portail captif et un système VPN.

5.3 Portails captifs

Les seules solutions permettant d'accéder à Internet sans installation de programmes 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' (dans le sens d'accès contrôlé). Un portail captif fournit donc un accès contrôlé à un réseau. Dans le cas des universités, il s'agit de donner un accès contrôlé à Internet.

Généralement, les portails captifs se servent d'applications présentes sur de nombreux équipements réseaux (PDA, ordinateurs Windows ou Linux ou MAC) : les navigateurs. Ces applications qui utilisent les protocoles HTTP et HTTPS sont massivement présentes dans tous les systèmes d'exploitation et les serveurs HTTP et HTTPS sont faciles à mettre en œuvre.

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 est autorisé à sortir du réseau local.

5.3.1 Squid et fonction de routage politique

SQUID (http://www.squid-cache.org/) est une application "serveur proxy cache", c'est-à-dire un système de relayage de requêtes HTTP et HTTPS capable d'optimiser les flux vers l'Internet. Il est facilement mutualisable (c'est même son principal intérêt) et permet donc de limiter l'utilisation de la bande passante en agissant comme serveur cache de fichiers.

5.3.1.1.a SQUID

Afin d'éviter aux utilisateurs une quelconque configuration, le serveur SQUIDa été configuré en mode transparent : ce mode permet de relayer toutes les trames web mais il n'est pas possible d'utiliser le mécanisme d'authentification intégré. Ce dernier nécessite en effet de configurer manuellement les navigateurs pour qu'ils interprètent un code d'erreur 407 comme une demande d'authentification. Cela n'est pas envisageable sur des machines nomades qui par définition, peuvent changer d'environnement réseau fréquemment.

5.3.1.1.b Routage politique

Bien que ne répondant pas à nos besoins dans ce mode, SQUID nous a quand même permis de découvrir et tester le routage politique (fonction "policy routing" sur le matériel Cisco) sur les routeurs interuniversitaires. Cela consiste à router les trames en tenant compte du protocole employé et plus seulement sur les adresses de destination.

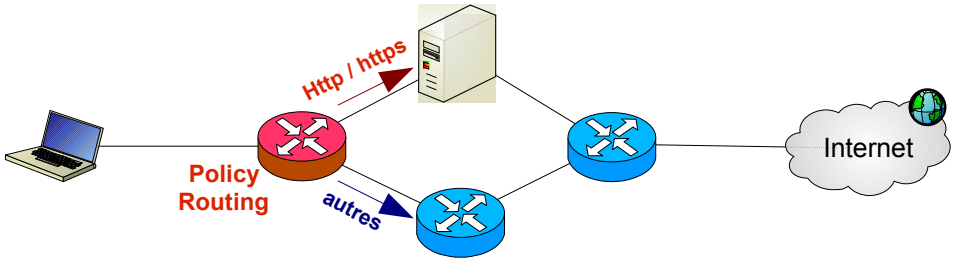


Illustration 60: Fonctionnement du routage politique (policy routing)

Ce routage très souple présente l'inconvénient majeur d'utiliser plus de ressources CPU du routeur. Cette fonctionnalité sera tout de même utilisée à chaque que nous aurons besoin de faire converger des trames utilisant un protocole particulier vers un serveur central.

5.3.1.2 Avantages

SQUID représente la solution la plus logique : un serveur SQUID est un serveur cache pour le web. Les avantages sont :

- solution centralisée,
- aucune configuration sur les postes des utilisateurs (mode transparent et routage politique),
- optimisation de la bande passante par mise en cache de fichiers Internet.

5.3.1.3 Inconvénients

Cette solution a deux inconvénients :

- elle nécessite une certaine puissance des routeurs pour le traitement du routage,
- elle ne permet pas l'authentification sans configuration des navigateurs.

5.3.1.4 Conclusion sur SQUID et sur le routage politique

La solution SQUID a rapidement été rejetée à cause de l'incompatibilité des modes de SQUID avec nos spécifications.

En revanche l'expérience acquise pour le routage politique nous permet d'adapter l'architecture du réseau pour répondre au besoin de mutualisation défini dans le cahier des charges.

5.3.2 M0n0wall et pfSense

Ces deux produits partagent les mêmes codes-sources, c'est pourquoi ils sont traités ensemble.

M0n0wall[108] est un projet gratuit (non en open-source) basé sur un ensemble d'outils disponibles sous FreeBSD. La philosophie de ce produit est d'une simplicité extrême : le système démarre sur un cédérom "bootable" et enregistre sa configuration sur une disquette. Il remplace un routeur avec une caractéristique supplémentaire : authentifier les utilisateurs voulant accéder à Internet.

L'autre programme – pfSense[109] – 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 6. De plus, il n'existe pas de version cédérom "bootable" pour pfSense.

Les fonctionnalités restent similaires et lorsqu'ils sont installés directement sur un disque-dur les mécanismes de cache améliorent leur performance...

5.3.2.1 Installation et configuration

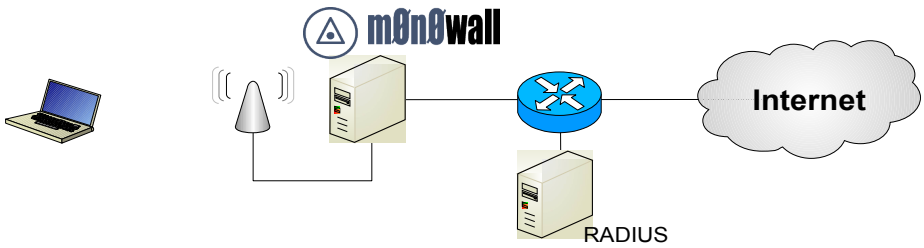


Illustration 61: Architecture typique m0n0wall

L'architecture testée est simple avec deux interfaces : une interface connectée sur le point d'accès sans fil (ou plus précisément dans le même VLAN), l'autre branchée sur Internet. Cette solution n'utilise pas le routage politique puisque m0n0wall intègre un routeur et des règles de filtrage (IP Table).

Après avoir téléchargé l'image ISO (version 1.1b7) de l'application depuis Internet et enregistré celle-ci sur un cédérom, nous utilisons une machine de test avec deux cartes réseaux. Le PC amorce le démarrage sur le cédérom. La configuration sur la machine elle-même (en utilisant son écran et son clavier) se limite à la configuration des adresses IP et des masques réseaux pour chaque carte réseau. Le reste de la configuration se fait à distance par l'interface web : http://m0n0wall.grenet.fr/

Cette interface est claire et agréable à utiliser, les paramètres sont nombreux. De plus, m0n0wall propose d'autres fonctionnalités, notamment :

- trois types de VPN (Ipsec, PPTP et OpenVPN),
- limitation de trafic (traffic shaper),
- des outils de diagnostic et de logs.

Les fonctionnalités VPN n'ont pas été testées car elles n'apportent aucune valeur ajoutée au VPN Cisco déjà en place.

108 http://www.m0n0.ch/wall/
109 http://www.pfsense.com/

Illustration 62: M0n0wall, panneau de configuration

5.3.2.2 Avantages

La solution m0n0wall est intéressante et probablement l'une des plus complète :

- 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 authentification de l'utilisateur,
- filtrage complet permettant l'utilisation de nombreux services ou applications (filtrage sur socket avec numéros de ports) autres que les services web,
- authentification par session https (à partir de la version 1.2 beta 7),
- enregistrement des logs du firewall.

5.3.2.3 Inconvénients

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

- nombreux bugs rencontrés sur les versions beta (1.2b7 et 1.2b8), notamment quelques plantages alors que la version stable (1.1) ne propose pas les fonctionnalités requises dans notre cahier des charges,
- la fermeture de session HTTPS (popup après 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 (m0n0wall ne peut être placé après un ou plusieurs routeurs),
- dans la configuration utilisée au CICG, l'accès à l'interface d'administration se fait par l'interface connectée sur le réseau privée (côté réseau sans fil, ce qui le rend plus sensible a une attaque),
- Les traces ne fournissent pas les tables de translation : il est impossible de retrouver une machine attaquante derrière m0n0wall (la seule possibilité est de retrouver toutes les personnes connectées au moment de l'incident).

5.3.2.4 Conclusion sur m0n0wall

M0n0wall représente une solution très intéressante dans un environnement simple : une petite société, un réseau limité ou un organisme désirant un ASFI à peu de frais. Ses capacités de portail captif utilisant le protocole HTTPS vont certainement évoluer et il faut attendre la version stable (1.11).

Malheureusement dans l'immédiat, la solution m0n0wall n'est pas utilisable dans notre environnement : outre le fait de devoir attendre une version stable, l'utilisation d'un filtrage sur les adresses physiques ne permet pas de placer m0n0wall comme portail captif au niveau des routeurs d'entrée de l'interuniversité.

5.3.3 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 son mode de fonctionnement est 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.

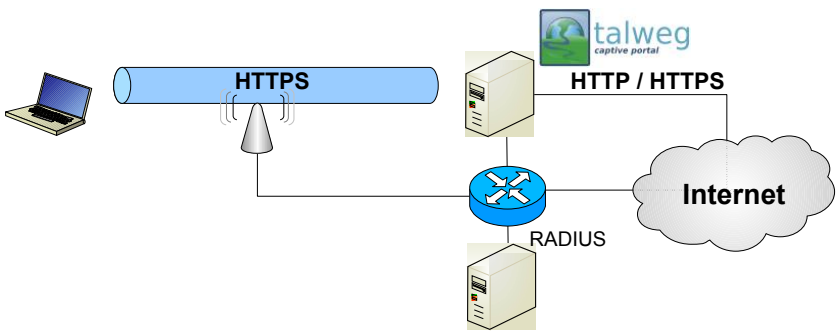


Illustration 63: Architecture Talweg

5.3.3.1 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 (technique de "policy routing" expliqué à la section 5.3.1).

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

Édition 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 ---
```

L'utilisation de Talweg est intuitive : en tapant n'importe quelle 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.

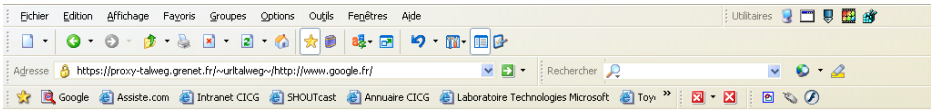


Illustration 64: Exemple de ré-écriture de liens sous Talweg

Dès la fermeture du navigateur, la session SSL est rompue, il est ainsi impossible pour une personne malveillante de récupérer la session d'un utilisateur précédemment connecté sur le poste. En charge, Talweg est écrit en Perl ce qui présage des performances moyennes.

5.3.3.2 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 intéressés :

- authentification sécurisée,
- communication entre le serveur et le client chiffrée (tunnel SSL),
- fonctionnement mutualisable (nécessite la mise en œuvre de routage politique (policy routing) pour fonctionner,
- logs très détaillés (de type proxy web),
- utilisation des 'favoris' (en lecture) ou de liens par copier/coller possible.

5.3.3.3 Inconvénients

En revanche, il y a un gros point négatif à améliorer pour en faire la solution idéale du réseau interuniversitaire :

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

5.3.3.4 Conclusion sur Talweg

Très réussi et assez complet pour une version 0.2 (RC), Talweg séduit par sa facilité d'utilisation : un surfeur novice n'aura aucune difficulté et seul l'affichage du lien dans le navigateur trahit la présence d'un portail captif. L'utilisation de liens déjà enregistrés rend possible l'utilisation du 'bookmark' ou des 'favoris' (en revanche, en cas d'ajout d'un lien dans les favoris, il faudra l'éditer pour supprimer la partie concernant Talweg). La fermeture du navigateur ferme automatiquement la session SSL, ce qui bloque toutes les attaques possibles.

La seule ombre au tableau est liée à la réécriture des liens contenus dans les pages car il semble y avoir un problème avec les liens relatifs. Nous avons donc pris contact avec le CRIUM pour les informer de notre constat et nous attendons une correction de leur part. De plus, les tests de performance confirment un ralentissement de trafic.

Cette solution reste malgré tout intéressante par sa simplicité d'utilisation et son niveau de sécurité : zéro configuration pour l'utilisateur et une navigation sécurisée !

5.3.4 Conclusion

Un tableau comparatif peut être établi sur les solutions évaluées en portails captifs :

	Squid	M0n0wall/pfSense	Talweg
Prix	0	0	0
Centralisable	Oui	Non	Oui
Authentification	Non *	Oui	Oui
Journaux	+	-	+
Interface	-	+	-
Capacités	+	+ **	-

** pas dans le mode transparent, le seul exploitable sans configuration utilisateur*

*** à condition d'installer le programme sur disque-dur pour bénéficier des caches.*

Tableau 12: Tableau comparatif des solutions portails captifs

5.4 Réseaux Virtuels Privés

Les réseaux virtuels privés (RVP ou VPN en anglais) connaissent un essor important depuis l'arrivée du haut débit : c'est la seule solution permettant de traverser des réseaux non-sécurisés (comme Internet) tout en assurant la sécurité des données transportées. Ce mécanisme implique seulement que les équipements terminaux utilisent les mêmes méthodes de chiffrement (et bien sûr une méthode commune d'authentification préalable). Il est généralement obligatoire d'installer un logiciel sur les postes des utilisateurs ainsi qu'un fichier de configuration : il s'agit d'un "client lourd".

Cependant, les deux systèmes choisis incluent également une fonction de "client léger" qui a été testée pour déterminer s'ils pouvaient répondre aux deux types de besoins (accès simplifié et accès étendu). Il s'agit des produits Firepass 1000 de F5 Networks et VPN 3030 de Cisco.

Le schéma ci-dessous illustre les deux modes de fonctionnement :

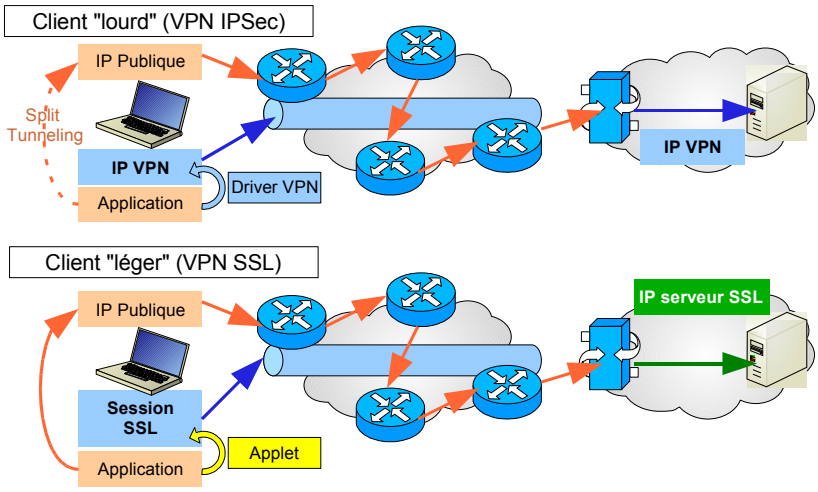


Illustration 65: VPN IPSec et VPN SSL

Dans le cas du VPN IPSec, l'installation d'un client "lourd" se traduit par la création d'une interface IP virtuelle. L'adresse IP publique est utilisée jusqu'au concentrateur VPN qui décapsule les trames IPSec : les trames restituées utilisent l'adresse IP virtuelle du poste client. S'il est nécessaire de configurer le client VPN IPSec lors de son premier fonctionnement, il devient par la suite totalement transparent et les applications fonctionnent normalement.

En revanche, le VPN SSL est établi au niveau "transport" et par conséquent, ne peut pas avoir ses propres adresses IP : il est alors nécessaire d'utiliser d'autres méthodes pour échanger des données à partir d'applications utilisant d'autres ports (client messagerie IMAP/POP/SMTP par exemple). La méthode la plus classique est une applet Java ou ActiveX qui émule un serveur sur la machine de l'utilisateur et qui transmet les trames au serveur réel via le concentrateur VPN SSL (proxy). Toutefois, la plupart des garde-barrières laissent passer le protocole SSL et tous les équipements multimédia propose un navigateur HTTP ce qui en fait une solution universelle.

Nous avons évalué trois types de solutions VPN basées respectivement sur les mécanismes SSL (Firepass 1000 de F5 Networks), IPSec (Cisco VPN3030) et WPA (équipements compatibles 802.11b/g).

5.4.1 VPN + Portail SSL F5 Networks

F5 Networks[110] est une société qui propose une ligne de produits appelés "Firepass". D'après celle-ci, l'utilisation du protocole SSL est une solution d'avenir qui permet de passer les communications web mais aussi d'autres flux. Nous avons donc testé un Firepass 1000 prêté par la société Telindus[111]. La gamme Firepass s'étend du Firepass 600 pour les PME au Firepass 4100 pour les grandes organisations. Le coût d'un Firepass 1000 se situe entre 10 et 20 k€ et permet 25 accès simultanés.

5.4.1.1 Installation et configuration

Le Firepass 1000 se présente comme un boitier (appliance) au format rack 1U avec une prise électrique, un port console et trois prises réseaux (LAN, WAN et DMZ). Une fois l'interface Eth0 configurée via un PC et un câble Ethernet croisé (le port console semble ne pas être utilisable dans cette phase), il est possible de passer à la configuration du serveur proprement dite via une interface web.

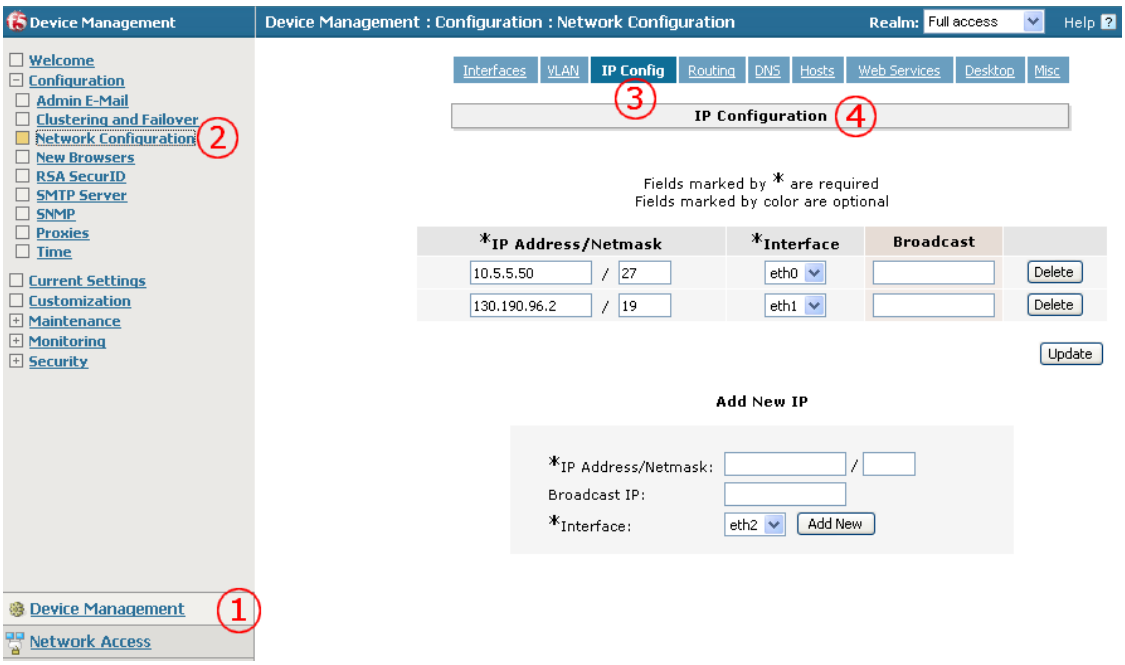


Illustration 66: Firepass, interface de configuration

Si le graphisme de l'interface est soigné, l'ergonomie est à repenser.

De plus, la version en prêt intègre toutes les licences mais la visite d'un commercial de F5 Networks nous a confirmé que la plupart sont des options payantes.

Les tests du client "léger" révèlent une interface très limitée : pour ouvrir un lien il faut saisir l'url dans un champ de la page d'accueil après authentification. Les fonctions additionnelles impliquent systématiquement une installation de code sur le poste client (soit par une applet JAVA ou une applet ActiveX). Pour utiliser le Firepass en serveur VPN-SSL, il faut également installer un client sur le poste.

110 F5 Networks : http://www.f5.com/
111 Telindus : http://www.telindus.fr/

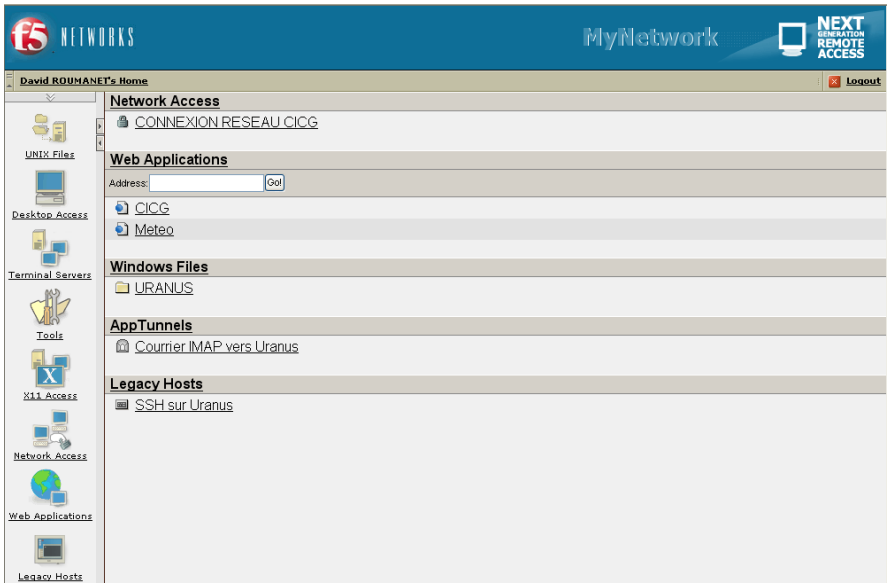


Illustration 67: Portail utilisateur sur Firepass 1000

Trois fonctions se démarquent par rapport à l'utilisation du client "lourd" : "Windows share", "Applications access" et "Desktop access".

- "Windows share" permet d'utiliser le portail pour accéder aux ressources partagées sur un serveur Microsoft (partage de fichiers notamment).
- "Application access" permet de passer dans un tunnel le trafic d'une application réseau en relayant le flux du port local de la machine vers le serveur (via le serveur Firepass). Pour cela une application locale doit être installée.
- "Desktop access" est une fonction qui – par l'intermédiaire d'une application lancée localement – remplace le bureau de Windows par un bureau virtuel : un document déposé sur le bureau n'existera plus lorsque la session sera fermée.

Ces fonctions ne correspondent pas à nos spécifications et leur utilité dans notre environnement reste très relative.

De même, les tests du client "lourd" n'ont pas montré de supériorité par rapport à la solution VPN déjà déployée sur le campus.

5.4.1.2 Avantages

Le Firepass a donc les avantages suivants :

- capacité de présenter un portail d'accueil et d'être serveur VPN,
- fonctions avancées de partage et de gestion de sessions,
- installation simplifiée des modules et applications nécessaires.

5.4.1.3 Inconvénients

Les inconvénients ci-dessous sont cependant assez nombreux :

- interface d'administration peu ergonomique,
- puissance limitée impliquant des coûts importants,
- nécessite les droits administrateurs et l'utilisation d'activeX ou applets Java,
- encapsulation d'un premier VPN dans un second VPN impossible,
- interface utilisateur en portail captif trop contraignante.

5.4.1.4 Conclusion sur un VPN F5 Networks

La solution de F5 Networks n'est donc pas plus intéressante que la solution VPN existante sur le campus. Elle démontre malgré tout que le protocole SSL permet de transporter autre chose que des flux web mais elle n'est pas aussi flexible que ne l'annonce le constructeur. De plus, le coût est vraiment prohibitif dans l'environnement interuniversitaire : en effet, si le portail peut être mutualisé, l'aspect VPN reste lié à chaque université, ce qui implique un serveur par université...

5.4.2 VPN + Portail Cisco 3030

Cette solution existe déjà sur le campus. Elle est basée sur le concentrateur VPN 3030 de Cisco. Le mode VPN peut être assuré en IPSec, PPTP, L2TP ou en SSL mais ce dernier mode est très gourmand en ressource (environ trois fois plus qu'IPSec). Il existe également un mode portail captif. L'équipement se présente en rack au format 2U. Il est le milieu de gamme de la série VPN 3000 avec une bande passante de chiffrement de 50 Mbps (chiffrement matériel) et une capacité en IPSec de 1500 utilisateurs simultanés.

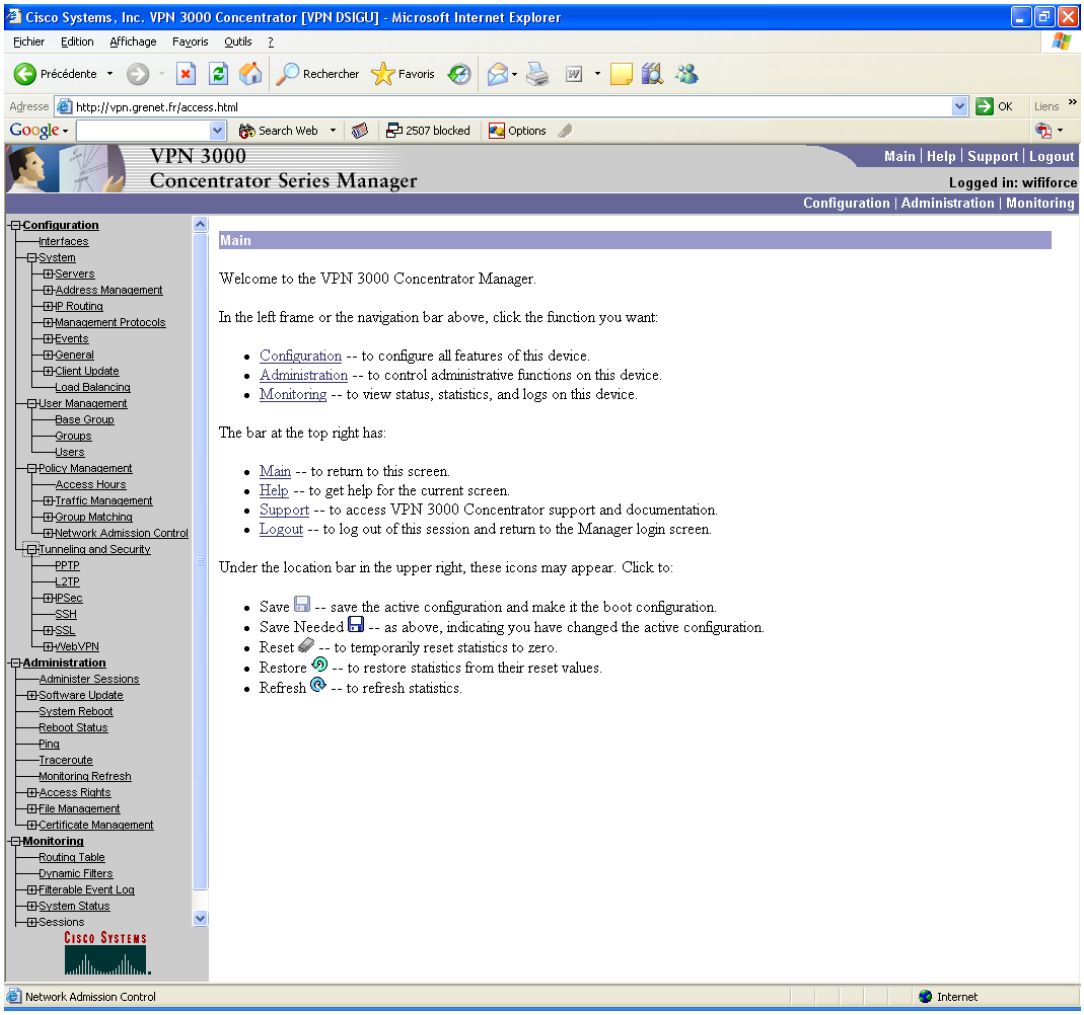


Illustration 68: Cisco VPN 3030, interface de configuration

La configuration par interface web est très sobre mais claire. L'utilisation de l'interface console (mode CLI[112]) est pratique pour les administrateurs confirmés.

112 CLI : Command Line Interface. C'est un modèle d'interface commun à tout les équipements Cisco.

Le client "léger" utilise une interface très limitée : pour ouvrir un lien il faut saisir l'url dans le champ d'un popup après authentification. Il présente donc le même inconvénient que le portail d'accès des équipements F5 Networks.

5.4.2.1 Avantages

Les intérêts du VPN Cisco sont différents de ceux du VPN de F5 Networks :

- les réseaux gérés par le CICG utilisent tous du matériel Cisco (homogénéité des IOS et interfaces, support simplifié vers un seul interlocuteur...),
- les équipements sont déjà en place (coût),
- il supporte les deux modes clients ("léger" et "lourd"),
- la partie cliente est gratuite et existe pour plusieurs plateformes.

5.4.2.2 Inconvénients

Les faiblesses du concentrateur Cisco sont :

- nécessite les droits administrateur et pas d'installation automatique (comme sur les Firepass),
- l'interface utilisateur en portail d'accès trop contraignante,
- encapsulation IPSec d'un premier VPN dans un second VPN impossible.

5.4.2.3 Conclusion sur un VPN Cisco 3030

Le VPN Cisco reste une solution pratique pour atteindre le réseau interne à partir de n'importe quel réseau et notamment Internet (maison ou séminaires par exemple). Les données étant chiffrées directement depuis la source, le type d'accès importe peu, seule la compatibilité avec TCP/IP est nécessaire. En revanche comme tout VPN basé sur IPSec, il n'est pas possible d'utiliser deux sessions IPSec l'une dans l'autre, à cause d'IKE (UDP 500).

Finalement, cette solution répond correctement au cahier des charges car les coûts sont limités par le fait que la structure et les équipements sont déjà présents.

5.4.3 Solution WPA

Cette solution est très récente et son déploiement a occupé une grande partie de l'étude. WPA s'appuie sur les mécanismes EAP. Cette solution s'applique actuellement sur les réseaux sans fil exclusivement car elle contient à la fois une méthode d'authentification forte (EAP) et le chiffrement des données (TKIP ou AES). C'est donc un VPN un peu particulier car il n'est pas possible d'y accéder à travers d'autres réseaux que le réseau sans fil local. Toutefois sont fonctionnement avec une authentification préalable puis un chiffrement des données entre l'équipement actif du réseau et l'équipement terminal de l'utilisateur en font par définition un système de réseau privé virtuel.

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

L'utilisation d'EAP implique le déploiement d'un ensemble d'équipements compatibles avec ce standard. Nous avons d'abord décidé d'une structure dont les caractéristiques seraient identiques à un système en production. La maquette suivante correspond à notre idée du projet.

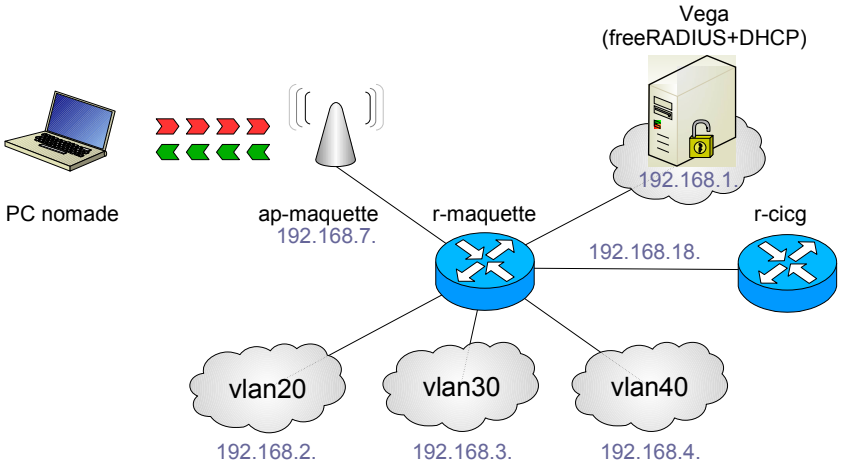


Illustration 69: Première maquette : tests EAP-TTLS

Il est nécessaire d'installer un logiciel client EAP sur le PC nomade : c'est la seule contrainte commune aux solutions basées sur un réseau privé virtuel (VPN).

5.4.3.1 Partie client (supplicant)

Le supplicant est un logiciel sur le PC nomade : sur Windows, nous avons testé AEGIS client de Meeting House (http://www.mtghouse.com/), SecureW2 de Alfa & Ariss (http://www.securew2.com/uk/) et le logiciel 3Com fournit avec les drivers des cartes Wi-Fi du constructeur (http://www.3com.com). Nous avons retenu SecureW2 de Alfa & Harris pour sa bonne intégration au système Microsoft, sa gratuité et son indépendance par rapport aux différents matériels. De plus, il est devenu open-source en cours d'année et devrait pouvoir remplacer l'interface GINA[113] de Microsoft. Sur Linux le logiciel Xsupplicant (http://www.open1x.org/) est satisfaisant hormis dans une structure ad hoc (ce qui ne pose donc aucun problème en EAP) et le client wpa_supplicant (http://hostap.epitest.fi/wpa_supplicant/) n'a pas été testé mais semble également convenir.

Illustration 70: SecureW2, interface de configuration

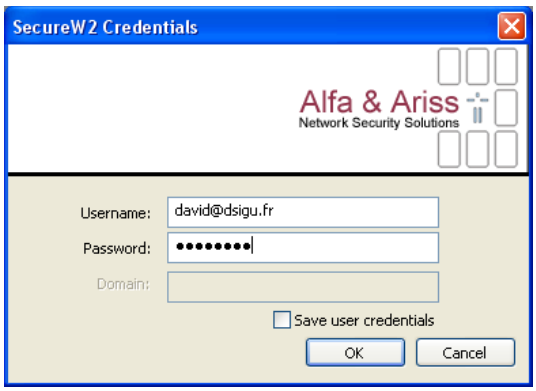


Illustration 71: SecureW2, interface de connexion

113 Graphical Identification aNd Authentication (MSgina.dll)

SecureW2 s'intègre dans le service d'authentification réseau de Microsoft Windows. Le choix de la méthode d'authentification est PAP ou EAP-MD5 : cela surprend mais il ne faut pas oublier que le tunnel EAP-TTLS est déjà établi avec l'identité "anonymous". L'authentification à l'intérieur du tunnel du véritable utilisateur ne nécessite donc plus un mécanisme très sécurisé. FreeRADIUS accepte les deux méthodes mais nous avons choisi PAP pour éviter la confusion.

5.4.3.2 Partie point d'accès (authenticator)

C'est l'équipement terminal de connexion, ici un point d'accès CISCO AP-1100 : les fonctions EAP sont implantées dans le firmware et comme tous les produits de moyen ou haut de gamme chez Cisco, il est utilisable avec le CLI. Nous avons toutefois préféré l'interface web qui effectue des tests de cohérence dans la configuration avant de l'enregistrer.

La mise à jour du firmware a rendu possible l'utilisation de plusieurs SSID ce qui pour l'utilisateur se traduit par plusieurs réseaux disponibles (un VLAN par SSID). Ainsi différentes solutions peuvent cohabiter car les flux restent bien isolés.

Nous avons choisi d'utiliser le mécanisme EAP-TTLS pour sa souplesse et sa compatibilité avec plusieurs systèmes (PC Microsoft, Linux ou Mac). En effet, la gestion d'une IGC en entreprise est déjà complexe, elle le serait encore plus dans les universités où les étudiants changent tous les ans. En EAP-TTLS, seuls les serveurs présentent un certificat ce qui se gère beaucoup plus facilement.

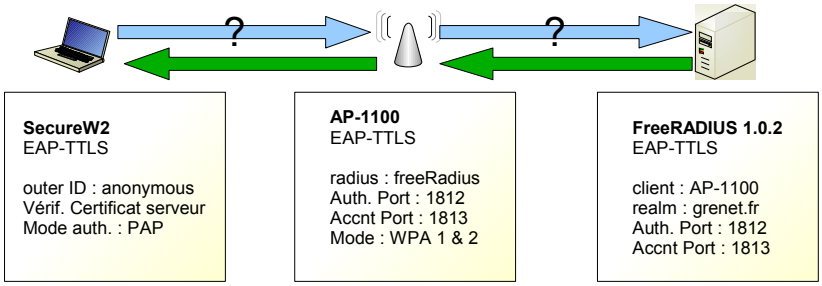


Illustration 72: Configuration des éléments de la chaîne EAP-TTLS

Le point d'accès AP-1100 de Cisco permet l'utilisation de plusieurs SSID, chacun devant correspondre à un VLAN. Le SSID supportant le mécanisme WPA (TKIP) ou WPA2 (AES) est un SSID configuré pour utiliser le protocole 802.1x : authentification EAP et chiffrement RC4 ou AES de la session.

Il ne faut pas oublier de configurer la partie "accounting" car c'est le point d'accès qui indiquera au serveur RADIUS lorsque le client se désassociera.

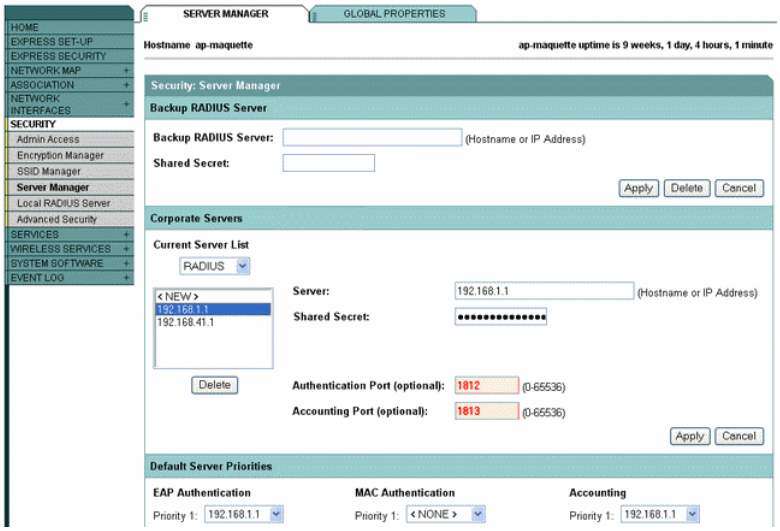


Illustration 73: Cisco AP-1100, interface web de configuration

5.4.3.3 Partie serveur

Le serveur d'authentification est un serveur linux Redhat avec une version stable de FreeRADIUS (au début des essais 1.0.1 et à la fin de l'étude 1.0.4). Nous avons dû installer OpenSSL afin de créer une autorité de certification factice et pouvoir émettre des certificats pour les serveurs. Cette opération ne sera pas nécessaire pour les universités car le CNRS peut leur fournir un certificat officiel (le CNRS est un IGC).

L'authentification étant opérationnelle, il faut activer la gestion des traces pour suivre les personnes se connectant à partir de notre réseau. Cette partie est un élément important du puzzle car si RADIUS gère correctement l'accounting lors de connexion PPP, il n'existe rien lorsque l'adresse IP est fournie par un serveur DHCP : c'est notamment le cas sur un réseau LAN ou WLAN.

En effet, si une adresse IP d'une université est mise en cause dans une pollution virale, une attaque contre un site ou toute opération interdite sur le réseau RENATER, alors le Président de l'université et l'ASSI sont responsables. La journalisation horodatée des couples "adresse IP" et "identifiant" reste le seul moyen d'en retrouver les auteurs.

Nous avons pour cela contacté la liste de diffusion "sans-fil" de Grenoble, puis celle du CRU pour finalement trouver un début de réponse sur la liste de diffusion de FreeRADIUS. Rok PAPEZ membre du groupe EDURoam et du groupe ARNES[114] (équivalent du réseau RENATER mais en Slovénie) nous a fourni un script que nous avons légèrement adapté.

Ce script s'appuie sur le langage Perl et il utilise une base de données MySQL et les fonctionnalités "syslog" des systèmes unix et linux. De plus, il faut modifier une partie de la configuration de FreeRADIUS pour écrire les données intéressantes dans la base MySQL.

Le schéma suivant (illustration 74) montre le principe de fonctionnement du script.

114 ARNES : Akademska in Raziskovalna mreza Slovenije (http://www.arnes.si/)

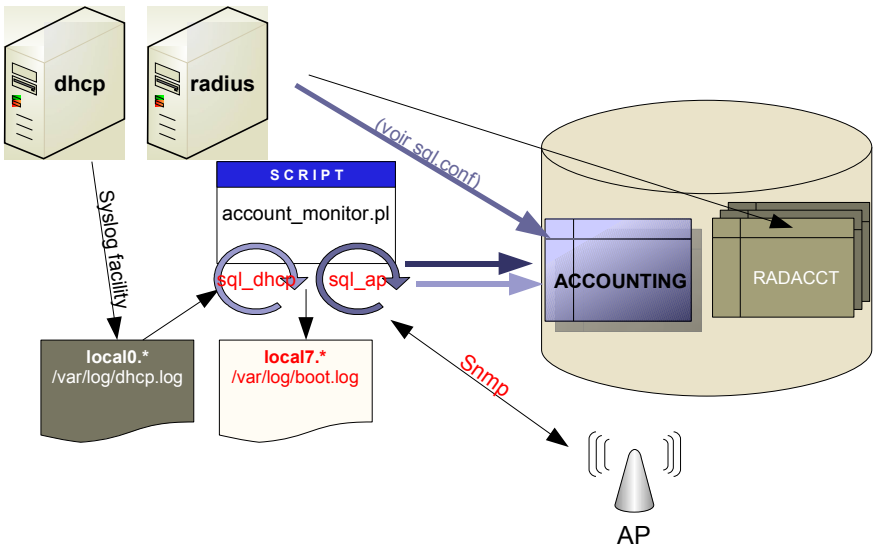


Illustration 74: Principe de fonctionnement du script Perl

Le script lance deux démons sur le serveur :

- un démon dont le rôle est de récupérer les données du serveur DHCP dans le fichier syslog associé et de les écrire dans la table 'Accounting' de la base "RADIUS",
- un démon dont la fonction est de vérifier régulièrement sur le point d'accès la table des associations, via le protocole SNMP.

Le serveur RADIUS écrit un nouvel enregistrement à chaque nouvelle authentification contenant l'identifiant d'utilisateur, l'adresse MAC de son poste, l'identifiant du point d'accès, un numéro de session unique et bien sûr la date.

Le script surveillant le fichier syslog vient compléter cet enregistrement lorsque le serveur DHCP fournit une adresse IP à l'adresse MAC reconnue.

Lorsque le supplicant se déconnecte, le point d'accès en informe le serveur RADIUS qui enregistre l'heure de déconnexion dans la base.

Le point d'accès et le serveur RADIUS dialoguant par le protocole UDP et le serveur pouvant être surchargé au moment de la déconnexion, le second script vérifie la présence ou non d'une session sur le point d'accès concernant l'adresse MAC.

L'intérêt d'enregistrer dans la base l'identifiant du point d'accès est de pouvoir retrouver sur quel point d'accès l'utilisateur s'est connecté. Il est même possible de "suivre" un déplacement d'un point d'accès à un autre (grâce au mécanisme de handover utilisé). Cette géolocalisation n'est pas très précise mais trouvera sûrement des applications dans l'avenir (par exemple, l'utilisateur pourra afficher un plan du site et demander où il se trouve);

L'illustration 75 est le résultat du script qui est fourni en annexe 7.6.

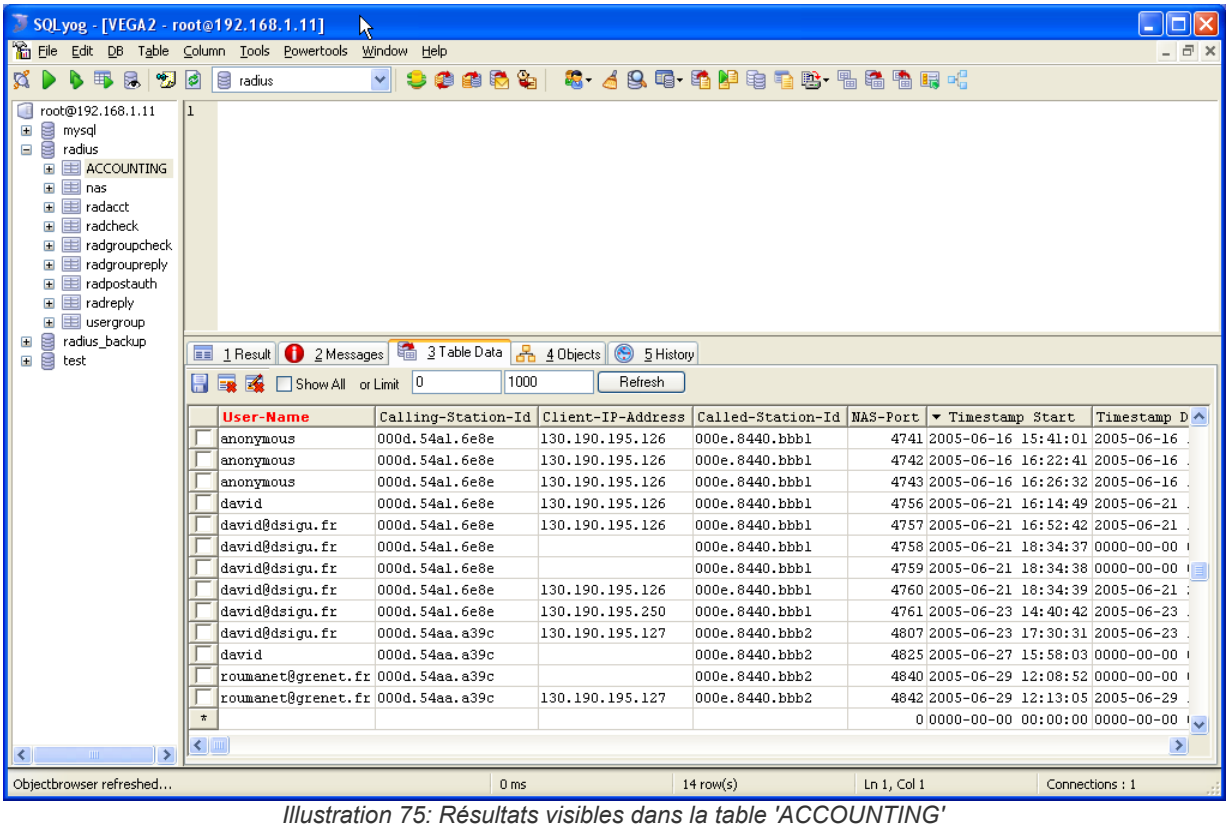


Illustration 75: Résultats visibles dans la table 'ACCOUNTING'

Les identifiants locaux n'ont pas de domaine tandis que les identifiants comportant le caractère arobase (@) font appels aux notions de domaine (realm en anglais). Le script enregistre donc l'identifiant et son domaine d'appartenance.

5.4.3.4 Avantages

Cette solution prometteuse offre les avantages suivants :

- pas d'accès au réseau avant authentification (attaques par déni de service, arp poisoning ou balayage de port impossibles de manière anonyme),
- mécanisme d'authentification indépendant des serveurs RADIUS intermédiaires (uniquement du serveur RADIUS contenant l'identifiant),
- après authentification, l'utilisation d'un client VPN IPSec n'est pas bloquée (sauf filtrage volontaire),
- solution ouverte et gratuite (utilisation d'un standard, logiciel client gratuit),
- sécurisation efficace des flux (AES pour WPA2 ou TKIP pour WPA),
- gestion de l'affectation dans un VLAN choisi,
- journaux (logs) contenant les données essentielles (identifiant, heures de connexions, point d'accès utilisé, adresse MAC et adresse IP),
- intégration aux réseaux ARREDU et EDURoam en accord avec la charte Renater et les réseaux d'éducation et de recherche.

5.4.3.5 Inconvénients

Cette solution présente néanmoins des inconvénients :

- installation d'un client nécessaire pour toute autre authentification que EAP-PEAP ou EAP-TLS sous Windows (l'installation est toujours nécessaire pour les machines linux/unix),
- droits d'administrateur nécessaires pour l'installation du client,
- mise en œuvre délicate pour les administrateurs des universités (nombreuses applications à configurer),
- nécessite de connaître la procédure à suivre (impossible d'accéder au réseau avant l'authentification pour récupérer le logiciel client),
- utilisation d'adresses de réseaux publiques (routables).

5.4.3.6 Résumé et conclusion sur WPA

La solution est satisfaisante pour une utilisation nomade à travers l'Europe : l'utilisation d'un mécanisme d'authentification pour lequel chaque organisme reste responsable de ses utilisateurs est un avantage indéniable. De plus, le serveur RADIUS terminal (local à la connexion) peut toujours modifier les attributs d'origine en fonction de la politique de sécurité locale. Le déploiement complet de la solution reste délicat mais nous avons rédigé une notice de 27 pages permettant de réduire les problèmes (un extrait est fourni en annexe). En revanche, WPA impose l'utilisation de deux SSID (VLAN) pour permettre le téléchargement du client car le réseau protégé par cette méthode est totalement injoignable tant que l'utilisateur n'est pas connecté (et donc identifié).

5.4.4 Architecture finale déployée

Les tests sur les différentes maquettes ont permis de choisir une architecture évolutive tout en conservant la structure des systèmes VPN.

5.4.4.1 Capacités de l'architecture

Aucune solution ne pouvant couvrir l'ensemble de nos besoins, nous avons choisi de les combiner ensemble; ainsi les intérêts de cette architecture sont les suivants :

- fonctionnement classique du VPN Cisco, permettant un accès depuis les réseaux sans fil mais aussi d'autres lieux (domiciles, séminaires...) : les utilisateurs connaissant ce système peuvent continuer à l'utiliser,
- accès authentifié à Internet sans configuration : aucune action nécessaire sur le poste de l'utilisateur (le portail captif intercepte les requêtes HTTP et HTTPS), hormis le choix du réseau, nommé "XXXX-ACCUEIL"[115],
- ajout du mode WPA assurant la compatibilité du réseau avec les spécifications du groupe de travail ARREDU et EDURoam (authentification EAP, chiffrement compatible WPA et WPA2),
- dans les trois cas, gestion de la traçabilité (accounting) en respect de la charte Renater,
- mutualisation du système d'authentification par le réseau STAR : chaque université conserve la gestion de ses utilisateurs dans son domaine mais ceux-ci peuvent accéder à leurs ressources depuis l'ensemble des universités,
- coûts relativement faibles pour étendre la structure existante. Les solutions choisies sont gratuites et publiques (évolutions régulières).

Le tableau suivant récapitule les fonctionnalités offertes aux utilisateurs ainsi que les avantages de cette architecture.

115 La convention de nommage des SSID impose de commencer avec l'identifiant de l'organisme.

	Cisco VPN	Talweg	WPA & WPA2
Authentification locale	✓	✓	✓
Authentification répartie (EDURoam, inter-U)	✗	✓	✓
Traçabilité	✓	✓	✓
Fonctionnement sans ajout de logiciel client	✗	✓	✗
Accès depuis extérieur (ADSL, congrès...)	✓	✗	✗
Utilisation d'un VPN privé	✗	✗	✓
Sécurisation des communications	✓	✓	✓
Utilisation à partir d'un LAN (libre service campus)	✓	✓	✗
Coût additionnel à la structure existante	0	0	0

Tableau 13: Tableau récapitulatif de l'architecture mixte

5.4.4.2 Intégration des différentes solutions

Le schéma ci-après décrit l'intégration des différentes solutions dans l'architecture déjà existante.

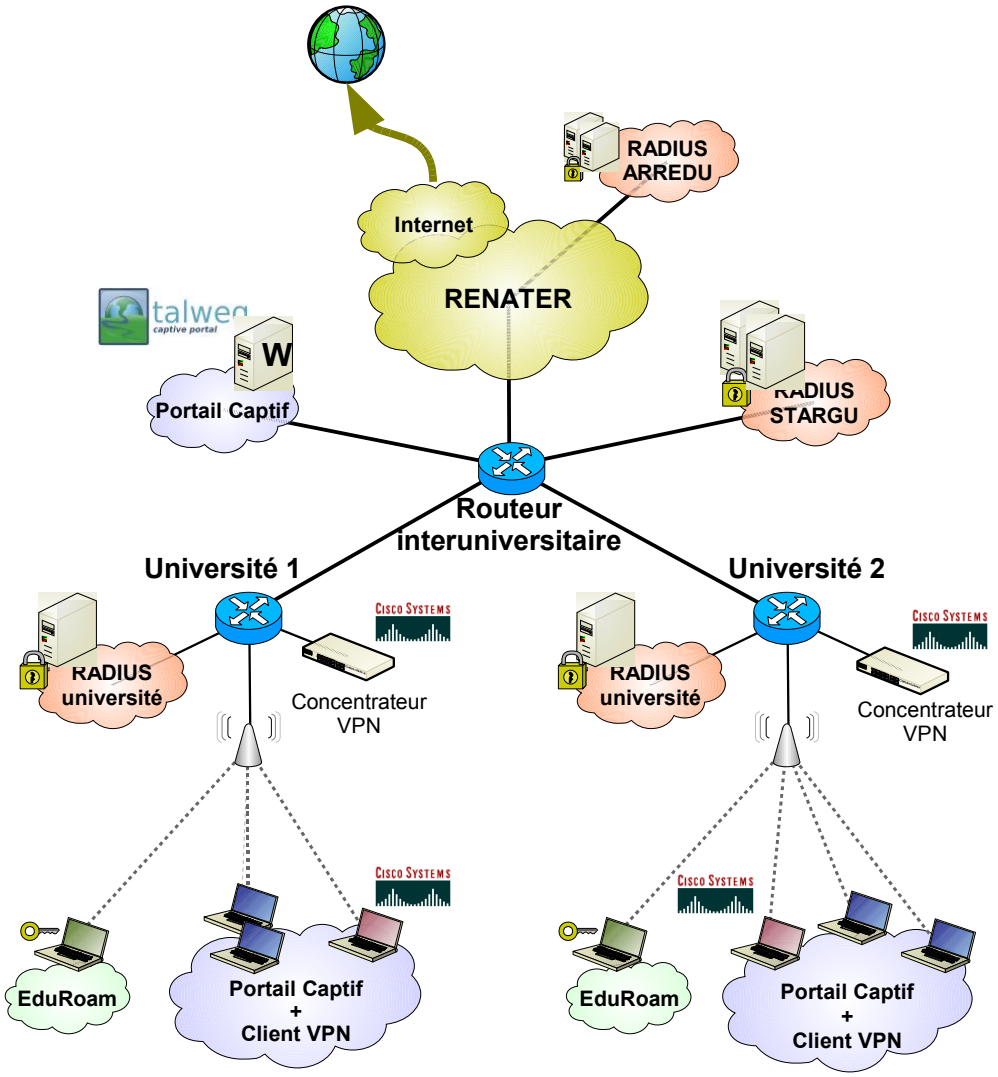


Illustration 76: Architecture STAR interuniversitaire finale

Chaque université possède déjà un concentrateur VPN Cisco et des points d'accès compatibles WPA permettant l'annonce de plusieurs SSID, dont celui alloué à EDURoam.

Il est nécessaire d'affecter une plage d'adresses IP routables pour ce VLAN/SSID car les équipements authentifiés dans ce SSID auront accès aux services suivants[116] :

- services web (protocoles HTTP et HTTPS mais aussi DNS),
- services VPN (protocole IPSec),
- services messagerie (protocoles POPS, IMAPS et protocole SMTP via le serveur de messagerie local),
- services divers (protocoles SSH, NTP et ICMP).

Grâce à cette architecture, un visiteur utilisant régulièrement le réseau ARREDU[117] ou EDUroam n'aura aucune difficulté à se connecter à Internet et utiliser l'ensemble des services définis lors de la réunion au CRU[118] en juin 2005.

L'architecture STAR permet ainsi une grande souplesse sur les autres moyens d'accès : le portail captif et le système VPN. Dans ce cas, le SSID "XXX-ACCUEIL" (où XXX représente l'abréviation de l'université où se trouve le point de connexion) est accessible à tout le monde dans un réseau privé sur lequel se trouve le serveur d'information : celui-ci contient les données d'informations ainsi que les fichiers à télécharger (client VPN, client EAP et patches WPA2 pour Windows). Le portail captif est également disponible dans cette plage pour un accès immédiat (mais plus limité) à Internet.

5.5 Salubrité de poste

Bien que ce point soit optionnel dans le cahier des charges, nous avons suivi le projet de salubrité de l'équipe placée sous la responsabilité de Daniel GUENICHE (CNRS). Cette équipe travaille sur un moyen de garantir la salubrité d'une machine lors de sa connexion au réseau. De notre côté, nous avons partagé le résultat de nos travaux sur l'authentification EAP.

5.5.1 Objectifs

Les vers et virus informatiques représentent une menace de plus en plus importante : la plupart des organismes sécurisent leurs réseaux des attaques extérieures mais négligent les attaques provenant de l'intérieur. Le nomadisme lève le voile sur ces risques mais les solutions ne se sont pas encore généralisées et sont coûteuses : Cisco Secure Agent, eTrust Intrusion Detection, Mcafee Entercept et IntruShield...

Nous avons donc défini les objectifs suivants :

- trouver un système peu coûteux,
- trouver un système ouvert et non propriétaire,
- trouver un système efficace.

Pour cela, le développement d'une application a paru intéressant au CNRS.

116 Accès définis lors de la réunion du 14 juin 2005 dans le cadre du projet ARREDU
117 ARREDU : Authentication & Roaming for Research and EDUcation
118 CRU : Comité Réseau des Universités

5.5.2 Moyens

Les solutions du marché étant très fermées, nous avons imaginé une application qui pourrait faire l'intermédiaire entre les systèmes de protection du poste et le système d'authentification. Pour cela, il faut déterminer les critères de salubrité :

- la présence en mémoire d'un processus antivirus et pare-feu connus,
- la validité du chemin de lancement de ces processus,
- l'intégrité des fichiers exécutables (empreinte MD5 par exemple),
- la validité des éléments comme la date ou la taille des fichiers,
- les clés de registre propres à ces applications (certaines donnent l'état du processus).

Ces critères peuvent être pondérés pour obtenir une application dotée d'une "rigueur" ajustable : il vaut mieux demander à l'utilisateur pourquoi une application a changé plutôt que de bloquer son accès suite à la mise à jour de son système ou à l'évolution des applications.

Notre application est ainsi capable – à partir de cet indice de confiance – de fournir un mot de passe à usage unique ou bien de lancer le système d'authentification. Cependant le passage de la théorie à la pratique présente de nombreuses difficultés.

5.5.3 Problèmes rencontrés

Nous avons créé quelques programmes de tests pour vérifier la faisabilité mais nous avons également découvert des obstacles qui n'ont pas permis la concrétisation du projet. Les questions suivantes restent en suspend :

- Comment empêcher un utilisateur d'utiliser le système d'authentification de son système plutôt que le nôtre ?
- Comment traiter une authentification EAP-TLS (par certificats client et serveur) ?
- Comment garantir au système d'authentification que l'application qui lui fournit les données (et l'indice de confiance du poste) soit bien la nôtre ?
- Comment obtenir des critères actualisés alors que le système n'a pas encore accès au réseau ?

Nous n'avons pas eu le temps d'approfondir le sujet mais il apparaît clairement que la salubrité et la médication de postes informatiques représentent un volet important et long à traiter.

5.6 Gestion du projet

Pour parvenir à la solution finale, nous avons dû utiliser une approche par enrichissement afin de valider chaque nouveau point et intégrer de nouvelles notions. Sur la fin du projet nous avons ainsi pu apporter notre contribution active au projet national ARREDU.

Le travail effectué pendant un an correspond donc à plusieurs sous-projets ou plusieurs étapes. Les différentes approches concernant le développement du projet, son organisation et les méthodes de communications employées sont décrites ici.

5.6.1 Déroulement du projet

Ce projet comporte une grande part de recherche et la représentation du travail effectué dans le temps est relativement simple : le rythme devient de plus en plus rapide, au fur et à mesure que les concepts sont intégrés. Alors qu'au début il fallait intégrer de nombreuses notions, la fin du projet fut surtout ralentie par des problèmes techniques.

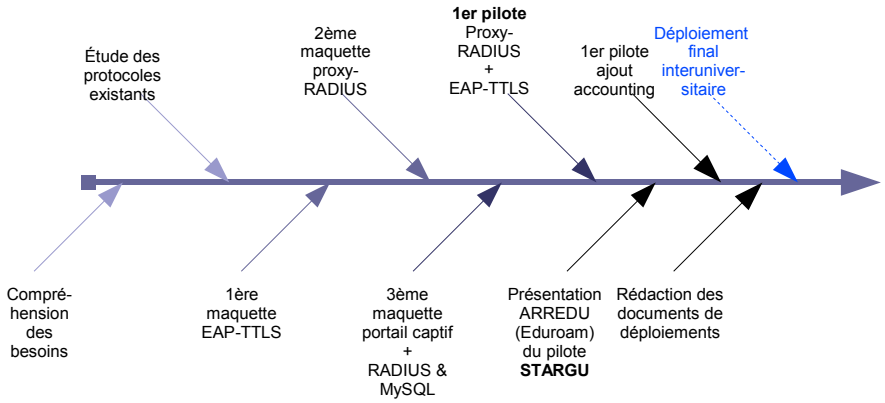


Illustration 77: Progression du travail dans le temps

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.

Nous avons ébauché une représentation par un diagramme de Gantt, toutefois, la plupart des étapes correspondent à de la recherche et des essais : dans ces conditions, il est difficile de quantifier précisément les différentes tâches et les temps alloués. Si cela peut fonctionner sur un déploiement – dans lequel la plupart des opérations sont connues – cela n'est pas opportun dans un projet de recherche et peut même entraver l'avancement.

De plus, la progression se faisant pas à pas, chaque nouvelle étape évolue en fonction des résultats obtenus aux précédentes.

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

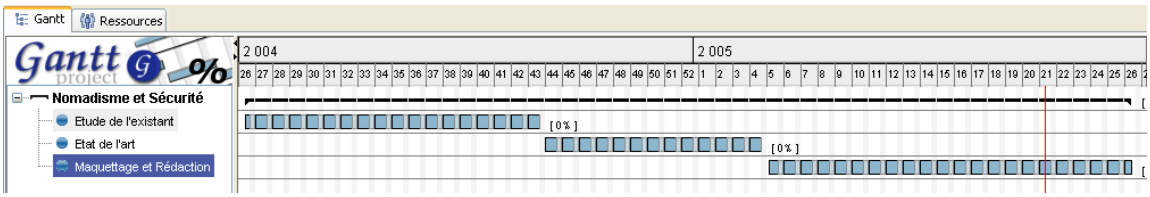


Illustration 78: Gestion de projet par diagramme de Gantt

En fait, le mode de développement du projet correspond à un ensemble de cycles itératifs :

- planification 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 œuvre),
- 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.

Ainsi, pour ne pas perdre de vue l'objectif final et gérer correctement le temps et les ressources nous avons choisi un ensemble d'applications et de méthodes nous permettant de faire le point à tout moment.

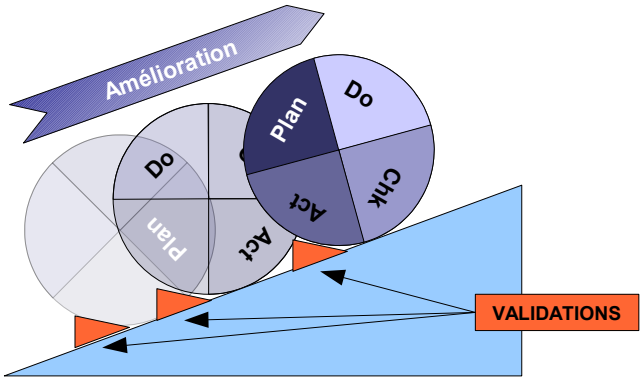


Illustration 79: Cycle de la roue de Deming

5.6.2 Organisation des idées

A la base, le sujet met en œuvre deux notions distinctes : le nomadisme et la sécurité. Nous avons rapidement constaté que le nomadisme touche plusieurs domaines et que la sécurité est l'un d'eux. La maîtrise du sujet nécessitant l'intégration de nombreuses connaissances, l'utilisation d'un outil pour organiser nos idées nous a semblé judicieux afin de ne perdre aucune piste ou possibilité.

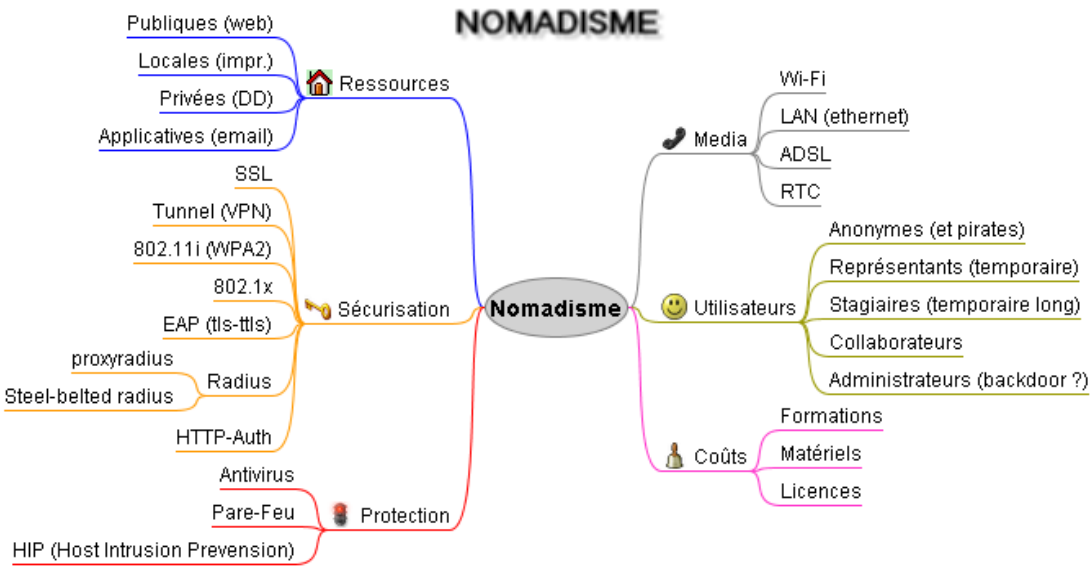


Illustration 80: Organisation d'idées... le projet au début de l'étude

Nous avons choisi Freemind (http://freemind.sourceforge.net/), un logiciel libre qui permet de tracer des cartes heuristiques. L'utilisation de cet outil très visuel permet d'organiser facilement et rapidement les thèmes (branches principales) et les idées (feuilles). Il est alors simple de ré-organiser, d'ajouter, déplacer et supprimer des feuilles afin de conserver une vue globale du projet. A chaque nœud on peut associer des commentaires, des icônes et des liens. Cet outil est vraiment pratique dans les projets de recherche et d'ordonnancement d'idées.

Le graphe ci-dessus montre la structure au début du projet : même si l'on constate que certaines notions n'étaient pas encore connues correctement (mauvaise position dans l'arbre, idées "en vrac") tous les thèmes à aborder ont été détaillés.

5.6.3 Communication

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

5.6.3.1 Communication interne

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

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 autres participants du projet.

Cet outil a les avantages suivants :

- accessible en ligne à plusieurs personnes (protection par mot de passe possible),
- organisation des billets publiés par date et par catégorie,
- recherche par mots-clés,
- ajout de commentaires par les lecteurs possible,
- accès asynchrone aux informations (plus souple que la messagerie car il n'est pas besoin de filtrer par projet).

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 fourni ci-dessous :

Illustration 81: Exemple de "weblog" employé pour le projet STAR

5.6.3.2 Communication externe

Les premières communications ont commencé sur la liste de diffusion de FreeRADIUS. Cette liste met en relation de nombreux utilisateurs de FreeRADIUS dans le monde, permettant ainsi un véritable partage des expériences de chacun ! C'est dans cette liste que j'ai obtenu des réponses sur l'utilisation de l'accounting, ses limites et les solutions développées par certains.

Nous avons également travaillé avec le CNRS et l'équipe de Daniel GUENICHE sur la partie salubrité. Bien qu'elle ne soit pas développée dans cette étude faute d'éléments concrets et de solutions matures (y compris dans les produits commerciaux), nous avons régulièrement fait le point sur l'avancement de nos travaux respectifs.

Ensuite, lorsque le projet du CRU appelé ARREDU a débuté en mars 2005, nous avons également présenté une dizaine de transparents sur l'état de notre projet STAR aux personnes inscrites à la première réunion de coordination (14 juin 2005). Nous avons pu faire partager notre expérience à d'autres universités françaises et répondre aux problèmes que nous avions nous mêmes rencontrés quelques semaines plus tôt.

La fin du cycle de test du projet STAR a également abouti à une présentation aux universités de Grenoble le vendredi 1er juillet 2005. Afin que le projet puisse prendre essor, un document écrit d'une vingtaine de pages a été fourni à cette occasion pour décrire comment mettre en œuvre l'authentification interuniversitaire : l'architecture générale, les applications utilisées, les configurations ainsi que les scripts facilitant sa mise en œuvre ont été décrits à cette occasion. La présentation des différentes solutions testées a été soutenue par une démonstration de toutes les solutions opérationnelles (VPN SSL Cisco, portail Talweg, WPA et WPA2) et notamment l'utilisation de l'authentification répartie (grâce à la participation à titre expérimental de l'UPMF qui utilise également un RADIUS pour ses authentifications).

Enfin, le résumé sur notre activité a été retenu pour la publication et la soutenance d'un article au congrès bi-annuel des JRES 2005. Cette manifestation "*contribue au déploiement et à l'essor des nouvelles technologies pour l'information et la communication*"[119]. L'article [JRES05] a été déposé (en septembre 2005) et la présentation correspondante est prévue le 6 décembre 2005.

119 Citation prise sur le site JRES : Journées RESeaux (http://www.jres.org/)

6 CONCLUSION ET PERSPECTIVES

Après plusieurs mois de travail, l'étude s'est terminée par le déploiement d'une solution fonctionnelle. Cette solution est constituée de plusieurs applications car les essais effectués ont démontré qu'il n'existait pas de solution idéale, simple, flexible et capable de répondre à tous les cas de figures.

En témoignent, les orientations des groupes de travail français ARREDU et européen EDURoam : la sécurisation d'un flux de données est un savoir-faire acquis mais l'authentification reste le point sensible...

Concernant l'architecture déployée au niveau des universités de Grenoble, nous avons tenté de préserver une structure qui soit ouverte et évolutive, en intégrant les moyens existants, en ajoutant les méthodes récentes et en préparant les systèmes futurs.

6.1 Pérennité de la solution VPN

L'étude démontre que l'utilisation d'un système VPN qui semblait une solution désuète reste actuellement la seule solution vraiment flexible pour l'utilisateur nomade : l'accès au réseau de son organisation depuis son domicile, son travail ou bien un congrès est un avantage qu'aucune autre solution ne possède. Bien que l'installation du client VPN et d'un fichier de configuration soit nécessaire à la connexion initiale, son utilisation reste aisée par la suite.

6.2 Validité des solutions déployées

L'architecture VPN est complétée par les solutions basées sur un système WPA et sur un portail captif pour répondre à l'ensemble des besoins des utilisateurs. Ainsi, muni d'un identifiant et d'un mot de passe, chaque utilisateur peut choisir son mode de connexion, en fonction de ses besoins. Néanmoins, cela n'est pas une réponse complètement satisfaisante car la problématique est déplacée plutôt que résolue : en effet, l'authentification répartie met en œuvre une politique de confiance entre les établissements ayant adhéré au projet ARREDU mais hors de ce périmètre, les autres universités ou bien les visiteurs extérieurs ne peuvent être authentifiés et demeurent des cas particuliers.

6.3 Perspectives émergeantes

Désormais en phase pilote, ce projet permet une ouverture plus grande et une flexibilité plus importante pour les utilisateurs nomades. L'architecture ainsi constituée reste robuste face aux attaques extérieures. Pourtant, le manque de temps et l'augmentation de connaissances soulèvent quelques réflexions qui restent en suspend.

6.3.1 Perspectives sur l'authentification

Concernant l'utilisation d'un serveur AAA, de nouvelles questions sont posées :

- A court terme, il reste à vérifier le fonctionnement de la redondance de serveurs 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 quels sont 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 serait le filtrage par protocole en fonction de l'utilisateur. Le filtrage de plages IP reste plus difficile à gérer car l'architecture ne permet pas de déterminer les adresses IP de l'utilisateur à l'avance. Cette limitation pourra-t'elle disparaître avec l'arrivée d'IPv6 ?
- A long terme, la mise en œuvre de la qualité de service (QoS) devrait permettre l'utilisation d'applications comme la voix sur IP. Cependant, RADIUS connaît certaines limitations que son successeur – Diameter – devrait faire disparaître et le processus de handover en 802.11 reste long (et encore plus en cas de changement de SSID) : quelles applications ou mécanismes ou standards permettront une authentification régulière et suffisamment rapide ?

6.3.2 Perspectives sur la protection

Bien que les travaux effectués en collaboration avec le CNRS n'aient pas abouti, ils permettent de lever le voile sur certaines interrogations :

- A moyen terme, les applications permettant l'authentification et l'acceptation sur le réseau devront intégrer des notions de salubrité. Nos travaux ont montré que les antivirus et les pare-feux intégrés peuvent fournir des éléments de réponse mais aucun supplicant n'est capable de les intégrer. Existera-t'il des supplicants intégrant la salubrité lors de l'authentification ?
- A long terme, l'utilisation d'une seule boîte d'authentification lors de la connexion principale devrait éviter les saisies de mots de passe multiples. L'interface GINA de Microsoft devrait donc évoluer vers un modèle plus ouvert (acceptant d'autres modes d'authentification) ou devrait être remplacée par l'interface des logiciels supplicants eux-mêmes. Un autre problème sera alors de pouvoir s'assurer que la boîte de dialogue d'identification ne soit pas une fausse interface mise en place par un cheval de Troie...

6.3.3 Perspectives sur les autorisations

Notre architecture ne permet pas encore de gérer les droits et autorisations d'accès à différents serveurs et protocoles. Les prochaines évolutions pourraient tenter de répondre aux faiblesses suivantes :

- A court terme, le système devrait être capable de gérer l'accueil d'un visiteur pour une durée déterminée ou bien fournir un moyen d'authentification temporaire aux personnes participantes à un congrès ou un séminaire. Dans l'état actuel, une modification manuelle du fichier 'users' sur le serveur RADIUS est possible mais reste une opération sensible puisqu'elle oblige à relancer le démon. Un script lancé régulièrement (crontable) avec un formulaire sur une page web pourrait accomplir ce travail de manière fiable.
- A moyen terme, l'unification du système d'authentification pourrait permettre à l'utilisateur de ne retenir qu'un seul mot de passe (systèmes SSO). Toutefois, même s'il s'appuie sur un annuaire, RADIUS ne peut gérer les autorisations sur des systèmes incompatibles. Les paires attribut-valeur restent liées au matériel employé (des AVP Cisco ne fonctionneront pas sur du matériel Nortel par exemple). L'affectation des autorisations reste donc soumise au système terminal (là où se trouve physiquement l'utilisateur). Les autorisations seront-elles gérées directement sur les serveurs ou bien une norme sera-t'elle créée ou étendue ?

- A long terme, chaque utilisateur d'un système informatique sera authentifiable par son système mais comment les systèmes pourront communiquer entre eux ? Si un utilisateur d'une société privée veut s'authentifier sur le campus, il faudra probablement que les serveurs d'authentification passent par un organisme de confiance capable de certifier les deux équipements.

6.4 Projections

Pour résoudre les problèmes posés, il faudrait un système unifié au niveau mondial : Microsoft a bien essayé d'imposer sa solution avec son système d'authentification Passport mais les craintes de tous les organismes ainsi que quelques failles de sécurité ont eu raison de lui.

Cependant, la voie est ouverte et d'autres sociétés tentent de créer un standard pour demain : Liberty Alliance (http://www.projectliberty.org/), fondé par Sun, IBM, Nokia et HP entres-autres. Ce standard devrait être une solution d'identification alternative basée sur des standards ouverts.

Ce marché sera donc certainement le défi des années à venir...

7 ANNEXES

7.1 Les standards PKCS

Extrait du document RSA : Introduction to the PKCS Standards

http://www.rsasecurity.com/products/bsafe/overview/IntroToPKCSstandards.pdf

Standard	Description
PKCS #1	The RSA encryption standard. This standard defines mechanisms for encrypting and signing data using the RSA public key system.
PKCS #3	The Diffie-Hellman key-agreement standard. This defines the Diffie-Hellman key agreement protocol.
PKCS #5	The password-based encryption standard (PBE). This describes a method to generate a Secret Key based on a password.
PKCS #6	The extended-certificate syntax standard. This is currently being phased out in favor of X509 v3.
PKCS #7	The cryptographic message syntax standard. This defines a generic syntax for messages which have cryptography applied to it.
PKCS #8	The private-key information syntax standard. This defines a method to store Private Key Information.
PKCS #9	This defines selected attribute types for use in other PKCS standards.
PKCS #10	The certification request syntax standard. This describes a syntax for certification requests.
PKCS #11	The cryptographic token interface standard. This defines a technology independent programming interface for cryptographic devices such as smartcards.
PKCS #12	The personal information exchange syntax standard. This describes a portable format for storage and transportation of user private keys, certificates etc.
PKCS #13	The elliptic curve cryptography standard. This describes mechanisms to encrypt and sign data using elliptic curve cryptography.
PKCS #14	This covers pseudo random number generation (PRNG). This is currently under active development.
PKCS #15	The cryptographic token information format standard. This describes a standard for the format of cryptographic credentials stored on cryptographic tokens.

Tableau 14: Les standards PKCS

7.2 Les groupes de travail de l'IEEE

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)

Tableau 15: Les groupes de travail de l'IEEE 802

7.3 Valeurs de fréquences et puissance d'émission

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

Tableau 16: Fréquences et puissances d'émission 802.11

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

7.4 Principe de l'étalement de spectre

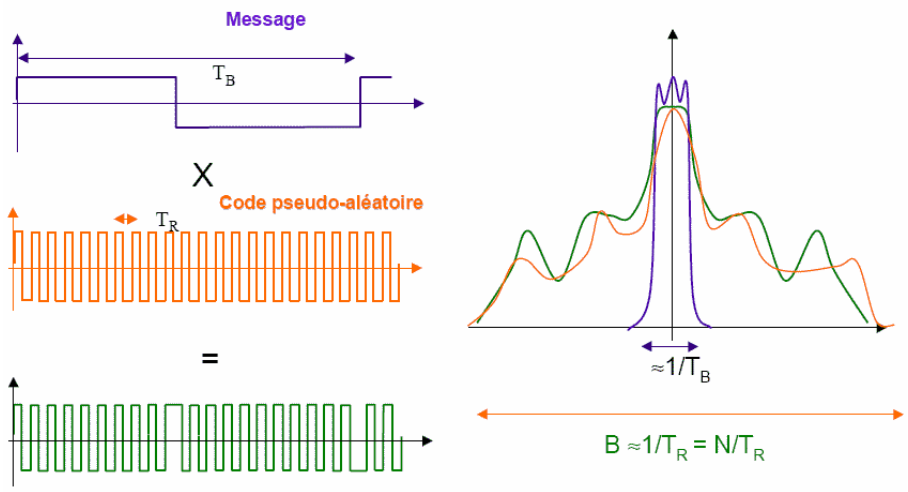


Illustration 82: Principe de l'étalement de spectre

Image extraite du cours "U23 Eléments sur l'étalement de spectre" de LAHC [WEB004]

7.5 Différences et similitudes entre protocoles VPN

	PPTP	*L2F*	*L2TP/IPSec*	*IPSec transport*
Le FAI doit s'impliquer dans la négociation du RPV	NON	OUI	Au choix	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)
Peut encapsuler autre chose que de l'IP	**OUI**	**OUI**	**OUI**	NON
Authentification de l'utilisateur	OUI via PPP	OUI via PPP	OUI via PPP	Standard en cours
Authentification des machines	OUI en attribuant un compte utilisateur à la machine	**OUI**	**OUI**	**OUI**
Confidentialité (cryptage)	**OUI**	**OUI**	**OUI**	**OUI**
Intégrité	NON	NON	**OUI**	**OUI**
Support du NAT-T (NAT traversal)	OUI	OUI	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

Tableau 17: Les différents protocoles VPN (niveau 2 et 3)

Tableau extrait du livre "Les VPN" [COCO03]

7.6 Script d'accounting

```
#!/usr/bin/perl -w
#
# ====================================================================
# This program is free software; you can redistribute it and/or modify
# it under the terms of version 2 of the GNU General Public License as
# published by the Free Software Foundation.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.
#====================================================================
# Author      : Rok PAPEZ (ARNES)
# Modified by : David ROUMANET (DSIGU)
# Date        : 22/06/2005
# Version     : 1.0
# Usage       : can account IP addresses, MAC addresses, username and
#               start/stop timestamp with FreeRadius and DHCP.
#               very useful for 802.1x - EAP authentication.
# --------------------------------------------------------------------
# How it works ?
# This script launch 2 daemons : one for parsing DHCP syslog and the
# second for AP associations (via snmp : be care about community name and
# OID). DON'T USE IT WITH 'AT' COMMANDS !
# ====================================================================

use strict;
use Time::Local;
use Sys::Syslog;
use POSIX;
use DBI;
use Net::SNMP;
use File::Tail;

##########################################
# Configuration                          #
##########################################
my $dsn = 'DBI:mysql:radius:localhost';
my $db_user_name = 'root';
my $db_password = 'database';
my $logfile = '/var/log/dhcp.log';

my $ap_community = 'ap_maquette';
my %ap_list = (
       "000e.8384.cd9e" => "10.5.240.16",
       "000e.8440.bbb1" => "10.5.240.16"
);
# Which facility should messages be logged to
my $facility = 'local7';
# Preveri odprte povezave na vsake X sekund.
my $poll_ap = 10;
#my $online_time_check = 60*60*24; # 24 hrs
my $online_time_check = 60; # 60 seconds
# ========================================
# and constants/variables
my $apClientTable = ".1.3.6.1.4.1.9.9.273.1.2.1.1.14";
my %months = ('Jan', 0, 'Feb', 1, 'Mar', 2, 'Apr', 3, 'May',  4, 'Jun',  5,
              'Jul', 6, 'Avg', 7, 'Sep', 8, 'Oct', 9, 'Nov', 10, 'Dec', 11);
my $pid_dhcp = 0;
my $pid_ap = 0;
my $file;
my $line;
my $rc;
```

```
my $dbh;
my $sql_dhcp;
my $sql_get;
my $sql_close;

# ========================================
sub signal_handler {
       syslog('err', "Received signal $_[0], TERMINATING!");
       exit(-1);
}

# ========================================
# Create daemon and setup syslog logging
sub daemonize {
    my $pid = 1;
    my $rc = 0;
    openlog('bio_monitor', 'ndelay,pid', $facility)
        or die "Can't open syslog: $!";
    chdir '/'                 or die "Can't chdir to /: $!";
    umask 0;
    open STDIN, '/dev/null'   or die "Can't read /dev/null: $!";
    setsid                    or die "Can't start a new session: $!";
    open STDOUT, '>>/dev/null' or die "Can't write to /dev/null: $!";
    open STDERR, '>>/dev/null' or die "Can't write to /dev/null: $!";
    $SIG{INT}='signal_handler';
    $SIG{TERM}='signal_handler';
    $SIG{KILL}='signal_handler';
    $SIG{__DIE__}='signal_handler';
    $pid = fork;
    defined($pid) or syslog('err', "Can't fork: $!");
    exit 0 if $pid;
}

# ========================================
# Create connection
sub connect_to_mysql {
       $dbh = DBI->connect($dsn, $db_user_name, $db_password);
       if(!defined($dbh)) {
              syslog('err', "ERROR: connect to MySQL database failed!\n");
              exit(-1);
       }
}

sub connect_to_mysql_dhcp {
       &connect_to_mysql;
       $sql_dhcp = $dbh->prepare(q{UPDATE ACCOUNTING SET
                `Client-IP-Address` = ?,
                `Timestamp Dhcp` = NOW()
        WHERE
                `Calling-Station-Id` = ? AND
                `Timestamp Start` <= FROM_UNIXTIME(?) AND
                `Timestamp Stop` = '0000-00-00 00:00:00'
        });
}

sub connect_to_mysql_ap {
       &connect_to_mysql;

        $sql_get = $dbh->prepare(q{SELECT
                `Calling-Station-Id`,
                `User-Name`,
                UNIX_TIMESTAMP(`Timestamp Start`),
                `Client-IP-Address`,
                `Called-Station-Id`
        FROM ACCOUNTING WHERE
                `Timestamp Stop` = '0000-00-00 00:00:00'
        ORDER BY
                `Timestamp Start` DESC
        });

        $sql_close = $dbh->prepare(q{UPDATE ACCOUNTING SET
                `Timestamp Stop`          = NOW(),
                `Acct-Terminate-Cause`    = 'Script-Cleanup'
        WHERE   `Calling-Station-Id` = ?
        AND     `User-Name` = ?
        AND     `Client-IP-Address` = ?
```

```
        AND     `Called-Station-Id` = ?
        AND     `Timestamp Stop` = '0000-00-00 00:00:00'
        AND     `Timestamp Start` = FROM_UNIXTIME(?)
        });
}

# ========================================
# Check if client with a given MAC is online
sub check_client {
        my $mac = $_[0];
        my $ap_mac = $_[1];
        my $ap_ip;
        my $key;
        my $mac_oid;
        my $result;

        defined($ap_list{$ap_mac}) or die "IP address for NAS $ap_mac isn't defined\n";
        $ap_ip = $ap_list{$ap_mac};

        $mac =~ m/(..)(..)\.(..)(..)\.(..)(..)/;
        $mac_oid = sprintf("%d.%d.%d.%d.%d.%d", hex $1, hex $2, hex $3, hex $4, hex $5, hex
$6);
        my ($session, $error) = Net::SNMP->session(
                -hostname  => $ap_ip,
                -community => $ap_community,
                -translate => [ -octetstring => 0x0 ],
                -version   => "snmpv2c"
        );

        if(!defined($session)) {
                syslog('err', "ERROR in SNMP session establish: %s\n", $error);
                return 1;
        }

        $result = $session->get_table(
                -baseoid => $apClientTable
        );
        if(!defined($result)) {
                if(!$session->error_index) {
                        return 0; # an empty table "error", that's OK.
                }
                # Complain and that's it. Return as if user is present.
                syslog('err',"ERROR in SNMP get_table: %s\n", $session->error);
                return 1;
        }
        $session->close;

        foreach $key (keys(%{$result})) {
                if ($key =~ m/$mac_oid$/) {
                        return $result->{$key} == 3;
                }
        }
        return 0;
}

# ========================================
# Monitor dhcp log file and insert IP address
sub monitor_dhcp {
       &connect_to_mysql_dhcp;
       # search in the DHCP logfile for new messages
       $file=File::Tail->new(name=>$logfile, maxinterval=>1, interval=>1);
       syslog('notice',"Running, PID: $$\n");

       while( 1 ) {
              $line = $file->read;
              if(!defined($line)) {
                     syslog('err',"Unable to get a line from DHCP log! TERMINATING!");
                     exit(-1);
              }
              $rc = $dbh->ping;
              if(1 != $rc) {
                     syslog('warning',"Lost connection to MySQL database! Restarting the
connection!");
                     $dbh->disconnect;
                     &connect_to_mysql;
                     $rc = $dbh->ping;
```

```
                        if(1 != $rc) {
                                syslog('err',"Again lost connection to MySQL database!
TERMINATING!");
                                exit(-1);
                        }
                }

                # search for a line wich contain "dhcpd: DHCPACK on" (regular expression)
                if ( $line =~ m/^(\w+)\s+(\d+)\s+(\d+):(\d+):(\d+) \S+ dhcpd: DHCPACK on (\S+)
to (\S+)/ ) {
                        my $month = $1;
                        my $day = $2;
                        my $h = $3;
                        my $m = $4;
                        my $s = $5;
                        my $ip = $6;
                        my $mac = $7;
                        my $year = (localtime)[5] + 1900;
                        $month = $months{$month};
                        # check year change!
                        if( 11 == $month && 31 == $day ) {
                                my $cur_day = (localtime)[3];
                                # If it's january the 1st, we missed a year change!
                                if( 1 == $cur_day) {
                                        $year--;
                                }
                        }
                        # change MAC from PC to Cisco AP format -- can also be changed in AP
config
                        $mac =~ s/(..)\:(..)\:(..)\:(..)\:(..)\:(..)/$1$2\.$3$4\.$5$6/;
                        my $timestamp = timelocal($s, $m, $h, $day, $month, $year);
                        # Execute SQL request with local arguments
                        $sql_dhcp->execute("$ip", "$mac", $timestamp ) || die $dbh->errstr;
                        syslog('info', "Inserted DHCP assigned address: $year-%02d-%02d,
%02d:%02d:%02d, IP: $ip, MAC: $mac, timestamp: $timestamp", $month + 1, $day, $h, $m, $s);
#                       $dbh->commit || die $dbh->errstr;
                }
        }
        $dbh->disconnect;
        exit(0);
}
# ========================================
# Check connections on every interval
sub monitor_connections {
        my $tmp;
        my $key;
        my $data;
        my $result;
        my %users;      # Key is a MAC, data is array[array[User, Start, IP, AP MAC]]

        &connect_to_mysql_ap;

        while (1) {
                %users = {};
                $sql_get->execute() || die $dbh->errstr;
                while ($result = $sql_get->fetchrow_arrayref) {
                        # The data returned is: Calling-Station-Id, User-Name, Timestamp Start,
Client-IP-Address, Called-Station-Id
                        syslog('debug', "User $result->[1], mac: $result->[0] on
$ap_list{$result->[4]}, Start: $result->[2]\n");
                        $tmp = $users{$result->[0]};
                        push(@$tmp, [$result->[1], $result->[2], $result->[3], $result->[4]]);
                        $users{$result->[0]} = $tmp;
                }

                foreach $key (keys(%users)) {
                        my $i = 0;
                        $tmp = $users{$key};
                        for $data (@$tmp) {
                                syslog('debug', "MAC($i): $key, USER: $data->[0], Start: $data-
>[1], IP: $data->[2], AP MAC: $data->[3]\n");
                                if(!$i and $data->[1] + $online_time_check < time()) {
                                        syslog('debug',"Record IS OLD, checking user\n");
                                        if(!check_client($key, $data->[3])) {
                                                syslog('debug', "User not present, closing the
accounting record\n");
```

```
                                                $sql_close->execute($key, $data->[0], $data->[2],
$data->[3], $data->[1]) || die $dbh->errstr;
                                                syslog('info', "Accounting closed. MAC: $key,
USER: $data->[0], Start: $data->[1], IP: $data->[2], AP MAC: $data->[3]\n");
                                        }
                                }
                                if ($i) {
                                        syslog('debug', "Record is a duplicate, checking
user\n");
                                        if(!check_client($key, $data->[3])) {
                                                syslog('debug', "User not present, closing the
accounting record\n");
                                                $sql_close->execute($key, $data->[0], $data->[2],
$data->[3], $data->[1]) || die $dbh->errstr;
                                                syslog('info', "Accounting closed. MAC: $key,
USER: $data->[0], Start: $data->[1], IP: $data->[2], AP MAC: $data->[3]\n");
                                        }
                                }
                        $i++;
                        }
                }
                sleep($poll_ap);
        }

        $dbh->disconnect;
        exit(0);
}
# ========================================

&daemonize;

while(1) {
        # If child doesn't exist, create it.
        if(!$pid_dhcp) {
                $pid_dhcp = fork;
                defined($pid_dhcp) or syslog('err', "FATAL: Can't fork: $!");
                if(!$pid_dhcp) {
                        monitor_dhcp();
                }
        }
        if(!$pid_ap) {
                $pid_ap = fork;
                defined($pid_ap) or syslog('err', "FATAL: Can't fork: $!");
                if(!$pid_ap) {
                        monitor_connections();
                }
        }

        $rc = wait();
         if($rc <= 0) {
                syslog('err', "Error $rc, waiting for child");
                exit -1;
        }
        if ($rc == $pid_dhcp) {
                syslog('warning', "DHCP child $pid_dhcp died, restarting it!");
        }
        if ($rc == $pid_ap) {
                syslog('warning', "AP child $pid_ap died, restarting it!");
        }
}

exit 0;
```

7.7 Extraits de la notice de configuration du réseau STAR

NOTICE DE CONFIGURATION

DES ELEMENTS CONSTITUANTS

LE RESEAU STAR

(Système Transversal d'Authentification Réseau)

GRENOBLE UNIVERSITÉS
Direction des Systèmes d'Information
Département Réseau
star@grenet.fr

Responsable projet : Eric JULLIEN
Auteur : David ROUMANET
Correcteur : Patrick PETIT
Version : 1.0 (juin 2005)

TABLE DES MATIÈRES

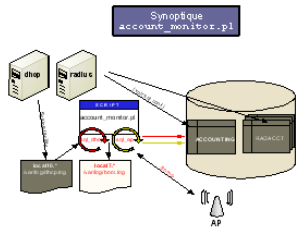
1 Architecture générale....3
1.1 Introduction....3
1.2 Schéma global de l'architecture....4
1.3 Conseils d'installation....4
2 Serveur DHCP....5
2.1 Installation serveur DHCP....5
2.2 Configuration serveur DHCP....5
2.3 Activation serveur DHCP et Syslog....6
3 Serveur AAA....7
3.1 Installation serveur AAA....7
3.2 Configuration serveur AAA....7
3.2.1 Configuration serveur AAA local....8
3.2.2 Configuration serveur AAA relais....11
3.3 Activation serveur AAA....11
4 Base de données MySQL....13
4.1 Installation base de données MySQL....13
4.2 Configuration base de données MySQL....14
4.3 Activation base de données MySQL....14
4.4 Client graphique sous Windows....15
5 Point d'accès et commutateur....16
5.1 Installation point d'accès et commutateur....16
5.2 Configuration point d'accès et commutateur....16
5.2.1 Configuration d'un point d'accès sans fil (Cisco)....16
5.3 Activation point d'accès et commutateur....17
6 Client (supplicant)....18
6.1 Installation Client....18
6.1.1 Microsoft Windows....18
6.1.2 Linux et Mac OS X....18
6.2 Configuration Client....18
6.2.1 SecureW2....18
6.2.2 XSupplicant....19
6.3 Activation Client....19
6.3.1 Activation SecureW2....19
6.3.2 Activation XSupplicant....20
7 Script d'accounting....21
7.1 Modification DHCP et Syslog....21
7.2 Modification MySQL....22
7.3 Modification FreeRADIUS....22
7.4 Modification du script account_monitor.pl....23
7.5 Lancement du script....24
7.6 Résultat....25
8 Annexes....27
8.1 Annexe 1 : script de lancement FreeRADIUS....27
8.2 Annexe 2 : script accounting_monitor.pl....28
8.3 Annexe 3 : installation SecureW2....32
8.4 Annexe 4 : Configuration SecureW2....33
8.5 Annexe 6 : configuration AP....35

7 SCRIPT D'ACCOUNTING

Le script account_monitor.pl est un script Perl écrit à l'origine par Rok PAPEZ (ARNES) qui permet de récupérer l'adresse IP d'un client qui vient d'être authentifié avec le protocole EAP. Il est fonctionnel et commenté et sous licence GPL2.

La mise en oeuvre de ce script n'est pas simple, c'est pourquoi il est recommandé de faire fonctionner l'authentification EAP d'abord.

Ce script lance deux démons qui tournent en permanence sur la machine. Le synoptique ci-dessous permet de comprendre le fonctionnement global du script :



Pour faire fonctionner le script (fournit en annexe 2), il faut modifier certains fichiers.

7.1 Modification DHCP et Syslog

L'accounting étant fait par le serveur RADIUS, si le serveur DHCP est différent du serveur RADIUS, il faut ajouter les lignes suivantes dans le fichier syslog.conf

```
# Syslog des DHCP : local0
local0.*                                /var/log/dhcp.log
local0.*                                @a.b.c.d

# Messages en provenance du script account_monitor.pl
local6.*                                /var/log/account_monitor.log
```


La première ligne logue les messages sur le serveur syslog local, la deuxième ligne envoie les messages vers le serveur a.b.c.d.

- Dans le cas d'un serveur syslog distant, il faudra également ajouter la première ligne dans son fichier de configuration.
- Il peut être utile de générer les fichiers vides lors de la première utilisation, commande `touch /var/log/dhcp.log` par exemple.
- Ne pas oublier de relancer le démon syslog !!!
- Les communications avec le démon syslog se font en TCP, port 514.

Pour vérifier si le syslog est lancé avec l'option -r (remote logging) :

```
ps -ef | grep syslog
root      525     1  0 Jun14 ?        00:12:14 syslogd -r -m 0
```

si ce n'est pas le cas, il faut modifier le fichier /etc/sysconfig/syslog comme suit :

```
SYSLOGD_OPTIONS="-r -m 0"
```

7.2 Modification MySQL

Il faut ajouter une table appelée ACCOUNTING. Dans l'interface mysqladmin :

```
use radius;
CREATE TABLE ACCOUNTING (
  User-Name  varchar(100) NOT NULL default '',
  Calling-Station-Id  varchar(100) NOT NULL default '',
  Client-IP-Address  varchar(100) NOT NULL default '',
  Called-Station-Id  varchar(100) NOT NULL default '',
  NAS-Port  int(10) unsigned NOT NULL default '0',
  Timestamp_Start  datetime NOT NULL default '0000-00-00 00:00:00',
  Timestamp_Dhcp  datetime NOT NULL default '0000-00-00 00:00:00',
  Timestamp_Stop  datetime NOT NULL default '0000-00-00 00:00:00',
  Acct-Unique-Session-Id  varchar(100) NOT NULL default '',
  Acct-Session-Time  int(10) unsigned NOT NULL default '0',
  Acct-Input-Octets  int(10) unsigned NOT NULL default '0',
  Acct-Output-Octets  int(10) unsigned NOT NULL default '0',
  Acct-Input-Packets  int(10) unsigned NOT NULL default '0',
  Acct-Output-Packets  int(10) unsigned NOT NULL default '0',
  Acct-Terminate-Cause  varchar(100) NOT NULL default ''
  TYPE=MyISAM;
```

Exemple de sortie :

```
mysql> show tables;
+-----------------+
| Tables_in_radius |
+-----------------+
| ACCOUNTING      |
| nas             |
| radacct         |
| radcheck        |
| radgroupcheck   |
| radgroupreply   |
| radpostauth     |
| radreply        |
| usergroup       |
+-----------------+
9 rows in set (0.00 sec)
```

8 ACRONYMES

AAA	Authentication, Authorization and Accounting
ART	Autorité de Régulation des Telecoms
ASK	Amplitude Shifting Key
BSS	Basic Service Set
CICG	Centre Interuniversitaire de Calcul de Grenoble
CSMA	Carrier Sense Multiple Access (CD : Collision Detect / CA : Collision Avoidance)
CTS	Clear To Send
DCF	Distributed Coordination Function
DHSS	Direct Sequence Spread Spectrum
DIFS	Distributed Inter Frame Space
DSIGU	Direction des Systèmes d'Information de Grenoble Universités
DSL	Digital Subscriber Line (ADSL : Asymetric DSL)
EAP	Extended Authentification Protocol
FHSS	Frequency Hopping Spread Spectrum
FSK	Frequency Shifting Key
GIP	Groupement d'Intérêt Public
HCF	Hybride Coordination Fonction
IANA	Internet Assigned Numbers Authority
IBSS	Independant Basic Service Set
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
ISM	Industrial, Scientific and Medical
ISO	du grec isos (égal) : représente l'Organisation Internationale de Normalisation
ITU	International Telecommunication Union
LCEN	Loi sur la Confiance en l'Économie Numérique
LLC	Logical Link Control
MAC	Media Access Control (réseau)
	Messages Authentication Codes (IPSec)
NAS	Network Access Server
NBS	National Bureau of Standards
NIST	National Institute of Standards and Technology
NREN	National Research and Education Network
NSA	National Security Agency

OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnection
OTP	One Time Password
PAC	Protected Access Credential
PCF	Point Coordination Function
PKCS	Public Key Cryptography Standards
POP	Point Of Presence
PPP	Point to Point Protocol
PPTP	Point to Point Tunneling Protocol
PSK	Phase Shifting Key (en transmission)
	Pre Shared Key (en WPA)
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RMU	Réseau Métropolitain Universitaire
RSSI	Responsable Sécurité des Systèmes d'Information (voir ASSI)
RTC	Réseau Téléphonique Commuté
RTS	Request To Send
SIFS	Short Inter Frame Space
SSID	Service Set IDentifiant
SSH	Secure SHell
SSL	Socket Secure Layer
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOS	Type Of Service
UDP	User Datagram Protocol
UFR	Unité de Formation et de Recherche
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless-Fidelity
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network (réseau local sans fil)
WPA	Wi-Fi Protected Area
WPAN	Wireless Personal Area Network
WRAP	Wireless Robust Authentication Protocol

9 INDEX LEXICAL

INDEX LEXICAL

A

AAA ... 9, 11, 58, 59, 71, 72, 74, 107, 121, 134
AAA . 5, 6, 10, 20, 23, 25, 29, 30, 36, 38, 49, 52, 56-60, 62, 64-67, 71-80, 82-87, 90, 92-94, 104, 107-109
AAA) 58
Accounting ... 6-8, 10, 12, 56, 59, 92-94, 96, 104, 114, 115, 117, 118, 121, 134
AES 8, 53, 54, 64, 69, 90, 92, 95
Alweg 104
Apple 3, 23, 24
ARREDU 5, 78, 95, 96, 98, 100, 104, 107
ARREDU 107
Authentification ...5, 7-10, 12, 23, 25, 26, 29, 30, 33, 36, 38, 49, 52, 56-60, 62-67, 69, 71-73, 75, 77-80, 82-87, 90, 92-96, 99, 100, 104, 107-109, 121, 134
Authentifications 104
Autorisation 6, 10, 52, 56, 72
Autorisations 6

B

Biométrie 1, 8, 56, 57
Blowfish 63, 64

C

Certification .. 5, 9, 11, 47, 51, 60-62, 66, 78, 92, 93
Certification .. 5, 9, 47, 51, 60, 61, 93
CHAP 65
Chiffrement ...6, 8, 10, 11, 33, 52-57, 61-65, 67-69, 71, 72, 86, 89, 90, 92, 96
CICG .. 1, 5, 7, 11, 15-21, 24, 26, 71, 74, 77, 83, 90, 121
Cisco . 10, 12, 24, 26, 27, 29, 66, 75, 80, 81, 86, 89, 90, 92, 96, 98, 99, 104, 108, 117
Cisco 3030 90
CRC 55
CRI 22, 28, 29, 83
CRU 5, 93, 98, 104
Cryptanalyse 6
Cryptologie 6, 7, 132
CSMA 11, 39, 49, 51, 121

D

DES 1, 3, 8, 53, 54, 62-64, 132
Dhcp 25, 76, 93, 94, 114-118
DSSS 8, 45, 47

E

EAP 36-38, 65-68, 74, 75, 77, 78, 90-92
EAP-FAST 66
EAP-LEAP 66
EAP-MD5 ..... 66, 92
EAP-PEAP 9, 66, 68, 75, 96
EAP-TLS ... 9, 12, 66-68, 75, 96, 100
EAP-TTLS .. 9, 12, 66, 68, 73, 75, 92
EAPOL 37
EDURoam ... 5, 7, 11, 20, 21, 72, 78, 93, 95, 96, 98, 107
Empreinte 5, 55-57, 99
Ethernet 8, 11, 31, 37, 39, 47, 49, 87
Ethernet" 39

F

F5 Networks 10, 86, 87, 89, 90
FHSS 8, 45, 47, 121
Firepass 12, 86-88, 90
FreeRadius ...5, 9, 12, 74-78, 90, 92, 93, 104, 107, 114
Funk Software 9, 72

I

IAS 9, 12, 21, 38, 73, 84, 132
IDEA 62, 63
IEEE 8, 10, 12, 33, 35-37, 39, 46, 49, 66, 112, 121
IETF 33, 59-62, 121
IGC 11, 60, 61, 66, 78, 92, 93
Intégrité ... 10, 23, 33, 52, 54, 55, 62, 64, 99
IP ..11, 13, 20, 25-28, 34, 37, 38, 41, 46, 50, 62-65, 71, 78, 81, 86, 90, 93-95, 98, 108, 114-118
IP 50
IPSec 9, 11, 12, 24, 27, 62-65, 86, 89, 90, 95, 98, 121
Ipsec, ... 81
ISO 12, 33, 36, 39, 81, 121
ITU 33, 41, 121

L

L2TP 89

M

M0n0wall 9, 12, 81-84
Marques ... 3, 4, 9, 10, 12, 22-24, 26, 27, 29, 30, 54, 66, 72, 73, 75, 76, 80, 81, 86-93, 96, 98, 99, 104, 108, 109, 111, 117
MD5 .....56, 62, 64-66, 92, 99
Meeting House 91
Message Digest 56
Microsoft .4, 9, 12, 22-24, 27, 30, 73, 88, 91, 92, 108, 109
Mobilité 3, 4, 7-10, 12-14, 20, 22, 24, 25, 33, 72, 132, 134
Mobilité. 4
Modulation 8, 11, 41-44, 48
Mot de passe 5, 8, 10, 26, 56, 57, 63, 66, 68, 84, 99, 102, 107, 108
Mots de passe 57
Mots de passe multiples 108
Mysql 75, 76, 78, 93, 114-117

N

Nomadisme 1, 3, 4, 7-10, 15, 20, 24, 26, 29, 33, 72, 99, 101, 132, 134
Normalisation . 33, 35-37, 39, 46, 49, 66, 81, 112
Norme IEEE 35, 36
Norme IEEE 802.1x 36
Normes 33, 35, 39, 41

O

OFDM 47, 122
One Time Password 8, 57, 122
Organismes .1, 5, 7, 8, 10-12, 15-22, 24, 26, 28-31, 33, 35-37, 39, 41, 46, 49, 59-62, 66, 71, 72, 74, 77, 78, 81, 83, 90, 93, 95, 96, 98, 104, 107, 112, 121
OSC 9, 73
OTP 56, 57, 122

P

PAP 68, 92
PfSense 9, 81
PKI 60, 61
Portail 89, 90
Portail captif ... 79, 83-85, 88, 89, 96, 99, 107
Portail d'accueil 88
Portails captifs 71
PPTP 9, 11, 65, 81, 89, 122
Protocoles . 34, 36-38, 41, 65-68, 71, 74, 75, 77, 78, 90-92
Protocoles 65, 90
PuTTY 12, 75

Q

QoS 36, 47, 108, 122

R

Radiator 9, 73
RADIUS ..5, 9, 12, 20, 38, 59, 71-78, 90, 92-96, 104, 107, 108, 114, 122, 132, 134
RC4 ..... 8, 53, 62, 63, 65, 69, 92
Redhat 23, 75, 76, 93
Renater 7, 11, 18-20, 28, 30, 31, 71,

93, 95, 96
RENATER, ... 93
RSA 54, 111

S

Sécurité 1, 3, 5-11, 14, 15, 19, 20, 23-26, 28-30, 33, 38, 47, 50, 52, 53, 57, 59, 60, 63, 65, 68, 71, 72, 75, 76, 85, 86, 96, 101, 109, 122, 132, 134
Sécurité 62, 65, 89, 90
Services d'authentification 72
SHA-1 ..... 56, 62, 64
Signature 8, 55-58, 60
SQUID 9, 79, 80
SSH 9, 11, 62, 63, 75, 98, 122
SSID 50, 67, 92, 96, 98, 99, 108, 122
SSL 9, 10, 12, 60, 62, 83, 85-87, 89, 93, 104, 122
SSL (p 78
SSL, ... 85
Standards 5, 9, 10, 31, 36-38, 44, 46-49, 51, 52, 66, 72, 92
Steel Belted Radius 9, 12, 72
Syslog 93, 94, 114-118

T

Talweg 9, 12, 83-85, 104
TCP ... 11, 34, 41, 62-65, 71, 90, 122
TCP/IP 34, 41, 65, 71, 90
Technologies 36, 47, 108, 122
Telindus 87
TERENA 7, 20
Token-Ring 37
Traçabilité 6, 9, 10, 30, 96, 134

U

UDP 25, 38, 59, 65, 90, 94, 122

V

VLAN . 11, 35, 36, 38, 67, 71, 81, 92, 95, 96, 98
VPN ...7, 8, 10-12, 20, 24-29, 31, 62, 63, 65, 71, 72, 79, 81, 86-91, 95, 96, 98, 99, 104, 107, 113, 114, 122, 132
VPN 24, 60, 62-65, 78, 81, 83, 85, 87, 89, 90, 93
VPN 36-38, 65-68, 74, 75, 77, 78, 90-92

W

WEP 53, 66-69, 71, 122
WEP. 66
Wi-Fi .. 4, 5, 7, 11, 21, 46, 47, 51, 91, 122, 132, 134
WPA ... 10, 62, 69, 86, 90-92, 95, 96, 98, 99, 104, 107, 122, 132, 134
WPA 98

X

X.509 62

..... 64, 80

3

3030 ..... 10, 12, 86, 89, 90
3com 91
3DES 54, 57, 62-64

8

802.11 ..... 5, 8-12, 31, 37, 44, 46-52, 66, 69, 108, 134
802.1q 8, 35, 36
802.1x 8, 11, 36-38, 66, 72, 92, 114, 132, 134
802.3 ..... 31, 39, 49, 66, 67, 69

10 BIBLIOGRAPHIE

BIBLIOGRAPHIE

[**ANDI99**] (Datasheet) "Programmable Digital QPSK/16-QAM modulator AD9853" (01/1999) Analog Devices ISBN : (Tipical plots of eyes diagrams and constellations)

[**COCO03**] R. & E. CORVOLAN, Y. LE CORVIC "Les VPN" (11/2003) DUNOD ISBN : 2-10-006632-3

[**FERO04**] F. ROMBAULT "Hot spots Wi-Wi : usages - moyens - Stratégies (livre blanc)" dernière consultation : 07/ 2003 - http://www.ebg.net/evenements/pdf/EBG_LBwifi.pdf

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

[**HASS02**] J. HASSELL "RADIUS" (10/2002) O'REILLY ISBN : 0-596-00322-6

[**IMAG01**] J. A. GARCIA-MACIAS, F. ROUSSEAU, G. BERGER-SABBATEL,L. TOUMI, A. DUDA "Quality of Service and Mobility for the Wireless Internet" (07/2001) LSR-IMAG

[**INRIA03**] Performance Analysis of Finite Load Sources in802.11b Multirate Environments "Performance Analysis of Finite Load Sources in802.11b Multirate Environments" (07/2003) INRIA

[**JLMO97**] J-L. MONTAGNIER "Pratique des réseaux d'entreprise" (1997) Eyrolles ISBN : 2-212-08920-1 (chapitre 4)

[**JRES05**] E. JULLIEN, P. PETIT, D. ROUMANET "Nomadisme : problématiques et solutions" (10/2005) JRes2005

[**LIBL04**] E. TSCHIEMBLER "Livre blanc - La mobilité en entreprise" (2004) EBG

[**MAPU04**] MALES, PUJOLLE "Wi-Fi par la pratique" (2004) Eyrolles ISBN : 2-212-11409-5 (Ch. 8, 11)

[**MISC10**] P. BIONDI, A. GUIGNARD, V. VUILLARD "MISC" (12/2003) Diamond Editions

[**MISC13**] F. NAMBOT "Misc (Multi-system & Internet Security Cookbook)" (06/2004) Diamond Editions

[**MITN04**] K. D. MITNICK "L'art de la supercherie " (2004) CampusPress ISBN : 2-7440-1976-3

[**PUJO05**] G. PUJOLLE "Les Réseaux" (/2005) Eyrolles ISBN : 2-212-11437-0 (ch. 20, 21, 32, 34, 37)

[**WEB001**] "Cryptologie et sécurité sur PC - cryptographie, stéganographie, espionnage, règles de sécurités." dernière consultation : 01/ 2005 - http://cryptologie.free.fr/crypto/lexique.html

[**WEB002**] "Introduction à DES" dernière consultation : 10/ 2004 - http://www.commentcamarche.net/crypto/des.php3

[**WEB003**] F. BAYART "La sécurité des cartes bancaires" dernière consultation : 10/ 2004 - http://www.bibmath.net/crypto/moderne/cb.php3

[**WEB004**] G. ANGENIEUX "U23 Eléments sur l'étalement de spectre " dernière consultation : 05/ 2005 - http://www.univ-savoie.fr/labos/lahc/MEMBRES_LAHC/Angenieux/Ens_Angenieux/

[**WEB005**] L. PHIFER "Deploying 802.1X for WLANs: EAP Types" dernière consultation : 03/ 2005 - http://www.wi-fiplanet.com/tutorials/article.php/3075481

Mémoire d'ingénieur CNAM en informatique

Nomadisme et sécurité des réseaux informatiques

David ROUMANET, Grenoble le 15 décembre 2005.

Résumé

L'évolution du mode de travail dans le monde actuel conduit de plus en plus de personnes à se déplacer. Les technologies peuvent rendre ces déplacements plus souples. Cependant, la sécurité des réseaux peut en pâtir. Comment ouvrir et en même temps sécuriser les réseaux informatiques ?

Ce mémoire s'attache à découvrir quels moyens existent, quelles solutions peuvent répondre aux besoins des utilisateurs qui demandent plus d'ouverture et aux administrateurs qui veulent plus de sécurité. Ce dilemme est abordé de la manière suivante : après avoir repris quelques définitions utiles et déterminé les besoins des utilisateurs, les différentes normes sont décrites pour permettre la compréhension des solutions techniques existantes. Ensuite l'expérimentation de plusieurs d'entre-elles permet d'en connaître les avantages et inconvénients. Enfin, le déploiement d'une architecture finale valide le travail effectué pour le réseau interuniversitaire de Grenoble.

Mots clés

authentification, nomadisme, mobilité, RADIUS, sécurité, 802.11, Wi-Fi, ASFI, AAA, 802.1x, WPA, EAP, journalisation, traçabilité, réseau sans fil

---

Keywords

authentication, mobility, RADIUS, security, 802.11, Wi-Fi, AAA, 802.1x, WPA, EAP, accounting, wireless network