Collection
Ressources Informatiques

Wi-Fi

Réseaux sans fil 802.11

Technologie - Déploiement - Sécurisation

Seconde Edition

Philippe ATELIN

INFORMATIQUE TECHNIQUE

eni éditions

Wi-Fi

Réseaux sans fil 802.11 : Technologie - Déploiement - Sécurisation

Philippe ATELIN

Résumé

Ce livre sur le **Wi-Fi** est destiné à aider les professionnels du réseau dans l´appréhension et le déploiement d´un **réseau local sans fil**. Le Wi-Fi est replacé dans le contexte des autres technologies réseaux (Ethernet, Bluetooth, WiMax, CPL, UMTS...).
Les **caractéristiques** des ondes, modulations et autres phénomènes ondulatoires sont décrites afin **d´optimiser au mieux le signal radio**. Les **aspects réglementaires** ne sont pas oubliés, tout comme les **critères de choix** d´une antenne, qu´elle soit de type fouet, patch ou yagi. Toutes les caractéristiques qui font la **qualité et la performance** d´un réseau Wi-Fi sont présentées.
L´accent est mis dans les derniers chapitres de ce livre sur les différents **aspects de la sécurisation** d´un tel outil de communication : WEP, WPA, WPA2 (802.11i) et autres solutions sont étudiées en détail. Les exemples de configurations logicielles tiennent compte des avancées de Microsoft Windows Vista et Windows Server 2008.
Cette nouvelle édition du livre apporte les éléments d´informations sur la **norme 802.11n draft.**

L'auteur

Formateur et consultant en entreprise dans le domaine des réseaux et du Groupware, **Philippe Atelin** s'est spécialisé sur les implications technologiques et organisationnelles des nouvelles technologies. Son expérience s'allie à ses compétences pédagogiques pour fournir au lecteur des ouvrages complets et opérationnels.

Classification des réseaux

Ces dernières années, les nouvelles technologies de l'information et de la communication (NTIC) ont considérablement modifié les comportements vis-à-vis de l'informatique, tant au niveau professionnel que personnel.

Le système d'information (SI) de l'entreprise, ensemble des moyens matériels et logiciels, assure le stockage, le traitement et le transport électronique des données. Cette dernière tâche est désormais essentiellement dévolue à des réseaux informatiques.

Pendant longtemps, ils ont été distincts de leurs pendants téléphoniques. Il devient désormais de plus en plus difficile de les différencier. En effet, les technologies de la téléphonie exploitaient autrefois exclusivement des solutions analogiques et de commutations de circuits. Elles ont évolué vers la commutation de paquets et des transferts en mode numérique. Au lieu de transmettre les différents niveaux de la voie à travers une ligne réservée pour le temps de la communication, elle est désormais échantillonnée en 0 et 1, puis découpée en bribes d'informations acheminées indépendamment et sans mobiliser une liaison. Même si cette solution numérique n'est pas exclusive, elle est désormais très étendue.

Non seulement il est donc devenu possible de mélanger les deux utilisations sur des médias similaires, mais ceux-ci ont eux-mêmes évolué. En effet, l'usage des supports filaires, câbles cuivres, fibres optiques... est désormais complété par ce qu'il est convenu d'appeler l'interface air. Ce support est exploité par des solutions utilisant les technologies infrarouges, laser et surtout ondes radioélectriques.

La multiplication des réseaux informatiques et de leurs interconnexions, particulièrement par Internet, a également entraîné de nouvelles possibilités d'exploitation. Les exigences de mobilité, itinérance et nomadisme, sont de plus en plus importantes.

Elles ont pu être concrétisées par les évolutions majeures que sont :

- les augmentations des débits, indispensables pour le confort et l'acceptation des solutions par les utilisateurs ;
- l'interopérabilité entre solutions techniques, avec, par exemple, la généralisation de TCP/IP ;
- la réduction des coûts des terminaux, permettant ainsi le déploiement en masse des solutions mobiles.

Les différents accès aux réseaux informatiques professionnels sont désormais :

- fixes, dans l'entreprise à partir d'un point de raccordement habituel ;
- itinérants, en dehors du point de raccordement habituel ;
- nomades, en dehors de l'entreprise.

Les utilisateurs disposent de nombreux types de terminaux d'accès au système d'information. En complément des ordinateurs de bureau, on peut citer les ordinateurs portables, les Tablets PC (ordinateurs portables sans utilisation de clavier), les Smartphones (téléphones incluant des capacités de gestion des données, utilisable avec une main) et les assistants personnels ou PDA (*Personal Digital Assistant*), nécessitant l'usage d'un stylet et dont la plupart sont désormais communiquant.

Les besoins en portabilité informatique ont fait exploser la demande de terminaux "de poche", et il devient normal, désormais d'avoir accès à Internet de partout, que ce soit par les protocoles de téléphonie mobile ou par le Wi-Fi.

Différents types de terminaux portables

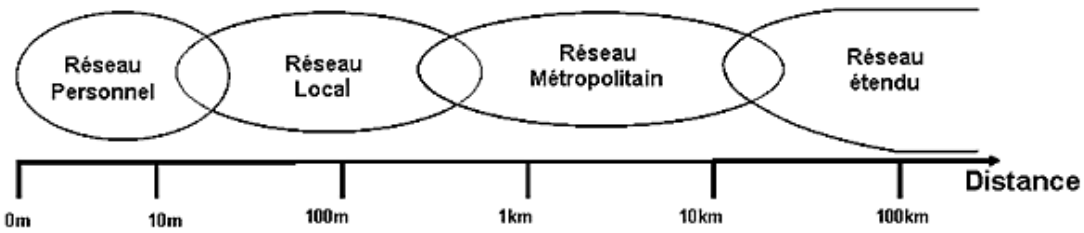
Enfin, la frontière entre exploitation personnelle et professionnelle des réseaux informatiques est devenue de plus en plus mince. La démocratisation des possibilités d'accès Internet haut débit, avec Asymmetric Digital Subscriber Line (ADSL) ou les nouvelles capacités de la téléphonie cellulaire généralisent les usages. La technologie Wi-Fi, elle-même, est utilisée à la maison comme en entreprise.

Il peut être important de connaître et reconnaître ces nouveaux moyens de communication informatique, leur standardisation et les technologies clés en entreprise.

1. Catégorisation

a. Les topologies de réseaux

Un réseau informatique, transmettant des données, est constitué d'équipements appelés nœuds. En fonction de leur étendue et de leur domaine d'application, ces réseaux sont catégorisés en quatre types.



Les étendues de réseaux

Réseau personnel

Le plus récent, également le plus petit, est nommé en anglais Personal Area Network (PAN). Centré sur l'utilisateur, il désigne une interconnexion d'équipements informatiques dans un espace d'une dizaine de mètres autour de celui-ci, le Personal Operating Space (POS). Deux autres appellations de ce type de réseau sont : réseau individuel et réseau domestique. Concrétisé de manière standard par l'Universal Serial Bus (USB), venu remplacer les différents ports PS2, série et parallèle, ce type de réseau peine à tenir ses promesses. On peut noter l'adoption de Bluetooth, qui permet la communication par les ondes radio avec les périphériques.

Réseau local

De taille supérieure, s'étendant sur quelques dizaines à quelques centaines de mètres, le Local Area Network (LAN), en français réseau local d'entreprise (RLE), relie entre eux des ordinateurs, des serveurs... Il est couramment utilisé pour le partage de ressources communes, comme des périphériques, des données ou des applications. Le protocole Ethernet entre dans cette catégorie.

Réseau métropolitain

Le réseau métropolitain, ou Metropolitan Area Network (MAN), est également nommé réseau fédérateur. Il assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN.

Il peut servir à interconnecter, par une liaison privée, différents bâtiments d'une administration, distants de quelques dizaines de kilomètres. Les protocoles utilisés ici sont Asynchronous Transfer Mode (ATM), Fiber Distributed Data Interface (FDDI)...

Réseau étendu

Les étendues de réseaux les plus conséquentes sont classées en WAN, acronyme de Wide Area Network. Constitués de réseaux de type LAN, voire MAN, les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. Le WAN le plus célèbre est le réseau public Internet, dont le nom provient de cette qualité : Inter Networking, ou interconnexion de réseaux.

Débits

Les réseaux personnels (PAN) sont peu rapides. Par contre, pour les autres types, plus l'étendue du réseau est importante, moins leur vitesse de transfert l'est. Ainsi, les débits sur des réseaux de petites tailles sont de l'ordre de quelques milliers de bits, ou kilobits par seconde (kbps). Ils peuvent parfois atteindre quelques mégabits (Mbps) par seconde, soit cent fois plus.

Les réseaux locaux sont les plus véloces, travaillant désormais à des vitesses de 100 Mbps, soit 100 millions de bits par seconde, voire 1 gigabit par seconde (Gbps), soit 1 milliard de bits par seconde. Pour les réseaux métropolitains, un débit de l'ordre de 10 Mbps voire au-delà est désormais d'usage, quand les interconnexions de type WAN dépassent couramment le mégabit par seconde.

b. Les supports de transmission

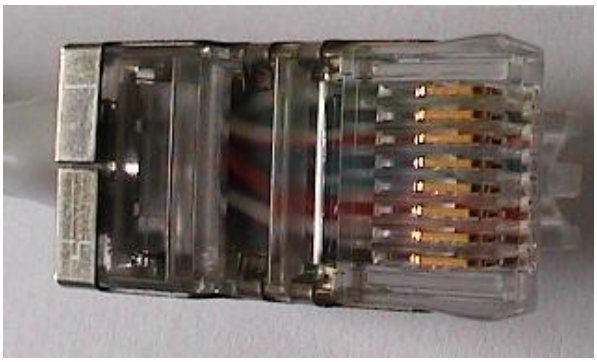
Historiquement, les quatre catégories de réseau présentées précédemment utilisent des interfaces filaires, pour transmettre les informations entre nœuds du réseau.

Interface filaire

Parmi les supports physiques, le câble coaxial a longtemps été le support privilégié des réseaux locaux. Bien isolé des interférences, il peut encore être avantageusement utilisé dans des milieux industriels.

Câble coaxial

Il a été supplanté, dans bien des cas, par les câbles en cuivre en paire torsadée. Très simples de mise en œuvre, ils sont pratiques à utiliser dans des locaux d'entreprise. D'autant plus que leurs caractéristiques sont proches des câbles téléphoniques. Le pré-câblage des bâtiments peut ainsi n'utiliser que ce support pour le transport prévisionnel de la voix comme des données.



Câble en paire torsadée

Réservée, il y a de cela quelques années à des interconnexions entre bâtiments, la fibre optique, très rapide et non sensible aux interférences, a fortement baissée de coût. On en retrouve de plus en plus dans des réseaux de type LAN, en complément de la paire torsadée.

Paire de câble fibre optique

Les réseaux de grande étendue utilisent, en plus de supports dédiés, souvent en fibre optique, le réseau téléphonique commuté (RTC), initialement prévu pour transporter la voix. Cette mutualisation des supports filaires se généralise. Nous pouvons citer, par exemple, la non-différenciation des câblages réseau et téléphonique dans les entreprises,à l'intérieur des bâtiments, comme à l'extérieur, où l'utilisation des fils électriques, pour transmettre les données informatiques par le courant porteur en ligne (CPL).

Interfaces infrarouge et laser

Complémentairement, de plus en plus de nouvelles technologies de transport de données informatiques utilisent des supports non limités, transportant l'information sur l'interface air. L'utilisation du faisceau de lumière infrarouge, directionnel en visibilité directe, en est une première illustration. Cette technologie est utilisée par le groupement Infrared Data Association (IrDA), qui a défini la principale spécification de communication de ce type.

Site Web de l'IrDA : http://www.irda.org

Plus rapide et de plus grande portée, la transmission par signaux laser permet d'interconnecter des bâtiments. Cette communication optique aérienne utilise des canons lasers autorisant des débits jusqu'à 200 Mbps, sur des distances dépassant le kilomètre.

Interface hertzienne

Mais la plus importante exploitation actuelle de l'interface air utilise les ondes radioélectriques. On peut classer, parmi elles, les communications satellitaires, mais d'autres techniques hertziennes sont apparues ces dernières années et sont devenues courantes.

c. Les appellations des réseaux sans fil

Même si le premier réseau sans fil, Aloha, utilisant les paquets de données, fut créé par l'université de Hawaï dès 1970, les réseaux informatiques restent essentiellement filaires. Les appellations des interconnexions entre nœuds, assurées par des liaisons physiques, ont donc été différenciées de celles sans fil.

Ainsi, la lettre "W", pour Wireless, positionnée devant l'acronyme d'étendue, vient spécifier que le réseau utilise l'interface air. Par exemple, la technologie IrDa peut être catégorisée comme WPAN. Pour préciser que le réseau sans

fil utilise les ondes radioélectriques, la lettre "R", pour Radio, peut être utilisée. Par exemple, Wi-Fi entre dans la catégorie des RLAN.

La plupart des nouvelles technologies de réseaux informatiques sont de type radio. Il est évident qu'elles accusent un certain retard par rapport à leurs homologues filaires, essentiellement pour des raisons de portée du signal et de débit. En effet, elles sont nettement moins rapides et des taux d'erreurs importants sont à prendre en compte. Les réseaux hertziens sont également soumis à des contraintes réglementaires. Un dernier frein a été pendant longtemps le foisonnement de solutions propriétaires, incompatibles entre elles.

2. Standardisation

a. L'organisme ISO et le modèle OSI

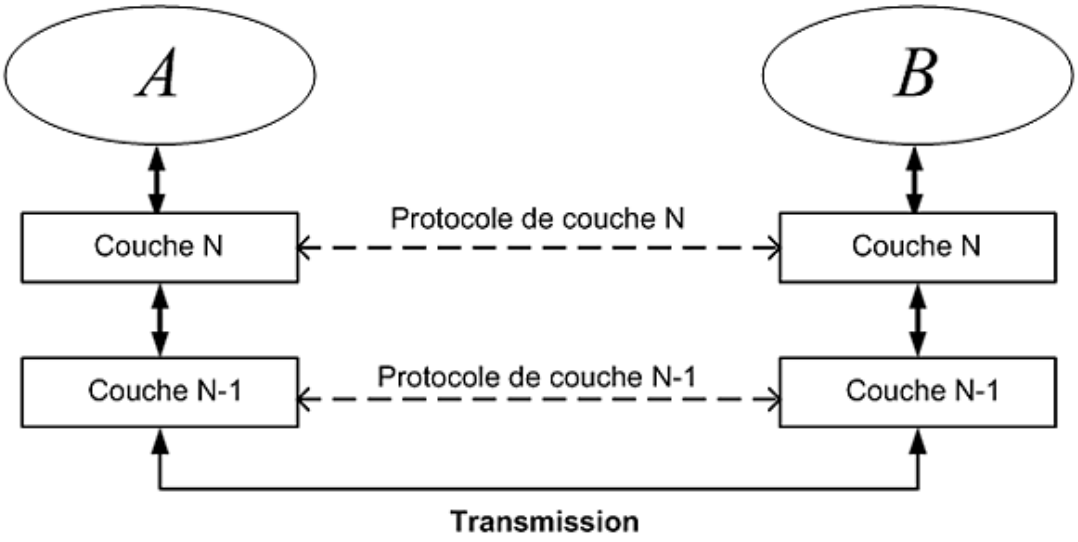
Spécialisée dans le développement et la normalisation de standards techniques, l'ISO est une organisation non gouvernementale internationale. Regroupant plus de 150 pays, son siège est basé à Genève, en Suisse. Son appellation n'est pas l'acronyme de International Organization for Standardization, qui pourrait être traduit en français comme organisation internationale de normalisation, mais provient du grec "isos", voulant dire égal.

Site Web de l'ISO : http://www.iso.org

Au niveau des réseaux informatiques, l'ISO a défini un modèle de référence, nommé Open Systems Interconnection (OSI) définissant ce que doit être une communication complète. L'ensemble du processus d'échange de données est ainsi découpé en sept couches hiérarchiques.

Les sept couches du modèle OSI

Chaque couche offre un ensemble de services, pour que deux entités communicantes symétriques de même niveau échangent des informations. Un protocole, ensemble de règles nécessaires à la réalisation du service, règle les échanges entre mêmes couches. Une communication complète nécessite donc que chaque protocole utilisé soit compréhensible des deux côtés.



La communication entre couches OSI

La couche Physique

Elle a pour rôle la transmission bit à bit sur le support, entre l'émetteur et le récepteur. Définissant le mode de propagation des signaux, elle gère au besoin les circuits physiques. Des matériels comme les modems (modulateur/démodulateur), les répéteurs ou la connectique des cartes réseaux, RJ45 par exemple, se placent à ce niveau.

La couche Liaison de données

Elle transmet les informations sous forme d'une succession de bits, ou trame, d'un nœud du réseau à un autre. Pour cela, elle amène une notion d'adressage. Le contrôle des flux, le multiplexage physique, ainsi que des fonctionnalités de fiabilisation et d'intégrité (code CRC...) sont gérés à ce niveau.

La couche Réseau

L'acheminement, ou routage, des informations de bout en bout est du ressort de cette couche. Elle forme, par segmentation ou réassemblage, des blocs d'information. L'adressage, avec choix de l'itinéraire, est une des fonctionnalités clés de ce niveau. En fonction des protocoles, le bloc peut être nommé message, cellule ou même paquet, comme dans Internet Protocol (IP).

La couche Transport

Elle prend en charge la qualité des transferts de bout en bout, et donc la bonne transmission des informations. Ici, peuvent être ajoutés des critères d'acquittement des échanges, par accusé de réception, et de sécurisation du trafic. Les évolutions de la couche transport autorisent de plus en plus l'usage de la qualité de service (QoS - *Quality of Service*). Grâce à elle, les flux peuvent être plus contrôlés. Certains, comme ceux transportant de la vidéo et de la voix, peuvent ainsi devenir prioritaires par rapport à ceux transportant des données.

De plus, la garantie de débits minimums, même en cas de fort trafic, devient concevable. La QOS peut également être prise en charge par d'autres couches du modèle OSI.

Le protocole le plus connu à ce niveau est Transmission Control Protocol (TCP).

La couche Session

Son rôle est l'organisation et la synchronisation des dialogues. Pour cela, elle met en œuvre des authentifications et des ouvertures/fermetures de session. Elle gère ainsi des points de synchronisation, afin d'être capable de retransmettre des données après un incident. Les appels de procédures distantes, Remote Procedure Call (RPC), constituent un protocole à ce niveau.

La couche Présentation

Afin d'utiliser des représentations d'information communes, la mise en conformité des contenus est prise en charge par cette couche. Elle peut également exploiter des fonctions de chiffrement et de compression. Des codages comme Multipurpose Internet Mail Extensions (MIME), American Standard Code for Information Interchange (ASCII), ou Abstract Syntax Notation number One (ASN.1), peuvent être utilisés ici.

La couche Application

Enfin, les fonctionnalités réseaux nécessaires pour les logiciels sont fournies par cette couche. Elle représente l'interface utilisateur pour accéder aux ressources du réseau.

Pour simplifier, ces sept niveaux peuvent être regroupés en trois :

- Les couches basses, Physique et Liaison de données, offrent la modulation et l'accès au média.
- Les couches moyennes, Réseau et Transport, gèrent les circuits, la fiabilisation et la fragmentation.
- Les couches hautes, Session, Présentation et Application, offrent des services de gestion des sessions, de connexions applicatives et de présentation des informations.

b. L'organisme IEEE

L'un des principaux instituts américains de standardisation des technologies de communication, l'Institute of Electrical and Electronics Engineers (IEEE) est issu de la fusion, en 1963 de l'Institute of Radio Engineers (IRE) et l'American Institute of Electrical Engineers (AIEE). Cet organisme, destiné à promouvoir les connaissances dans l'ingénierie électrique, est à l'origine de nombreux standards ratifiés par l'ISO.

Site Web de l'IEEE : http://www.ieee.org

Site Web de l'antenne française : http://www.ieeefrance.org

Dans cette organisation, un groupement de personnes collaborant sur un thème donné forme un comité. Par exemple, celui intitulé "1394" travaille sur les bus série, de type Firewire.

Les comités "802", doivent leur nom à leur date de mise en place, en février 1980. Ils œuvrent sur l'évolution des standards réseaux, au niveau des couches basses. Plus précisément, le projet 802 divise le niveau physique en deux sous-couches. La première est nommée contrôle d'accès au média, ou Medium Access Control (MAC). Elle est propre à chaque type de réseau. La seconde, nommée contrôle de la liaison logique, ou Logical Link Control (LLC), est indépendante du type de réseau.

Les différents thèmes de travaux sont répartis entre des groupes de travail. On peut citer, parmi eux :

- 802.2, Logical Link Control (LLC) Working Group ;
- 802.3, Ethernet Working Group (type LAN) ;
- 802.11, Wireless LAN Working Group (type WLAN) ;
- 802.15, Wireless Personal Area Network Working Group (type WPAN) ;
- 802.16, Broadband Wireless Access Working Group (type WMAN).

Site Web des comités 802 : http://grouper.ieee.org/groups/802/dots.html

c. Autres organismes : ETSI et FCC

L'European Telecommunications Standards Institute (ETSI) est également un organisme indépendant à but non lucratif. Basé à Sophia Antipolis, en France, il fut créé en 1988 par la conférence européenne des administrations des postes et télécommunications (CEPT). L'ETSI est chargé de la standardisation des technologies de l'information et de la communication, à l'échelle de l'Europe.

Site Web de l'ETSI : http://www.etsi.org

Une partie des travaux actuels de l'ETSI porte sur les technologies radio, comme le Digital European Cordless Telephone (DECT), pour la téléphonie sans fil. Le projet de normes de réseaux radio à large bande, Broadband Radio Access Networks (BRAN), a donné naissance à l'HiperLAN, dont nous reparlerons.

Site Web de FCC : http://www.fcc.gov

L'agence américaine Federal Communications Commission (FCC) est chargée de la régulation des communications aux USA, qu'elles soient radio, filaires ou autres.

Elle réglemente également les appareillages électroniques en y apposant son logo après validation. L'impact de ces règles est mondial, étant donné que tous les matériels sont conçus pour fonctionner sur le territoire américain. Mais, bien souvent, une adaptation doit être effectuée pour répondre aux critères nationaux d'autres pays, moins permissifs. C'est le cas du Wi-Fi en France.

Le logo apposé sur les matériels

3. Réseaux en entreprise

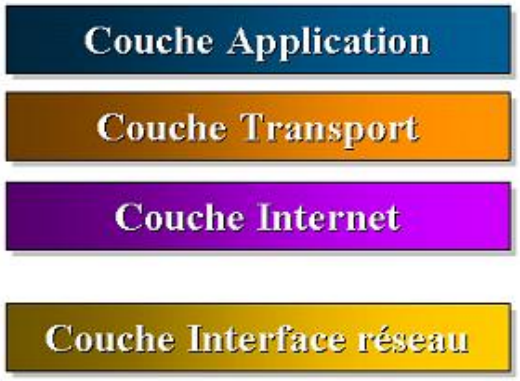
a. La suite de protocoles TCP/IP

Le réseau Arpanet, du nom de l'organisme militaire Advanced Research Project Agency (ARPA) est né en 1969. Il a été créé par le Department of Defense (DoD) des USA, pour connecter différents sites informatiques et a d'abord relié quatre instituts universitaires. Un certain nombre de centres militaires et de recherche, publics comme privés, participant à cette mise au point, y furent progressivement reliés.

Au début des années 70, Bob Kahn, du Defense ARPA (DARPA), ex ARPA, travaille avec Vinton Cerf, chercheur à Stanford Institute, sur de nouveaux protocoles permettant de relier des réseaux. Ainsi naît TCP/IP. En 1976, Arpanet migre sur TCP/IP. En 1978, un second réseau est connecté à Arpanet. Il utilise les lignes téléphoniques et prend le nom d'Internet.

Ayant prouvé sa fiabilité à grande échelle, la suite de protocoles TCP/IP devient progressivement la norme de facto de couches moyennes et hautes des réseaux informatiques. On la retrouve actuellement dans la quasi-totalité des réseaux locaux d'entreprise.

De définition antérieure au modèle OSI, celui de TCP/IP ne comporte que quatre niveaux.



Le modèle TCP/IP

La couche application regroupe les trois services de niveau supérieur du modèle OSI. On y retrouve des dizaines d'applications telles que la messagerie électronique (SMTP - *Simple Mail Transfer Protocol*), le Web (HTTP - *HyperText Transfer Protocol*), le transfert de fichier (FTP - *File Transfer Protocol*)...

Le transport peut être assuré de manière fiable, par Transmission Control Protocol (TCP), ou non fiable, par User Datagram Protocol (UDP).

La couche Internet regroupe plusieurs protocoles, dont Internet Protocol (IP), fournissant, entre autres, un adressage logique.

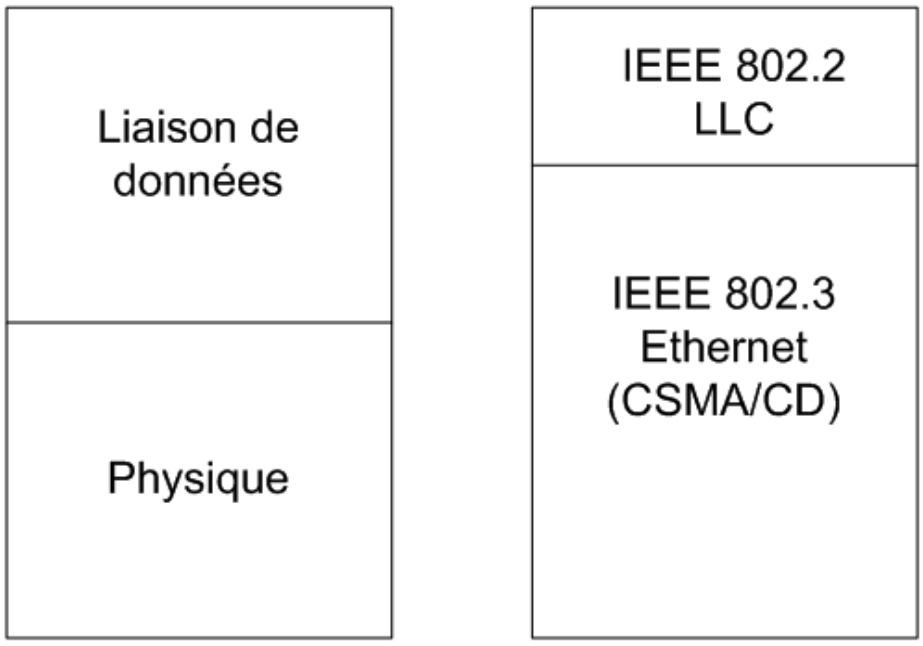
Une des grandes qualités de cette pile de protocoles est que la technologie réseau utilisée en couche basse est transparente. Ainsi quelles que soient l'étendue et l'interface de transmission, la pile de protocole TCP/IP peut être utilisée, ce qui est le plus souvent le cas.

Dans la suite de cet ouvrage, nous ne reviendrons plus sur ces protocoles de couches moyennes et hautes, supposant que les trames Ethernet, Wi-Fi, Bluetooth et autres encapsulent ce type de protocoles.

b. Le protocole Ethernet

Deux technologies de couches basses, sur les réseaux locaux filaires, se sont affrontées pendant les années 90. Apparu en 1980, le protocole Ethernet est issu des travaux de DEC, Intel et Xerox. Il est moins efficace que Token Ring, soutenu par IBM. Mais, plus économique, il a fini par devenir omniprésent en entreprise.

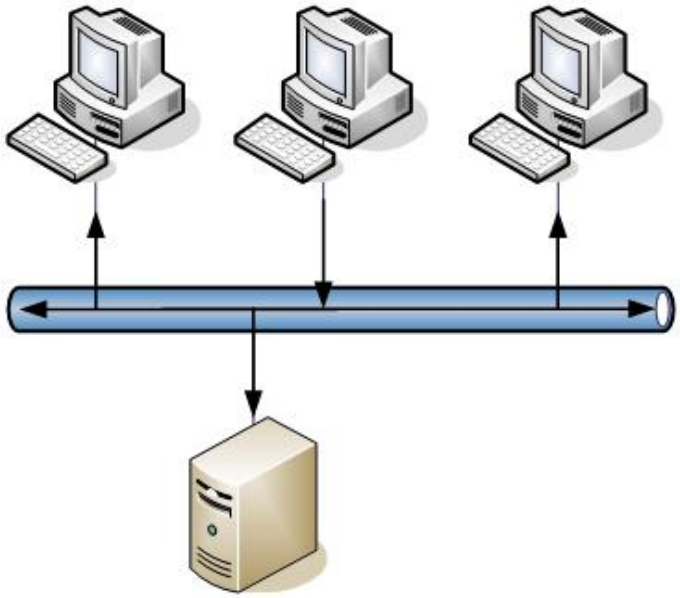
Son évolution a été standardisée dans la norme IEEE 802.3, qui couvre la couche Physique et une partie de celle Liaison de données.



Standards IEEE 802.2 et 802.3 par rapport au modèle OSI

Sur un réseau local Ethernet, la transmission des informations s'effectue par diffusion. Ainsi, tous les nœuds

présents reçoivent les trames. Comme chacun possède une adresse qui lui est propre, il suffit que celles d'émission et de destination soient contenues dans les trames. À réception des informations, chaque nœud analyse l'adresse de destination pour savoir si elles lui sont destinées.



Diffusion de trames sur un réseau Ethernet

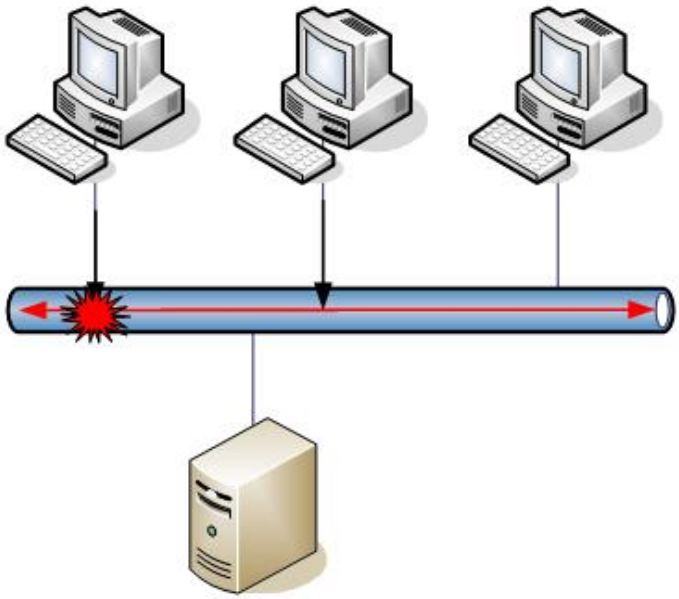
Pour qu'un tel système fonctionne, il est nécessaire, lorsqu'une station souhaite communiquer, que les autres soient en écoute. Plusieurs méthodes peuvent être utilisées pour gérer cet état de fait. Ethernet est basé sur un principe simple d'écoute avant émission : la contention. Avec Token Ring, une station ne peut émettre que lorsqu'elle est en possession d'un jeton, unique. Une dernière méthode, l'interrogation, ou polling, consiste à mettre en œuvre un équipement administrateur qui distribue les temps de parole.

Une méthode d'accès au support par contention est simple à mettre en œuvre, mais non déterministe. Il n'est pas concevable de prioriser, ni de prévoir dans combien de temps un nœud pourra émettre. De plus, en fonction du nombre d'émetteurs potentiels sur un même réseau, sa vitesse réelle peut être très vite réduite.

La technique par contention utilisée par Ethernet met en œuvre une gestion de conflits. Elle porte l'acronyme CSMA/CD (*Carrier Sense Multiple Access/ Collision Detection*), en français accès multiples avec détection de porteuse et de collision.

Comme le support de transmission est commun aux différents nœuds du réseau et que son accès doit être exclusif lors d'une transmission, toute émission est précédée d'une écoute. Seule l'absence de communication détectée sur la ligne autorise la prise de parole.

Par contre, si cette action est simultanée sur deux postes, les deux trames émises vont entrer en collision. Lorsque celle-ci est détectée par l'un des nœuds en écoute, il prévient les stations émettrices par une trame de brouillage, appelée JAM. Ainsi, elles peuvent, après avoir attendu un délai aléatoire, réémettre l'information.



Collision lors d'une communication Ethernet

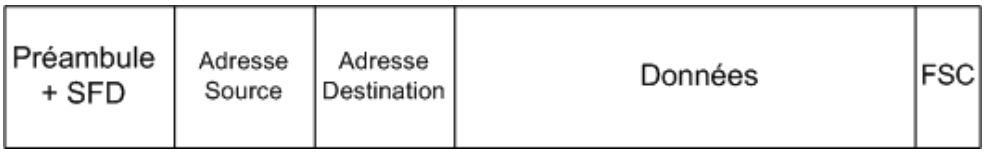
Chaque carte réseau Ethernet possède une mémoire, contenant une adresse physique. Celle-ci doit être unique sur l'ensemble du réseau local. Constituée de 48 bits, soit 6 octets, ses 24 bits de poids fort identifient le fabricant. Ce numéro est appelé Organizationally Unique Identifier (OUI). Les autres bits de l'adresse MAC sont aléatoires.

La trame Ethernet, très légèrement différente de celle IEEE 802.3, est constituée de trois parties. L'en-tête comprend d'abord un préambule, sur 7 octets, qui permet la synchronisation. Ensuite, un délimiteur de début de trame (SFD - *Start Frame Delimiter*), sur un octet, indique le début des informations.

Celles-ci sont d'abord constituées des adressages source et destination. Un champ EtherType, sur deux octets, précise le protocole de couche supérieure utilisé. Il n'existe pas en 802.3, et son utilisation permet de se passer de l'usage de LLC. Par exemple, ce champ notifie la valeur 800 pour TCP/IP.

Le champ de données, contenant les informations de niveau 3, doit avoir une taille minimale de 46 octets. Au besoin, des bits de bourrage (padding) sont ajoutés pour obtenir cette valeur. La taille maximale de ce contenu est de 1500 octets, ce que l'on nomme le Maximum Transfer Unit (MTU).

Enfin, un code de contrôle d'erreur Cyclic Redundancy Code (CRC) marque le délimiteur de fin de trame FSC (*Frame Check Sequence*).



Le contenu de la trame Ethernet

Il n'y a pas eu d'évolution récente du protocole Ethernet en lui-même. Par contre, son exploitation a évolué, avec le changement de l'infrastructure réseau. Ainsi, les traditionnels répéteurs (Hub), utilisés pour raccorder les stations, ne sont pratiquement plus utilisés, au profit de commutateurs (Switchs). Ces matériels sont capables de mettre en relation un numéro de leur port et l'adresse MAC de l'ordinateur qui y est relié, généralement par auto apprentissage. Ainsi, en effectuant une lecture des adresses source et destination d'une trame, ils peuvent ne la retransmettre que sur le port concerné. Les collisions ne représentent ainsi plus un problème. Exploitant la même topologie physique, Ethernet est devenu commuté, et non plus diffusé.

De plus, l'adoption de câbles cuivre de catégorie 5, voire 6 a permis d'augmenter les débits. La vitesse de base d'Ethernet, de 10 Mbps, est dépassée, au profit de Fast Ethernet, à 100 Mbps, et Gigabit Ethernet, à 1 Gbps. L'usage de commutateurs permet de régler les cartes réseaux en mode full duplex, pour rendre encore plus efficace la communication.

c. La technologie CPL

La transmission par courants porteurs en ligne (CPL), en anglais Power line Communications (PLC) ou Broadband Power Line (BPL), existe depuis les années 1950. La technique utilisée à cette époque était unidirectionnelle et ne procurait que des faibles débits. Elle reste exploitée pour, par exemple, l'allumage et l'extinction des lampadaires de rues ou le basculement des compteurs électriques entre tarifs jours et nuits.

Vers la fin des années 1990, les recherches ont permis au CPL de devenir bidirectionnel et d'autoriser des hauts débits. Cette solution peut être mise en œuvre pour des communications à l'intérieur de bâtiments, sur de faibles distances. D'autres exploitations, tel l'accès à Internet par CPL, seront très rapidement possibles. En France, ce n'est, en effet, que durant le premier semestre 2005, que le caractère expérimental de cette possibilité a été levé, ouvrant la porte aux solutions commerciales.

Site Web du consortium : http://www.homeplug.org

Dans la perspective de l'utilisation des lignes électriques pour les réseaux locaux, un consortium américain, appelé HomePlug Powerline Alliance, a été créé. Il regroupe différents acteurs du domaine, comme par exemple, Intel, Linksys et Motorola, dans le but de travailler sur un cadre standard pour le courant porteur en ligne.

Des certifications ont été définies, ainsi que des tests, pour vérifier l'interopérabilité des matériels. Après validation, le constructeur est autorisé à utiliser le logo correspondant, par exemple sur la boîte du matériel.

Sigles de certification HomePlug

La première certification fut HomePlug 1.0, proposant des débits théoriques de 14 puis 85 Mbps. À cette certification initiale a succédé HomePlug AV (HPAV) destinée au réseau multimédia domestique. Compatible avec la version 1.0, elle autorise un débit théorique de 200 Mbps. Plus sécurisée, elle permet en outre la qualité de service et le streaming audio et vidéo.

Les deux autres sigles correspondent aux spécifications HomePlug Access BPL (Broadband Power Line), pour l'accès haut débit vers les habitations et HomePlug CC (Command & Control) pour le pilotage d'appareil par cette technologie.

Site Web des spécifications : http://www.homeplug.org/products/whitepapers

Le consortium HomePlug se rapproche également de l'IEEE et de son groupe P1901 (http://grouper.ieee.org/groups/1901), destiné à standardiser ce type de communications.

Cette technologie utilise donc le réseau d'installation électrique d'un bâtiment pour véhiculer des données informatiques. Pour cela, une puissance beaucoup plus faible et des hautes fréquences (bande 1,6 à 30 MHz) sont exploitées sur les câbles électriques. Des filtres passe-bande permettent de différencier ce signal superposé à celui

220V et 50 Hz, ne conservant que la donnée informatique.

Ce signal est reçu par tout adaptateur CPL branché sur le réseau électrique interne. Cet équipement le transforme ensuite en signal Ethernet, voire USB. Un ordinateur peut donc y être connecté.

Interface réseau CPL à brancher sur prise électrique

Le transport de hautes fréquences sur les câbles électriques peut poser un problème de perturbation radioélectrique. La puissance injectée ne doit pas être trop importante, afin de ne pas empêcher le fonctionnement des appareils non réseaux. De plus, ces perturbations peuvent entraîner un manque de confidentialité des communications. HomePlug prévoit d'ailleurs l'usage possible d'un chiffrement Advanced Encryption Standard (AES), venu succéder au Data Encryption Standard (DES).

La couche physique du HomePlug utilise la modulation par étalement de spectre, ou Spread Spectrum, avec la technique de transmission Orthogonal Frequency Division Multiplexing (OFDM).

La méthode d'accès est de type CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Ces moyens sont également utilisés lors des communications Wi-Fi.

Le CPL manque quelque peu de normalisation pour l'entreprise. Avec des débits un peu plus importants, cette technologie peut être un bon complément au Wi-Fi. En effet, l'interconnexion du réseau Wi-Fi avec la dorsale Ethernet n'est pas toujours possible, par exemple pour des raisons de distance. Dans un tel cas, la mise en œuvre d'un prolongement avec courant porteur en ligne peut apporter une souplesse non négligeable.

Il est fort probable que les évolutions de cette technologie prometteuse permettent rapidement un usage encore plus intéressant dans l'entreprise, voire à l'extérieur.

Technologies de réseaux hertziens

Les dernières avancées techniques de la transmission de données à travers des réseaux sans fils, plus particulièrement radio, ont permis de les banaliser. Ainsi, il est désormais possible de faire correspondre à chaque type d'étendue, au moins une technologie hertzienne. Nous remarquerons également que certaines solutions, qui ne semblaient pas pérennes, ont finalement été écartées au profit de concurrents désormais standardisés.

Comblant progressivement leur incapacité à effectuer des transmissions rapides, ces technologies hertziennes couvrent actuellement tous les besoins du nomadisme et de l'itinérance. La plupart sont mêmes devenues des solutions également proposées au grand public.

1. Réseaux personnels (RPAN)

a. HomeRF

Un consortium industriel, composé d'acteurs majeurs du monde informatique, tels que Compaq, Hewlett Packard, Siemens, Motorola et Intel se forme à la fin des années 1990. Ils composent un groupe de travail qu'ils nomment Home Radio Frequency (HomeRF), destiné à travailler sur une solution de liaisons sans fil domotique.

Le logo HomeRF

Afin de réaliser une liaison complète entre équipements informatiques et de téléphonie à la maison, un nouveau protocole réseau, nommé Shared Wireless Access Protocol (SWAP) est mis en œuvre. Évolution du Digital Packet Radio Service (DPRS), pendant, pour la donnée, de la norme de téléphonie sans fil Digital Enhanced Cordless Telephone (DECT), il reprend également des techniques proposées dans 802.11.

Initialement prévu pour offrir des débits de 1,6 Mbps, HomeRF prévoyait une nouvelle génération à 11 Mpbs, afin de permettre le passage de données multimédia.

À la limite entre les étendues RPAN et RLAN, cette solution aurait pu entrer en concurrence avec Wi-Fi et surtout Bluetooth. Finalement, la perte de deux soutiens de poids, que sont Intel et Microsoft, signe l'arrêt de cette technologie au début de l'année 2003.

b. Bluetooth

Sans solution réellement concurrente, Bluetooth est devenu, depuis quelques années, le standard des réseaux de type RPAN.

Lancée en 1994 par la société Ericsson, cette technologie porte le nom d'un roi danois "Harald II". Surnommé Harald II Blåtand (dent bleue - blue tooth), grand mangeur de myrtilles, il unifia le Danemark, ainsi qu'une partie de la Suède et de la Norvège, au IXe siècle. Cette appellation marque la volonté, de la part d'Ericsson, de rassembler le monde de la téléphonie mobile.

D'autres grands industriels, tels que Nokia, Intel, Microsoft, Toshiba, et IBM ont ainsi rejoint ce constructeur, à partir de 1998, pour former le Bluetooth Special Interest Group (SIG). Il compte actuellement plus de 10000 sociétés membres.

Site Web du SIG : http://www.bluetooth.org

Site Web de la technologie : http://www.bluetooth.com

Destiné à faire communiquer des équipements hétérogènes et peu éloignés, Bluetooth regroupe, sur une puce unique de moins d'un centimètre de côté, des capacités très avancées.

Ainsi, la spécification 1.0, publiée en juillet 1999 est adaptée aux transmissions de voix, données et images. Son débit théorique est de 1 Mbps. Sa fréquence de travail est la même que celle du Wi-Fi, soit 2.4 Ghz. Enfin, elle est très économe en énergie.

La deuxième spécification date de la fin de l'année 2004. Encore plus économe en énergie, elle est capable de débits théoriques de 10 Mbps, autorisant ainsi la transmission de vidéos.

Des équipements Bluetooth peuvent être interconnectés de deux manières. La première consiste à former un réseau unique, le piconet, composé d'un terminal maître prenant en charge jusqu'à 7 terminaux esclaves. Toutes les communications, même entre esclaves, sont gérées et transitent par le maître.

Une deuxième solution est d'interconnecter plusieurs réseaux en étoile. Ceux-ci forment un scatternet, dans lequel le maître d'un piconet peut devenir l'esclave d'un autre piconet.

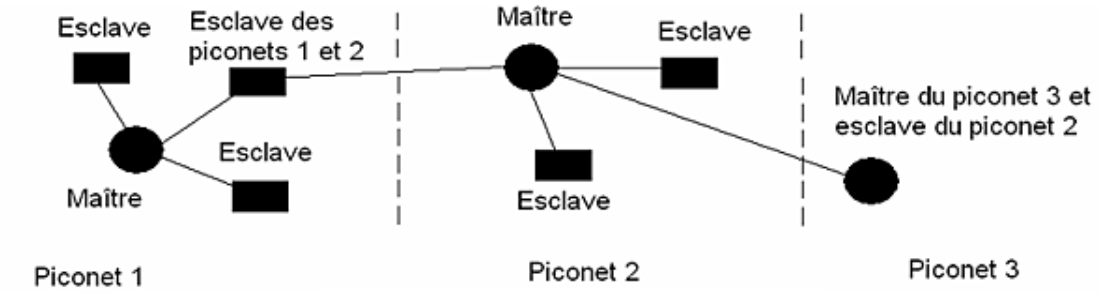


Schéma d'un réseau complexe Bluetooth

Au sein de tels schémas, différents débits sont autorisés entre équipements, pour un total de 1 Mbps en spécification 1.0. Une communication bidirectionnelle full-duplex atteindra environ 434 Kbps dans chaque sens, alors qu'une autre, dite déséquilibrée, autorisera 732 Kbps dans un sens et 58 Kbps dans l'autre.

Destinée à prendre en charge de multiples types de transmissions, cette technologie autorise des communications synchrones (SCOL - *Synchronous Connections Oriented Link*) à 64 Kbps. Cette valeur est celle de la voie téléphonique numérisée : modulation par impulsion codée (MIC) des réseaux numériques à intégration de services (RNIS). Elle autorise la qualité de service. Pour les débits supérieurs, l'asynchronisme, par Asynchronous Connections Oriented Link (ACOL), est utilisé.

Trois classes d'appareils Bluetooth sont définies :

- Classe 1, d'une puissance de 100 mW, pour des grandes distances jusqu'à 100 mètres ;
- Classe 2, d'une puissance de 2,5 mW, pour des distances moyennes d'environ 15 à 20 mètres ;
- Classe 3, de puissance 1 mW, pour des petites distances, sur une dizaine de mètres.

L'essentiel des équipements du commerce sont de classe 3. Cette technologie est actuellement beaucoup utilisée pour des kits mains libres universels de téléphonie mobile. On la retrouve également dans des liaisons entre périphériques (assistants personnels numériques...) ou entre ordinateurs et périphériques (imprimantes...). Dans ce dernier cas, elle remplace la solution filaire Universal Serial Bus (USB).

Quelques équipements communicant par Bluetooth

En effet, Bluetooth est véritablement construit pour de multiples utilisations. Les fonctionnalités d'un périphérique sont ainsi répertoriées en tant que profils. Pour que deux équipements puissent communiquer, leur usage doit correspondre. Parmi les différents profils, on peut citer :

- GAP (*Generic Access Profile*), définissant les procédures de recherche d'appareils, de connexion et de sécurité ;
- HS Profile (*Headset Profile*), pour les kits mains libres ;
- LAN Access Profile ;
- Fax Profile ;
- FTP (*File Transfer Profile*) ;
- CTP (*Cordless Telephony Profile*)...

Ainsi, un réseau TCP/IP radio entre plusieurs machines (Ad hoc) peut être composé grâce au profil réseau local Bluetooth. Au sein de celui-ci, trois rôles sont possibles, afin de déterminer plusieurs topologies. Si un des ordinateurs est configuré comme point d'accès réseau, il peut servir d'interface avec un réseau filaire. La communication directe entre deux ordinateurs peut être effectuée par les rôles Personal Area Network User (PANU). Un dernier rôle, réseau GN, peut être possédé par une et une seule machine, à laquelle vont se connecter des PANU.

Bien que de tels usages soient possibles, les débits autorisés restent faibles par rapport à de véritables solutions WLAN. Et le groupe IEEE 802.15 (*Wireless Personal Area Network Working Group*) a choisi de se baser sur Bluetooth pour son standard.

Site Web du groupe 802.15 : http://grouper.ieee.org/groups/802/15/

En fait, 4 subdivisions, les groupes de projet, ou Tasks Groups, ont été formées.

Du projet 802.15.1, publié en juin 2002, a découlé un standard, basé sur Bluetooth v1.1.

Le second projet, 802.15.2, finalement mis en hibernation, avait pour charge des travaux sur la coexistence entre WPAN (802.15) et WLAN (802.11).

La solution haut débit (HR - *High Rate*) du groupe 802.15.3 a été finalisée en juin 2003. Elle permet le transfert de fichiers audio et vidéo en streaming, en se basant sur la technologie Ultra Wide Band (UWB), issue de l'armée américaine. Ce standard est capable de débits de plusieurs centaines de mégabits par seconde, sur quelques dizaines de mètres. De plus, cette solution ne craint pas de passer les obstacles, tels que les murs d'un bâtiment.

Enfin, à l'autre extrémité, la solution bas débit, avec économie d'énergie très avancée du groupe 802.15.4, a été approuvée en 2006. Cette norme, également appelée ZigBee est le prolongement de HomeRF. Elle peut être utilisée pour transmettre des commandes, plus que des données. Son débit est au maximum de 250 Kbps sur une distance d'une dizaine de mètres.

2. Réseaux locaux (RLAN)

a. HiperLAN

La proposition High Performance LAN (HiperLAN) développée par le groupe Broadband Access Radio Networks (BRAN) de l'ETSI comprend plusieurs familles.

HiperLAN Type 1 est destinée aux communications réseaux sans fil à l'intérieur de bâtiments, offrant un débit de 20 Mbps. D'une portée d'environ 50 mètres, elle prévoit la possibilité d'un déplacement jusqu'à environ 10 mètres/seconde de l'équipement relié. HiperLAN 2 étend la portée à 200 mètres et le débit à 54 Mbps. HiperLAN

3, appelé également Hiper-Access, et HiperLAN 4 (HiperLink) sont réservées à des accès plus étendus.

Devant l'impact commercial du Wi-Fi, il existe fort peu de références d'équipements HiperLAN. Pourtant, certaines des études effectuées pour cette technologie européenne sont à l'origine de techniques utilisées dans le projet 802.11.

b. Wi-Fi

Pour les réseaux radio locaux, les spécifications du groupe de travail IEEE 802.11 sont finalement devenues celles du standard commercial. Et Wi-Fi est venu offrir une appellation grand public à ces équipements... comme nous le verrons plus tard.

Wi-Fi reste cependant limité par ses portées restreintes et ses débits, qui peinent à évoluer.

3. Réseaux métropolitains (RMAN)

a. La boucle locale radio

La boucle locale est la partie d'un réseau de télécommunications placée entre les équipements de l'opérateur et l'utilisateur final. En France, les fils de cuivre de la boucle locale sont propriétés de France Télécom, sur le réseau téléphonique commuté (RTC). Ils conduisent aux matériels de commutations appelés Digital Subscriber Line Access Multiplexor (DSLAM), qui sont placés dans les centraux téléphoniques.

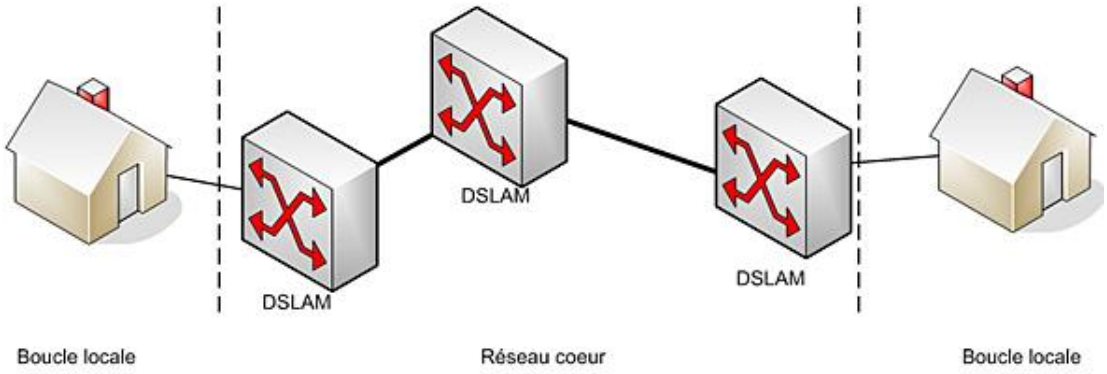


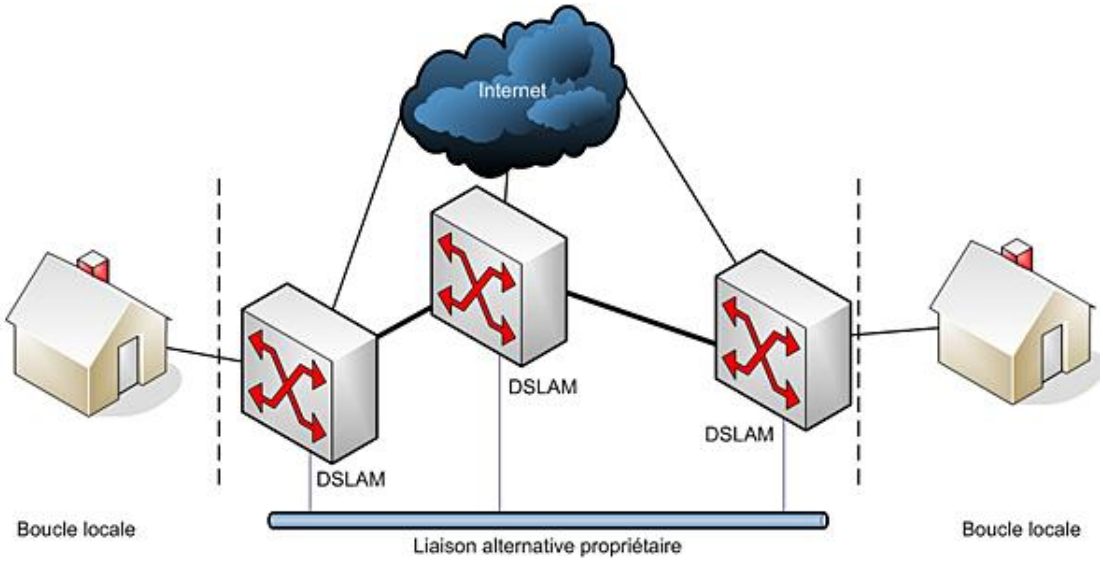
Schéma du RTC

Les solutions d'accès à Internet haut débit xDSL, dont Asymmetric Digital Subscriber Line (ADSL), utilisent ces lignes RTC. Malheureusement, ces technologies ne peuvent couvrir l'ensemble de la population, ne permettant pas l'accès rapide à Internet pour tous. En effet, un foyer distant de plus de 6 kilomètres d'un répartiteur DSLAM ne peut être connecté à l'ADSL. Des évolutions sont venues enrichir l'offre pour augmenter les débits et/ou prolonger les distances d'exploitation. Nous pouvons citer, par exemple, Reach Extended ADSL2 (RE-ADSL2) et ADSL2+.

L'exploitation de la solution boucle locale radio (RLL - *Radio Local Loop* ou WLL - *Wireless Local Loop*) permet de s'affranchir de ce problème de distance. La BLR devient ainsi une solution complémentaire aux techniques xDSL en autorisant des sites professionnels et foyers à accéder à Internet haut débit.

Des opérateurs alternatifs à France Télécom peuvent ainsi créer leurs propres réseaux hertziens de BLR, moyennant autorisation, comme nous le verrons plus tard.

Pour les Fournisseurs d'Accès Internet (FAI), la BLR est également une solution potentielle à certains problèmes actuels du dégroupage. En effet, il est difficilement concevable pour ces opérateurs de reproduire un réseau de télécommunications complet arrivant jusqu'au client final. Dans une offre de dégroupage partiel, l'opérateur alternatif relie la boucle locale, appartenant à France Télécom, à son propre réseau. Pour cela, il place ses équipements de transmission dans les locaux de l'opérateur historique, dont il est concurrent. Le dégroupage total impose, en plus, au FAI la location de la ligne de la boucle locale. On comprend donc que l'utilisation de la BLR permettrait de simplifier certaines opérations.



RTC, l'alternative

b. WiMax

Les solutions de type RMAN, exploitables pour la BLR, sont standardisées par le groupe de travail IEEE 802.16 (*Broadband Wireless Access Working Group*). Pour promouvoir celles-ci, les sociétés Intel et Alvarion sont à l'origine, en 2002, d'une association, le Worldwide Interoperability for Microwave Access (WiMax) forum. Ce groupement compte aujourd'hui de nombreuses sociétés membres.

Site Web du WiMax Forum : http://www.wimaxforum.org

En plus de la promotion de cette technologie, le but de cette association est de faciliter la certification des équipements, afin de garantir leur compatibilité.

Le standard IEEE 802.16a, ratifié en janvier 2003, a servi de base au WiMax. Il autorise des débits symétriques théoriques, allant jusqu'à 70 Mbps, pour une portée pratique d'environ 50 kilomètres. En réalité, les opérateurs parlent d'un débit réel maximum de 12 Mbps pour une portée de 10 à 20 kilomètres, en fonction de l'environnement.

Quelques antennes d'infrastructure peuvent ainsi suffire à mettre en œuvre une connexion point à multipoints à l'échelle d'un département. Ce premier standard, qui ne gère que la connexion fixe, est devenu obsolète au profit du 802.16d, également appelé 802.16-2004, ratifié en juin 2004.

L'évolution 802.16e, validée en décembre 2005 apporte la mobilité au Wi-Max. Elle prévoit le passage d'une antenne à l'autre (Hand-over) et le déplacement à bord d'un véhicule sans incidence pour la communication. Son débit théorique est de 30 Mbps et sa portée jusqu'à 3,5 kilomètres. Pour communiquer, les PC portables et autres équipements nomades devront intégrer un composant dédié.

Le logo WiMax

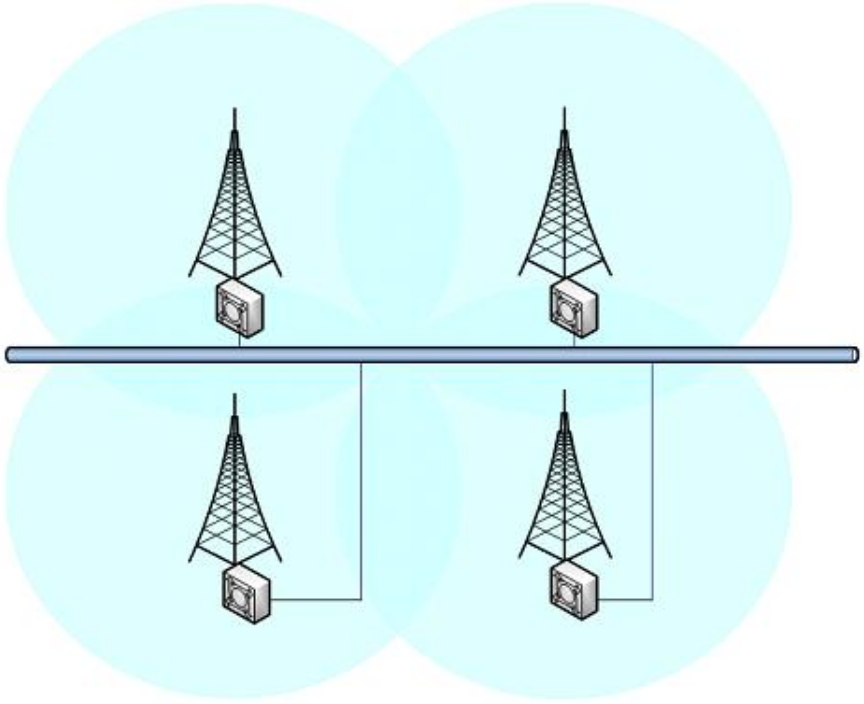
Face aux autres spécifications concurrentes, que ce soit Wi-Fi ou standard de téléphonie mobile, l'avenir commercial du 802.16e reste en suspens, contrairement au 802.16d, de plus en plus exploité.

4. Réseaux étendus (RWAN)

a. Les réseaux cellulaires

La téléphonie cellulaire est devenue courante et là encore, la convergence des réseaux voix et données est d'actualité.

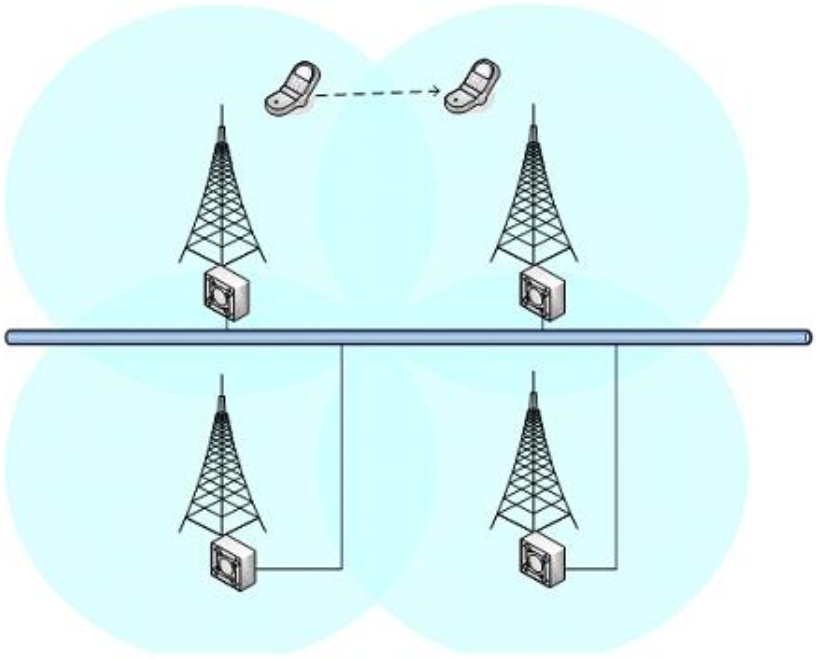
Dans ces réseaux, une antenne (RAN - *Radio Access Network*) couvre une zone géographique donnée. Tous les points qui peuvent être atteints à partir de cet équipement forment une cellule. Une station de base, liée à l'antenne, assure le rôle de serveur pour tous les clients de la cellule. Un réseau Cœur (CN - *Core Network*) relie entre elles les différentes stations de base.



Réseau de téléphonie mobile

Cette organisation en cellules géographiques recouvrantes permet le transfert de l'une à l'autre durant une communication. En effet, l'équipement mobile teste en continu la qualité des signaux reçus. Si sa station de base ne lui fournit pas le meilleur, il demande au gestionnaire, sur le réseau cœur, le basculement. Cette action, en communication, porte le nom de hand-over, handover, ou handoff. En téléphonie cellulaire, une capacité de roaming, ou itinérance, indique un accord entre opérateurs pour accéder à leur réseau depuis l'étranger.

De telles notions et appellations peuvent être retrouvées dans des réseaux de taille inférieure, RMAN ou RLAN. Le terme de hand-over indique parfois également un changement de technologie. En Wi-Fi, le terme roaming indique un transfert entre cellules.



Le hand-over en téléphonie mobile

b. L'évolution des systèmes cellulaires

À la fin des années 70, le réseau Radiocom 2000 devient la première génération (1G) de téléphonie mobile. Le fonctionnement en est complètement analogique, en commutation de circuit. Le réseau est composé de cellules de quelques kilomètres de portée.

Combiné Radiocom 2000

Au début des années 80, la conférence européenne des postes et télécommunications (CEPT) commence à normaliser un système de téléphonie mobile numérique. Elle réserve pour cela des bandes de fréquences près des 900 MHz. Et en 1987, le groupe d'étude GSM, *Groupe Spécial Mobile*, du CEPT lance le système de téléphonie Global System for Mobile (GSM). Dans cette 2^{e} génération (2G), le transport est numérique, optimisé pour la parole.

Une évolution de cette dernière, exploitant la bande 1800 MHz, le Digital Cellular System (DCS 1800) arrive rapidement et est finalisé en 1990.

Rien ne s'opposant techniquement à cela, un premier service de données par GSM est tenté : le Wireless Application Protocol (WAP). La donnée est modulée en signal voix, pour être ensuite reconstituée par démodulation. Son débit est de 9,6 Kbps.

Cette solution, qui fut un échec commercial, trouvera un successeur avec General Packet Radio Service (GPRS), parfois qualifiée de génération 2.5. Il s'agit d'une véritable adaptation des réseaux cellulaires aux transferts de données : la connexion peut être permanente, puisqu'elle exploite la technique de commutation de paquets. Sur les terminaux, les transferts de voix sont toujours pris en charge par GSM (facturation possible au temps de communication), tandis que les transferts de données sont pris en charge par GPRS (facturation possible au poids de données transmises).

Cette nouvelle technique permet un débit théorique allant jusqu'à 115 Kbps, 40 Kbps en pratique, adaptant sa vitesse à la qualité du réseau. Grâce à elle, les assistants personnels deviennent réellement communicants et de nombreuses solutions voient le jour.

Les terminaux mobiles désormais utilisables pour la donnée

GPRS évolue en EDGE (*Enhanced Data for GSM Evolution*), technologie également dédiée au transfert de données en mode paquets. Tout en réutilisant les infrastructures réseaux GSM existantes, elle permet d'augmenter la vitesse d'exploitation. Son débit théorique peut atteindre 384 Kbps. EDGE est considérée comme une solution intermédiaire entre GPRS et UMTS et est qualifiée de génération 2.75.

Mais les débits demeurent quand même insuffisants et il est difficile de proposer avec GPRS ou EDGE des applications multimédia, comme, par exemple, la télévision sur les téléphones mobiles ou la visiophonie. De plus, à l'échelle mondiale, les différents systèmes de communication mobile 2G sont incompatibles. L'union internationale des télécommunications (UIT) propose donc, dès 1985, la définition d'un programme Future Public Land Mobile Telecommunications (FPLMTS), pour exploiter une bande de fréquences unique et suffisante, pour proposer des accès jusqu'à 2 Mbps.

L'ensemble de spécifications de ce programme, finalement baptisé système International Mobile Telecommunication (IMT 2000) intéressa l'ETSI qui proposa sa solution y répondant : Universal Mobile Telecommunications System (UMTS). D'autres organismes se regroupèrent, autour de cette solution, pour former le consortium 3rd Generation Partnership Project (3GPP), qui adopte l'UMTS au niveau mondial début 1998. Les USA préféreront finalement adopter le système CDMA2000, issu des travaux du groupe 3GPP2.

En Europe, L'UMTS devient la 3e génération (3G) de téléphonie mobile.

Pour répondre aux fortes contraintes du hand-over, un débit maximal est retenu : 384 Kbps en réception. Il autorise le transfert entre deux cellules à la vitesse d'un véhicule automobile. De plus, des basculements sans perte de communication entre 2G et 3G sont possibles.

L'investissement nécessaire aux opérateurs de téléphonie mobiles pour passer en UMTS est important. Les débits demeurent trop limités pour des applications permettant un retour sur investissement suffisant. Rapidement, l'UMTS évolue logiciellement en HSDPA (*High Speed Downlink Packet Access*), considéré comme l'ADSL pour la téléphonie mobile. Cette génération 3G+ autorise des débits de plus de 3 Mbps.

Cartes modem 3G ou 3G+ aux formats PCCard ou USB

La future révolution des réseaux hertziens pourrait être l'exploitation de la norme de communication Unlicensed Mobile Access (UMA). Celle-ci autorisera le roaming entre réseaux 2G ou 3G vers Wi-Fi ou Bluetooth, sans coupure de communication. Cette solution, dite Intelligent Transportation Systems (ITS), pourrait imposer de disposer d'une adresse IP permanente.

Les usages d'un réseau Wi-Fi

Nous l'avons vu précédemment, le Wi-Fi est loin d'être la seule solution de réseau hertzien. Demeurant depuis plusieurs années la seule technologie ayant un succès commercial notable sur l'étendue RLAN, elle n'est pas concurrencée. L'Ultra Wide Band (UWB) comme le Wimax, auraient pu devenir concurrent du Wi-Fi, en débordant de leur usage premier. Elles n'ont, jusqu'ici, pas tenu leur promesses.

La simplicité d'utilisation et le coût réduit du Wi-Fi lui ont permis de conquérir le grand public comme les professionnels. Après des débuts difficiles aux USA, puis en Europe en 2001, elle a démocratisé une nouvelle tendance qui est loin d'être éphémère, de communications sans fil.

1. Réseau local Wi-Fi

a. Pourquoi utiliser du Wi-Fi ?

Cette technologie est d'abord à considérer comme la version sans fil d'Ethernet. Elle arrive de concert avec une exigence de mobilité à l'intérieur de l'entreprise. En effet, à quoi bon utiliser des terminaux portables, voire ultra portables, s'il est nécessaire de rechercher une prise pour se connecter au réseau ?

Au-delà d'un usage bureautique, où il s'avère que l'on utilise toujours son terminal posé sur une table, le Wi-Fi autorise une véritable itinérance. Dans les milieux hospitaliers, industriels, voire dans les entrepôts, cette solution standard est très prisée, car elle autorise une liberté de mouvements sans s'enchaîner à un fournisseur de matériel.

Une autre qualité de cette technologie réside dans sa facilité de mise en œuvre. Une autre utilisation importante est l'extension du réseau d'entreprise. Amener le réseau local là où il n'est pas encore disponible est désormais beaucoup plus évident qu'avec une solution filaire. En plus de la facilité et de la rapidité de déploiement, le coût représente un critère de choix important. S'il est nécessaire d'ajouter des équipements, l'interconnexion d'un ordinateur à un réseau Wi-Fi est beaucoup moins onéreuse. De plus, la topologie dynamique, autorisée par un réseau sans fil, permet d'envisager des implantations provisoires.

Finalement, un terminal Wi-Fi n'est pas obligatoirement un ordinateur, puisque ces capacités de communications sont désormais ajoutées à des lecteurs de code-barres, des imprimantes, des vidéo-projecteurs, des caméras... et des téléphones.

Téléphone et vidéo-projecteur communicant par Wi-Fi

Cette technologie est également utilisée à domicile, pour composer des réseaux familiaux et partager une connexion à Internet.

b. Les avantages et les inconvénients

Comme nous l'avons vu précédemment, la principale qualité du Wi-Fi est la simplicité. De plus, les fréquences exploitées par ses techniques de transmission sont d'usage libres et ne nécessitent donc pas de licence. Ainsi, tout le monde peut mettre en œuvre un réseau de ce type, sans toutefois outrepasser certaines règles, qui seront exposées plus tard. Faire communiquer des appareils en Wi-Fi ne présente pas de difficultés et ne demande qu'un minimum de connaissances.

Malheureusement, le principal inconvénient provient du support lui-même, l'onde radio, et de l'utilisation anarchique des fréquences utilisées. En effet, les limites de communication sont plus difficilement maîtrisables que celles d'un réseau filaire. Et bien souvent, par manque de compétence, la personne qui déploie le réseau n'est pas sensible à cette notion. Potentiellement, les ondes peuvent aller polluer les communications d'un réseau voisin, qui devient moins performant.

De plus, les données étant transmises dans l'air, la sécurité doit être pensée en conséquence. Il est très facile d'intercepter des communications Wi-Fi non protégées et de lire les fichiers transmis.

Idéalement, un RLAN se rapproche du réseau LAN, sans contrainte filaire. Mais il faut concevoir que l'état actuel de la technologie radio n'autorise pas des débits aussi importants que sur un support filaire.

Un dernier point faible du Wi-Fi est paradoxalement son universalité. En effet, il est nécessaire de faire la distinction entre les matériels familiaux et professionnels. Non seulement les équipements d'infrastructure sont distincts, pour des raisons de performances et de fonctionnalités, mais les possibilités de configuration et de protection ne sont généralement pas les mêmes.

Déployer des équipements Wi-Fi en entreprise nécessite donc quelques compétences, afin de profiter pleinement d'un réseau représentant un très bon complément à la solution filaire Ethernet. L'interconnexion entre ces deux réseaux peut être facilitée par la solution CPL.

2. Hot-Spots

a. Les utilisations

Un Hot-Spot permet un accès à Internet par la technologie Wi-Fi. La commission générale de terminologie et de néologie a francisé ce terme en Accès Sans Fil à Internet (ASFI). De tels accès permettent d'exploiter son propre ordinateur portable, ou autre terminal mobile. Le service fourni est donc exclusivement l'accès, ce qui permet de garder son environnement de travail.

Les ASFI se sont multipliés depuis plusieurs années et de nombreux sites tels que aéroports, gares, hôtels, restaurant en proposent. Des ASFI sont même désormais mis à disposition des internautes par certaines mairies dans les centres villes.

Cette utilisation du Wi-Fi dépasse le cadre habituel du RLAN. On pourrait donc penser que de tels services pourraient être rendus par l'une ou l'autre technique présentée précédemment. Mais la technologie Wi-Fi présente actuellement une maturité, une simplicité d'emploi et des débits qui satisfont pleinement cet usage.

La mise en place et l'exploitation d'un Hot-Spot peut vite devenir complexe, nécessitant la création et la gestion d'un réseau complet. Cette spécialité est celle d'opérateurs appelés fournisseurs d'accès à Internet sans fil (WISP - *Wireless Internet Service Providers*). Parmi les principaux, on peut citer ADP Télécom, filiale de Aéroports de Paris (ADP) l'un des plus importants, ou Naxos, filiale de la RATP.

b. Les Hot-Spots des opérateurs de téléphonie mobile

Les opérateurs français de téléphonie mobile ont également investi le marché des Hot-Spots. Pour eux, Wi-Fi a représenté une bonne alternative aux solutions cellulaires UMTS, GPRS et EDGE en attendant la généralisation de HSDPA. À l'intérieur de bâtiments, dans les hôtels par exemples, l'ASFI est plus rapide et moins onéreux par le Wi-Fi. D'autres accès sont prévus dans les transports, tels que les trains, et les avions. Le déploiement de tels points d'accès ne fait que commencer.

La facturation de ces services d'accès haut débit à Internet peut être effectuée directement sur le compte du téléphone mobile. Et des accords de roaming entre opérateurs Wi-Fi se sont développés, afin d'utiliser en toute transparence le réseau du concurrent.

Caractérisation des ondes

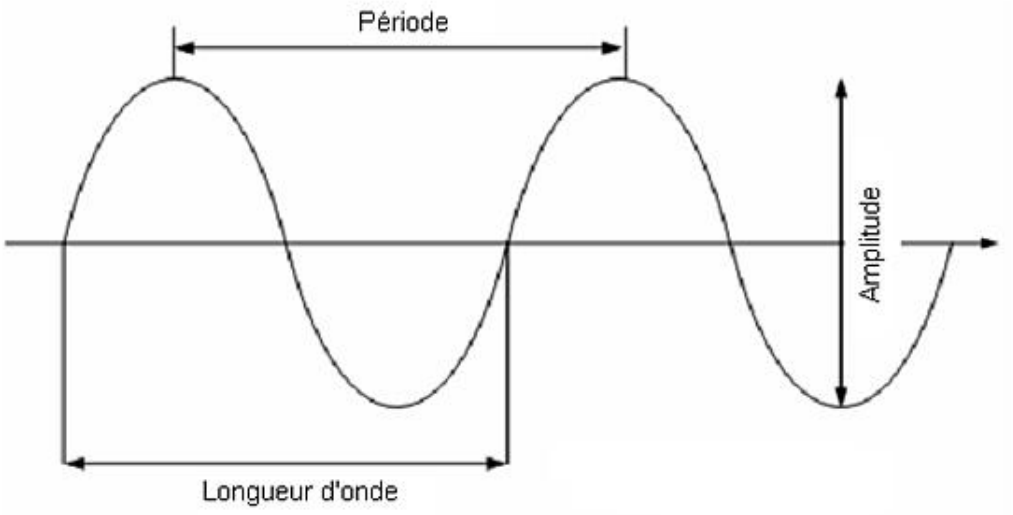
Afin de mieux appréhender la mise en œuvre d'un réseau radio, il est recommandé d'acquérir quelques connaissances physiques sur les ondes électromagnétiques. L'intérêt en est la compréhension des contraintes inhérentes à ce type de transmission. En effet, si des limites de propagation existent sur une interface filaire, elle n'est pas sujette aux mêmes perturbations que l'onde dans l'atmosphère.

Dans les environnements intérieurs, particulièrement, les contraintes de l'interface air sont multiples et doivent être prises en compte. Bien sur, les matériels, tant sur leurs composants radio qu'au niveau électronique, sont conçus en conséquence. Mais leur mise en place doit permettre d'optimiser les fonctionnements.

1. Propagation

a. Le phénomène ondulatoire

L'onde radio, utilisée par la technologie Wi-Fi, fait partie de la famille des ondes électromagnétiques, oscillations générées par le courant alternatif. Découvert par le physicien allemand Heinrich Hertz au seuil des années 1890, ce phénomène ondulatoire peut être utilisé pour la transmission d'informations à travers l'air ambiant. Contrairement aux rayons infrarouges, une visibilité directe n'est pas obligatoire dans la cellule de communication, entre l'émetteur et le récepteur. La première utilisation de cette onde a été la radiotélégraphie, ou télégraphie sans fil (TSF), dès la fin du XIXe siècle.



Caractéristiques basiques de l'onde électromagnétique

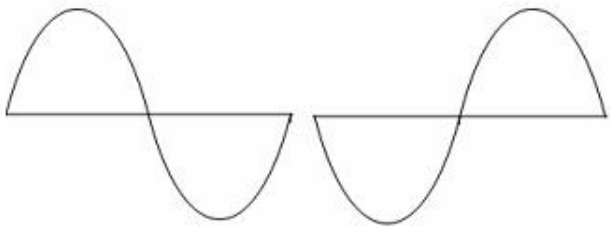
La première caractéristique d'une onde radio est sa fréquence, d'unité le Hertz (Hz) en hommage au découvreur. Elle représente le nombre d'oscillations par seconde de l'onde.

La période qualifie la durée d'une oscillation complète, en secondes. Il s'agit de l'inverse de la fréquence.

On peut également calculer la longueur d'onde, distance parcourue par une oscillation, en mètres.

La hauteur de l'onde est qualifiée d'amplitude. Elle est mesurée en Volt/mètre si le phénomène est électrique, ou en Teslas, dans une mesure magnétique. Nous utiliserons plutôt le terme de puissance pour la qualifier.

La phase indique le sens de l'onde.



Phases opposées d'une onde

La propagation est le trajet de l'onde radioélectrique dans l'espace, à partir de l'antenne de l'émetteur. Les signaux diffusés dans toutes les directions seront reçus par tout récepteur, calé sur la même fréquence, dans la cellule de communication, en ligne droite et à vue.

La vitesse de propagation est qualifiée de célérité, en mètres par seconde. Le vide représente le milieu parfait pour l'onde, soumise à quantité de contraintes dans l'air. Sa vitesse, dans ce cas, y est d'environ 300 000 kilomètres par seconde (km/s), soit celle de la lumière.

Prenons pour exemple une onde hertzienne de 2.4 GHz, une des fréquences de travail des RLAN et donc du Wi-Fi. Elle oscille 2,4 milliards de fois par seconde. Chaque oscillation dure 0,42 nanoseconde (unité représentant 10-9 secondes). La longueur d'onde, λ, est le résultat de la multiplication de la période par la vitesse. Si l'on se base sur la vitesse de la lumière, la longueur de l'onde λ est de 12,56 cm.

b. Les différentes perturbations

Types d'ondes

L'altération d'un signal radio dépend tout d'abord du type d'onde utilisé. Pour se propager, l'onde de sol, de faible fréquence, entre quelques kilohertz et 1 MHz, suit la courbure de la terre. Les ondes courtes, entre 1 et 50 MHz, se réfléchissent entre le sol et l'atmosphère.

Les réseaux de transmission de données que nous utilisons utilisent des ondes très courtes, ainsi qualifiées à partir de 50 MHz. Elles ne se réfléchissent pas dans l'atmosphère, mais sur les couches basses de l'air, présentant des différences de température. De plus, elles sont sensibles aux obstacles, mêmes petits.

Rapport signal/bruit et atténuation

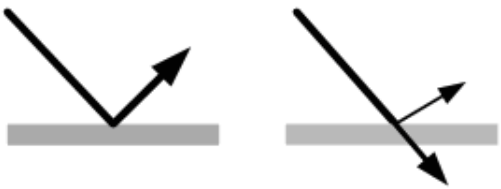
La portée et la qualité d'un signal dépendent également des interférences rencontrées sur son passage, le bruit, rassemblant les ondes radio perturbantes. Si le niveau de bruit est trop important, l'information contenue dans l'onde hertzienne sera tellement modifiée qu'elle en deviendra incompréhensible par le récepteur. Le rapport signal/bruit (SNR - *Signal to Noise Ratio*) est une comparaison des ondes exploitables avec celles d'interférence. Il doit être en faveur des premières. Plus ce ratio est important, meilleures sont la qualité et les performances du réseau sans fil.

Les premières sources de bruit sont des émissions d'ondes, de fréquences très proches. Parmi celles-ci, un autre réseau Wi-Fi, dont la cellule de transmission est recouvrante et le choix de fréquence proche du votre, peut être très perturbateur. La technologie Bluetooth peut également venir causer quelques interférences, mais sa distance d'émission est faible. Pour l'anecdote, le four micro-onde, fonctionnant à des fréquences équivalentes à celles du Wi-Fi, peut être un élément perturbateur. Notre atmosphère contient de multiples sources de bruits, voitures, industries... qui rendent ce phénomène inévitable.

L'intensité du signal hertzien, délivré par l'émetteur, diminuera avec la distance dans l'interface air, jusqu'à se confondre avec le bruit. Cette atténuation, ou absorption, peut être également dépendante de la traversée d'obstacles. En fonction de ceux-ci, la perte peut être plus ou moins importante.

Réflexion de l'onde

Mais cet affaiblissement n'est pas le seul phénomène auquel est soumise l'onde. Un obstacle peut l'atténuer, mais également la réfléchir. La réfraction est un changement de direction, dû à un rebond, qui peut être total ou partiel. Un réflecteur parfait peut être représenté par un plan ne laissant pas traverser le signal.



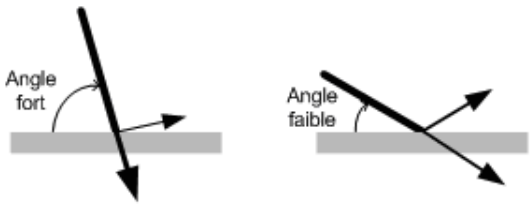
Ces deux incidences dépendent à la fois de l'épaisseur et de la nature de l'obstacle. Par exemple, le béton et le métal sont beaucoup plus absorbants que le plastique et le verre, qui eux, sont plus réfléchissants. Il faut noter que l'eau absorbe beaucoup les ondes très courtes.

Exemples d'absorption en fonction du matériau

OBSTACLE	ATTENUATION

Air ambiant (Espace ouvert)	Faible
Vitre en verre non teinté	Faible
Bois sec (Portes, planchers...)	Faible
Eau et matériau humide	Moyenne
Papier (Bibliothèques..)	Elevée
Béton (Murs porteurs, planchers...)	Elevée
Verre blindé	Elevée
Métal	Très élevée

La pénétration d'un obstacle dépend non seulement de sa consistance, mais également de la fréquence du signal. Plus celle-ci augmente, plus la traversée est difficile. Enfin, l'angle d'incidence de l'onde venant frapper le matériau est également un facteur. Plus cette attaque est proche de la perpendiculaire, moins la réflexion est importante.



Angle d'incidence et réflexion

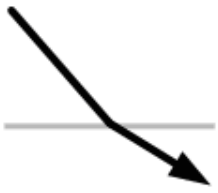
Le phénomène d'absorption du à l'humidité a une incidence notable sur les ondes. En extérieur, les conditions météorologiques peuvent modifier le signal. L'être humain est lui-même perturbateur. En effet, il est essentiellement constitué d'eau. Ainsi, les trajets de l'onde ne seront pas les mêmes dans une pièce vide ou en la présence d'hommes.

Diffraction et réfraction de l'onde

Une diffraction est une zone d'interférence qui peut être rencontrée après passage ou contournement d'un obstacle. En fonction de celui-ci et de la fréquence du signal, l'angle de diffraction est différent. Une onde dupliquée, mais très atténuée, est ainsi créée.

Diffraction

Sur certains obstacles non opaques, comme le verre, le signal peut être à la fois réfléchi et réfracté. Ce brusque changement de transmission modifie l'angle de traversée de l'onde, sans absorber le signal.

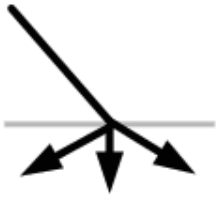


Réfraction

Diffusion de l'onde

Lorsque le trajet suivi par l'onde contient des obstacles de dimension comparable à celle-ci, elle est diffusée. Ce

phénomène peut également avoir lieu sur une surface non plane contenant des aspérités. Deux résultats sont possibles : la dispersion en de multiples ondes ou la transmission pure et simple.



Diffusion

Cheminements multiples

En plus d'une réduction de la portée de l'onde, ces différents phénomènes entraînent ce que l'on qualifie de cheminements multiples, multipath en anglais. Le signal reçu est donc l'addition de celui émis et des composantes de propagation. Ces ondes dupliquées, avec un léger décalage dans le temps, provenant de chemins multiples, varient en fonction des conditions, obstacles mouvants..., et de la position du récepteur. Un signal peut même être annulé par une autre onde tellement décalée dans le temps qu'elle se retrouve en opposition de phase.

Signaux reçus

Signal combiné résultant

Un traitement électronique du signal doit donc être réalisé par le récepteur. En intérieur particulièrement, certains matériels utilisent même plusieurs antennes. Par exemple, lorsque deux antennes en diversité sont exploitées. Les ondes, provenant du même émetteur, sont reçues sur l'une et l'autre. Elles sont distinguées et les meilleures ondes sont retenues. La distance entre ces deux antennes correspond à un sous-multiple de la longueur d'onde. À l'extrême, un signal pourrait être reçu par un seul de ces deux composants. Il est ainsi distingué, ce qui n'aurait peut-être pas été possible avec une seule antenne.

Le travail sur le signal est même poussé encore plus loin dans la technologie MIMO (*Multiple Input Multiple Output*), sur laquelle nous reviendrons. Ici, les antennes, le plus souvent au nombre de 3, sont capables de traiter des signaux distincts qui, de plus, utilisent le rebond sur les murs et autres surfaces.

Cette nécessité de travail du signal radio est moindre en environnement extérieur, où il est plus facile de capter le signal d'origine, en ligne droite et à vue.

En résumé, plus la fréquence est élevée, plus la vitesse de transmission des données peut être importante. Mais en conséquence, l'onde radio est plus sensible aux obstacles, ce qui réduit la couverture. Et le signal reçu a subi de nombreuses modifications.

c. Les autres incidences

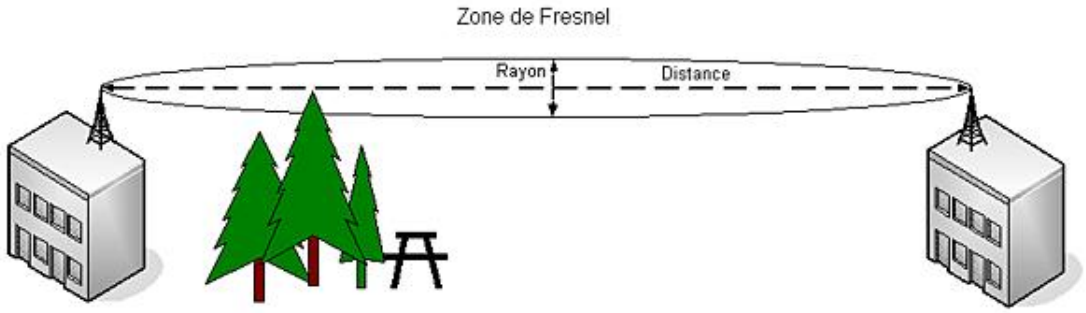
Comme nous l'avons vu précédemment, la meilleure transmission hertzienne correspond toujours à une portée en vision directe, avec le moins possible de signaux perturbés en multicheminements.

Ce cas est qualifié de Line of Sight (LoS). Pour concrétiser cette ligne de visée directe entre les antennes, une ellipse imaginaire peut être dessinée. On la qualifie de zone de Fresnel. Son axe rejoint les deux antennes. Celles-ci doivent être positionnées suffisamment haut pour que la zone soit la plus dégagée possible.

Le rayon maximal de cette ellipse dépend de la distance entre les deux antennes ainsi que de la fréquence de transmission. Par exemple, à 2.4 GHz, il n'est que de quelques dizaines de centimètres pour un espacement d'une centaine de mètre. 60 % de cette zone doit être dégagée pour éviter des perturbations trop importantes. Si la moitié de l'ellipse est obstruée, la perte de signal est évaluée à 75 %, ce qui revient à diviser la portée par 2.

Sur des distances longues, la courbure de la terre peut même avoir une incidence.

Quand, grâce à la réflexion et à la diffraction, un signal est reçu malgré les obstacles, on parle de portée Non Line of Sight (NLoS).



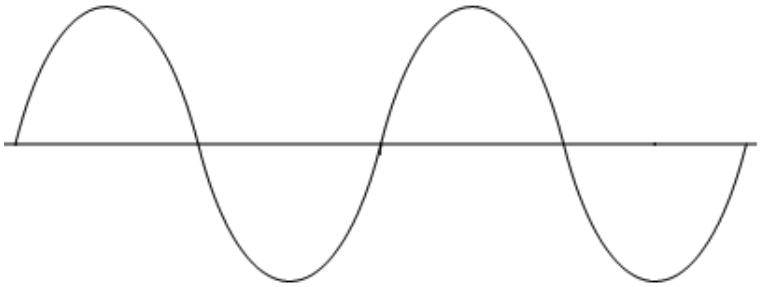
Transmission LoS et zone de Fresnel

Ainsi, le choix et le positionnement des antennes peuvent s'avérer cruciaux pour le bon fonctionnement d'un réseau Wi-Fi. Nous en reparlerons plus loin dans ce même chapitre.

2. Fréquence et modulation

a. Les différentes modulations

La transmission hertzienne véhicule l'information par une onde appelée porteuse.

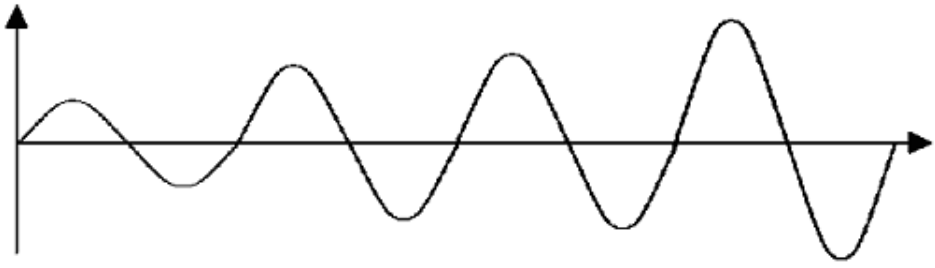


La porteuse

Ce signal propage une information de forme analogique, contenant de multiples valeurs, ou numérique, constituée de seulement deux niveaux : 0 et 1.

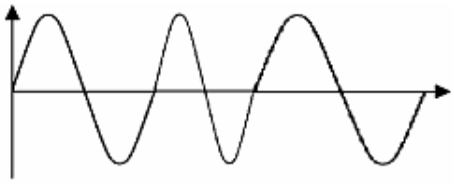
Dans un cas comme dans l'autre, c'est par une modulation de la porteuse que le signal deviendra significatif.

La plus simple modulation, et la première utilisée, consiste à faire varier l'amplitude (AM - *Amplitude Modulation*). On l'utilise pour les communications longues distances, à basses fréquences et puissances élevées, comme en téléphonie.



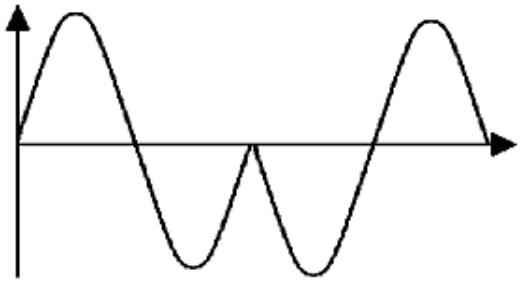
Modulation d'amplitude

La modulation de fréquence (FM - *Frequency Modulation*) présente une très bonne résistance aux interférences. Elle nécessite également moins de puissance que la première. On l'utilise pour les transmissions de télévision et de radio stéréo.



Modulation de fréquence

La modulation de phase (PM - *Phase Modulation*) ne présente basiquement que deux niveaux : la phase elle-même, dont le degré est 0, et son opposition décalée dans le temps, à 180°. Elle est particulièrement indiquée dans les transmissions numériques.



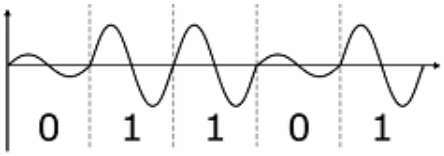
Modulation de phase

b. Les modulations numériques

Modulations à 2 niveaux

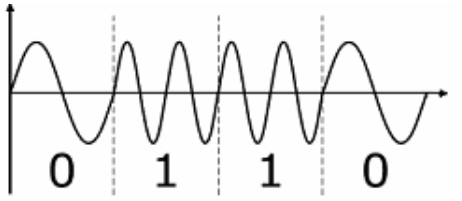
La transmission d'informations numériques nécessite un codage, ou keying, sur 2 niveaux seulement. Le signal de synchronisation reste la porteuse, avec ses caractéristiques initiales de fréquence, d'amplitude et de phase.

Par exemple, en codage par modulation d'amplitude (ASK - *Amplitude Shift Keying*), le signal indiquant le "0" a pour amplitude la moitié de celui du "1".



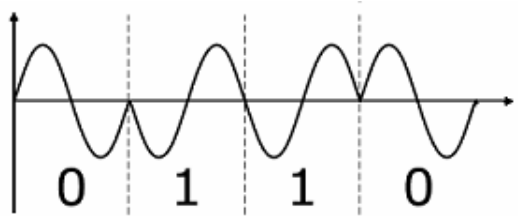
Codage ASK

En modulation de fréquence numérique (FSK - *Frequency Shift Keying*), la fréquence indiquant le "0" peut être la moitié de celle du "1".

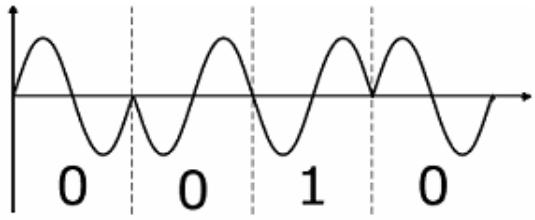


Codage FSK

Pour coder en modulation de phase (PSK - *Phase Shift Keying*), deux solutions sont utilisées. Dans la première, un même état du signal indique toujours la même valeur. Dans la seconde, la convention peut indiquer qu'un changement de phase marque une valeur "0", et qu'une absence de changement est un "1". Cette méthode de codage différentiel (Differential PSK) est utilisée par la technologie Wi-Fi.



Codage PSK, avec phase correspondant à la valeur binaire



Codage Differential PSK, avec changement de phase pour le 0

Notion de valence et de baud

Dans les exemples ci-dessus, les modulations ne transmettent qu'un seul bit à chaque période, soit deux états possibles. Elles sont qualifiées de bivalentes. La notion de valence précise le nombre d'états que peut avoir un signal. L'unité baud mesure ce nombre d'états par seconde.

Par exemple, si la fréquence de la porteuse est de 1 Hz, soit une période d'une seconde, les modulations présentées précédemment transmettent à 1 bit par seconde (1 bps), correspondant à 1 baud (1 état par seconde).

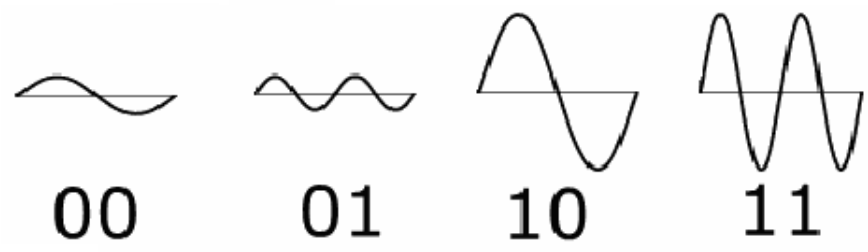
Pour permettre des débits plus rapides à une fréquence donnée, il est nécessaire d'augmenter la valence. Ainsi, si un codage permet de transmettre 2 bits à chaque période, 22 états, soit quatre (quadrivalence) sont possibles. Une modulation regroupant plusieurs bits est appelée un symbole.

Si un symbole regroupe 2 bits et que la porteuse a une fréquence de 1 Hz, le débit binaire est de 2 bps et la rapidité de modulation 4 bauds. Un baud n'est donc pas forcément égal à 1 bps.

c. Les combinaisons de modulations

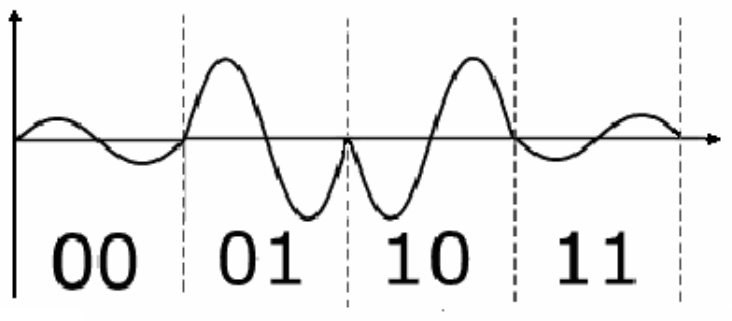
Combinaisons simples

Pour augmenter le nombre de bits transmis à chaque période de la porteuse, des combinaisons de modulations peuvent être utilisées. Par exemple, en exploitant à la fois de la modulation de fréquence et d'amplitude, 4 niveaux au moins peuvent être définis. On peut concevoir que les combinaisons sont très nombreuses.



Codage en quadrivalence, utilisant modulation de fréquence et d'amplitude

Si l'on fige la fréquence, une combinaison de modulations d'amplitude et de phase peut être réalisée. Là encore, de multiples solutions sont possibles.



Combinaison de phase et d'amplitude pour quadrivalence

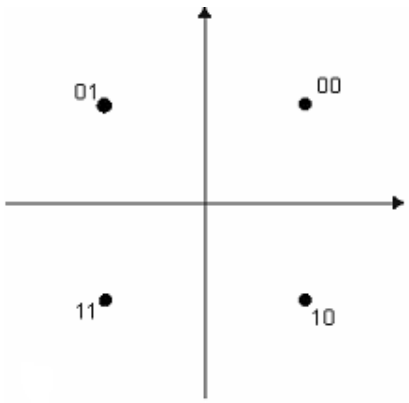
Combinaisons avec quadrature

Une autre technique, pour gagner en vitesse de transmission, consiste à utiliser plusieurs porteuses de même fréquence, mais déphasée de 90° (quadrature). Additionnées, elles donneront une unique porteuse à 4 états. En effet, l'électronique est capable de reconstituer les deux sous-porteuses initiales à partir de la résultante. Cette méthode de modulation appelée Quadrature Phase Shift Keying (QPSK) est peu sensible aux interférences et permet de reconstituer l'information, même si le bruit est important.

Exemple de quadrature de phase :

Valeur binaire transmise	Phase de la 1ère sous-porteuse	Phase de la 2e sous-porteuse
00	0°	0°
01	180°	0°
10	0°	180°
11	180°	180°

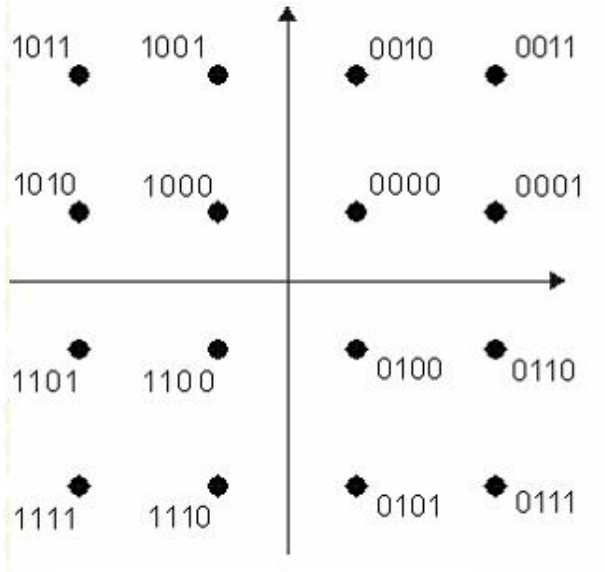
Un graphique en 2 dimensions, dont chaque axe représente une sous-porteuse, permet de visualiser ces valeurs. Dans celui d'après, la partie positive de l'axe représente un déphasage nul, quand celle négative est de 180.



Quadrature à 4 états

Le nombre de bits codés par symbole peut être augmenté par combinaison de sous-porteuses et de modulation d'amplitude. Cette technique est appelée Quadrature Amplitude Modulation (QAM).

Par exemple, si chacune des 2 sous-porteuses est combinée à 2 modulations d'amplitude, le symbole comprend 4 bits, soit 2^4 = 16 états (QAM 16 ou 16 QAM). Dans le graphique ci-dessous, comme précédemment, chaque axe représente une sous-porteuse.



Quadrature à 16 états

Une telle technique de modulation combinée est utilisée par la technologie Wi-Fi, dans les débits élevés. Afin d'augmenter encore celui-ci, des codages avec 5 bits par symbole (QAM 32 ou 32 QAM), 6 bits par symbole (QAM 64 ou 64 QAM), voire 7 bits par symbole (QAM 128 ou 128 QAM) sont possibles.

3. Puissance et gain

a. La puissance

La puissance électrique, P, est mesurée en Watt (W). Elle résulte du produit de l'intensité du courant, I, par sa tension, U : P=UI.

Une loi physique de la radio précise que plus la puissance d'émission de l'onde est élevée, plus sa portée est importante. Par contre, il est nécessaire d'augmenter l'intensité du courant, ce qui réduit la durée de vie de batterie d'un appareil mobile.

Pour doubler la portée d'un signal, la puissance de l'émetteur doit être quadruplée.

En Wi-Fi, les puissances émises seront mesurées en milliwatt (mW) : 1000 mW = 1 W.

b. Le gain

Le gain mesure la capacité d'un équipement à concentrer les ondes, en comparant deux tensions, donc deux puissances, à une échelle logarithmique. Son unité est le décibel (dB) et il est noté G.

Le rapport entre le gain et la puissance est donnée par : G = 10 Log P. Dans cette formule, P est égale à P_{Sortie}/ $P_{Entrée}$.

Si la puissance est exprimée en mW, le gain est mesuré en décibel par milliwatt (dBm). Un résultat positif indique une amplification du signal, qui nécessite donc une source d'énergie pour augmenter la puissance. Les sources de pertes, ou atténuations, sont, comme nous l'avons vu précédemment, multiples.

Par exemple, quelques rapports entre la puissance et le gain sont :

- Si P=1 mW, G=0 dBm ;
- Si P=10 mW, G=10 dBm ;
- Si P=100 mW, G=20 dBm.

Quadrupler une puissance en mW, pour doubler la portée du signal, c'est donc ajouter un gain d'environ 6 dBm à l'émetteur, composé d'un équipement électronique et d'une antenne.

Dans les fréquences des RLAN, le gain d'une antenne est exprimé dans un rapport isotrope. Une antenne idéale, qualifiée d'isotrope, est représentée par un point, rayonnant de manière équivalente dans toutes les directions, comme une étoile. Son gain serait de 1. Un tel composant n'existe pas dans la réalité.

Cette mesure, associable uniquement à une antenne, est notée décibel isotrope (dBi).

La conversion entre dB et dBi s'effectue par un ajout de 2,14. Par exemple :

- Si G=0 dB, le gain isotrope G' est égal à 2,14 dBi ;
- Si G=10 dB, le gain isotrope G' est égal à 12,14 dBi.

c. La puissance isotrope rayonnée équivalente (PIRE)

Le gain d'une station d'émission radio est donc l'addition de la puissance de l'émetteur avec le gain de l'antenne. Si un câble relie l'un à l'autre, une perte est engendrée. Le résultat de cette formule donne la puissance isotrope rayonnée equivalente (PIRE), en anglais Equivalent Isotropic Radiated Power (EIRP).

Cette mesure de la puissance de rayonnement moyenne est exprimée normalement en décibel/ par Watt (dBm), le plus souvent en décibel (dB). C'est elle qui est utilisée dans le cadre de la réglementation.

Pour simplifier le calcul, les unités sont transformées. Ainsi, en Wi-Fi le calcul peut être le suivant :

- PIRE = Gain du transmetteur (en mW, reporté en dBm) + Gain de l'antenne d'émission (en dBi, converti en dBm) - Perte dans le câble (en dBm).

Par exemple, un émetteur de puissance 100 mW, soit 20 dBm, est relié directement à une antenne de gain 2,14 dBi, soit 0 dB. Le PIRE de la station est de 20 dBm. La puissance totale de l'équipement reste de 100 mW.

Si l'on souhaite doubler la portée, en changeant l'antenne par une autre de gain 6 dBi, soit 3,86 dB, le PIRE devient : 23,86 dBm. La station délivre donc une puissance d'environ 350 mW.

Ce PIRE peut être réglé au niveau de l'émetteur comme du récepteur. Dans ce dernier cas, on parlera de sensibilité de l'appareil plutôt que de puissance.

Même si la qualité de transmission dépend à la fois de la puissance et du gain, il est préférable d'améliorer ce dernier. Non seulement le signal sera plus lisible, mais, de plus, l'intensité consommée sera réduite.

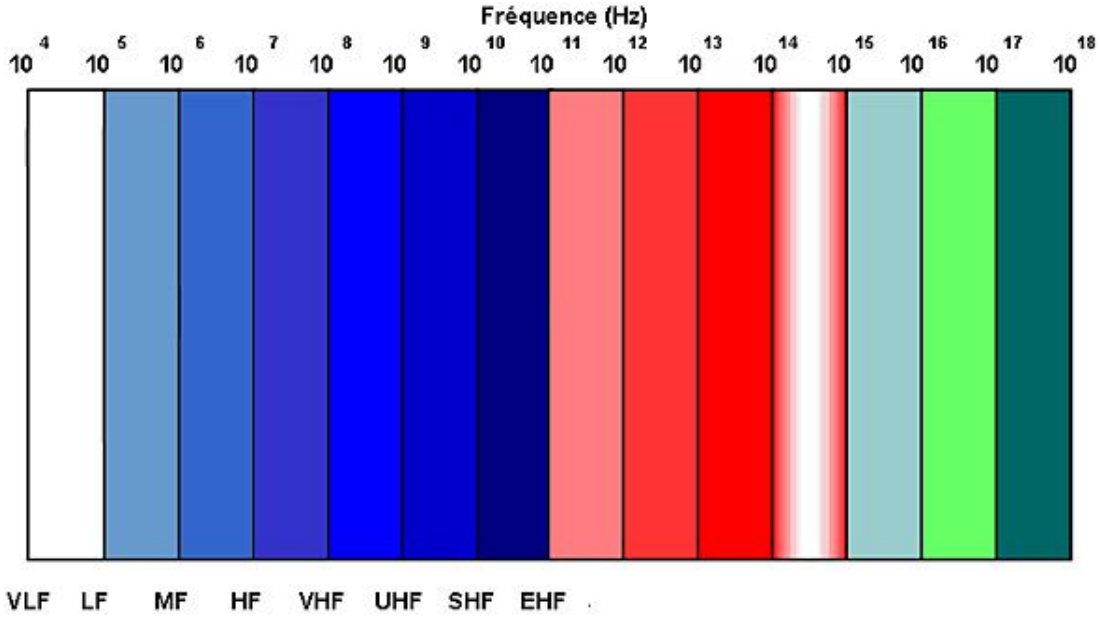
Réglementation

Les ondes électromagnétiques sont présentes partout autour de nous. Leurs propriétés sont tellement nombreuses que les usages qui en sont fait sont multiples. Dans cette grande famille, les ondes radio ne peuvent être exploitées librement.

1. Bandes de fréquences

a. Le spectre électromagnétique

Les ondes électromagnétiques possèdent des caractéristiques très différentes en fonction de leur fréquence. Le spectre électromagnétique répertorie ces différents types de rayonnement, en bandes de fréquences bornées.



Le spectre électromagnétique

Les différents phénomènes ondulatoires sont qualifiés par la longueur d'onde, rapportée à la fréquence. Ces ondes sont :

- Kilométriques, bandes Very Low Frequencies (VLF), de 9 KHz à 30 KHz et Low Frequencies (LF), de 30 KHz à 300 KHz ;
- Hectométriques, bande Medium Frequencies (MF), de 300 KHz à 3 MHz ;
- Décamétriques, bande High Frequencies (HF), de 3 MHz à 30 MHz ;
- Métriques, bande Very High Frequencies (VHF), de 30 MHz à 300 MHz ;
- Décimétriques, bande Ultra High Frequencies (UHF), de 300 MHz à 3 GHz ;
- Centimétriques, bande Supra High Frequencies (SHF), de 3 GHz à 30 GHz ;
- Millimétriques, bande Extremely High Frequencies (EFH), de 30 GHz à 300 GHz.

Les fréquences les plus basses sont celles des ondes radio, produites par les antennes. De fréquences plus élevées, les micro-ondes, aux environs de 2.4 GHz, ont pour propriété, à très forte puissance, de faire vibrer, donc chauffer, les molécules d'eau.

Dans les fréquences dites submillimétriques, au-delà de 300 GHz, se retrouvent, par ordre croissant :

- les infrarouges, émis par les objets chauds ;
- la lumière visible, mesurée en nanomètres ;
- les ultra-violets, incluant la lumière noire ;
- les rayons X, utilisés en radiographie ;
- les rayons gamma, produits par la réaction nucléaire.

Le phénomène électromagnétique regroupe donc de nombreux types d'ondes, très différentes les unes des autres. Plus la fréquence augmente, plus leur énergie est importante.

b. L'utilisation des fréquences radio en France

Dans le cadre de la transmission d'informations, seule la famille des ondes radio nous intéresse. Son spectre est très large, avec des utilisations très diverses.

Les émissions de radiodiffusion se retrouvent d'abord dans la bande LF avec les grandes ondes (GO), entre 150 et 280 KHz et MF, avec les petites ondes (PO), entre 525 et 1605 KHz. La radio qualifiée de FM utilise les fréquences comprises entre 87.5 et 108 MHz. Différentes bandes sont également exploitées par la télévision.

Les radio amateurs exploitent particulièrement des fréquences MF et HF, sur lesquels des canaux leur sont réservés.

Les institutions possèdent leurs bandes de fréquences réservées, en VHF, voire en UHF, parmi lesquelles la direction départementale de l'équipement (DDE), la gendarmerie nationale, la police, EDF, les pompiers... Les fréquences militaires sont très réparties, en VHF particulièrement.

La téléphonie mobile exploite les bandes :

- 890 à 915 MHz et 935 à 960 MHz (GSM) ;
- 1.71 à 1.785 GHz et 1.805 à 1.88 GHz (GSM1800) ;
- 1.92 à 1.98 GHz et 2.11 à 2.17 GHz (UMTS).

Les téléphones sans fil DECT exploitent la bande 1.88 GHz à 1.9 GHz.

Des bandes ont également été réservées pour le transfert de données par ondes radio. Les fréquences dédiées aux RLAN vont de 2.4 GHz à 2.4835 GHz. La boucle locale radio utilise celles allant de 3.465 à 3.495 GHZ, de 3.565 à 3.595 GHz, puis de 25.557 à 26.005 GHz.

c. Les fréquences privées et publiques

Au niveau international, les fréquences radio sont possession des états. Mais comme ces ondes ne connaissent pas les frontières, la plupart des bandes et leurs usages sont définis à l'échelle d'un continent, comme en Europe, ou mondiale.

Parmi les organismes de régulation des bandes de fréquences, on retrouve la conférence européenne des administrations des postes et télécommunications (CEPT) et la Federal Communications Commission (FCC) aux USA.

Site Web du CEPT : http://www.cept.org

Au sein du spectre, l'usage des bandes privées est soumis à licence. Il peut être nécessaire d'acheter les droits d'émettre avant l'exploitation d'une telle fréquence. Un exemple récent fut l'achat des licences UMTS par les

différents opérateurs de téléphonie mobile.

L'exploitation de bandes de fréquence publique est libre. Il suffit de se conformer à la réglementation en vigueur dans le pays d'usage. Parmi toutes les fréquences citées précédemment, seules celles des RLAN, donc du Wi-Fi, sont ainsi qualifiées.

2. Organismes de réglementation

a. L'agence nationale des fréquences et autres organismes liés

En France, l'agence nationale des fréquences (ANFR), est une entité indépendante créée en 1996. Elle est chargée de la bonne gestion du spectre et du bon emploi des fréquences. Elle représente également la France au niveau international sur ces sujets.

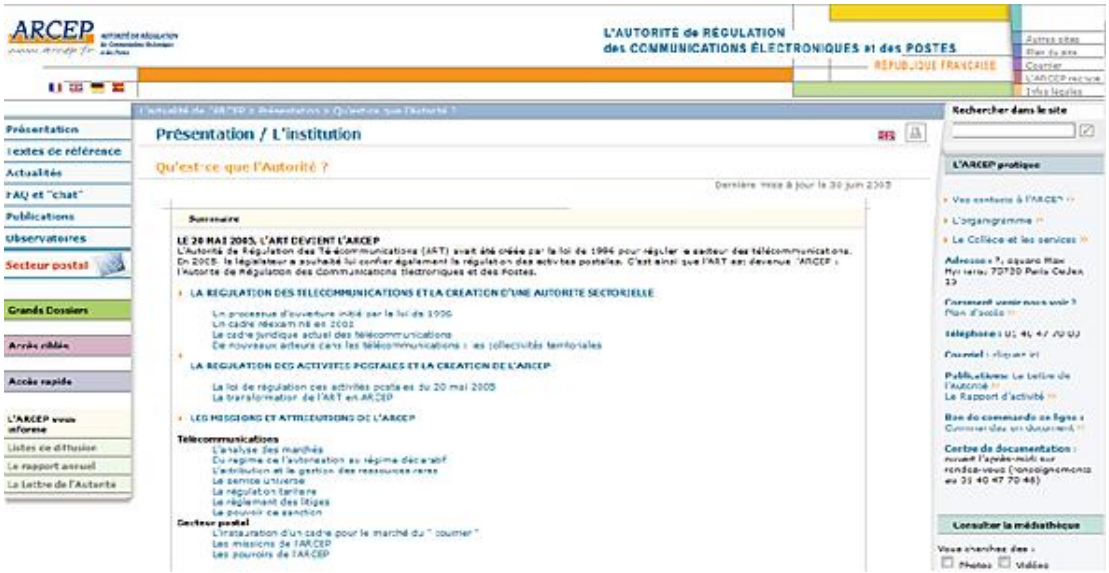
Site Web de l'ANFR : http://www.anfr.fr

Neuf organismes délégués sont autorisés à affecter des licences, parmi lesquels :

- le ministère de l'intérieur pour la police, les pompiers... ;
- le ministère de la défense ;
- l'autorité de régulation des communications électroniques et des postes (ARCEP) ;
- le conseil supérieur de l'audiovisuel (CSA)...

b. L'autorité de régulation des communications électroniques et des postes

Cette nouvelle appellation, étrennée en mai 2005, vient remplacer celle d'autorité de régulation des télécommunications (ART). Elle marque également une évolution des missions de cet organisme.



Site Web de l'ARCEP : http://www.arcep.fr

Une tâche importante de l'ARCEP est la gestion des fréquences de télécommunications, privées comme publiques. Il veille au respect de la concurrence sur ce marché et présente également un certain nombre de réglementations, comme celles qui nous intéressent au niveau des RLAN.

3. Bandes radio RLAN

a. Les bandes ISM et UNII

Comme nous l'avons vu précédemment, la dominance commerciale des USA guide parfois les usages. C'est le cas pour la définition des bandes publiques.

Ainsi, l'utilisation des bandes 900 MHz (de 902 à 928 MHz) et 2.4 GHz (2.4 à 2.4835 GHz) est autorisée en 1985, par la FCC, pour les communautés industrielles, scientifiques et médicales. Devenues publiques ces bandes de fréquence porteront le nom Industrial Scientific and Medical (ISM).

Elle viennent ainsi compléter celle, Unlicensed National Information Infrastructure (UNII), déjà libérées en 5 GHz :

- UNII 1 entre 5.15 et 5.25 GHz, pour WLAN en intérieur ;
- UNII 2 entre 5.25 et 5.35 GHz, pour liaisons extérieures de courte portée ;
- UNII 3, entre 5.625 et 5.825 Ghz, pour liaisons intérieures de longue portée.

Le portage en Europe de ces fréquences publiques pose quelques problèmes.

En effet, le CEPT avait déjà réservé, pour l'HiperLAN de son entité fille ETSI, les fréquences 5.15 à 5.30 GHz, entre autres. Il en résulte que les bandes UNII 1 et 2, très larges et utilisées par le Wi-Fi aux USA ne sont pas réellement exploitables en Europe. De plus, en fonction des pays, des fréquences proches sont utilisées par des radars, balises d'approches aéronautiques, radionavigation maritime...

La bande des 900 Mhz, très utilisée par le matériel médical, est également très proche, voire confondue, avec celle allouée pour le GSM. Les perturbations générées par ce conflit impliquent d'ailleurs l'extinction des téléphones mobiles dans les locaux médicaux.

Il ne reste donc plus qu'à utiliser la bande des 2.4 GHz, pour les RLAN, ce qui a été décidé au niveau mondial, avec une ratification en Europe. Pourtant, ceci ne sera pas aussi simple en France, où certaines fréquences étaient déjà exploitées par les militaires.

En résumé, les réseaux locaux hertziens, et plus particulièrement le Wi-Fi, exploiteront désormais cette bande de 83.5 MHz de large, gérée par l'ARCEP.

b. La libération des bandes de fréquences

Avant novembre 2002, l'utilisation de RLAN était réservée à un usage privé, et très réglementé. En 2002, l'ART autorise l'usage de point d'accès publics Wi-Fi, les Hot-Spots, sans demande d'autorisation :

- sur la bande des 2.4 GHz ;
- dans certaines conditions de puissance et de fréquence ;
- avec une certaine libéralisation sur 38 départements.

À partir de février 2003, les négociations avec les autorités militaires autorisent un complément de 20 nouveaux départements.

Le 25 juillet 2003, un nouveau cadre réglementaire complet est fixé par l'ART, en France métropolitaine. Il deviendra celui du développement initial du Wi-Fi.

Les grandes dates récentes du dossier Wi-Fi pour l'ARCEP sont surtout l'ouverture de la bande 5.47 à 5.725 GHz en décembre 2005, puis la levée du caractère expérimental des réseaux RLAN ouverts au public, en avril 2007.

c. Le cadre réglementaire actuel

Cette réglementation stipule que, même si l'exploitation de la fréquence est libre, l'usage par un opérateur doit en être déclaré. Un formulaire est d'ailleurs disponible pour cela sur le site de l'ARCEP.

Les puissances des équipements sont également soumises à réglementation.

France métropolitaine

Fréquence	**PIRE max à l'intérieur**	**PIRE max en extérieur**
De 2.4 à 2.454 GHz	100 mW	100 mW
De 2.454 à 2.4835 GHz.	100 mW	10 mW

Guadeloupe, Martinique, Saint Pierre et Miquelon, Mayotte

Fréquence	**PIRE max à l'intérieur**	**PIRE max en extérieur**
De 2.4 à 2.454 GHz	100 mW	100 mW
De 2.454 à 2.4835 GHz.	100 mW	100 mW

Même si cette bande de 2.4 Ghz est celle de prédilection du Wi-Fi, l'ARCEP fournit un cadre réglementaire à son exploitation sur celle des 5 GHz, sur l'ensemble du territoire français.

Fréquence	**PIRE max à l'intérieur**	**PIRE max en extérieur**
De 5.15 à 5.25 GHz	200 mW	Impossible
De 5.25 à 5.35 GHz	200 mW ou 100 mW (fonction de la puissance de l'émetteur)	Impossible
De 5.47 à 5.725 GHz.	500 mW ou 1 W (fonction de la puissance de l'émetteur)	500 mW ou 1 W (fonction de la puissance de l'émetteur)

Ainsi, même si la largeur de bande, plus importante en 5 MHz, aurait permis de s'affranchir d'un grand nombre de contraintes de perturbation, elle n'est pas vraiment utilisée par le Wi-Fi en France, contrairement aux USA.

Les PIRE réglementaires limitent bien l'usage de ces différentes fréquences du RLAN, puisque les portées utiles n'excéderont pas quelques centaines de mètres, plus souvent bien inférieures. Il est nécessaire de veiller à ne pas dépasser ce cadre, ce qui peut se faire très rapidement. En effet, les équipements sont souvent commercialisés en France avec des antennes de faible gain. L'ajout d'une antenne plus importante peut imposer la diminution de la puissance de l'émetteur/récepteur.

Antennes

La technologie Wi-Fi allie à la fois des caractéristiques radio et informatiques. Très souvent, lors de la mise en œuvre d'un tel réseau, seules ces dernières font l'objet d'attention, par exemple pour sécuriser la communication.

Malheureusement, la qualité de la transmission et la zone de couverture de la cellule peuvent être négligées. Il s'agit pourtant des premiers réglages à effectuer, avec entre autres, l'utilisation d'une antenne adaptée à l'usage ou à l'environnement.

1. Théorie des antennes

a. Les caractéristiques principales

En radio, une antenne émettrice est un conducteur métallique dans lequel passe un courant d'une fréquence donnée. L'excitation des électrons va ainsi former un champ électromagnétique, qui se propage ensuite : l'onde porteuse.

Le gain d'une antenne passive, telle qu'utilisée en Wi-Fi, est l'amplification appliquée au signal lors de la conversion du courant électrique, exprimé en décibel isotrope (dBi).

L'antenne de réception présente, heureusement, les mêmes qualités. Lorsqu'elle reçoit l'onde radio, elle la concentre et les électrons métalliques sont mis en mouvement au même rythme (fréquence) que lors de l'émission. Le gain est ici exploité pour améliorer la sensibilité de réception.

Cette valeur exprimée en décibel (dB), est la mesure du rapport signal/bruit en réception. Plus la sensibilité de l'antenne est importante, plus elle peut reconnaître le signal (information significative) dans le bruit (information non significative). Ce dernier est mesuré aux alentours de -100 dB. Le débit de réception d'un équipement Wi-Fi est directement dépendant de ce rapport signal/bruit. Nous y reviendrons un peu plus loin.

Les transmissions numériques sont moins exigeantes que leurs équivalents analogiques. En effet, il ne s'agit plus de distinguer précisément de multiples niveaux, mais d'en reconnaître seulement deux. Cette acceptation d'une certaine imprécision a permis de diminuer très fortement la taille des antennes numériques.

Il est rappelé que la puissance de transmission en sortie de l'antenne, le PIRE, doit respecter le cadre réglementaire. Par exemple :

- un gain de 2,14 dBi (0 dBm) correspond à une puissance en sortie de 1 mW ;
- un gain de 12,14 dBi (10 dBm) correspond à une puissance en sortie de 10 mW ;
- un gain 22,14 dBi (20 dBm) correspond à une puissance en sortie de 100 mW.

On conçoit donc que la puissance délivrée à l'antenne, par l'équipement actif auquel elle est reliée, doit être diminuée si le gain augmente.

b. La polarisation

La forme et le positionnement physique des éléments de l'antenne orientent le champ électrique de l'onde. Cette polarisation est une combinaison de directions horizontales, c'est-à-dire parallèles à la surface de la terre et verticales, soit perpendiculaires. L'antenne isotrope, ce fameux modèle théorique de référence, possède une polarisation de 360°, horizontalement comme verticalement.

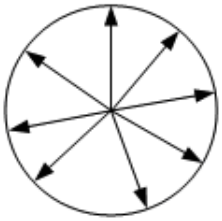
La réduction de l'angle du faisceau de l'antenne augmente le gain et donc la portée du signal. En contrepartie, une zone d'ombre est créée, sous ce faisceau, dans lequel l'émission/réception est très incorrecte.

En Wi-Fi, deux types de polarisation sont utilisés : omnidirectionnelle ou directionnelle.

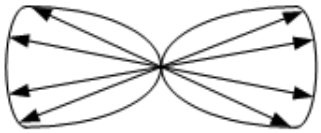
Antennes omnidirectionnelles

Les antennes omnidirectionnelles sont les plus courantes. Leur faisceau horizontal est de 360°. Celui vertical est relativement large, se rapprochant de 90°. La zone d'ombre est relativement réduite, sous l'antenne.

Les représentations suivantes sont théoriques.



Omnidirectionnel : Polarisation horizontale



Omnidirectionnel : Polarisation verticale

Antennes directionnelles

Une antenne de polarisation directionnelle a une portée plus étendue, car l'angle du faisceau est plus réduit. Mais elle n'est plus le point central de l'émission. Sa largeur verticale peut être sensiblement équivalente à celle horizontale, comme sur les exemples ci-dessous.

Directionnel : angle ouvert (vertical et horizontal)

Directionnel : angle plus fermé (vertical et horizontal)

Directionnel : angle très fermé (vertical et horizontal)

Pour une communication optimale, les antennes émettrices et réceptrices doivent être polarisées selon le même axe. Pour des antennes directionnelles, ce réglage implique de bien les mettre en face l'une de l'autre. Pour leur équivalent omnidirectionnel, les axes doivent être conservés lors du positionnement. La perte engendrée est appelée Polarization Loss Factor (PLF). À partir de 20, elle peut être conséquente.

c. Le diagramme de rayonnement

Le diagramme de rayonnement, ou pattern, d'une antenne est la polarisation de celle-ci, à partir d'une mesure et non d'un schéma théorique comme précédemment. Il représente non seulement l'angle d'ouverture, mais également les lobes principaux et secondaires des antennes.

Ces derniers marquent les débordements de l'onde radio hors de la polarisation théorique. Il est nécessaire d'en tenir compte pour connaître exactement la portée des informations transmises.

Le rayonnement vertical réel d'une antenne omnidirectionnelle forme un 8, le long de son axe. On peut imaginer avoir pressé le lobe sphérique du modèle isotrope au-dessus et au-dessous de cet axe.

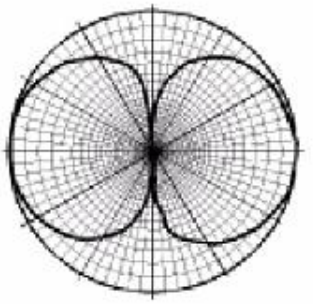


Diagramme de rayonnement vertical d'une antenne omnidirectionnelle

En Wi-Fi, plusieurs types d'antennes directionnelles sont utilisés. En fonction de leur technologie, leur portée sera plus ou moins importante. On peut remarquer sur tous les diagrammes les débordements : soit le lobe principal est peu régulier, soit de nombreux lobes secondaires apparaissent.

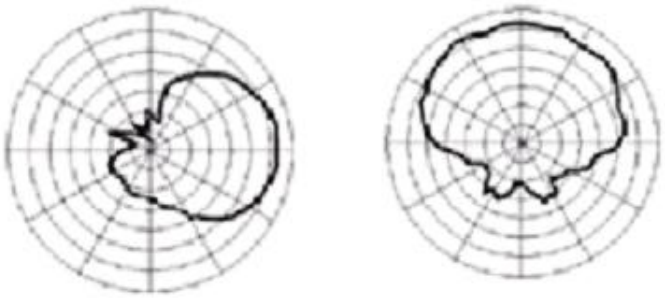


Diagramme de rayonnement vertical (gauche) et horizontal (droite) d'une antenne Patch<

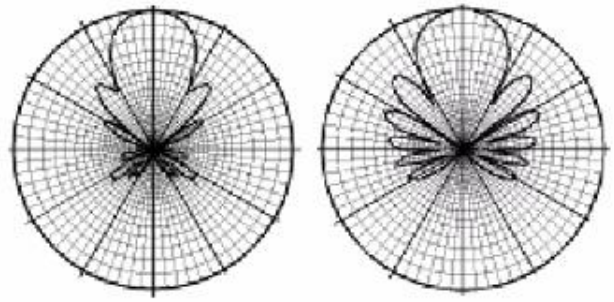


Diagramme de rayonnement vertical (gauche) et horizontal (droite) d'une antenne Yagi

Les antennes directionnelles de plus grande portée sont des paraboles, dont les polarisations horizontales et verticales sont identiques. On peut remarquer la fermeture de l'angle du lobe principal.

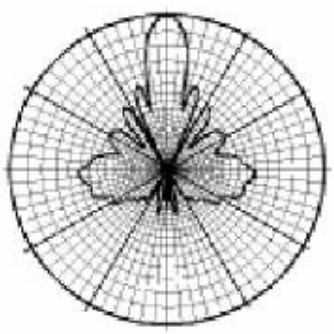


Diagramme de rayonnement d'une antenne parabolique

2. Modèles d'antennes Wi-Fi

Pour respecter la réglementation sur la puissance rayonnée, les antennes Wi-Fi sont passives. Elles ne contiennent pas elles-mêmes un amplificateur, comme une antenne active. En France, on trouvera relativement peu de modèles de bande passante 5 GHz.

Les catalogues de sociétés fabricantes d'antennes, comme Radiolabs (www.radiolabs.com) ou Cushcraft (www.cushcraft.com) permettent de mieux appréhender le choix de l'antenne et les différents modèles existant.

Les informations techniques données par le fournisseur renseignent précisément sur les gains et les largeurs de faisceau. Par contre, il est nécessaire de toujours relativiser la portée donnée, qui est idéale, et souvent très loin de la réalité, particulièrement en intérieur.

Il est fortement recommandé d'utiliser une même technologie, avec une polarisation correspondante, pour les antennes de l'émetteur et du récepteur. Si un équipement permet le montage de deux antennes, le même modèle doit être utilisé sur chaque embase.

a. Les antennes omnidirectionnelles

L'antenne fouet, très courante en intérieure, est constituée d'un brin métallique, polarisé selon son axe. Sa taille est généralement un sous multiple simple de la longueur d'onde, par exemple la moitié ou le quart, soit environ 6.3 ou 3.15 cm pour les modèles 2.4 Ghz.

Sur un équipement d'infrastructure, elle se positionne plutôt au centre d'une pièce, en hauteur. Beaucoup de ces matériels permettent de connecter deux antennes, en diversité (dipôle). Certaines, dites de plafond, incluent ces dipôles dans des éléments plus esthétiques et moins voyants.

À l'extérieur, la tige utilisée, colinéaire, est beaucoup plus longue : sa portée est directement dépendante de cette taille.

Le gain obtenu n'est généralement pas très important. Il est de 2,2 dBi à environ 6 dBi sur les modèles les plus courants.

Modèle fouet à visser sur l'équipement, souvent doublé

Modèle à poser sur un bureau

Modèle fouet en diversité (dipôle)

Modèle fouet de plafond

Dôme de plafond omnidirectionnel

Modèle colinéaire pour extérieur

b. L'antenne Patch

Cette antenne est formée par une plaque de métal, généralement rectangulaire, mais qui peut prendre d'autres formes. Elle contient des éléments rayonnants, placés par paires, en diversité. Assez plats, ces modèles s'utilisent généralement à l'intérieur, où il peuvent être quelque peu camouflés.

Leur gain est supérieur aux antennes précédentes, allant couramment de 5 à 9 dBi. L'angle de faisceau large, en polarisation axiale, les destine particulièrement à une pièce ou un couloir.

Antenne Patch pour mur intérieur

c. L'antenne Yagi

En forme de râteau, cette antenne est fabriquée avec une tige métallique à laquelle sont accrochées perpendiculairement d'autres tiges. Le tout est enchâssé dans un tube plastique. Sa polarisation est également axiale.

Antenne Yagi à nue

Antenne Yagi complète, avec attache de mât

Son gain, relativement important, dépend de la longueur de la tige principale. Mesuré le plus souvent entre 10 et 15 dBi, il destine son usage plutôt à l'extérieur, pour couvrir des distances plus importantes entre deux bâtiments.

d. L'antenne parabolique

Le dernier modèle courant d'antennes Wi-Fi est la parabole. Elle n'est utilisée qu'en extérieur. Son faisceau présente un angle faible, mais sa portée est très conséquente. Des gains supérieurs à 20 dBi sont courants pour ce type d'antenne, le PIRE est donc à surveiller de très près.

Antenne parabolique pleine

Antenne parabolique grillagée (meilleure prise au vent)

3. Câbles et connectique

Dans un certain nombre de cas, l'antenne ne peut être reliée directement au reste du matériel, carte réseau ou équipement d'infrastructure. L'insertion d'un câble coaxial permet cette déportation, moyennant une perte de gain dépendante de la qualité et de la longueur de celui-ci.

Il est recommandé d'utiliser des câbles dédiés au Wi-Fi, dont l'impédance est adéquate. Les qualités varient fortement, entraînant des pertes d'environ 0,1 à 1 dB par mètre.

En fonction des constructeurs de matériels, les connectiques sont différentes. Les principaux modèles sont présentés ci-dessous. Une perte de 0,5 à 1 dB par connecteur est normale.

MMCX

RP-SMA

RP-TNC

Si l'antenne est positionnée à l'extérieur, elle doit être isolée par un élément parafoudre, ou lighting arrestor, relié à la terre.

Groupe et standard 802.11

Les liaisons sans fil RLAN ont trouvé, pour leurs déclinaisons commerciales, des standards adéquats avec les travaux des groupes IEEE 802.11. Évoluant encore fortement, ils répondent au besoin de solutions non propriétaires, gages d'une certaine pérennité, et surtout de compatibilité entre marques de matériels.

1. Présentation

C'est en 1997 que le groupe de travail 802.11 standardise, après plusieurs années de travaux, sa définition des réseaux de type Wireless LAN, qui est retouchée en 1999 puis en 2003. Les différents travaux, décrits dans des documents séparés, sont finalement centralisés dans un document global, en 2007.

Comme d'autres normes IEEE 802, ces spécifications couvrent les couches Physique et Liaison de données du modèle OSI. Cette dernière est divisée en deux sous-couches : Medium Access Control (MAC), pour l'accès au support de transmission et Logical Link Control (LLC), pour le contrôle de la transmission. Les spécifications 802.1 regroupent la gestion des réseaux locaux, l'authentification et les VLAN.

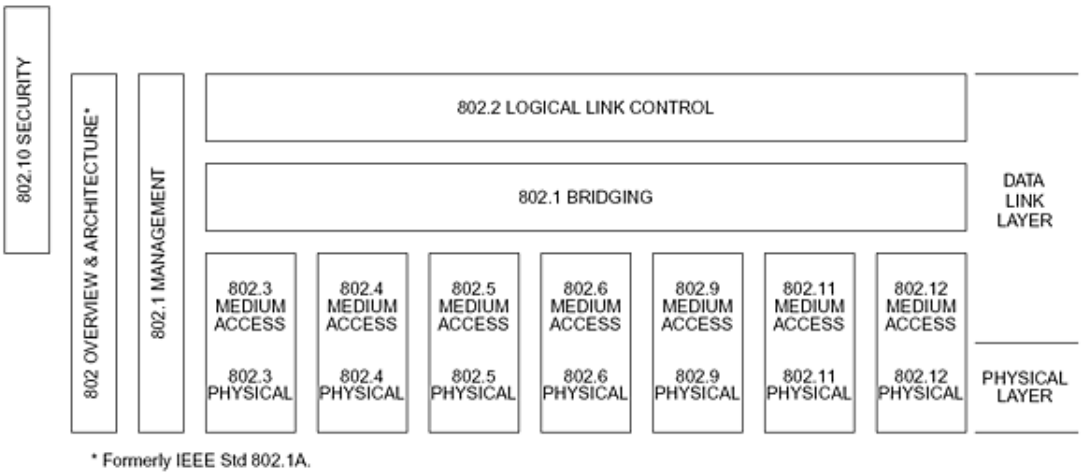
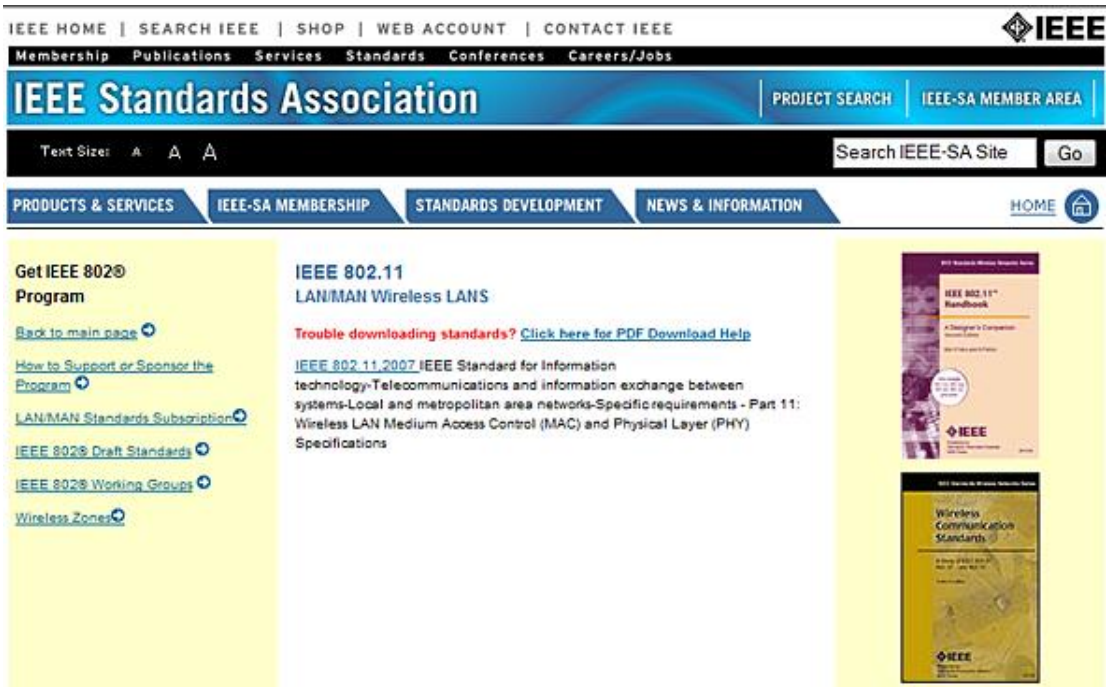


Schéma structurel des travaux des groupes 802.x (source : IEEE)

Les architectures des réseaux WLAN sont basées sur celles des réseaux de radiocommunication : les transferts d'informations s'effectuent à l'intérieur d'une cellule. Plusieurs types de communications entre stations fixes ou mobiles sont définis, en direct ou via relais.



2. Norme 802.11

a. Les généralités

En couche physique, trois modes de transmission sont définis dans ces spécifications. Le premier utilisant la diffusion infra-rouge, de 850 à 950 nm, ne nous intéresse pas dans le cadre de cet ouvrage. Les deux autres exploitent les ondes radio, sur la bande des 2.4 GHz, par les techniques Frequency Hopping Spread Spectrum (FHSS) ou Direct Sequence Spread Spectrum (DSSS), que nous détaillerons plus loin.

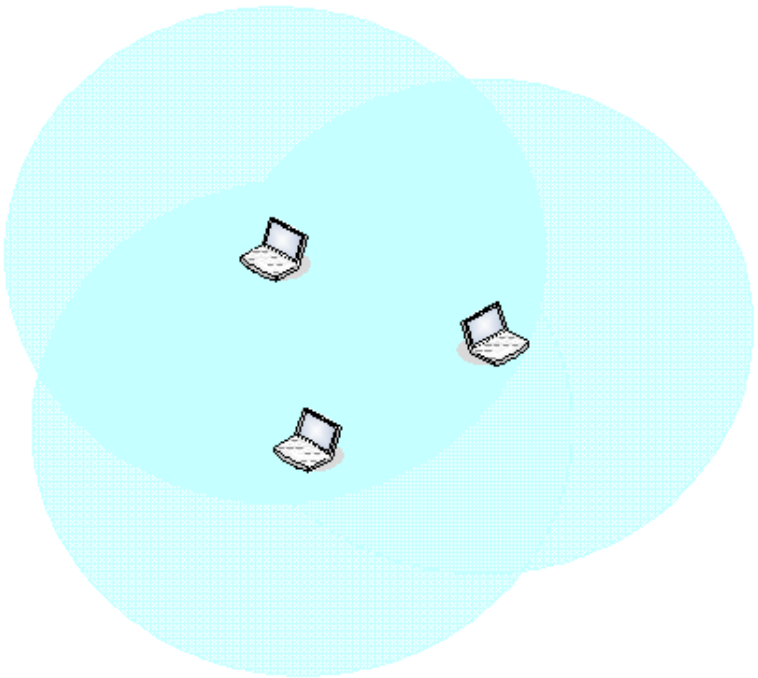
Les débits initiaux de la norme 802.11 étaient de 1 et 2 Mbps.

La couche Physique, qui définit le codage et les caractéristiques de la transmission de données, est divisée en deux sous-couches :

- Physical Layer Convergence Protocol (PLCP), pour la traduction des trames MAC ;
- Physical Medium Dependent (PMD), pour la modulation et le codage.

b. L'architecture Independent Basic Service Set (IBSS)

La première architecture définie dans la norme 802.11 permet une communication d'égal à égal entre au moins deux stations mobiles ou fixes. Elle est nommée Independant Basic Service Set (IBSS), pour former des réseaux ad hoc. Elle autorise une communication en direct entre les différents postes dont les cellules sont recouvrantes, au sein d'un réseau autonome, auquel ils sont associés. Par exemple, il peut être intéressant de mettre en œuvre ponctuellement un tel réseau pour un échange de fichiers entre ordinateurs portables. Les tailles de cellules définies par de tels matériels étant généralement relativement peu importantes, l'étendue est plus de type RPAN, mais avec un débit supérieur à Bluetooth.



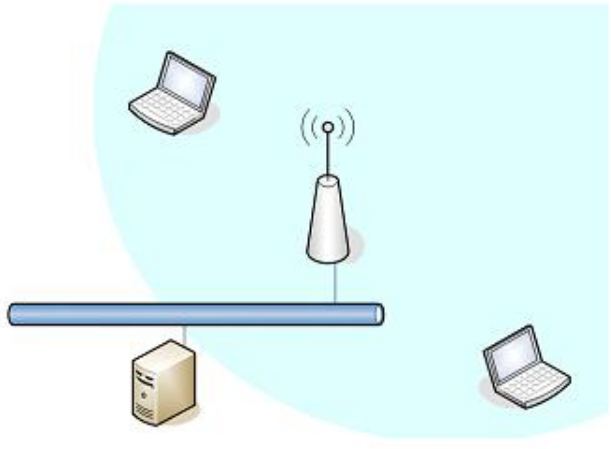
Réseau ad hoc entre ordinateurs portables

c. L'architecture Basic Service Set (BSS)

La seconde architecture nécessite un composant d'infrastructure, nommé Access Point (AP), en français point d'accès. Il permet l'interconnexion du réseau sans fil avec le réseau local filaire de l'entreprise, nommé dans les standards Distribution System (DS). Dans ce Basic Service Set (BSS), le point d'accès agit comme un maître pour les stations périphériques qui lui sont associées. Toutes les communications doivent passer par lui.

Le point d'accès définit ici une cellule nommée Basic Service Area (BSA), dont le nom est l'adresse MAC du point d'accès, ce qu'on appelle le Basic Service Set IDentification (BSSID). Ce réseau peut être nommé et saisi sur le point d'accès.

Une salle de réunion peut ainsi être équipée, offrant un accès sans fil aux serveurs de l'entreprise, eux-mêmes connectés au réseau filaire.

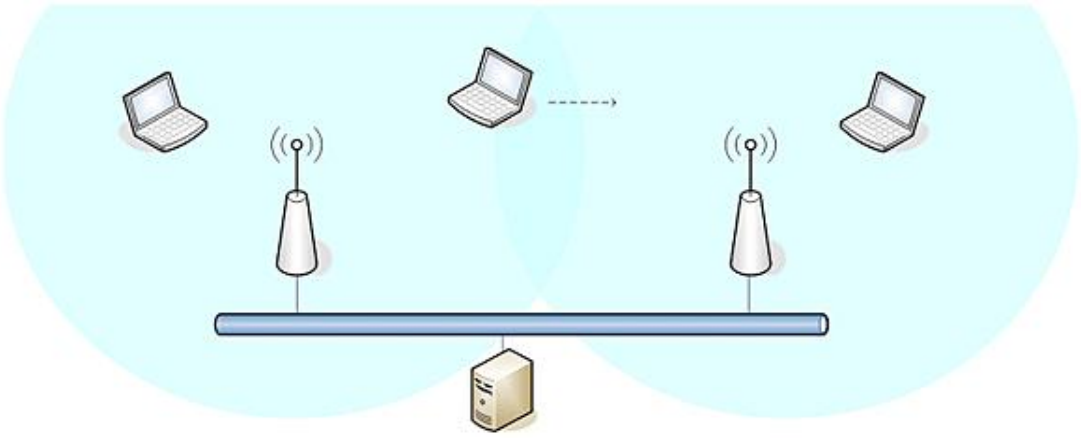


Réseau BSS, permettant l'accès au réseau Ethernet

d. L'architecture Extended Service Set (ESS)

Un réseau de plus grande étendue, Extended Service Area (ESA) peut être défini avec plusieurs AP. On parle dans ce cas de réseau Extended Service Set (ESS), qui permet une communication sans fil entre ordinateurs associés à des points d'accès distincts. Pour cela, les cellules définies par ces derniers ne sont pas obligatoirement recouvrantes, étant donné que le système de distribution (DS) est utilisé pour prolonger la communication.

Si l'itinérance complète des équipements portables est souhaitée, un recouvrement des cellules est recommandé. En effet, l'ordinateur peut ainsi s'associer à un autre point d'accès sans coupure de communication. Cette action de roaming utilise, pour ce basculement, le réseau filaire.



Réseau ESS, autorisant le roaming

Ce type de réseau est qualifié de Extended Service Set IDentifier (ESSID). Il est unique pour tous les points d'accès et les stations qui y sont associés.

3. Wi-Fi Alliance

Les spécifications 802.11 intéressent tellement certains éditeurs qu'ils forment, en 1999, le regroupement Wireless Ethernet Compatibility Alliance (WECA). Leur but est non seulement de promouvoir ce nouveau standard, mais également de certifier les matériels, afin de garantir sa bonne application. Un label Wireless Fidelity (Wi-Fi), brevet d'interopérabilité, peut être décerné après différents tests. Finalement, cet organisme sera rebaptisé Wi-Fi Alliance.

Site Web de la Wi-Fi Alliance : http://www.wi-fi.org ou http://www.wi-fi.com

Wi-Fi qualifiait à l'origine des matériels de la norme 802.11b. Progressivement, et par abus de langage, cette appellation vint supplanter celle du standard RLAN, s'appliquant même à ses évolutions.

Après les tests de compatibilité, le constructeur du matériel peut apposer sur les boîtes le logo ci-dessous, en fonction des standards respectés.

Le logo de la certification, pour des matériels respectant les standards 802.11a, b, g et draft n

Avant d'acheter du matériel, et si ce logo n'est pas disposé sur la boîte, cette compatibilité peut être vérifiée à partir du lien adéquat sur la page d'accueil du site : www.wi-fi.org ou www.wi-fi.com

Normes IEEE 802.11x

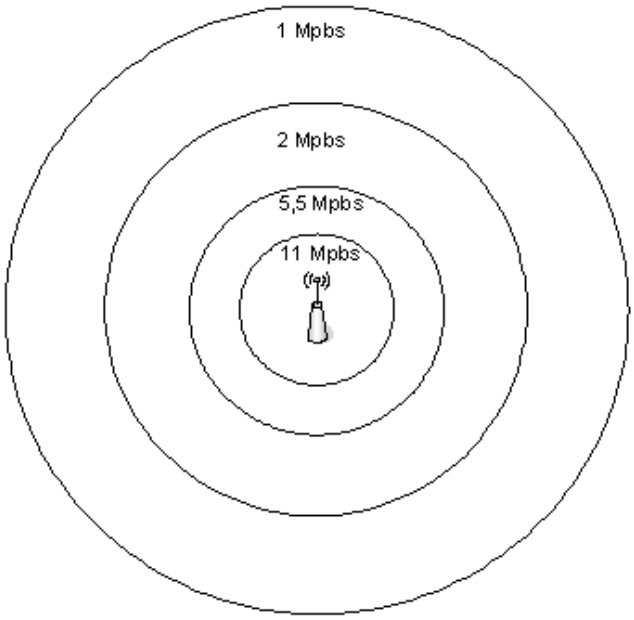
Le groupe de travail 802.11 a déjà publié un certain nombre de spécifications déjà appliquées par les matériels. D'autres sont encore en cours d'élaboration, particulièrement la très attendue 802.11n. Mais le succès de ces réseaux entraîne une exigence de capacité et de fonctionnalité, qui est désormais fournie dans bien des cas.

Après avoir fait évoluer essentiellement la vitesse et les moyens de sécurisation, le nouveau challenge du Wi-Fi est d'autoriser enfin des débits et une qualité de service autorisant les flux multimédia, par exemple streaming audio et vidéo de haute définition.

1. 802.11b

Cette norme, publiée en septembre 1999, vient améliorer les vitesses de transmission insuffisantes du 802.11, toujours dans la bande de fréquence 2.4 GHz. Son succès concrétise l'avènement des RLAN Wi-Fi.

La vitesse maximale de transmission est de 11 Mbps. Des replis sont possibles à 5.5, 2 et 1 Mpbs, pour agrandir la cellule ou permettre une communication dans des environnements très perturbés.



Les vitesses de transmission du 802.11b, autour d'une antenne omnidirectionnelle

Le 802.11b n'utilise plus la technologie FHSS, mais exclusivement DSSS. Les réseaux ESS et BSS portent désormais un nom commun de réseau : le SSID (*Service Set IDentifier*).

2. 802.11a

Comme 802.11b, la norme 802.11a est publiée en septembre 1999. Par contre, sa couche physique est prévue pour travailler sur les bandes UNII en 5 GHz, normalement non dédiées aux RLAN.

Ces bandes, beaucoup plus larges, de 300 MHz au maximum au lieu de 83.5 MHz en 2.4 GHz, permettent de réduire fortement les risques d'interférences entre réseaux. Malheureusement, comme nous l'avons vu précédemment, elles se sont avérées beaucoup moins exploitables que prévues en Europe, et surtout en France. Cette montée en fréquence n'est pas sans conséquence pour la portée des équipements. En effet, les ondes radio à 5 GHz sont freinées beaucoup plus vite par l'environnement que celles à 2.4 GHz.

Les spécifications 802.11a autorisent une montée en débit significative par rapport au 802.11b. La transmission maximale est de 54 Mpbs. Comme précédemment, des solutions de replis sont prévues, à 48, 36, 24, 18, 12, 9 et 6 Mbps. Pour atteindre de tels débits, 52 sous-porteuses sont exploitées, selon la technique Orthogonal Frequency Division Multiplexing (OFDM), que nous expliquerons dans le chapitre suivant.

À cause du changement de fréquence, les antennes 802.11a sont incompatibles avec celles 802.11b.

3. 802.11g

Ce standard, ratifié en juin 2003, succède finalement au 802.11b. Exploitant, comme cette dernière, la bande des 2.4 GHz, il autorise des débits à 54 Mbps. Les replis possibles sont les mêmes que 802.11a, soit 48, 36, 24, 18, 12, 9 et 6 Mbps.

Exploitant la même technique OFDM que le 802.11a, il apporte la compatibilité de fréquence avec 802.11b. Les matériels appliquant ces spécifications sont donc capables de fonctionner en 802.11b et 802.11g, avec une conséquence sur le débit de fonctionnement.

Par exemple, si un client 802.11b se connecte sur un point d'accès configuré en mode mixte, tous les clients 802.11g verront leur débit chuter, comme le montre le tableau ci-dessous.

	Débit (Avec en-têtes)	Débit réel (Sans en-têtes)	Rapport avec 802.11b
802.11b	11 Mbit/s	6 Mbit/s	100%
802.11g avec clients 802.11b (Mode mixte)	54 Mbit/s	8 Mbit/s	133%
802.11g seul	54 Mbit/s	22 Mbit/s	367%
802.11a	54 Mbit/s	25 Mbit/s	417%

Les différentes vitesses de transmission en fonction des modes (source : Cisco)

802.11g améliore également le traitement des trames. Les spécifications de celles-ci sont quelque peu simplifiées et améliorées, afin de gagner encore en efficacité, donc en débit. Nous y reviendrons dans l'étude détaillée de ces couches.

4. 802.11n

802.11g reste, depuis 2003, la spécification la plus exploitée commercialement. L'évolution 802.11n tarde à être finalisée par l'IEEE. En effet, elle reste encore à l'état de brouillon (draft) et le moment de sortie de la spécification définitive, qui a déjà été beaucoup retardé, reste encore incertain.

Après les versions 1.0 et 1.1, le groupe de travail de l'IEEE a adopté, en mars 2007, la version 2.0 du brouillon, qui s'approcherait enfin du stan- dard définitif. En terme de capacités, le 802.11n en version brouillon inclut d'ores et déjà, la qualité de service (QOS - *Quality of Service*), le WMM (Wi-Fi MultiMedia) pour les applications VoIP (*Voice over IP*) et le streaming.

Les évolutions à définir sont importantes, car il s'agit à la fois d'améliorer considérablement le débit et la couverture radio. Un certain nombre de procédés sont donc mis en œuvre et leur définition dans le cadre d'un standard est un compromis parfois difficile à avaliser.

Tout d'abord, au niveau du travail sur le signal (couche Physique) la segmentation des données par OFDM (*Orthogonal Frequency Division Multiplexing*), utilisée en 802.11a et 802.11g est améliorée. Cette avancée seule permet d'envisager un débit de 65 Mbps au lieu de 54 Mbps avec les spécifications précédentes.

La seconde amélioration sur les transmissions est amenée par une série de techniques liées à la technologie MIMO (*Multiple Input Multiple Output*). Par multiplexage spatial, ce sont jusqu'à 4 flux, au lieu d'un seul, qui peuvent être traités simultanément. En utilisant plus d'antennes de réception que de flux, il est possible de travailler en diversité, afin de recevoir des signaux de plusieurs chemins. Comme de tels systèmes sont gourmands en énergie, il est prévu de les utiliser uniquement quand les transmissions le nécessitent.

802.11n utilise les bandes de fréquence 2.4 et 5 GHz. Dans cette dernière, il est possible de doubler la largeur de canal exploité, ce qui permet de gagner encore en vitesse. Le débit maximal de la version finale du 802.11n devrait être de 300 Mbps. Les techniques utilisées permettraient d'aller en théorie jusqu'à 600 Mbps.

Nous reviendrons en détail sur ces différentes techniques dans le chapitre suivant.

Les publications des premiers standards de l'IEEE 802.11 ont été relativement rapprochées. Il a été d'ailleurs parfois reproché au Wi-Fi son instabilité, d'un point de vue commercial. Ce n'est pas le cas avec le 802.11n, qui se fait attendre. Sa longue gestation a entraîné différentes interprétations propriétaires, donc incompatibles, par les constructeurs de matériels. Le consortium Wi-Fi Alliance a mis un terme aux spéculations et propose, depuis avril 2007, une certification "802.11n Draft".

Le logo "N draft"

En étant certifiés, les matériels redeviennent enfin compatibles entre eux. Il est très probable qu'une simple mise à jour du firmware des puces incluses permette de leur faire adopter la norme définitive. La tendance la plus marquée est l'inclusion dans ces puces de 3 émetteurs et 3 récepteurs, au lieu d'un seul de chaque précédemment. Les appareils adoptent ainsi 3 antennes, externes ou internes.

Exemple d'une carte réseau compatible "N draft"

5. Autres standards

Les travaux du groupe 802.11 ne se limitent pas aux quatre standards principaux décrits précédemment. Des spécifications complémentaires ont été définies et appliquées dans les matériels. D'autres sont encore en travaux.

a. 802.11d

Les spécifications 802.11 doivent être applicables au niveau international et suivre pour cela les réglementations, différentes, par exemple aux USA, en Europe ou au Japon. Grâce à l'amendement 802.11d, les matériels deviennent capables de s'échanger les informations de fréquences et puissances de leur pays d'origine, afin de rester conformes. Pour cela, les trames transmises sont modifiées. L'application de la norme par le constructeur du matériel est certifiée par la Wi-Fi alliance.

b. 802.11e

802.11e définit les améliorations nécessaires au Wi-Fi en terme de qualité de service (QOS- *Quality Of Service*). Ainsi, le transport du multimédia, voix et audio et vidéo est vraiment possible.

Pour cela, la sous-couche MAC de la couche Liaison de données est modifiée. Les besoins en bande passante et en délai de propagation sont insérés. Les flux sont ainsi priorisés.

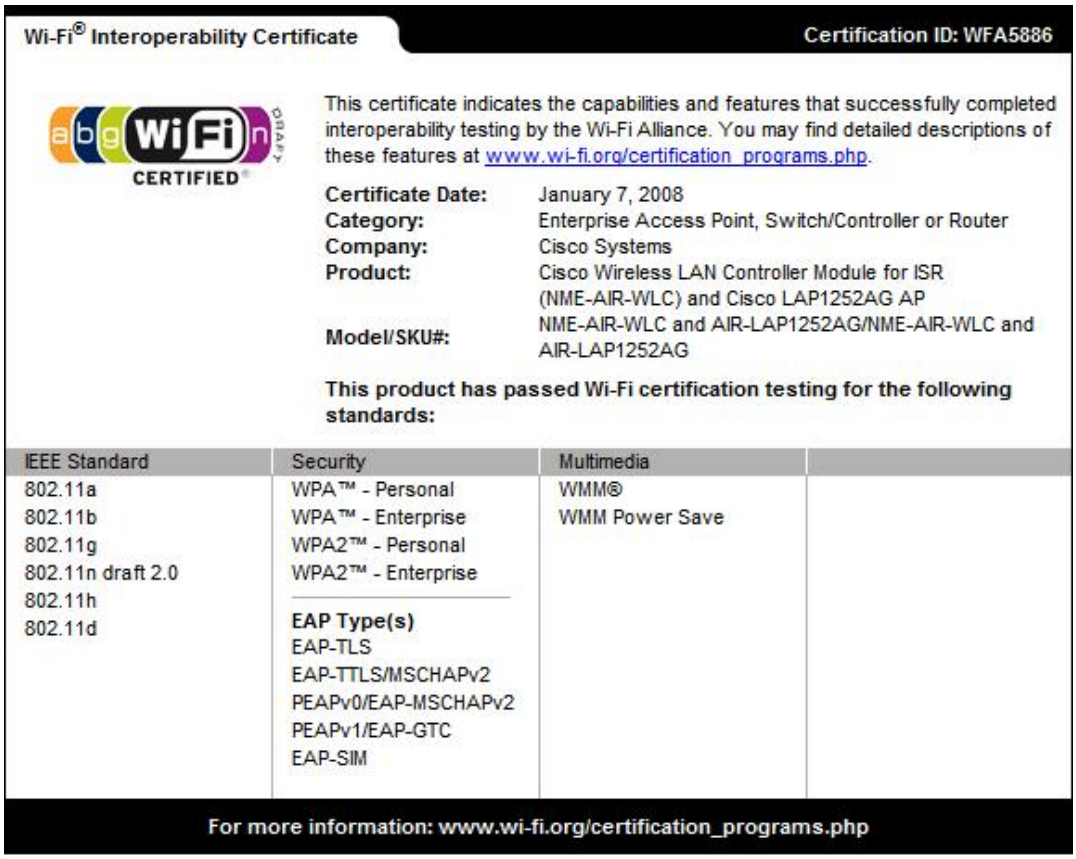
L'approbation de ce standard, important pour le 802.11n, date de septembre 2005.

c. 802.11f

802.11f propose l'usage du protocole Inter-Access Point Protocol (IAPP) pour faciliter l'itinérance entre points d'accès à travers un système de distribution (DS) commun. Ces spécifications permettent de s'affranchir de solutions propriétaires pour monter un ESS. Le transfert des informations entre points d'accès utilise des paquets multicast, sur le port 3517, TCP ou UDP. L'utilisation d'un système dédié à l'authentification permet le suivi de celle-ci entre AP.

d. 802.11h

802.11h est une extension destinée à rapprocher 802.11a des contraintes européennes. Pour cela, un mécanisme de contrôle de la puissance Transmit Power Control (TPC) est mis en œuvre. Un second, Dynamic Frequency Selection (DFS), permet la détection de l'occupation d'un canal et son changement dynamique sur l'équipement. Le respect de ses spécifications, validées en 2003, est testé par la Wi-Fi Alliance pour les matériels 802.11a.



Wi-Fi® Interoperability Certificate — Certification ID: WFA5886

CERTIFIED

This certificate indicates the capabilities and features that successfully completed interoperability testing by the Wi-Fi Alliance. You may find detailed descriptions of these features at www.wi-fi.org/certification_programs.php.

Certificate Date:	January 7, 2008
Category:	Enterprise Access Point, Switch/Controller or Router
Company:	Cisco Systems
Product:	Cisco Wireless LAN Controller Module for ISR (NME-AIR-WLC) and Cisco LAP1252AG AP
Model/SKU#:	NME-AIR-WLC and AIR-LAP1252AG/NME-AIR-WLC and AIR-LAP1252AG

This product has passed Wi-Fi certification testing for the following standards:

IEEE Standard	Security	Multimedia
802.11a	WPA™ - Personal	WMM®
802.11b	WPA™ - Enterprise	WMM Power Save
802.11g	WPA2™ - Personal	
802.11n draft 2.0	WPA2™ - Enterprise	
802.11h		
802.11d	**EAP Type(s)**	
	EAP-TLS	
	EAP-TTLS/MSCHAPv2	
	PEAPv0/EAP-MSCHAPv2	
	PEAPv1/EAP-GTC	
	EAP-SIM	

For more information: www.wi-fi.org/certification_programs.php

Exemple d'une certification par la Wi-Fi Alliance

e. 801.11i

802.11i, longtemps attendu, a été ratifié en juin 2004. Ce standard est également nommé Wi-Fi Protected Access 2 (WPA2). Il apporte enfin des mécanismes de sécurisation de haut niveau, pour l'authentification et la confidentialité. Ils seront longuement détaillés plus loin. L'utilisation de l'algorithme Advanced Encryption Standard (AES), pour le chiffrement, demande une puissance de calcul supérieure à celle disponible sur beaucoup d'équipements.

f. Autres

802.11j spécifie des extensions pour le Japon, sur la bande des 5 GHz.

De nombreuses autres spécifications sont encore en cours d'élaboration par le groupe 802.11, restant pour l'instant à l'état de brouillon (draft).

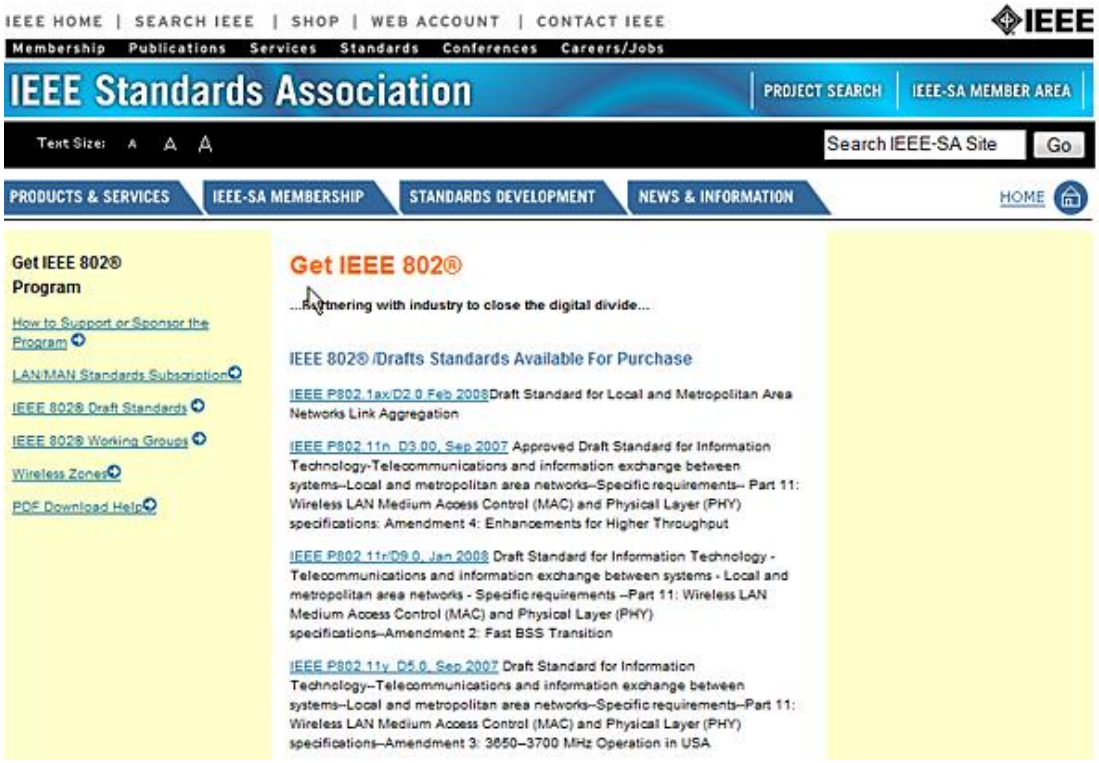
Les amendements 802.11k (RRM - *Radio Resource Management*) et 802.11r (*Fast roaming*) traitent de la liaison entre un client et un point d'accès. Le premier permet de remonter des informations telles que la performance, la quantité d'erreur ou le rapport signal/bruit vers la borne, afin d'établir des statistiques de performance. Au besoin, le point d'accès peut demander d'autorité la déconnexion au profit d'un autre qui proposerait un meilleur compromis. 802.11r est destiné à faciliter la transition de la communication entre deux points d'accès, sans rupture sensible de la communication, ni perte de contenu.

L'extension 802.11p (WAVE - *Wireless Access in Vehicular Environment*) est nécessaire au support des applications de type Intelligent Transportation Systems (ITS). Le but est de permettre l'interconnexion par le Wi-Fi depuis un véhicule, vers un autre ou vers des infrastructures routières. Ici, un roaming très rapide est nécessaire. Par exemple, un péage autoroutier sans arrêt pourrait être effectué par ce moyen.

L'adoption des techniques de réseau maillé, ou mesh, dans lesquelles chaque nœud est à la fois client et serveur, en relayant la communication, fait également l'objet de recherches par le groupe de travail 802.11s.

Les travaux sur des meilleures capacités d'interopérabilité avec des réseaux non Wi-Fi, comme ceux de la téléphonie sont réalisés par 802.11u.

Enfin, bien que d'autres spécifications soient encore en cours d'élaboration, nous pouvons citer 802.11v, destiné à la gestion des équipements. Ainsi, il pourrait être possible de surveiller, configurer et de mettre à jour de manière centralisée les matériels.



URL répertoriant les brouillons : http://standards.ieee.org/getieee802/drafts.html

Équipements

Comme nous l'avons vu précédemment, le choix d'un matériel Wi-Fi nécessite d'abord de s'assurer de sa certification par la Wi-Fi Alliance. Il peut être intéressant de s'assurer au moins de la compatibilité 802.11n draft, avant d'espérer envisager mettre à jour son matériel dans la version définitive. La capacité de sécurisation par WPA2/802.11i paraît également impérative dans l'entreprise.

Pour les équipements d'infrastructure, le choix se fait également entre point d'accès, répéteur, pont, pont pour groupe de travail, en fonction des besoins.

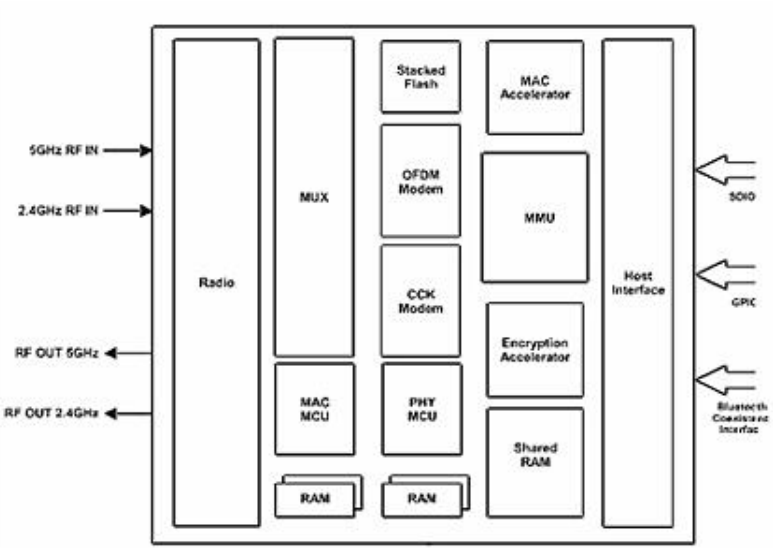
1. Interfaces d'accès

a. Les puces Wi-Fi

Le cœur d'un adaptateur Wi-Fi est constitué par une simple puce, ou chipset. Celle-ci est pilotée par un micro-programme, le firmware, qui doit pouvoir être mis à jour. En effet, la compatibilité à certaines évolutions de normes présentées précédemment y est directement dépendante.

Un tel composant est ni plus ni moins qu'un microcontrôleur, avec :

- des capacités radio (un transmetteur et un receveur par fréquence...) ;
- au moins un processeur et de la mémoire RAM ;
- des modems, en fonction des standards supportés ;
- des capacités de chiffrement.



Puce UniFi de marque CSF et son diagramme

La dernière génération de puces Wi-Fi, adaptées au MIMO, intègre plusieurs transmetteurs et plusieurs récepteurs, en modérant au mieux la consommation d'énergie. Elles sont capables de travailler sur les deux fréquences 2.4 et 5 GHz.

b. Les modèles de cartes réseaux

Un adaptateur Wi-Fi est avant tout composé d'une puce connectée à une antenne. Il est intégré à l'équipement informatique, ordinateur portable, PDA..., ou inséré sur une carte périphérique. Dans un cas comme dans l'autre, il est souvent difficile de connaître la marque du composant utilisé. En fait, relativement peu de fondeurs se partagent le marché. Les fabricants d'ordinateurs ou de cartes viennent s'approvisionner auprès d'eux.

Dans le cas d'une solution intégrée, l'antenne l'est également. Elle est, par exemple, positionnée le long de l'écran de l'ordinateur portable. Beaucoup de constructeurs ont adopté la plate-forme Intel Centrino, remise à niveau récemment. Elle inclut des capacités Wi-Fi annoncées comme compatibles avec 802.11n.

De très nombreux modèles de cartes réseaux Wi-Fi permettent d'ajouter une telle fonction à un ordinateur. On retrouve des formats PC Card/PCMCIA, Compact Flash, PCI ou USB. Pour les deux premières, l'antenne est inclue dans la partie restant visible une fois connectées. Pour les cartes PCI, il est recommandé d'envisager des modèles avec antennes déportées, reliées par un câble pour des machines de type tour, afin de les remonter. Cette problématique est la même pour les modèles USB.

Différents modèles d'adaptateurs Wi-Fi

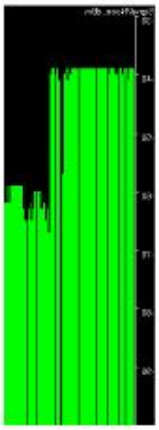
c. Les caractéristiques techniques

En plus de son emplacement, il est recommandé de veiller au positionnement optimal de l'antenne, en fonction de sa polarisation. Par exemple, celle-ci est généralement horizontale sur des modèles PC Card, s'enfichant dans le connecteur du portable. Pour une carte PCI, la polarisation est plutôt verticale. Dans le cas d'antennes en diversité, comme pour le 802.11g, leur positionnement doit être similaire, afin de conserver le même sens de polarisation.

Pour MIMO, exploité en 802.11n draft, les antennes peuvent être positionnées dans des sens de polarisations distincts, afin de profiter des fonctions de réception de signaux provenant de plusieurs chemins. Les antennes fournies avec les cartes réseaux ou matériels intégrés ont des gains de l'ordre de 0 à 2 dBi.

Les caractéristiques de niveaux de sensibilité de réception sont parfois ajoutées dans les documentations. Elles renseignent sur les différents seuils de débit en fonction du rapport signal/bruit, comme dans l'exemple ci-dessous. Des logiciels de scan réseau, comme Netstumbler (www.netstumbler.com, gratuit) permettent de mesurer cette valeur.

-95 dBm pour 1 Mbps
-91 dBm pour 2 Mbps
-89 dBm pour 5.5 Mbps
-90 dBm pour 6 Mbps
-84 dBm pour 9 Mbps
-89 dBm pour 11 Mbps
-82 dBm pour 12 Mbps
-80 dBm pour 18 Mbps
-77 dBm pour 24 Mbps
-73 dBm pour 36 Mbps
-72 dBm pour 48 Mbps
-71 dBm pour 54 Mbps



Caractéristiques de débit d'une carte réseau Cisco en fonction du rapport signal/bruit

Parmi les autres informations radio, quelques précisions de distance en fonction de la vitesse sont parfois indiquées. D'autres données importantes sont les seuils de puissance rapportés à la vitesse, comme dans l'exemple ci-dessous.

20 dBm (100 mW) à 1, 2, 5.5 et 11 Mbps
18 dBm (63 mW) à 1, 2, 5.5, 6, 9, 11, 12, 18 et 24 Mbps
17 dBm (50 mW) à 1, 2, 5.5, 6, 9, 11, 12, 18, 24 et 36 Mbps
15 dBm (30 mW) à 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36 et 48 Mbps
13 dBm (20 mW) à 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 et 54 Mbps
10 dBm (10 mW) à 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 et 54 Mbps

La quantité de caractéristiques techniques fournies n'est pas du tout la même pour des matériels destinés à une utilisation professionnelle ou personnelle.

D'un point de vue informatique, la compatibilité des pilotes avec le système d'exploitation est, bien sûr, à vérifier.

Une carte réseau Wi-Fi, même intégrée, possède, comme toute carte Ethernet une adresse physique MAC qui doit être unique dans le réseau.

```
Carte Ethernet Wi-Fi intégré:

        Suffixe DNS propre à la connexion :
        Description . . . . . . . . . . . : Carte réseau sans fil Mini-PCI doubl
e bande 1450 de Dell
        Adresse physique . . . . . . . . . : 00-90-4B-BF-90-21
        DHCP activé. . . . . . . . . . . . : Oui
        Configuration automatique activée . . . . : Oui
```

2. Composants d'infrastructure

a. Le point d'accès

Le point d'accès est le principal composant d'infrastructure d'un réseau Wi-Fi. Concentrateur (Hub), toutes les communications des stations qui lui sont associées passent par lui. Pont entre les réseaux Ethernet et Wi-Fi, il est également capable de traduire les couches basses du modèle OSI pour transférer les communications. On le qualifie de racine (root) dans ce cas. Certains modèles sont prévus pour une utilisation en extérieur.

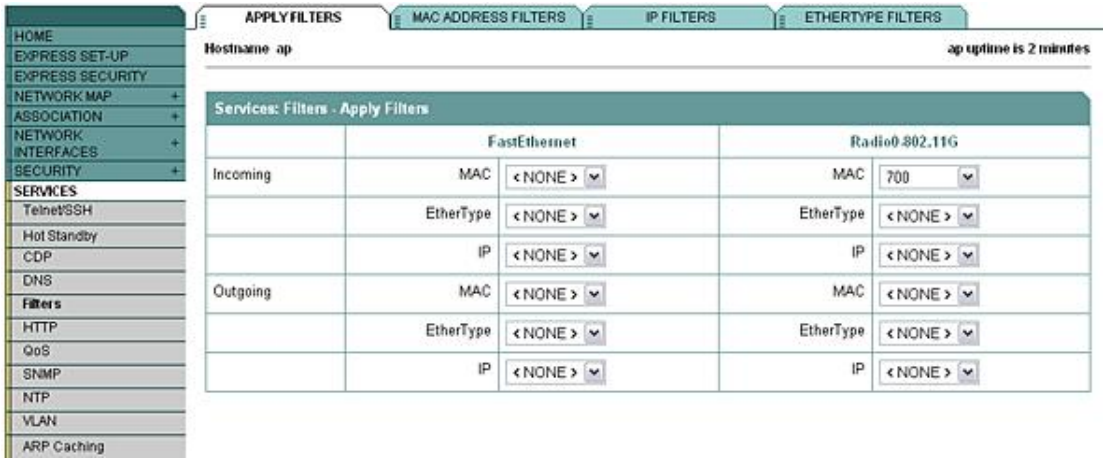
Cette fonctionnalité de pont inclut un apprentissage de l'emplacement du client, afin de savoir s'il est connecté à l'interface Wi-Fi ou Ethernet. Une optimisation du trafic, non négligeable, peut être ainsi effectuée, sans retransmission inutile. On y retrouve même parfois l'exploitation de l'algorithme de détection de boucle Spanning Tree (IEEE 802.1d), utile dans un réseau ESS, avec plusieurs points d'accès racines. Cette capacité de pont rend également possible le filtrage des adresses MAC des clients Wi-Fi, fonctionnalité intégrée aux spécifications 802.11.

Ces équipements ont beaucoup évolué. Dans les générations actuelles, ils sont capables de remonter les traitements jusqu'à la couche 3, Réseau, du modèle OSI.

Par contre, une très grande disparité de fonctionnement est à noter entre les modèles prévus pour la maison et ceux destinés aux réseaux d'entreprise. Très souvent la différence n'est malheureusement pas faite par l'administrateur de l'équipement. Tout d'abord, un point d'accès pour la maison n'est pas conçu pour supporter autant de communications simultanées que son équivalent professionnel. De plus, comme le but n'est pas le même, leurs niveaux de sécurité ne seront pas vraiment comparable. Le particulier peut souhaiter que son équipement soit routeur, voire qu'il intègre un modem ADSL. Un administrateur réseau préférera des fonctions de filtrage et la capacité d'isolation des réseaux par Virtual LAN (VLAN).

Parmi les constructeurs de matériels, la politique de Cisco est la plus claire, qui réserve ses gammes, pilotées par leur propre système d'exploitation IOS, aux entreprises. Leur filiale Linksys propose des produits plutôt orientés grand public. Certaines autres marques sont réservées à l'un ou l'autre marché, ou d'autres encore proposent des modèles dédiés. Lors de l'achat, les caractéristiques du point d'accès doivent être étudiées, afin de bien correspondre au but recherché.

Les fonctions de couche 3 d'un point d'accès professionnel peuvent être assez diverses, mais elles le rapprochent de plus en plus de certains commutateurs. Une première capacité peut résider dans des possibilités de filtrage avancé entre les deux types de réseau, au niveau de l'adresse IP et des ports TCP/UDP.



Exemple de filtres sur point d'accès de marque Cisco, en entrée et en sortie

La segmentation logique de réseaux Wi-Fi par VLAN est possible sur certains modèles. Elle permet au point d'accès de proposer des services différenciés. Par exemple, un même équipement pourrait servir des communications publiques d'accès à Internet, pour des visiteurs, et des transferts sécurisés et authentifiés pour les employés de l'entreprise vers le réseau filaire.

La complexification de ces équipements n'empêche pas de garder un socle de fonctionnalités communes indispensables. Par exemple, un point d'accès est un matériel réseau administrable et nommé, doté de deux adaptateurs réseau (Wi-Fi et Ethernet).

Prévu pour un fonctionnement en TCP/IP, il offre très souvent des capacités de serveur DHCP, afin de distribuer les adresses IP à ses clients Wi-Fi. Intégrant généralement un serveur Web, un point d'accès peut être paramétré à travers un navigateur. À cela s'ajoute souvent des capacités d'administration par SNMP, Telnet...

Il n'est pas obligatoire d'être connecté au réseau filaire pour configurer un point d'accès et il est vivement recommandé de protéger les comptes d'administration, en utilisant au moins un mot de passe complexe.

En fonction des marques, la finesse de configuration des paramètres radio est plus ou moins évoluée. On y retrouve :

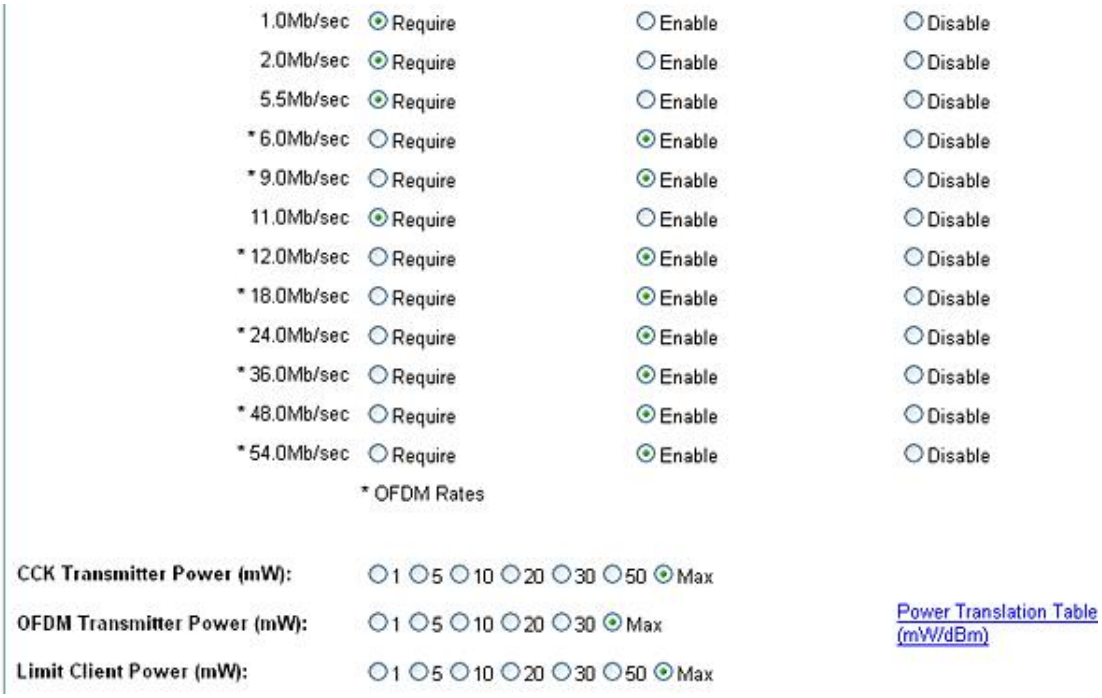
- un champ de saisie du SSID ;
- son critère de diffusion ;
- le choix du mode Wi-Fi ;

- le choix du canal de diffusion.

Nous reviendrons plus tard sur la diffusion (broadcast) du SSID et le choix de la fréquence d'exploitation.

Écran de configuration des paramètres radio d'un point d'accès de marque Linksys

Les points d'accès peuvent être livrés avec une à plusieurs antennes fouet (souvent 3 dans le cadre du MIMO) Avec le 802.11g, une capacité de travail en diversité (dipôle) est un atout. Pour un environnement professionnel, il peut être important de veiller à ce que d'autres modèles d'antennes soient disponibles, afin de pouvoir optimiser, au besoin, la portée du réseau Wi-Fi. Si le gain de l'antenne est important, la possibilité de diminuer la puissance du point d'accès est indispensable, afin de respecter le PIRE.



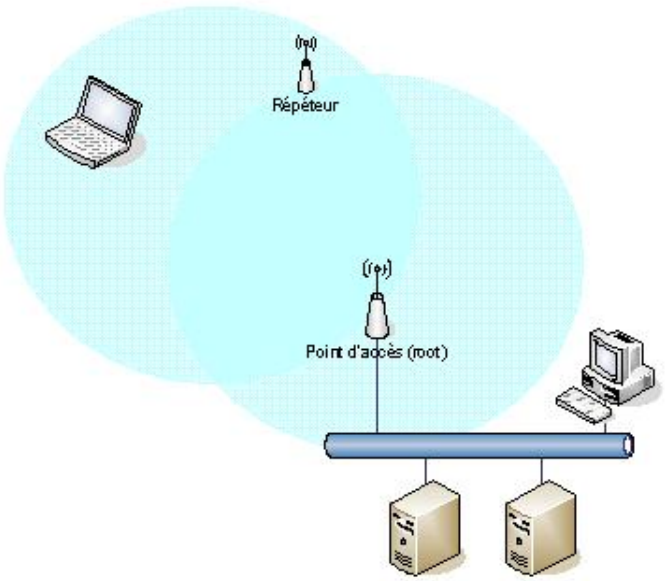
Choix des débits et limitation de la puissance, sur un point d'accès de marque Cisco

L'alimentation électrique d'un point d'accès peut être fournie par le câble réseau lui-même, en exploitant le standard Power Over Ethernet (IEEE 802.3af). Ceci présente l'avantage de ne pas devoir positionner une prise électrique à côté de la borne.

b. Le répéteur

Cet équipement est destiné à réamplifier le signal, afin d'augmenter la portée de la cellule. En quelque sorte simple antenne active, il n'est pas connecté au réseau filaire. Il est devenu de plus en plus difficile d'acheter des répéteurs.

En effet, leur prix se rapproche tellement de celui des points d'accès que cette fonctionnalité est plutôt désormais ajoutée à certains de ces derniers.



Architecture BSS prolongée avec un répéteur

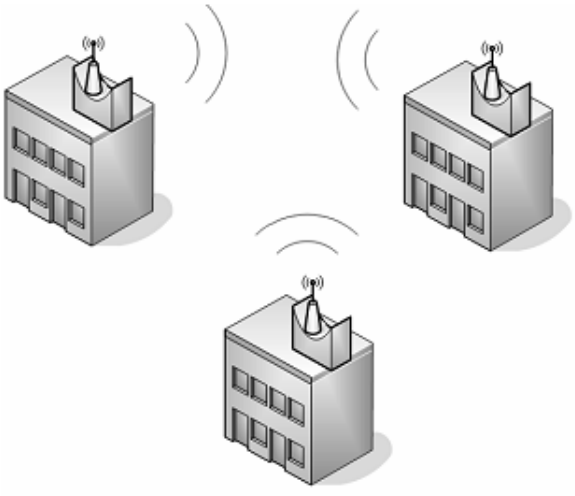
Pour un fonctionnement correct, la cellule définie par le répéteur contient le point d'accès, et réciproquement. L'extension est donc d'environ 50 % de la cellule.

Le relayage de la communication provenant du point d'accès, vers le poste de travail par l'intermédiaire du répéteur, sur la même fréquence, est assez polluant. En effet, la transmission est également renvoyée vers ce point d'accès. L'exploitation du mécanisme de Spanning Tree permet de cantonner ce problème aux seules ondes radio, et d'éviter des traitements informatiques inutiles.

Le fonctionnement Wireless Distribution System (WDS), spécifié dès 802.11, spécifie dans les trames, le relais entre deux points d'accès. Bien que très basique, il permet de s'affranchir de solutions propriétaires. Nous détaillerons le contenu de ces trames plus tard.

c. Le pont

La fonction principale d'un pont (bridge) Wi-Fi est d'interconnecter deux réseaux filaires Ethernet, par l'interface air. Les ponts Wi-Fi fournissent ainsi une solution à prix réduit pour relier les réseaux Ethernet de plusieurs bâtiments, sans avoir recours à la fibre optique. Bien sur, cette dernière sera nettement plus rapide.



Interconnexions entre bâtiments par ponts Wi-Fi

Deux types de communications sont possibles avec de tels équipements :

- Point à point, entre 2 ponts seulement, avec des antennes directionnelles ;

- Point à multipoints, d'un pont vers plusieurs, là encore avec les antennes adéquates.

Une telle fonctionnalité de pont peut avoir été ajoutée à un point d'accès, par son constructeur. Mais des modèles dédiés existent. Ils peuvent être installés à l'intérieur d'un bâtiment, l'antenne étant déportée à l'extérieur, ou directement placés à l'extérieur. L'alimentation électrique du pont par le est intéressante.

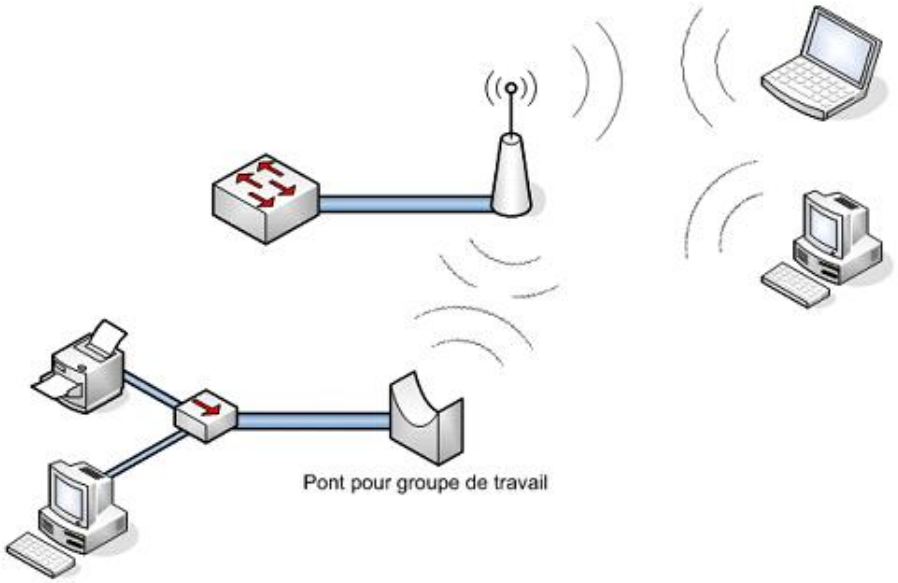
Modèle de pont intégrant une antenne directionnelle, le tout dans une boîte hermétique

La mise en place d'un pont réseau Wi-Fi d'interconnexions de bâtiments est souvent déléguée à un installateur spécialisé, particulièrement lorsqu'il est placé en hauteur. L'étude avant mise en œuvre doit être précise, car les cellules débordent souvent sur le domaine public. La sécurisation des communications doit être à l'avenant.

d. Le pont pour groupe de travail

Le pont pour groupe de travail (Workgroup bridge) est une version allégée d'un tel dispositif. Il permet d'interconnecter quelques équipements filaires au réseau Wi-Fi de l'entreprise.

Le réseau peut ainsi être étendu, comme avec une fonction de répéteur, mais sans équiper l'ordinateur d'une carte Wi-Fi. Un tel équipement permet également l'inclusion au réseau sans fil de périphériques (imprimante, scanner...) uniquement prévus pour Ethernet.



Exemple d'utilisation d'un pont pour groupe de travail

3. Périphériques Wi-Fi

Les terminaux Wi-Fi les plus courants restent les ordinateurs, particulièrement portables, et les périphériques mobiles, types assistants personnels communiquant. Dans les bureaux, d'autres équipements communiquent désormais en Wi-Fi : les vidéo-projecteurs, les imprimantes, les caméras...

Au niveau industriel ou dans les entrepôts, les douchettes de lecture de code barres, depuis longtemps sans fil, se sont standardisées en adoptant le Wi-Fi.



Le succès de la téléphonie sur IP (VoIP) a même conduit des constructeurs à proposer des solutions sans fil exploitant le réseau Wi-Fi (VoWi-Fi). Celles-ci ont actuellement plutôt recours à des fonctionnement propriétaires, par exemple pour le roaming, en attendant les standards.

Transmission des informations

La couche physique du modèle OSI prévoit la transmission bit à bit des informations entre l'émetteur et le récepteur. Le support constitué de l'interface d'accès (carte réseau...) transforme le signal numérique en signal radio et réciproquement. Dans le standard 802.11, ce niveau allie donc à la fois des aptitudes de communication radio et des capacités informatiques. Ainsi, deux sous-couches prennent chacune en charge une partie de ces fonctions.

L'envoi d'informations en sortie de l'équipement, par l'antenne, demande au préalable que le signal ait été mis en forme. Ces 0 et 1 doivent parvenir au récepteur avec le maximum d'efficacité. Cette sous-couche basse, Physical Medium Dependent (PMD), liée au média, utilise des techniques de transmission résistantes aux interférences. Elle assure l'encodage de la porteuse, en symbolisant les informations et la modulation en états binaires.

La sous-couche haute, Physical Layer Convergence Protocol (PLCP), procédé de convergence de la couche physique, assure plutôt une tâche informatique.

1. Étalement de spectre

Une transmission d'ondes électromagnétiques est d'abord dépendante de la bande de fréquence choisie et de la puissance d'émission. Elle est malheureusement très sensible aux parasites comme aux interférences intentionnelles.

Les hautes fréquences, 2.4 GHz et 5 GHz, utilisées en Wi-Fi permettent d'exploiter un spectre large, autorisant des montées conséquentes en débit, tout en évitant de trop grosses consommations d'énergie.

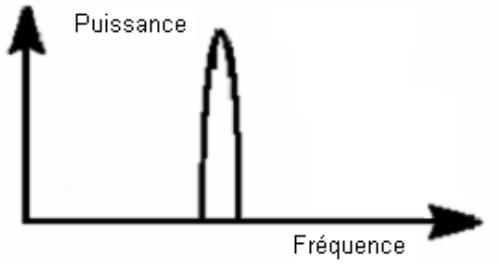
Les transmissions sont effectuées en mode half-duplex. C'est-à-dire qu'à un instant donné, un équipement ne peut être à la fois émetteur et récepteur. Ce dernier doit être positionné sur la même fréquence d'exploitation que la source de l'information.

a. Narrow band

Le premier mode de transmission d'ondes électromagnétiques significatives fonctionne par bande étroite (Narrow band). En utilisant un spectre de fréquence le plus étroit possible, il permet la juxtaposition d'un certain nombre de diffusions sur une bande réduite.

Par exemple, les transmissions radioamateurs Citizen Band (CB) exploitent une largeur de 3 kHz et la radio FM, 175 kHz.

Cette technique est gourmande en énergie et plutôt sensible aux brouillages. En effet, une interférence juste sur la fréquence empêche toute communication.

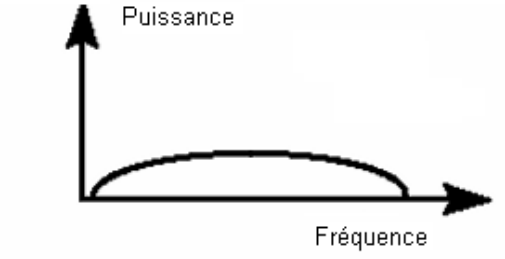


Signal bande étroite

b. Spread spectrum

L'autre moyen de transmission des informations par les ondes radio est l'étalement de spectre (*Spread spectrum*). C'est en 1942 que l'actrice Hedy Lamar et le compositeur George Antheil exposent ce concept.

La solution réside en l'étalement d'un signal sur de nombreuses fréquences. Cette bande exploitée, plus large que dans la solution précédente, convient très bien aux transmissions sur les hautes fréquences. De plus, l'immunité du signal aux bruits et brouillages est importante. D'ailleurs, cette technique est utilisée par les militaires.



Signal bande étalée

Pour transmettre ce signal proche du bruit, une faible puissance est nécessaire. Deux méthodes d'étalement de spectre sont couramment utilisées.

2. Étalement de spectre à saut de fréquence

a. Principe

La première exploitation de ce mode de transmission est la technique Frequency Hopping Spread Spectrum (FHSS), ou étalement de spectre à saut de fréquence. Elle fut utilisée pour le guidage des torpilles sans risque d'interférence.

La communication utilise successivement plusieurs fréquences de porteuse, selon une séquence connue seulement de l'émetteur et du récepteur. Ces changements synchronisés sont définis par une clé, qui précise les sauts (*Frequency Hopping*). Pour permettre ce fonctionnement, la bande utilisée doit auparavant être divisée en spectres étroits.

Étalement de fréquence par saut FHSS

Cette technique est traitée par le standard IEEE 802.11 et utilisée par les technologies Bluetooth et de téléphonie DECT.

La résistance aux interférences est apportée par le fait que, si un signal est brouillé sur l'une des fréquences, il peut être renvoyé après le saut suivant. De plus, un grand nombre de communications sont possibles simultanément, correspondant sensiblement au nombre de zones de fréquence définies.

Les spécifications 802.11 proposent la division de la bande des 2.4 GHz, depuis 2.402 GHz jusqu'à 2.482 GHz, en un maximum de 79 zones de 1 MHz. Chacune forme un canal numéroté. Le nombre exact de canaux dépend de la réglementation du pays d'utilisation, et des limites inférieures et supérieures de la bande.

b. Fonctionnement

La communication réelle est effectuée durant une période appelée Dwell Time, qui dure de quelques dizaines à quelques centaines de millisecondes. Ce temps ne doit pas être trop court, pour garder un débit global correct, ni trop long, pour éviter les interférences. L'organisme FCC recommande un temps de 400 ms.

Le temps de saut de fréquence (*Hop Time*) est un compromis entre la capacité des équipements et la volonté de réduire ce temps. La réduction du temps de saut améliore le débit global de la communication, mais le coût des composants électroniques s'accroît.

La taille minimale d'un saut est de 6 MHz en Amérique du Nord et en Europe. Les séquences Frequency Hopping contiennent 26 sauts. La France, comme l'Espagne et le Japon, dispose de ses propres sauts de fréquence. Pour notre pays, 3 séquences de 11 sauts sont définies.

c. Débits

Les débits du FHSS sont limités par la largeur de canal de 1 MHz. De plus, les sauts et la synchronisation coûtent. Par contre, le récepteur est moins sensible aux trajets multiples.

En 802.11, le canal de 1 MHz permet un débit de 1 Mbps, qualifié de Basic Rate. Par un doublement du nombre de bauds, la transmission peut augmenter à 2 Mbps, en Enhanced Rate. Le débit est automatiquement adapté en fonction du rapport signal/bruit.

Il n'a pas été prévu de monter en vitesse avec cette technique FHSS, même si cela est techniquement possible.

3. Étalement de spectre à séquence directe

a. Principe

La technique Direct Sequence Spread Spectrum (DSSS) exploite une fréquence continue et élargie. Autorisant des meilleurs débits, elle est exploitée dans les différentes spécifications du Wi-Fi, sur les bandes 2.4 GHz et 5 GHz.

L'étalement de spectre est obtenu par des transitions d'état très rapides, le chipping. Elle consiste à envoyer une séquence complète de bits, le chip, pour un seul bit de données. Plus le code est long, plus il est considéré étalé et le débit démultiplié.

Par exemple, un 0 informatique peut devenir une séquence 10011, le 1 devenant 01100.

Une immunité importante au bruit est apportée par ces codes d'étalement. En effet, le récepteur peut quand même interpréter le code, même si plusieurs bits de la séquence ont été modifiés durant la transmission. Par exemple, la séquence 00111 reste plus proche de 10011 que de 01100.

Bien que 2 bits sur les 5 aient été modifiés, le récepteur saura reconnaître un 0. Considérant les taux d'erreurs des transmissions radio, ce fonctionnement présente un intérêt majeur.

Une première caractéristique de DSSS est donc la longueur du code d'étalement. Nous verrons plus loin qu'elle varie en fonction des débits.

La largeur du canal de transmission a également son importance. Elle est basée sur le théorème de Shannon, qui précise que la fréquence d'échantillonnage doit être au minimum égale au double du signal à numériser. Ainsi, pour un débit de 11 Mbps, ce canal doit être large de 22 MHz.

b. Fonctionnement

Par exemple, pour étaler le signal par chipping, la bande de 2.4 GHz à 2.4835 GHz a été divisée en 14 canaux de 22 MHz chacun. Un masque de transmission est défini dans les spécifications IEEE 802.11. Les lobes secondaires, entre 11 et 22 MHz, au-dessus et au-dessous de la fréquence fixée, sont au moins inférieurs de 30 dB par rapport au niveau de celle-ci. Au-delà, une réduction de 50 dB est nécessaire.

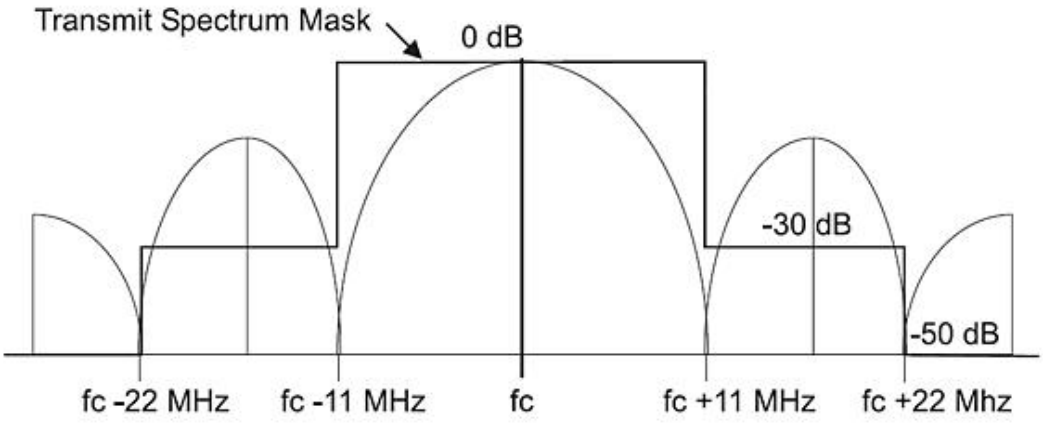


Schéma simplifié du masque de transmission DSSS (source : IEEE)

Seuls les canaux numérotés de 1 à 11 sont exploitables aux U.S.A, quand le Japon les autorise tous. En France, les 13 premiers peuvent être utilisés, en respectant le PIRE, avec les spécificités extérieures :

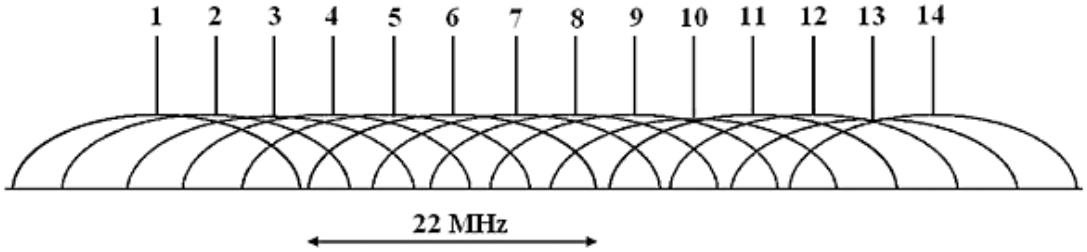
- 100 mW pour les canaux 1 à 7 ;

- 10 mW pour ceux de 8 à 13.

Canal	Fréquence basse (GHz)	Fréquence centrale (GHz)	Fréquence haute (GHz)
1	2.401	2.412	2.423
2	4.406	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473
12	2.456	2.467	2.478
13	2.461	2.472	2.483
14	2.473	2.484	2.495

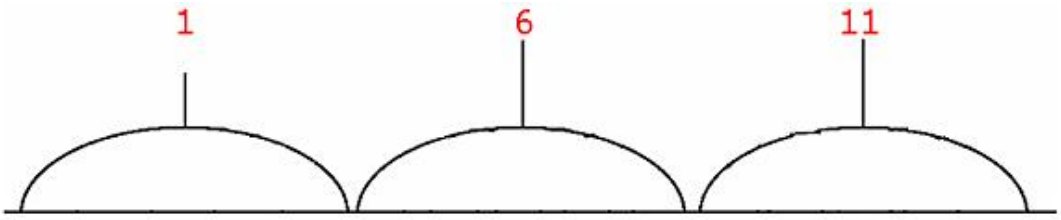
Les fréquences des 14 canaux 2.4 GHz

Pour émettre en DSSS, le choix du canal de transmission doit d'abord être effectué. Il doit, bien sur, correspondre à celui du récepteur.



Les 14 canaux de la bande 2.4 GHz en DSSS

Sur les 83.5 MHz de la bande de fréquence utilisée en France, les 13 canaux se chevauchent. En fait, ils ne sont séparés que de 5 MHz. Cet entrelacement provoque d'importantes perturbations électromagnétiques si des cellules recouvrantes en utilisent deux contigus. Il est donc nécessaire d'espacer les canaux d'au moins 5 unités. Au niveau international, le choix s'est imposé sur ceux numérotés 1,6 et 11, disponibles partout.



Canaux 1, 6 et 11 non recouvrants

La bande des 5 GHz est beaucoup plus large que celle des 2.4 GHz. Par contre, la réglementation française était, jusqu'à récemment, très contraignante, réduisant de beaucoup l'usage potentiel. À la fin de l'année 2005, l'ARCEP a modifié les autorisations d'usage. Cette mise en conformité par rapport à l'ETSI et aux utilisations européenne a enrichi les perspectives. Il devient enfin possible d'exploiter un grand nombre de canaux, de largeur 20 MHz, dans cette bande de fréquences supérieures.

Parmi tous les canaux disponibles en UNII, 19 sont désormais exploitables en Europe, donc en France, dans les bandes UNII 1 (5.15 à 5.25 GHz) et UNII 2 étendu (5.25 à 5.35 GHz puis 5.49 à 5.71 MHz). Non chevauchants, ils ne se perturbent pas les uns les autres.

Le nombre de communications simultanées possibles sur cette bande de fréquences est donc beaucoup plus important que sur celle de 2.4 GHz.

Canal	Fréquence basse (GHz)	Fréquence centrale (GHz)	Fréquence haute (GHz)
36	5.17	5.18	5.19
40	5.19	5.20	5.21
44	5.21	5.22	5.23
48	5.23	5.24	5.25
52	5.25	5.26	5.27
56	5.27	5.28	5.29
60	5.29	5.30	5.31
64	5.31	5.32	5.33
100	5.49	5.50	5.51
104	5.51	5.52	5.53
108	5.53	5.54	5.55
112	5.55	5.56	5.57
116	5.57	5.58	5.59
120	5.59	5.60	5.61
124	5.61	5.62	5.63
128	5.63	5.64	5.65
132	5.65	5.66	5.67
136	5.67	5.68	5.69
140	5.69	5.70	5.71

Les canaux 36 à 140 agréés pour une utilisation européenne

L'efficacité de beaucoup de réseaux Wi-Fi est amoindrie dans un certain nombre d'endroits, où ils se sont multipliés, par exemple dans des immeubles de bureau. Ainsi, Les perturbations radio sont courantes sur la bande des 2.4 GHz. L'adoption en France du 5 GHz, avec le choix de canal automatique par le mécanisme DFS (*Dynamic Frequency Selection*) du 802.11h, laisse présager d'une bien meilleure efficacité.

En France, il est probablement trop tard pour adopter, en masse, le standard 802.11a. Mais l'exploitation du 802.11n en sera facilitée. De plus l'utilisation simultanée d'un canal primaire et d'un canal secondaire en agrégation est autorisée. La largeur exploitable passe ainsi de 20 MHz à 40 MHz.

c. Débits

DSSS est la première technique d'étalement de spectre utilisée dans la pratique pour le Wi-Fi. Elle autorise les débits de 1 Mbps (Basic rate) et 2 Mbps (*Enhanced rate*) comme FHSS.

Les spécifications 802.11b apportent une extension qualifiée de High rate, à des débits de 5,5 et 11 Mbps. Le rapport signal/bruit détermine toujours la vitesse possible.

4. Optimisation par multiplexage OFDM

a. Principe

Une des options retenues par l'IEEE pour augmenter le débit au-delà des 11 Mbps est l'utilisation de la technique Orthogonal Frequency Division Multiplexing (OFDM). Apparue dans les années 60, elle est également utilisée dans les réseaux CPL, l'ADSL et certaines des communications de téléphonie mobile.

L'OFDM consiste à diviser le canal en de multiples sous-canaux. La porteuse elle-même est donc divisée en sous-porteuses (subcarriers) par l'émetteur. C'est au récepteur de reconstituer la communication, à partir de ces différentes informations.

La fréquence utilisée devient donc un multiplexage de sous-fréquences (*Division Multiplexing*). Pour éviter les interférences, les sous-porteuses sont traitées par une transformation de Fourier nommée Fast Fourier Transform (FFT). Cet algorithme échantillonne les différentes sous-porteuses, de façon à ce que le niveau correspondant à l'information sur l'une d'elles, corresponde à des niveaux nuls sur les autres. Cette transformation de la fréquence

est dite orthogonale (*Orthogonal Frequency*).

Dans les standards actuels, la fréquence est d'abord fixée sur celle d'un canal de base DSSS, soit 1 à 13 pour 802.11g et 802.11n draft ou bien 36 à 140 pour 802.11a et 802.11n draft. Ensuite est mise en œuvre, par exploitation de sous-canaux, la technique OFDM. On parle d'ailleurs parfois de DSSS-OFDM.

Elle permet une utilisation optimale de la bande de fréquence, tout en apportant une très bonne résistance aux interférences. En effet, les perturbations peuvent n'affecter qu'une à quelques sous-porteuses, et non pas l'ensemble de la transmission. De plus la problématique des multitrajets est réduite, par introduction de codes de redondances.

En OFDM, le risque d'interférence entre symboles, qui pourrait arriver en même temps au récepteur, par le biais de chemins différents (multipath) est multiplié. Ainsi, un délai d'attente est respecté entre deux envois. Appelé "Guard Interval" (GI), cette temporisation est de 0,8 s (800 nanosecondes) en 802.11a et 802.11g. Si l'environnement le permet, ce paramètre peut être réduit à 0,4 s en 802.11n draft. Ainsi, le temps total d'envoi du symbole, incluant le GI passe de 4 s à 3,6 s, ce qui augmente encore un peu plus le débit possible.

b. Fonctionnement et débits

Dans l'application des standards 802.11a et 802.11g, le canal est divisé en 52 sous-porteuses de 312.5 KHz chacune. Parmi celles-ci, 48 sont utilisées pour transférer les données. Les autres servent à la synchronisation et aux corrections associées.

Le principe de sous-porteuses est utilisé pareillement pour 802.11n draft. Par contre, jusqu'à 4 émissions simultanées décalées peuvent être envoyées en même temps grâce au MIMO. Avec l'adoption de l'agrégation sur 2 canaux (40 MHz), on conçoit que les gains en débit peuvent être très importants.

5. MIMO (Multiple Input Multiple Output)

Cette technologie est le cœur du 802.11n, qui propose d'utiliser jusqu'à quatre flux radio simultanés. Elle allie différentes techniques qui améliorent considérablement les capacités du signal. Comme la multiplication des flux transmis augmente la consommation électrique, un mode d'économie d'énergie (*Power Save Mode*) a été défini. Il stipule que ces techniques ne seront utilisées que si cela est nécessaire.

a. Multiplexage et diversité spatiale

L'utilisation de plusieurs antennes émettrices/réceptrices est déjà courante en Wi-Fi. Leur exploitation en diversité permet la sélection du meilleur flux reçu sur l'une ou l'autre. Ceci permet, en intérieur, d'augmenter les chances de recevoir un signal, et donc d'éviter de devoir le ré-émettre.

Utiliser plusieurs antennes permet également d'envisager un multiplexage des données (SDM - *Spatial Diversity Multiplexing*). Ainsi, MIMO se permet d'envoyer à chaque antenne des informations différentes, en utilisant des sous-porteuses OFDM. Utilisant les réflexions inévitables du signal en intérieur, la technique de diversité spatiale (spatial stream) augmente l'efficacité de réception du signal et le débit global de la communication.

Cette technique est plus efficace quand le nombre de récepteurs est supérieur au nombre d'émetteur. Par exemple, si une carte réseau d'ordinateur ne possède que deux antennes, elle peut émettre deux flux. En réception, un point d'accès équipé de trois antennes pourra reconstituer simultanément les deux flux.

b. Transmit Beam Forming

Ici, un signal est déphasé, et ces composantes émises à partir de plusieurs antennes, deux par exemple. Il résulte de ce déphasage une augmentation de la puissance du faisceau, qui exploite plus facilement les contraintes d'obstacle. Une seule antenne de réception reconstitue le signal initial à partir de ces composantes. Cette technique complète donc la précédente.

Il n'est pas possible d'entendre de telles transformations pour des signaux de diffusion (broadcast) ou multidiffusion (multicast), ce qui réduit l'intérêt de la technique.

c. Space Time Bloc Code (STBC)

Pour que les techniques précédentes augmentent réellement les vitesses de transmission, il est nécessaire d'améliorer la robustesse du signal. En effet, la ré-émission d'une trame mal reçue est pénalisante pour le débit global. Le système STBC fiabilise la transmission par introduction d'une redondance, en conjuguant l'inverse des trames, tout en utilisant les antennes multiples.

Encodage et modulation

Les différentes spécifications 802.11 recommandent donc trois moyens d'étalement de spectre pour la transmission des informations. Et, en fait, seuls DSSS et OFDM sont utilisés, qui encodent en utilisant un chipping.

Des séries plus ou moins longues de 0 et de 1, vont donc qualifier un bit informatique. Ces codes ne doivent pas permettre de longues suites de 0 ou de 1. Ils doivent être suffisamment longs pour autoriser une tolérance d'erreur importante. Mais il n'est pas incompatible d'essayer de peaufiner une telle technique pour gagner en débit.

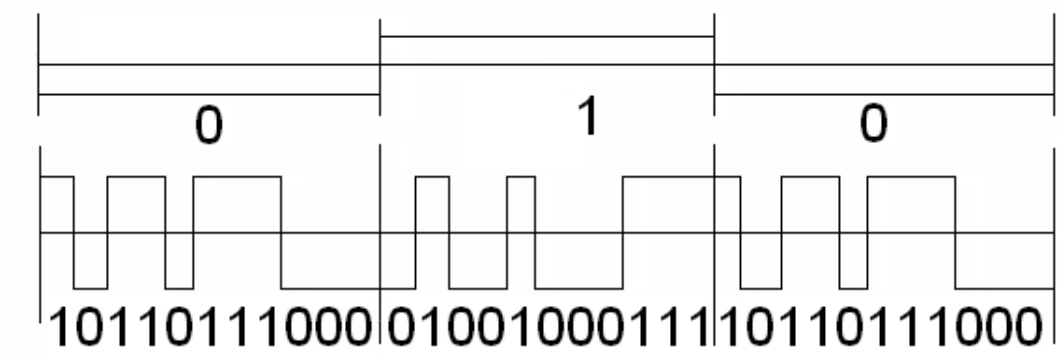
Il ne reste ensuite plus qu'à définir les types de modulations utilisées, afin de reconnaître les 0 et les 1. L'augmentation de la valence, déjà abordée dans le deuxième chapitre, permet, là encore de gagner de la vitesse de transmission.

1. Étalement du signal par chipping

a. La séquence Barker

Les spécifications 802.11 et 802.11b précisent que l'étalement du signal DSSS à 1 et 2 Mbps utilise une série de 11 caractères pour définir un bit de données. Le code d'étalement fait partie d'une série définie par le mathématicien Barker dans les années 50. Ces codes allient de bonnes facultés d'étalement de spectre et de synchronisation entre l'émetteur et le récepteur.

La séquence Barker utilisée en Wi-Fi vaut : 10110111000. Ce code est appliqué par un calcul XOR, au bit à transmettre. Ainsi, le 0 est encodé comme 10110111000 et le 1 comme chip inverse, 01001000111.



Exemple d'encodage par code Barker, sur 11 bits

b. L'encodage Complementary Code Keying (CCK)

L'étalement de spectre en chipping est amélioré pour les débits supérieurs, par l'encodage CCK. La séquence Barker précédente est très performante en terme de résistance aux interférences. Mais elle a le tort de n'utiliser que 2 niveaux sur les 2048 (2^{11}) possibles sur 11 bits.

CCK définit des symboles sur 8 bits au lieu de 11, soit 256 niveaux potentiels. Bien sûr, il faut tenir compte des aspects codes complémentaires pour les corrections d'erreurs. En fait, au maximum 64 codes sont considérés significatifs avec l'encodage CCK, en utilisant les 8 bits.

Ils permettent, sur les communications de plus courtes distances, des débits de 11 Mbps. Si les conditions ne permettent pas ce fonctionnement, la vitesse rétrograde à 5,5 Mbps, en n'utilisant plus que 4 bits sur les 8 du code.

2. Modulations

a. La modulation Gaussian Frequency Shift Keying (GFSK)

L'étalement de spectre FHSS utilise une modulation en fréquence dans laquelle les niveaux significatifs sont des fréquences décalées de la porteuse de base.

À 1 Mbps, l'utilisation du 2-GFSK (*Gaussian Frequency Shift Keying*) stipule un décalage de plus ou moins la moitié

d'une valeur fixée 320 KHz. Le signal varie donc entre :

- + 160 KHz de la fréquence centrale pour la valeur 1 ;
- - 160 KHz de la fréquence centrale pour la valeur 0.

À 2 Mbps, 2 bits sont transportés par symbole. Cette modulation 4-GFSK est basée sur un décalage de 144 KHz, avec des multiplicateurs d'écart correspondant à 1/2, -1/2, 3/2 ou - 3/2, soit des décalages de :

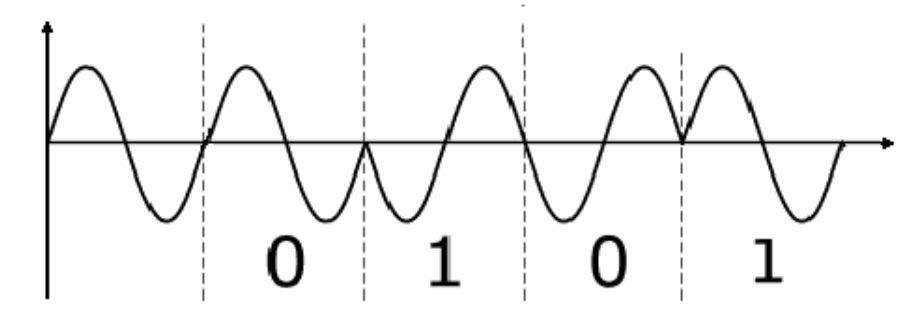
- - 216 KHz de la fréquence centrale pour 00 ;
- - 72 KHz de la fréquence centrale pour 01 ;
- + 216 KHz de la fréquence centrale pour 10 ;
- + 72 KHz de la fréquence centrale pour 00.

Un filtre Gaussien est appliqué au signal carré numérique, afin de rendre moins brutales les transitions et d'avoir une modulation qui se rapproche plus de la forme sinusoïdale.

b. Les modulations Differential Phase Shift Keying (DPSK)

Differential Binary Phase Shift Keying (DBPSK)

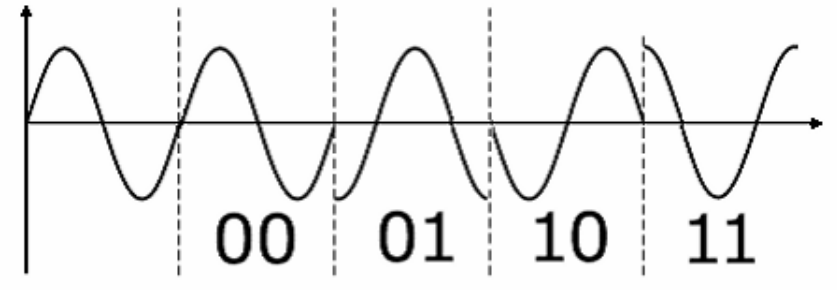
Cette première modulation de phase est utilisée dans les bas débits, c'est-à-dire le 1 Mbps du 802.11b ainsi que les 6 et 9 Mbps des 802.11g et 802.11a. Pour un 0, il n'y a pas de modification de phase de la porteuse. Le 1 est indiqué par un décalage de 180°.



Exemple de modulation DBPSK

Differential Quadrature Phase Shift Keying (DQPSK)

Comme nous l'avons vu précédemment, la quadrivalence permet le codage de 2 bits par impulsion de la porteuse. Ici, le décalage de phase est de 4 valeurs : 0 (00), 90° (01), 180° (10) et 270° (11).

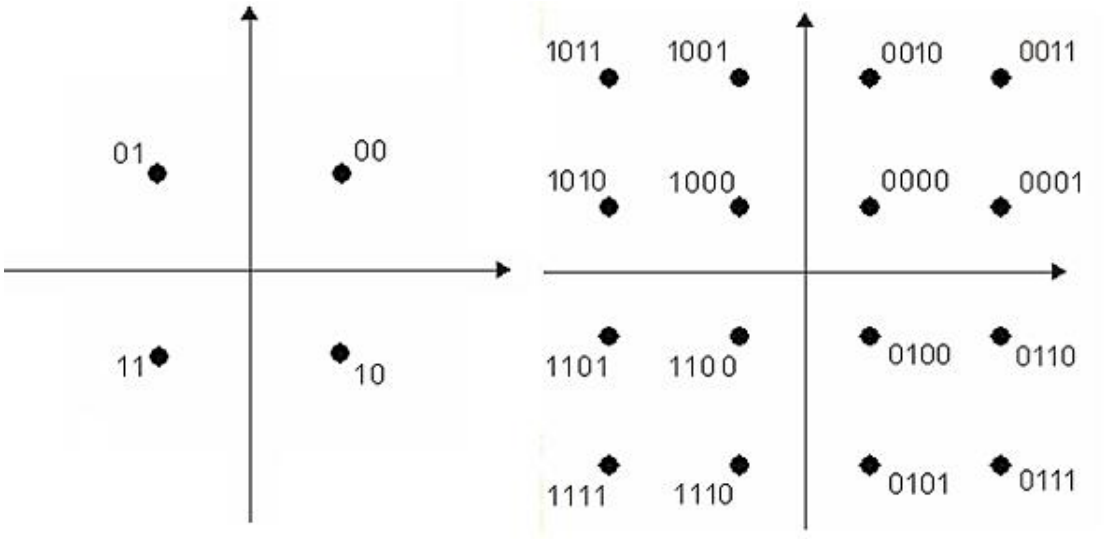


Exemple de modulation DQPSK

Cette modulation est utilisée pour les débits supérieurs de 802.11b, 5,5 et 11 Mbps, ainsi que pour ceux à 12 et 18 Mbps des 802.11g et 802.11a.

c. La modulation de type Quadrature Amplitude Modulation (QAM)

La combinaison des modulations d'amplitude et de phase se retrouve dans les débits supérieurs des standards 802.11g et 802.11a.



Rappel : modulation 16 QAM à gauche et 64 QAM à droite

3. Signal en fonction des spécifications IEEE

Les spécifications 802.11b ne proposent que des débits peu élevés. Le traitement sur le signal radio n'est pas poussé.

Vitesse	Transmission	Encodage	Modulation
1 Mbps	DSSS	Barker sequence	DBPSK
2 Mbps	DSSS	Barker sequence	DQPSK
5,5 Mbps	DSSS	CCK	DQPSK
11 Mbps	DSSS	CCK	DQPSK

Caractéristiques des transmissions 802.11b

La mise en œuvre de 802.11g et 802.11a demande, par contre, un multiplexage par OFDM systématique. Plus le débit s'élève, plus la modulation est travaillée.

Vitesse	Transmission	Encodage	Modulation
6 et 9 Mbps	Multiplexage OFDM	CCK	DBPSK
12 et 18 Mbps	Multiplexage OFDM	CCK	DQPSK
24 et 36 Mbps	Multiplexage OFDM	CCK	16 QAM
48 et 54 Mbps	Multiplexage OFDM	CCK	64 QAM

Caractéristiques des transmissions 802.11g et 802.11a

802.11n est compatible avec 802.11b, g et a. Son fonctionnement natif nécessite l'usage du multiplexage OFDM, un encodage CCK 5/6 et une modulation 64 QAM. Les différents débits sont obtenus, comme pour les autres standards, par combinaison de ces paramètres auquels nous devons désormais ajouter le nombre de flux en diversité spatiale et la valeur de l'élément Guard Interval (GI). Il est délicat de déjà détailler ces seuils, alors que la spécification n'est pas définitive. Le tableau ci-dessous ne présente donc que les extrêmes, qui peuvent être retrouvées dans les fiches techniques des constructeurs de matériel.

	20 MHz - GI = 0,8 µs	40 MHz - GI = 0,8 µs	20 MHz - GI = 0,4 µs	40 MHz - GI = 0,4 µs
Minimum	6.5 Mbps	13.5 Mbps	7.2 Mbps	15 Mbps
Maximum	130 Mbps	270 Mbps	144.4 Mbps	300 Mbps

Exemples de débit du 802.11n draft

En-tête et préambule de couche physique

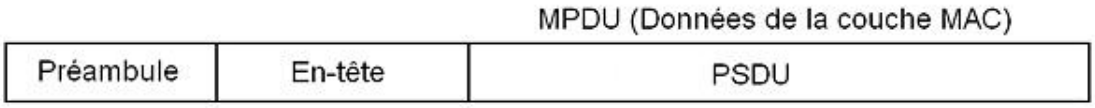
Au-dessus de la sous-couche Physical Medium Dependent (PMD) présentée précédemment, celle nommée Physical Layer Convergence Protocol (PLCP), procédé de convergence de la couche physique, assure plutôt une tâche informatique.

Avant transmission à PMD, elle encapsule les trames en provenance de la sous-couche MAC, nommée MAC Protocol Data Unit (MPDU), en y ajoutant un préambule et un en-tête. En réception, elle interprète ces informations supplémentaires, avant de fournir à la couche Liaison de données les MPDU.

Ces actions transforment les successions de bits. Ce contenu de sous-couche PLCP est nommé PHY Protocol Data Unit (PPDU). Les données transportées, MPDU, peuvent également être qualifiées, dans les spécifications 802.11x, de PLCP Service Data Unit (PSDU).

1. Constitution de la sous-couche PLCP

Dans les spécifications, la sous-couche PLCP est constituée de trois parties. Un en-tête et un préambule encapsulent le PSDU.



La sous-couche PLCP

Le préambule est toujours transmis à la vitesse de 1 Mbps.

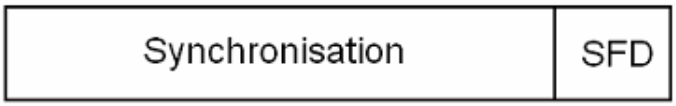
En DSSS, l'utilisation de préambule et en-tête réduits (*short preamble and header*) est possible. Dans ce cas, la contenance de la première partie est réduite. La deuxième partie reste de même taille mais est transmise à 2 Mbps au lieu de 1 Mbps. Une telle possibilité est prévue en OFDM, mais de forme un peu différente.

Cette option permet d'améliorer la bande passante générale. Pour être utilisée, elle doit être prise en charge et configurée sur l'émetteur comme sur le récepteur. Elle ne peut être utilisée avec le débit de 1 Mbps.

2. Préambule

De différentes longueurs, en fonction des spécifications et de son état long ou court, le préambule est basiquement composé de deux champs :

- Preamble Synchronization (SYNC) ;
- Start Frame Delimiter (SFD), toujours sur 16 bits.



Structure du préambule PLCP pour 802.11, 802.11b et 802.11g

En 802.11, le champ de synchronisation est une alternance de valeurs binaires, commençant par 0 et terminant par 1. Il permet à un récepteur la détection du signal et sa comparaison entre les antennes en diversité, avant synchronisation réelle. L'OFDM compose le préambule de douze symboles prédéfinis.

Le début de trame est indiqué dans le SFD. Des séquences différentes sont utilisées en fonction de la spécification.

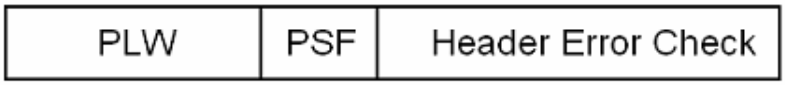
Après analyse de ce préambule, le récepteur s'est donc synchronisé avec l'émetteur. Il a également choisi son antenne de réception, s'il travaille en diversité, et connaît quel standard est utilisé pour la transmission.

3. En-tête PLCP

Plusieurs en-têtes sont définis. Dans les spécifications 802.11, il comporte trois champs :

- PSDU Length Word (PLW), sur 12 bits, soit 4095 valeurs possibles, informe du nombre d'octets du PSDU ;
- PLCP Signaling Field (PSF), sur 4 bits donne le débit du PSDU ;
- Header Error Check (HEC), sur 16 bits, est un code de signalement d'erreur par contrôle de redondance cyclique (CRC - *Cyclic Redundancy Code*).

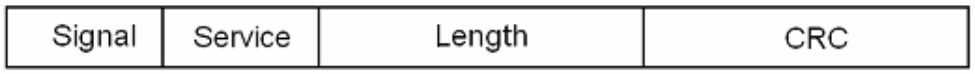
Le point de départ du calcul de CRC, dont le résultat sur 16 bits est ajouté dans le champ HEC, est un polynôme générateur de 17 bits, dont la valeur binaire est connue : 10001000000100001. Un calcul est effectué à partir de ce polynôme et des bits à vérifier, puis le résultat est ajouté dans le champ adéquat. Les mêmes opérations sont refaites par le destinataire, qui compare le résultat. Le système est conçu pour repérer toutes les erreurs réparties aléatoirement, ainsi que toutes celles en série de longueur inférieure à 17 bits. La plupart des rafales d'erreurs supérieures ou égales à 17 bits peuvent également être signalées.



En-tête 802.11

Cet en-tête est modifié par les spécifications suivantes, dans lesquelles il contient quatre champs distincts :

- Signal, sur 8 bits, indique le débit du PSDU ;
- Service, sur 8 bits, précise les spécificités de transmission, d'encodage et de modulation ;
- Length, sur 16 bits, donne la longueur du PSDU ;
- CRC, sur 16 bits, est un code correcteur d'erreur.



En-tête 802.11b et 802.11g

L'en-tête 802.11a est plus complexe, mais les informations données sont globalement les mêmes.

La réception de cet en-tête permet de connaître précisément à quel débit, voire selon quelles caractéristiques de transmission, seront ensuite reçues les données de la couche MAC, MPDU. Le récepteur sait désormais combien il peut en attendre et a pu vérifier l'exactitude de ces informations par le code CRC.

Caractéristiques principales

La couche Liaison de données du modèle OSI est constituée, comme celle au-dessous, de deux sous-couches. Celle de partie haute est le standard IEEE 802.2, Logical Link Control (LLC), contrôle de la liaison logique. Elle permet aux protocoles de couche Réseau, quels qu'ils soient, de toujours reposer sur un même socle et de rester indépendants des spécificités physiques. Son étude complète, puisqu'elle ne comporte pas de spécificités dans son utilisation par le Wi-Fi, ne sera pas effectuée dans cet ouvrage.

La partie basse de la couche Liaison de données est la sous-couche Medium Access Control (MAC), contrôle de l'accès au média. Il s'agit du cœur d'un réseau 802.11. L'essentiel du fonctionnement de ce type de réseau sans fil fait appel à ses fonctionnalités.

La première tâche du niveau MAC est la gestion du média, ou plutôt de l'absence de média physique, caractérisé par une fréquence radio. Elle doit être partagée entre les différents nœuds du réseau Wi-Fi. Chacun possède une adresse qui lui est propre, comme dans Ethernet.

Les amendements 802.11e et 802.11n draft font évoluer la couche MAC d'origine, en y apportant des notions qualité de service et d'optimisation des communications.

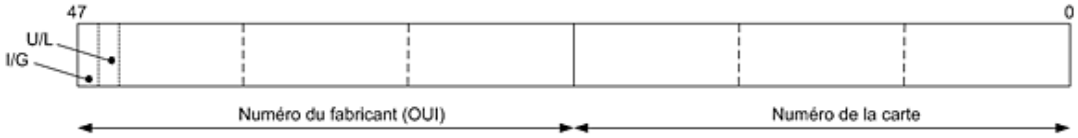
1. Adressage

Les adresses MAC des cartes 802.11 possèdent les mêmes caractéristiques que celles Ethernet. Cet identifiant est numéroté sur 48 bits, soit 6 octets. Les 24 premiers, le Organizationally Unique Identifier (OUI), désignent le fabricant du matériel. Les 24 suivants sont assignés à la carte et doivent être uniques sur le réseau.

Lors de sa transmission, une trame contient au moins l'adresse de l'émetteur et celle du destinataire. Ces valeurs sont contenues dans des champs spécifiques de l'en-tête MAC. Si cette information est destinée à un récepteur unique, elle est qualifiée de "unicast". Envoyée à un groupe de nœuds, elle est appelée "multicast", ou multidiffusion. Si tout le monde est destinataire, la transmission est de type "broadcast", ou diffusion.

Les deux bits de poids fort de l'adresse MAC de destination, permettent de différencier ces types de communication. Le premier précise si l'adresse est individuelle ou de groupe (I/G). Le second indique si elle est universelle ou locale (U/L). Les trois combinaisons exploitées de ces bits sont :

- I/G= 0 et U/L= 0 pour unicast ;
- I/G= 0 et U/L= 1 pour multicast ;
- I/G= 1 et U/L= 1 pour broadcast.



Format d'une adresse physique, ou adresse MAC

2. Types de trames

Les spécifications 802.11 définissent trois types de trames de couche MAC. Celles de gestion servent à l'authentification des équipements et leur incorporation dans le réseau. Le partage du média est pris en charge par les trames de contrôle. Le transport effectif des informations provenant des couches supérieures est réalisé par celles de données.

De manière générique, ces séries de bits mis en forme sont qualifiées de MAC Service Data Unit (MSDU). Les trames de gestion possèdent l'appellation spécifique de MAC Management Protocol Data Unit (MMPDU).

Les principales contraintes auxquelles sont confrontées les trames de contrôle lors des communications sont l'absence de média de transport et donc de limitation d'espace.

3. Qualité de service

La couche MAC originelle des spécifications 802.11 ne permet pas d'introduire dans les flux une qualité de service (QoS - *Quality of Service*). Elle est pourtant nécessaire pour les transports de la vidéo et de la voix. En effet, la réception de données peut s'effectuer dans le désordre et avec du retard, pas pour ces autres flux, qui doivent être prioritaires.

L'amendement 802.11e, approuvé en septembre 2005, apporte ces fonctionnalités en ajoutant à la couche MAC les extensions indispensables. Quand elles sont utilisées, le réseau est dit QBSS (*QoS Basic Service Set*). Cet acronyme qualifie une communication entre une station QSTA (*QoS Station*) et un point d'accès QAP (*QoS Access Point*).

La communication sur un réseau QBSS met en œuvre des trames MAC modifiées et des modes d'accès au média spécifiques. Le transport des informations qui s'effectue au mieux (BE - *Best Effort*) devient contrôlé par un identifiant de trafic (TID - *Traffic Identifier*).

Les 8 niveaux de classe de trafic (TC - *Traffic Category*) qualifient une trame dite UP (*User Priority*). Ils sont repérés par des entiers, de 0 à 7, identiques aux priorités de l'algorithme spanning tree (IEEE 802.1d). Ils sont mis en correspondance avec quatre catégories (AC - *Access Category*). Plus le UP est haut, plus le niveau de priorité l'est.

UP	AC	Type
1	AC_BK	Arrière-plan
2	AC_BK	Arrière-plan
0	AC_BE	Au mieux
3	AC_BE	Au mieux
4	AC_VI	Vidéo
5	AC_VI	Vidéo
6	AC_VO	Voix
7	AC_VO	Voix

Correspondance UP et AC

L'émetteur exploite une file d'attente par catégorie. Elle est vidée par ordre de priorité croissante.

Pour accélérer les transmissions, possibilité est donnée à l'émetteur d'émettre une rafale (burst) de trames, durant une période donnée. Cet intervalle de temps, limité, est qualifié de TXOP (*Transmission Opportunity*).

Il faut entendre la qualité de service comme étant une fonction des communications unicast, plus que multicast ou broadcast. Elle est plus délicate à gérer dans ces deux derniers cas.

Bien que nous n'aborderons pas, dans ce chapitre, l'ensemble des évolutions apportées par l'amendement 802.11e, nous reviendrons sur les modes d'accès au média et certaines extensions de la couche MAC.

4. Évitement de collision

Différentes méthodes sont utilisées pour partager l'interface air, support de la transmission d'informations. Contrairement à des réseaux filaires, elles doivent toutes tenir compte de l'impossibilité de détecter une collision entre trames. Les solutions retenues privilégient donc l'évitement de collision.

a. La technique CSMA

Comme nous l'avons vu précédemment, les communications DSSS et OFDM-DSSS utilisent un canal fixé.

Plusieurs méthodes permettent de multiples accès simultanés à un canal donné, par multiplexage. Frequency Division Multiple Access (FDMA) joue sur une répartition des fréquences. Elle est surtout destinée aux réseaux analogiques. Time Division Multiple Access (TDMA) partage la porteuse en intervalle de temps. Code Division Multiple Access (CDMA), utilisée en téléphonie mobile, attribue un code à chaque communication.

Dans les spécifications 802.11 une seule communication à la fois est gérée. Pour cela, la méthode Carrier Sense Multiple Access (CSMA) impose une écoute préalable du canal. S'il est occupé, la tentative d'émission est retardée. En cas de faible charge du réseau, cette méthode allonge les délais de transmission. Par contre, elle est très efficace si un certain nombre d'équipements doivent se partager la bande de fréquence. Cette gestion devient à nouveau problématique avec l'augmentation du nombre de tentatives de communication.

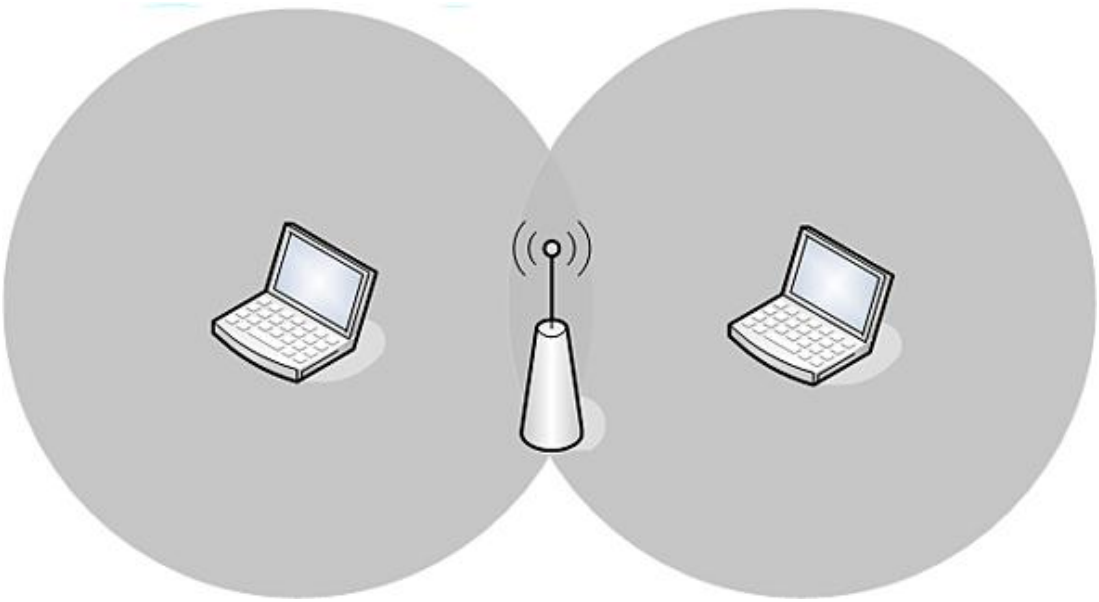
Plus précisément, quand une station souhaite communiquer, elle écoute d'abord le média. S'il est libre, elle attend quelques instants de silence. Cette période d'attente possède une durée maximale, appelée Contention Window (CW). Elle est composée d'un paramètre fixe additionné à un autre, aléatoire. Si, durant ce temps, aucune communication n'a été déclenchée, elle commence à émettre. Sinon, elle recommence complètement le processus d'attente.

b. Le mécanisme CSMA/CA

La technique CSMA précise la marche à suivre avant émission. Mais deux stations pourraient quand même choisir d'émettre strictement en même temps. L'injonction du paramètre aléatoire dans la période d'attente permet de réduire encore ce risque, mais il existe.

Ethernet ajoute à l'écoute initiale un mécanisme de détection de collisions. Nous avons vu que cela n'est pas fiable pour les transmissions hertziennes. D'autant plus que les interfaces d'accès Wi-Fi, communiquant en half-duplex, ne permettent pas une émission et une écoute simultanées.

La communication en mode infrastructure présente un cas particulier qui, de toute façon, ne permet pas d'envisager de tenir compte des collisions. En effet, imaginons deux stations placées de telle sorte que la cellule de l'une ne recouvre pas l'autre. Si la première transmet une trame au point d'accès commun, l'autre ne l'entendra pas. Le point d'accès pourrait donc couramment recevoir plusieurs trames en même temps.



Problématique de la station cachée

Ainsi, le partage du média inclut une gestion d'évitement des collisions (CA - *Collision Avoidance*), obligeant une station à n'émettre que lorsqu'elle en possède l'autorisation exclusive.

c. L'allocation et l'acquittement

Lorsqu'une station peut bénéficier du média, elle émet donc. Par contre, non seulement il n'est pas question qu'elle monopolise la parole pendant un temps indéfini, mais il peut être intéressant de bloquer une écoute inutile des autres stations durant une transmission.

Un système de temporisation, le Network Allocation Vector (NAV), est donc utilisé. Cette information est renvoyée avec l'autorisation de prise de parole, à la station souhaitant émettre. Comme les autres sont également en écoute, elles sont informées que le média a été réservé pour la durée spécifiée.

Chaque trame de données émise doit être acquittée par le récepteur. Pour cela, une trame de contrôle Acknowledge (ACK) est systématiquement renvoyée.

5. Partage du média

a. Le mode centralisé DCF

Le mode de partage du média par défaut, défini dans les spécifications 802.11 et suivantes, est une fonction de contention : Distributed Coordination Function (DCF). Cette fonction de coordination distribuée est une version du CSMA/CA.

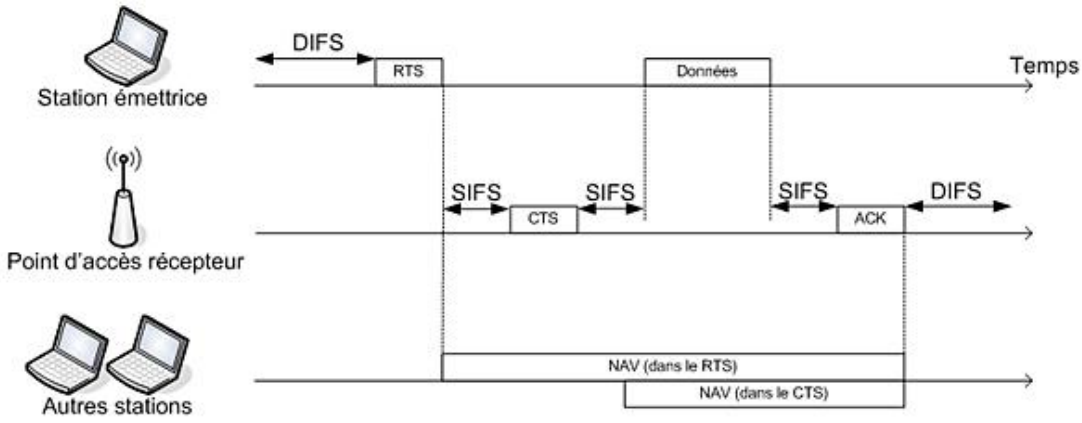
Le DCF peut être utilisé dans les réseaux de type ad hoc comme infrastructure. Son implémentation est obligatoire dans les équipements Wi-Fi.

Comme dans CSMA, une station souhaitant prendre la parole attend d'abord un temps, appelé Distributed Inter Frame Space (DIFS). Il comprend une durée fixe additionnée à un complément aléatoire. Si le silence a été vérifié tout au long de cette période, la station envoie au récepteur une demande de réservation. Cette courte trame de contrôle est nommée Request To Send (RTS). Entre autres champs, elle contient les adresses MAC de l'émetteur et

du destinataire. Elle fournit également un champ d'estimation du temps que prendra l'émission des données, pour le NAV, en micro-secondes.

Après un bref délai, qualifié de Short Inter Frame Space (SIFS), le récepteur renvoie une trame de contrôle Clear To Send (CTS), acceptant ainsi la transmission. Un peu plus courte que RTS, elle contient, elle aussi, les adresses et le champ de durée.

L'émetteur ayant reçu l'acceptation attend finalement une période de temps SIFS, puis il envoie les trames de données. À chacune, il recevra un acquittement ACK.



Le dialogue basique de couche MAC

La durée de l'intervalle de temps minimal à attendre entre deux trames SIFS est définie par l'IEEE.

Standard	Temps SIFS
802.11	28 µs
802.11b	10 µs
802.11a	16 µs
802.11g	10 µs

Durées du délai SIFS

Le paramètre SIFS est additionné à une valeur "SlotTime" pour donner le DIFS.

Standard	SlotTime	Temps DIFS
802.11	50 µs	78 µs
802.11b	20 µs	30 µs
802.11a	9 µs	25 µs
802.11g long	20 µs	30 µs
802.11g court	9 µs	19 µs

Durées du délai DIFS

Ce fonctionnement n'est utilisé que pour les trames à destination unicast. En effet, les types multicast et broadcast n'utilisent ni RTS, ni CTS, ni ACK. Dans une communication en mode infrastructure, une station s'adresse toujours à un point d'accès, donc en unicast, même si ce dernier peut ensuite diffuser l'information.

On peut comprendre qu'un tel fonctionnement provoque de grosses pertes de débit dues à ces échanges de trames de contrôle. Par contre, il reste simple à l'usage.

Comme le risque de collision n'est souvent pas très élevé, il est possible de configurer, sur les équipements, une taille de trames au-dessous de laquelle le mécanisme RTS/CTS n'est pas utilisé. Ce paramètre est nommé RTS Threshold. Il est même parfois utile de supprimer purement et simplement ces dialogues.

b. Le mode distribué PCF

La méthode précédente, DCF, est non déterministe. En effet, une station ne peut pas prévoir quand elle pourra

prendre la parole. L'utilisation du mode Point Coordination Function (PCF) permet de pallier à cet inconvénient, pour la transmission de données synchrones, telles que vidéo et voix.

PCF nécessite l'utilisation d'un point d'accès, qui tiendra le rôle de coordinateur (PC - *Point Coordination*). Il doit lui-même pouvoir se considérer comme client du réseau.

Pour éviter les collisions, le coordinateur distribue successivement la parole aux stations associées. Ce fonctionnement centralisé par interrogation (polling) est qualifié de Contention Free (CF) dans les spécifications.

L'allocation d'un temps de parole à un client est distribuée par une trame de contrôle CF-Poll. Si elle souhaite exploiter cette période, la station renvoie une trame CF-ACK. Sinon, au bout d'un temps PCF Inter Frame Space (PIFS), la distribution continue.

PCF n'est pas obligatoirement pris en charge par les équipements, contrairement à DCF. Leur coexistence est donc nécessaire. En fait, le point d'accès coordinateur alterne entre deux périodes :

- Contention Free Period (CFP), utilisant le mode PCF ;
- Contention Period (CP, avec le mode DCF.

Afin de mêler correctement ces deux modes, le temps PIFS est plus court que DIFS. Ainsi, si une station ne reconnaît pas les trames d'interrogations, elle ne détectera pas de silence assez long durant cette période CFP. Elle est ainsi obligée d'atteindre la période de contention.

Comme SIFS, le paramètre PIFS est calculé par rapport à la valeur "SlotTime". Par contre, il est additionné à 2 fois cette valeur.

Standard	SlotTime	Temps PIFS
802.11	50 µs	128 µs
802.11b	20 µs	50 µs
802.11a	9 µs	34 µs
802.11g long	20 µs	50 µs
802.11g short	9 µs	28 µs

Durées du délai PIFS

On constate qu'une bonne partie de la bande passante est gâchée pour la gestion du fonctionnement. Le temps SIFS atteint des valeurs qui peuvent vite être non négligeables dans le cas où beaucoup de stations sont associées au réseau du point d'accès.

Concrètement, beaucoup d'équipements n'incluent pas un tel fonctionnement, bien qu'il ait été prévu dès le standard 802.11 d'origine.

c. Les bases de temps

Pour utiliser les temps SIFS, DIFS et PIFS, une base commune entre les composants du réseau est nécessaire. Cette synchronisation est apportée par une trame spécifique de balise (beacon frame) qui sera détaillée plus loin.

Dans un réseau d'infrastructure, le point d'accès sert de référence. Il envoie généralement 10 trames de balise par seconde. Celles-ci contiennent une copie du compteur d'horloge interne du point d'accès. Les stations vont utiliser cette valeur pour réajuster leur horloge.

Dans un réseau de type ad hoc, ce sont les stations qui émettent, à tour de rôle, une trame de balise contenant ses informations.

d. Les évolutions EDCA et HCCA

Le partage du média avec les modes DCF et PCF ne permet pas de prévoir l'allocation du temps de paroles, ce qui est pourtant nécessaire aux exigences QoS.

Deux nouveaux modes, utilisables indépendamment des standards de "communication", 802.11g, ou 802.11n draft par exemple, sont ajoutés. Ils sont basés sur une fonction de coordination baptisée HCF (*Hybrid Coordination Function*), elle-même extension des modes DCF et PCF.

HCF (Hybrid Coordination Function)

Toutes les communications ne nécessitent pas un partage d'accès au média imposant QoS. La fonction HCF permet

de combiner différentes périodes de transport. Elle alterne donc entre les deux modes "Best Effort" DCF et PCF et les deux nouveaux "QoS".

Après avoir obtenu l'accès au média, la station peut le conserver. Ainsi, elle peut émettre un certain nombre de trame, durant un laps de temps donné (TXOP - *Transmission Opportunity*). Cette information est reçue par la station dans une trame de balises.

Enhanced Distributed Channel Access (EDCA)

Ce premier mécanisme également appelé Contention-based Channel Access est équivalent au mode DCF. Le délai DIFS avant prise de parole est désormais qualifié d'Arbitration Inter Frame Space (AIFS). Sa durée est au moins égale à son prédécesseur.

Pour rendre un paquet prioritaire, il est associé à une valeur d'AIFS plus courte. Chaque AIFS est associé à une fenêtre de contention (CW - *Contention Window*) spécifique.

La Wi-Fi Alliance a associé une certification à ce fonctionnement : Wi-Fi Multimedia (WMM). Il n'y a donc pas de certification associée à 802.11e dans son ensemble, mais seulement au mode EDCA.

HCF Controlled Channel Access (HCCA)

Ce mode est une amélioration du PCF. Ici l'autorisation d'émettre est distribuée par un coordinateur hybride (HC - *Hybrid Coordinator*), typiquement le point d'accès. Les classes de trafic (TC) sont également utilisées.

L'alternance du PCF entre les différentes périodes est maintenue. Durant la phase Contention Period (CP), les stations fonctionnent en mode EDCA. Par contre, la phase Contention Free Period (CFP) est transformée en Controlled Access Phase (CAP), période de temps durant laquelle le HC garde le contrôle du support.

Ce dernier prend l'initiative de passer en période CAP, lorsqu'il a besoin d'envoyer ou de recevoir des trames. Il garde une mainmise permanente sur la circulation du trafic. Par exemple, durant une phase EDCA, les stations lui envoient l'état de leur file d'attente, par classe de trafic. Il choisira ensuite d'autoriser une émission, en fonction des informations collectées précédemment.

La possibilité d'envoi d'informations par une série TXOP est conservée.

Ce fonctionnement autorise une grande précision dans la gestion de la qualité de service. Le point d'accès HC doit pouvoir gérer au moins plusieurs des 8 classes de trafic possibles. Pour autoriser une station à émettre, il peut non seulement tenir compte de cette classe, mais également de la longueur de la file d'attente de chacune sur le client. D'autres critères de choix sont, par exemple, d'éviter l'accumulation des temps de parole sur une station ou de réguler le débit, en évitant les à-coups (jitter).

Le mode HCCA est de mise en œuvre complexe, pour un apport finalement pas si évident. Il est peu utilisé.

Fonctions de la couche MAC

La gestion du partage de bande passante n'est pas la seule exploitation de la couche MAC, loin de là. Avant d'émettre des données vers un point d'accès, une station doit être connectée au Basic Service Set (BSS), réseau de l'équipement maître. Un processus d'association est auparavant nécessaire. Et avant cela, une authentification de la station peut être demandée par le point d'accès.

D'autres problématiques sont également prises en compte à ce niveau. La fragmentation/défragmentation des trames transmises, ainsi que la capacité à communiquer à différents débits sont gérées. Les contrôles d'erreur et les économies d'énergie ne sont pas, non plus, oubliés. La sécurisation peut être également gérée au niveau de la couche MAC. Mais elle reste un sujet tellement important qu'elle nécessitera un traitement particulier.

Les amendements 802.11e et 802.11n draft ont entraîné quelques modifications de la couche MAC, tant au niveau du format de l'en-tête que de son contenu.

1. Association au réseau

a. Les trames de balises

Nous avons vu plus haut que les trames de balises (beacon frames) diffusent des informations à intervalles réguliers. Toutes les 100 millisecondes par défaut, les points d'accès émettent une telle trame. Les stations de travail prennent elles-mêmes en charge ces trames de balises dans les réseaux de type ad hoc, les unes après les autres.

Dans ce dernier cas, chaque poste du réseau maintient un décompte aléatoire entre deux trames de balises. Le premier arrivant à échéance de ce compteur en émet une. Tous les compteurs reprennent ensuite ce cycle.

D'origine, les trames de balises contiennent 21 informations possibles, plus un dernier élément réservé à des fonctions constructeur. L'adoption de l'amendement 802.11e ajoute 3 nouveaux éléments. Ils permettent au QAP (*QoS Access Point*) d'informer ses clients de la prise en charge de la qualité de service (information QBSS Load) et des capacités associées (informations EDCA Parameter Set et QoS Capability).

Ces trames assurent la synchronisation entre les éléments du réseau (informations TimeStamp et Beacon Interval). Elles peuvent également contenir les débits autorisés sur celui-ci (information Supported Rates).

Une autre donnée importante contenue dans les balises est le nom du réseau Wi-Fi, qui est nécessaire dans toutes les architectures (informations SSID et IBSS Parameters Set). Avant un quelconque échange de données les nœuds doivent être calés sur la même fréquence (*Information Channel Switch Announcement*). Mais ils doivent également être associés au sein d'un même réseau.

Dans l'architecture Independant Basic Service Set (IBSS), formant la configuration ad hoc, les différentes stations associées doivent toutes connaître le nom du réseau avant association. Il doit donc être saisit à la main dans les paramètres de configuration. Si elles possèdent un nom de réseau commun, elles pourront ensuite communiquer.

Dans les architectures structurées Basic Service Set (BSS) et Extended Service Set (ESS), ce sont uniquement les éléments d'infrastructure, pont ou point d'accès, qui émettent des trames de balises. Dans ce cas, le réseau porte le nom de Service Set IDentifier (SSID) et peut y être intégré.

Lorsque la diffusion (broadcast) est activée dans une trame de balises, elle fournit toutes les informations qui permettront ensuite à un client de communiquer sur ce réseau, y compris le SSID. Cette méthode permet à un équipement client Wi-Fi, de se connecter sans configuration prédéfinie. Elle est intéressante pour offrir un accès public à un réseau.

Exemple de champ de saisie de SSID et de choix de sa diffusion, sur un point d'accès de marque Linksys

Il est préférable, dans une configuration privée, de ne pas autoriser la diffusion. Dans ce cas, le SSID n'est pas incorporé dans les trames de balises. Pour se connecter, un client, passera en revue les SSID qu'il connaît, par des requêtes de sondage (probe request), en balayant les différents canaux radio.

Une réponse de sondage (probe response), similaire à celle de balise, pourra être renvoyée par le point d'accès ou le pont. Elle informera la station qu'un réseau qu'elle connaît est disponible.

Les trames de balises contiennent d'autres informations, dont certaines sont spécifiques aux constructeurs.

Après réception de ces trames, ou d'un dialogue sondage/réponse, le canal radio, le nom de réseau et les débits possibles sont connus. Si plusieurs réseaux ont été reconnus, un choix manuel ou par priorité devra être effectué.

De nombreuses autres informations sont également délivrées par ces trames. Après réception, le client dispose de tous les éléments qui lui permettront de s'associer et de communiquer.

b. L'authentification

Lorsqu'elle sait comment elle peut communiquer avec un point d'accès, une station envoie une requête d'authentification à celui-ci. Cette action n'est pas nécessaire dans un réseau IBSS.

Si le point d'accès authentifie la station, celle-ci peut ensuite demander à s'associer au réseau SSID, pour y avoir enfin accès et transmettre des données.

c. Le processus d'association

Association

Cette association est demandée par une trame de gestion. Elle contient les adresses MAC de la station émettrice et du point d'accès auquel la station souhaite s'associer. Elle fournit également ces débits. En retour, l'équipement d'infrastructure lui confirme ou non l'association effective. Si la réponse est positive, la trame de réponse contient un identifiant d'association (AID - *Association IDentifier*) unique. Le client mémorise cette information. Après une dernière confirmation renvoyée au point d'accès, le client fait enfin partie du réseau.

Réassociation et roaming

Comme il est prévu que la station puisse être mobile durant une communication, elle vérifie en permanence la présence d'autres points d'accès de même réseau. Si elle trouve un tel équipement plus proche, voire plus disponible, elle pourra s'y connecter.

Pour effectuer cette action de roaming, une station émet tout d'abord une trame de désassociation auprès du point d'accès maître actuel. Ensuite, elle renvoie une demande de réassociation auprès du nouvel équipement choisi.

Cette trame de gestion contient l'adresse de la station, mais également les références du nouveau et de l'ancien point d'accès. Ces deux derniers se mettent en relation à travers la liaison filaire du système de distribution. Les informations sur la station, ainsi que d'éventuelles données en attente sont ainsi transmises.

Ce processus est complètement transparent pour la communication, qui n'est pas interrompue. Finalement, la station se retrouve associée avec un autre point d'accès.

Désassociation

Une trame de désassociation peut être envoyée par un point d'accès, par diffusion, à toutes les stations.

Lorsqu'elle souhaite quitter un réseau, ou comme nous l'avons vu précédemment, se réassocier, une station émet une telle trame de gestion. Elle informe ainsi le point d'accès, ne demandant pas de réponse.

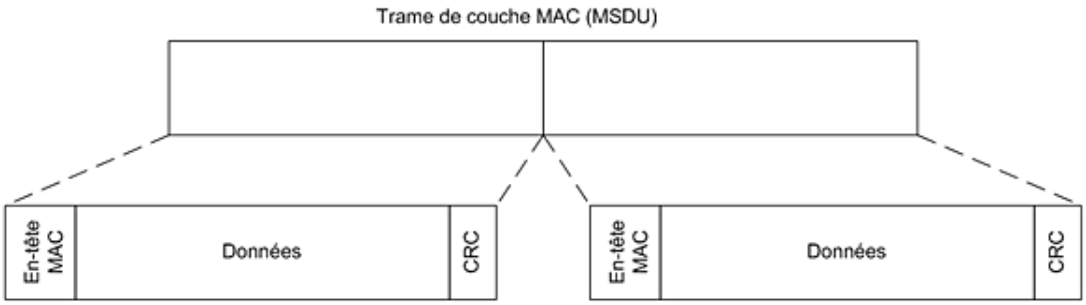
2. Gestion des trames

a. La fragmentation

Afin d'améliorer la qualité générale de la transmission, des opérations de fragmentation/défragmentation des trames peuvent être mises en œuvre. Leur utilisation n'a pas pour but de s'adapter à une technologie différente, mais d'apporter une fiabilisation du transport.

Ainsi, dans les environnements radio très perturbés, une telle opération permet un découpage des trames MAC Service Data Unit (MSDU) et MAC Management Protocol Data Unit (MMPDU) en d'autres plus petites, appelées MAC Protocol Data Unit (MPDU).

La conséquence d'un bit erroné dans une petite trame sera réduite, puisque moins d'informations seront à renvoyer.



Fragmentation d'une trame en deux parties

La trame est donc découpée en portions égales, sauf la dernière qui peut être plus petite. Les fragments composent eux-mêmes une information complète et sont transmis indépendamment les uns des autres. Ils incluent un en-tête qui leur est propre, de taille fixe et contenant :

- le type de trame transportée ;
- les adresses de l'émetteur et du destinataire ;
- le numéro du fragment ;
- un indicateur de dernier fragment.

Ces informations permettront le réassemblage des informations par le destinataire.

Le seuil de fragmentation (*Fragmentation Threshold*) ne doit pas être trop petit. Dans ce cas, une proportion trop faible de données est fournie par trame fragmentée. La valeur par défaut du seuil est 2346 bits, correspondant à la taille maximale de la trame Wi-Fi. Elle peut descendre jusqu'à 256 bits dans des environnements très fortement perturbés.

La prise en charge de la fragmentation est améliorée sur certains équipements, capables de gérer plusieurs trames fragmentées en même temps. Ainsi, la communication n'est pas bloquée en attendant le renvoi de trames erronées. Bien sur, un compteur est également géré, pour ne pas attendre inutilement un fragment qui n'arriverait pas. Le mode rafale (burst) permet l'envoi de tous les fragments dans le même temps de parole, même si le temps alloué doit être dépassé.

Aucune fragmentation des trames de balises, ou des transmissions broadcast et multicast ne peut être réalisée.

b. La variation des débits

En fonction de la spécification 802.11x appliquée lors d'une transmission, plusieurs débits sont possibles au niveau de la couche physique. Selon la distance et les obstacles rencontrés, la vitesse de transmission entre deux équipements peut être variable.

Un mécanisme, géré par un algorithme, permet l'adaptation de cette vitesse, en fonction des conditions de communication. Il permet à un point d'accès, par exemple, d'adapter dynamiquement son débit en fonction du client auquel il s'adresse.

Ces règles sont suivies lors des émissions des trames de gestion et de données. Celles de contrôle doivent être adaptées aux capacités de la station la moins performante associée au point d'accès. Elles circulent donc souvent à 1 Mbps.

Lors de l'envoi d'une trame unicast, l'émetteur connaît les débits possibles du récepteur et s'adapte en conséquence. Pour les trames destinées à de multiples récepteurs, un compromis doit également être trouvé.

c. L'économie d'énergie

Les communications radio sont très gourmandes en énergie. Cette consommation peut être fortement préjudiciable avec l'usage de matériels alimentés par batterie, comme les assistants personnels et ordinateurs portables. En effet, même si, en France, la puissance maximale autorisée est de 100 mW, l'alimentation en continue des équipements Wi-Fi peut diminuer très fortement l'autonomie, déjà très juste de ces appareils.

Il est possible de diminuer la puissance d'usage, souvent au détriment de la qualité de transmission. Cette dernière peut être améliorée par le choix d'une autre antenne, directionnelle ou de gain supérieur.

Mais il s'avère qu'il n'est pas nécessaire d'alimenter électriquement un composant radio en permanence. Les pics de consommation les plus importants se retrouvent lors de l'émission des données. La réception et l'écoute sont toutes deux aussi gourmandes, bien qu'inférieures au premier cas. Une veille peut être possible, qui n'utilise que très peu d'énergie. Un dernier cas reste la possibilité d'éteindre l'adaptateur lorsque aucune communication Wi-Fi n'est souhaitée.

Dès la définition des spécifications 802.11, une capacité d'optimisation de la consommation électrique a été prévue. La couche MAC prévoit donc un mode d'économie d'énergie. En fait deux fonctionnements sont disponibles :

- une alimentation en permanence, Active Mode (AM) ;
- une mise en veille dès que possible, Power Save (PS).

Dans ce dernier mode, l'interface radio est tout simplement éteinte entre deux envois ou réceptions. Le fonctionnement exact dépend du type de réseau, infrastructure ou IBSS.

Dans le premier type, l'envoi régulier de trames de balises (beacon frames) par le point d'accès est utilisé. L'intervalle entre deux trames est connu par les stations, qui se sont synchronisées par elles. Le mode Power Save, permet la mise en veille entre deux réceptions de ces trames de balises. Elles ne peuvent ainsi ni recevoir, ni envoyer, mais leur consommation électrique est très réduite.

Le point d'accès, informé auparavant du fonctionnement de la station en mode PS, sait qu'elle ne peut directement recevoir. Il stocke donc les trames qui doivent lui être adressées. Pour la prévenir de cet état, une information complémentaire, Traffic Indication Map (TIM) est ajoutée à la trame de balise. Jointe à l'identificateur de station, elle lui indique qu'elle doit se positionner en réception. En retour, celle-ci renvoie une trame Power Save Poll (PS-Poll) pour indiquer au point d'accès qu'elle attend. Après réception des informations, elle se remettra en veille.

Si plusieurs stations, attachées au point d'accès, utilisent le mode PS, c'est toute une liste d'identificateurs de stations et de trames en attente qui est jointe à celle de balise.

Un autre indicateur, Delivery TIM (DTIM) informe toutes les stations de se réveiller quand du trafic broadcast ou multicast va être envoyé. Ce paramètre est positionné, en lieu et place du TIM, à intervalle régulier, par exemple toutes les 6 trames de balise.

Lorsque des stations doivent communiquer directement entre elles, dans un réseau de type ad hoc, nous avons vu précédemment qu'elles sont synchronisées par une trame de balise, qu'elles prennent en charge chacune leur tour. Le réveil est donc possible pour l'écouter. Si une station doit émettre en direction d'une autre, elle lui envoie à ce moment un Ad hoc Traffic Indication Message (ATIM) pour lui demander de rester en veille. Pour les trafics à destination de plusieurs stations, le fonctionnement est le même que précédemment.

Ces fonctions d'économie d'énergie sont malheureusement très préjudiciables pour le débit global de transmission, puisque beaucoup de temps peut être perdu entre deux trames de balises. Elles doivent donc être paramétrées sur les postes de travail en fonction des besoins.

Les nécessités de qualité de service sont pénalisées par cette fonction d'économie d'énergie en mode polling. L'amendement 802.11e en décrit une extension de nom Automatic Power Save Delivery (APSD). La Wi-Fi Alliance reconnaît cette fonction sous le nom de WMM Power Save, et le certifie.

IEEE Standard	Security	Multimedia
802.11a	WPA™ - Personal	WMM®
802.11b	WPA™ - Enterprise	WMM Power Save
802.11g	WPA2™ - Personal	
802.11n draft 2.0	WPA2™ - Enterprise	
802.11h		
802.11d	**EAP Type(s)**	
	EAP-TLS	
	EAP-TTLS/MSCHAPv2	
	PEAPv0/EAP-MSCHAPv2	
	PEAPv1/EAP-GTC	
	EAP-SIM	

Extrait d'une certification de matériel, compatible WMM et WMM Power Save

802.11e définit deux mécanismes, Unscheduled APSD (U-APSD) et Scheduled APSD (S-APSD). Le premier est utilisé par une station durant des périodes d'envoi non programmée, le second pour des périodes programmées.

Les matériels ayant nécessité d'utiliser un mode d'économie d'énergie compatible avec la qualité de service mettent généralement en œuvre U-APSD. Il permet à un point d'accès de mémoriser des trames d'un niveau donné, comme la voix, pour ne pas devoir maintenir le client à un niveau de consommation élevé.

La gestion de l'économie d'énergie en 802.11 a beaucoup gagné en complexité. C'est la condition pour que les communications puissent gagner en performances et en capacité, tout en restant adaptées aux ordinateurs portables et périphériques mobiles, y compris les téléphones.

d. La correction d'erreur

Comme les taux d'erreurs prévisibles des transmissions radio sont importants, la couche MAC du 802.11 gère elle-même un contrôle d'erreur, comme sur la couche physique, par un calcul de code de redondance cyclique (CRC), ici sur 32 bits.

Le polynôme utilisé pour le calcul est donc de degré 32 et vaut 100000100110000010011101101101111. L'opération prend en compte tous les autres champs de la trame MAC.

Le même calcul est effectué par le récepteur, qui rejette la trame s'il ne trouve pas le même résultat, supposant que la trame est erronée.

3. Évolutions

La sécurisation de la communication peut également être prise en compte par la couche MAC, en terme d'authentification et de chiffrement. Certaines caractéristiques ont été définies dès le premier standard. D'autres sont venues avec l'évolution majeure que sont les spécifications 802.11i.

L'apparition de la qualité de service implique également une évolution du contenu de la couche MAC.

Les en-têtes MAC ne sont donc pas figés, même si l'essentiel de ses caractéristiques est désormais défini.

La trame MAC

Nous avons donc vu que la couche MAC propose de nombreuses fonctionnalités, à travers des trames de contrôle et de gestion. Toutes, y compris celles de données, doivent être transportées avec l'assurance d'une bonne transmission.

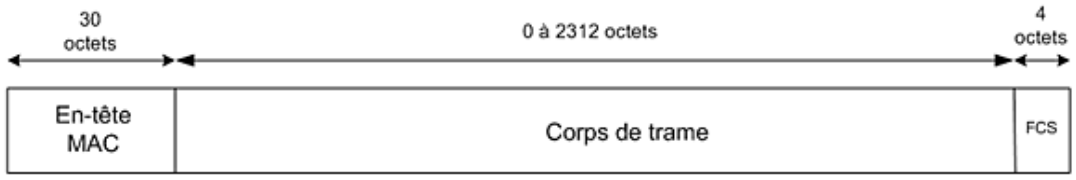
La structure de la trame MAC Service Data Unit (MSDU) est complexe, en rapport avec la richesse des services proposés par cette couche.

1. Structure globale

a. L'agencement

La trame MSDU est composée de trois parties. Celle qui peut avoir la taille la plus importante est le corps de trame (frame body), de longueur variable entre 0 et 2312 octets. Les informations qu'elle contient sont différentes en fonction du type de trame.

Elle est précédée d'un en-tête MAC (Mac Header), qui regroupe toutes les informations utiles à la transmission. Le suffixe est composé d'une séquence de vérification de trame (FCS - *Frame Sequence Check*), calcul CRC sur 32 bits de vérification de bonne transmission.



Format de la trame MAC d'origine

b. L'en-tête MAC

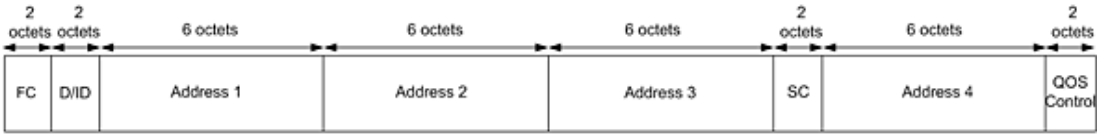
Les trois premiers champs sont systématiquement utilisés. Jusqu'à 4 champs d'adressage sont prévus, dépendamment du contexte.

Les 2 octets du contrôle de trame (FC - *Frame Control*) sont subdivisés en plusieurs champs, détaillés plus loin.

Le champ Durée/ID (*Duration/ID*) a deux utilités. En temps normal, il contient une valeur indiquant la durée d'émission de la trame, en microsecondes, afin de réserver le support pendant toute cette période. Dans les trames Power Save Poll (PS-Poll), sa valeur est l'identifiant de la station (AID - *Association IDentity*), indiquant qu'elle est prête à recevoir en mode d'économie d'énergie.

Le champ de contrôle de séquence (SC - *Sequence Control*) est découpé en deux parties. La première, couvrant les 12 bits de poids faible, donne le numéro de séquence de la trame. Incrémenté d'une unité à chaque fois, il repasse à 0 après 4095. La seconde partie, sur 4 bits, reste à 0 si la trame émise n'est pas fragmentée. Dans le cas contraire, elle contient le numéro d'ordre du fragment.

Le champ de qualité de service (*QoS Control*) n'existait pas dans le standard originel. Il permet la prise en compte de ces capacités.



L'en-tête MAC

c. Le contrôle de trame

Ce ne sont pas moins de 11 champs qui composent les deux octets FC.

La version du protocole (*Protocol Version*) reste pour l'instant à 0. Elle pourrait être exploitée si un changement important de structure d'en-tête survenait.

La fonction de la trame est identifiée dans le champ type : gestion, contrôle ou données. Des informations

complémentaires sont précisées dans le champ suivant, sous type (*Sub Type*).

La direction de l'information transportée est précisée par les deux champs ToDS et FromDS.

Si le champ More Fragment contient la valeur 1, cela indique que d'autres MPDUs suivent. Il reste à 0 dans le cas contraire.

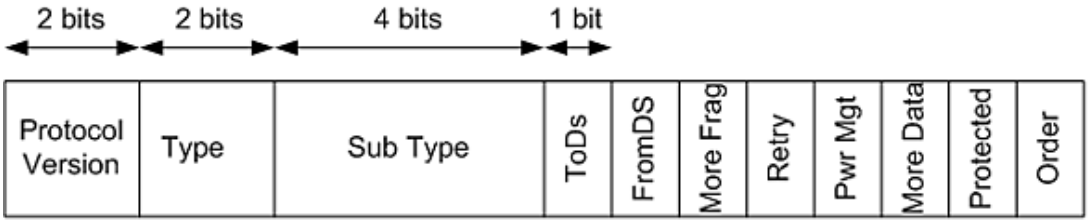
Si cette trame est une réémission, le champ Retry est positionné à 1. Le cas échéant, cela permet au récepteur de supprimer la trame qui aurait pu être réceptionnée initialement.

C'est dans le champ de gestion d'énergie (*Power Management*) qu'une station indique qu'elle utilise ce mode. S'il est positionné à 1, ce bit annonce qu'elle sera en veille après cette transmission.

Le champ de gestion d'énergie est toujours à 0 pour une trame envoyée par le point d'accès. En revanche, cet équipement peut obliger une station à rester en écoute, en mettant une valeur 1 dans le champ More. Ainsi, les trames suivantes pourront être réceptionnées immédiatement grâce à ce forçage.

L'usage d'un chiffrement dans le corps de trame est indiqué par une valeur 1 du champ Protected Frame. Seules les trames de données et de gestion servant à l'authentification l'utilisent. Ce champ était nommé Wireless Equivalent Privacy (WEP) dans les premiers standards.

Enfin, Order oblige le relayage de trames fragmentées dans l'ordre reçu. Cela peut être imposé par certains protocoles de couche supérieure ne gérant pas l'ordonnancement. Ce bit est positionné à 0 pour des communications en QoS.



Le champ de contrôle de trame (FC)

2. Trames de gestion

a. Le format

Pour indiquer que les trames sont de gestion, les deux bits du type sont positionnés à 0. Le champ sous type précise l'utilisation de la trame.

Les valeurs qu'il peut prendre sont données dans le tableau ci-après.

Valeur du sous type	Indication
0000	Requête d'association
0001	Réponse d'association
0010	Requête de réassociation
0011	Réponse de réassociation
0100	Requête de sondage
0101	Réponse de sondage
0110- 0111	Réservées
1000	Balise
1001	Message ATIM
1010	Désassociation
1011	Authentification
1100	Désauthentification
1101-1111	Réservées

Valeurs de champ sous type d'une trame de gestion

Les informations contenues dans une trame de gestion ne sont pas destinées aux couches supérieures. Le corps de

trame sera donc utilisé pour transporter des informations complémentaires à l'en-tête. En fonction de la valeur du champ sous type, divers paramètres sont transportés dans ce corps de trame. Deux types d'informations peuvent être fournies :

- des valeurs simples, dans un champ de taille fixée (FF - *Fixed Field*) ;
- des valeurs complexes et de taille variable, dans des éléments d'informations (IE- *Information Elements*).

Un même champ fixe peut être utilisé dans différents sous types des trames de contrôle. Sa taille est généralement de deux octets, sauf pour l'horodatage de la trame de balises et l'adresse du point d'accès.

Les informations d'éléments sont constituées de trois parties :

- le numéro de l'élément (Element ID), sur 1 octet, soit 256 valeurs possibles ;
- sa longueur (Length), sur 1 octet ;
- une fraction de taille variable, dont le contenu est fonction du numéro d'élément.

La structure d'un élément d'information (IE)

Les numéros des éléments d'information sont figés. Comme pour les champs fixes, ils peuvent être utilisés dans plusieurs des trames de contrôle. Celles définies dans les spécifications 802.11 sont :

- numéro 0, fournissant le nom du SSID dans la fraction variable ;
- numéro 1, pour les débits supportés (*Supported rates*), dont le contenu comprend 8 octets, chacun donnant l'une des vitesses autorisées, en multiple de 500 kbps ;
- numéro 2, pour les paramètres FHSS ;
- numéro 3, contenant le numéro de canal DSSS ;
- numéro 4, pour les paramètres CF ;
- numéro 5, pour le Traffic Indication Map (TIM) ;
- numéro 6, pour les paramètres IBSS ;
- numéro 16 à 31 pour le texte de challenge, lors de l'authentification.

b. Le contenu du corps de trame

Trame de balises

La trame de gestion de sous type balise fournit de nombreuses informations dans le corps de trame :

- un horodatage (*Timestamp*), sur 8 octets, destiné à la synchronisation ;
- l'intervalle entre deux trames (*Beacon interval*) ;
- des informations de capacités (*Capability Information*) ;

- le SSID ;
- les débits supportés (*Supported Rates*) ;
- les paramètres FH, si la transmission utilise FHSS ;
- les paramètres DS, si DSSS est utilisé ;
- une information IBSS si besoin ;
- le TIM, utilisé pour les stations en mode d'économie d'énergie.

Quelques champs du corps de la trame de balise

Les informations de capacité regroupent, sur deux octets, plusieurs sous champs :

- ESS, dont le bit est positionné à 1 dans un réseau d'infrastructure ;
- IBSS, dont le bit est positionné à 1 dans un réseau ad hoc ;
- CF-Pollable, à 1 si l'équipement utilise le mode PCF ;
- CF Poll request, à 1 pour demander l'usage du mode PCF ;
- Privacy, indiquant, s'il a valeur 1, chiffrement des trames de données ;
- QoS, à 1 pour requérir une association en mode QBSS ;
- APSD, pour la prise en compte de ce mode ;
- ...

Trames de requête et de réponse d'association

Le corps de trame de la requête contient une dizaine d'informations :

- Les informations de capacité (*Capability information*), semblables à celles de la balise ;
- La périodicité de réveil de la station (*Listen interval*) ;
- L'élément d'information SSID ;
- La liste des débits supportés (*Supported rates*), également jointe comme élément d'information ;
- Les débits étendus supportés (*Extended Supported Rates*), s'il y a plus de huit ;
- Les capacités d'alimentation (*Power Capability*) ;
- Les canaux supportés (*Supported Channels*) ;

- Les informations RSN, pour préciser les modes de chiffrement ;
- Les capacités de QoS (*QoS Capability*) ;
- Un élément d'information constructeur (*Vendor Specific*).

Les différentes parties de la réponse indiquent :

- les informations de capacité (*Capability Information*) ;
- un code d'état (*Status Code*) ;
- l'identifiant d'association (AID - *Association ID*) ;
- les débits supportés (*Supported Rates*).
- Les débits étendus ;
- Le paramètre EDCA (*EDCA Parameter Set*) ;
- L'élément d'information constructeur.

La numérotation des codes d'état est effectuée sur 2 octets. Une dizaine de codes sont utilisés dans les spécifications 802.11 d'origine. Avec les complexifications entraînées par les adoptions de la QoS et des sécurisations avancées, d'autres ont été ajoutés. On en compte actuellement plus d'une trentaine exploités.

L'identifiant d'association est également un champ fixe. Ce numéro est attribué par le point d'accès pour repérer une station.

Trames de désassociation et de réassociation

La demande de désassociation ne contient qu'une seule information, un code de justification du retrait (Reason Code). Là encore, ce sont désormais plus d'une trentaine de raisons différentes, allant d'une cause non spécifiée à la désassociation pour inactivité, qui sont précisées. Comme les codes d'état, elles sont numérotées et ont évoluées au gré des besoins.

Trames de requête et de réponse de sondage

La requête de sondage ne contient que deux parties et leurs éléments d'information :

- un SSID ;
- les débits supportés.

Le contenu d'une réponse de sondage est plus important. Les mêmes informations que dans une trame de balises, sauf le TIM, sont renvoyées dans le corps de trame.

Trames d'authentification et de désauthentification

Deux algorithmes sont proposés par les spécifications 802.11. Dans l'authentification ouverte (*Open System Authentication*), le point d'accès se contente de renvoyer une autorisation à la demande initiale. La deuxième version utilise un texte de challenge et une clé WEP prépartagée (*Shared Key Authentication*). Nous reviendrons sur ces méthodes dans le chapitre Premières solutions de sécurisation.

Les trames d'authentification comprennent :

- le numéro de l'algorithme d'authentification (*Authentication Algorithm Number*), de valeur 0 pour open et 1 pour shared ;
- le numéro de séquence de la transaction d'authentification (*Authentication Transaction Sequence Number*) ;
- un code d'état (*Status Code*) ;

- un texte de challenge (*Challenge Text*), si l'algorithme utilisant la clé partagée est demandé.

Parmi les différentes parties citées précédemment, seul le transfert du texte de challenge est un élément d'information.

À la demande de désauthentification est juste joint un code de raison.

3. Trames de contrôle

a. Le format

Le champ de corps de trame n'est pas utilisé par les trames de contrôle, dont le type vaut 01. Elles restent très basiques, particulièrement au niveau des champs d'adresse et de sous type. Ainsi, les valeurs des champs ToDS, FromDS, More Frag, Retry, More Data, WEP et Order reste positionnées à 0.

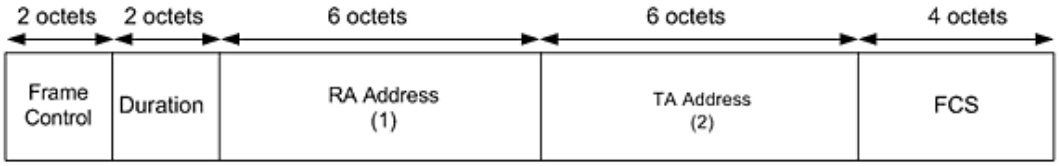
L'adoption du 802.11e a nécessité l'ajout de deux nouvelles trames de contrôle relatives aux accusés de réception.

Valeur du sous type	Indication
0000-0111	Réservées
1000	Block Ack Request (BlockAckReq)
1001	Block Ack (BlockAck)
1010	PS-Poll
1011	RTS
1100	CTS
1101	ACK
1110	CF-End
1111	CF-End + CF-Ack

Valeurs de champ sous type d'une trame de contrôle

b. Le détail de l'en-tête

La trame Request To Send (RTS) utilise les champs de contrôle de la trame (Frame Control), de durée (Duration), d'adresse 1 pour le destinataire et d'adresse 2 pour l'émetteur.



La trame RTS

La réponse Clear To Send (CTS) y ressemble fortement, mais n'utilisera pas le champ d'adresse d'émetteur.

La trame d'accusé de réception (ACK) originelle a été complétée, afin de prendre en compte des accusés de réception par blocs, sur lesquels nous reviendrons en fin de chapitre. Par rapport à la trame RTS ci-dessus sont rajoutées des informations relatives aux éléments dont la réception est validée, juste avant le FCS.

Le format de l'information Power Save Poll (PS-Poll) comprend un AID, le BSSID et l'adresse de l'émetteur.

4. Trames de données

Dans ce cas, le champ type est positionné à la valeur 10. Là encore, la valeur de sous type est importante. En effet, le propre d'une trame de données est une capacité à regrouper plusieurs fonctions.

Valeur du sous type	Indication
0000	Données
1000	Données + CF-Ack
0010	Données + CF-Poll
0011	Données + CF-Ack + CF-Poll
0100	Paquet sans données
0101	CF-Ack, sans données
0110	CF-Poll, sans données
0111	CF-Ack + CF-Poll, sans données
1000	Données QoS
1001	Données QoS + CF-Ack
1010	Données QoS + CF-Poll
1011	Données QoS + CF-Poll + CF-Ack
1100	QoS sans données
1101	Réservée
1110	QoS CF-Poll, sans données
1111	QoS CF-Poll + CF-Ack, sans données

Valeur de champ sous type d'une trame de données

En mode DCF, le point d'accès peut, tout en transmettant une information vers une station, lui donner la parole. Un équipement peut également profiter d'une transmission pour accuser réception d'une trame. Ainsi de nombreux dialogues gourmands en bande passante peuvent être évités.

Les communications en qualité de service sont signalées comme telles.

Comme on peut le voir dans le tableau ci-dessus, certaines trames de données n'en contiennent même pas, se contentant de transférer des autorisations de prise de parole ou d'accusé de réception.

5. Adressages et direction des trames

a. L'usage des bits de direction des trames

Dans la partie Frame Control (FC), les deux bits ToDS et FromDS donnent de précieuses indications sur le sens de la trame. En effet, les différents cas de transmission, sans point d'accès, avec un, voire plusieurs, ne permettent pas de se fier seulement aux champs d'adressage.

Ces valeurs renseignent donc également sur le type de réseau. Si elles sont toutes deux à 0, la communication a lieu directement entre deux stations, en mode ad hoc. Dans tous les autres cas, au moins un point d'accès est concerné et doit être adressé.

ToDS	FromDS	Signification
0	0	Trame envoyée d'une station vers une autre de même IBSS
0	1	Trame de données provenant du système de distribution
1	0	Trame de données destinée au système de distribution
1	1	Trame relayée successivement par deux points d'accès pour arriver à destination

Combinaison des bits ToDS et FromDS

b. L'usage des quatre champs d'adressage

Ils ne sont pas tous les quatre systématiquement utilisés. Les valeurs qu'ils peuvent contenir sont :

- un Basic Service Set IDentifier (BSSID) ;
- une adresse source (SA - *Source Address*) ;
- une adresse de destination (DA - *Destination Address*) ;
- une adresse d'émetteur (TA - *Transmitter Address*) ;

- une adresse de récepteur (RA - *Receiver Address*).

L'emplacement de ces informations dans les quatre champs d'adresse dépend du contexte et des bits ToDS et FromDS.

Le premier champ d'adresse contient celle de la prochaine étape de la trame. Le deuxième comprend celle de l'émetteur de la trame. Les deux derniers apportent renseignements complémentaires au besoin.

FC	D/ID	Address 1	Address 2	Address 3	SC	Address 4

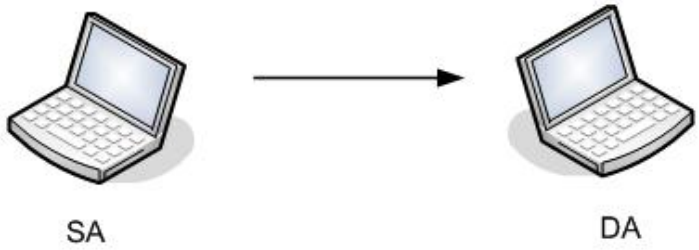
Rappel : l'en-tête MAC

Communication en mode ad hoc

Dans le cas d'un réseau de type Independent Basic Service Set (IBSS), les champs ToDS et FromDS ont 0 pour valeur. Le BSSID est indiqué sur 48 bits, comme une adresse MAC. Il est composé d'une valeur aléatoire pour les 46 bits de poids faible.

Dans une trame unicast, I/G (Individuel/Groupe) est positionné à 0 et U/L (Universel/Local) à 1. Dans ce mode ad hoc, un signal de broadcast n'est utilisé que pour la trame de requête de sondage.

Adresse 1	Adresse 2	Adresse 3	Adresse 4
DA	SA	BSSID	Non utilisée

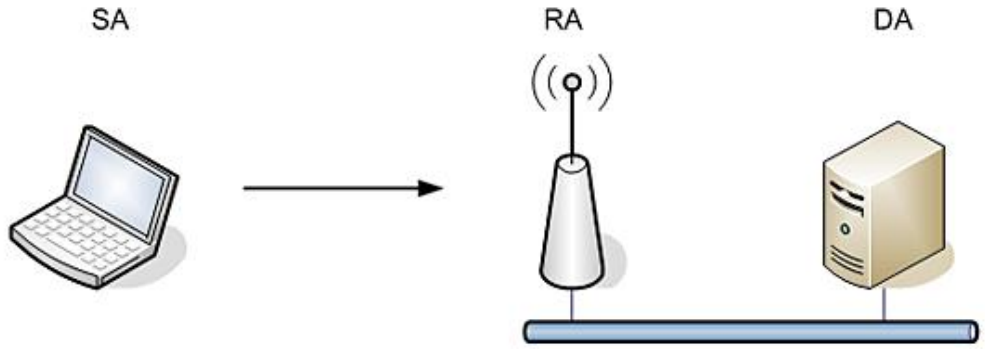


Communication d'une station vers un point d'accès

Le point d'accès n'est pas une destination en soit. Une station l'utilise comme intermédiaire vers le réseau filaire, ou vers une autre station. Dans ce cas, ToDS=1 et FromDS=0.

Dans l'exemple ci-dessous, le point d'accès comprendra ainsi qu'il doit transmettre la trame, sur le réseau Ethernet, au serveur possédant l'adresse MAC correspondant à DA.

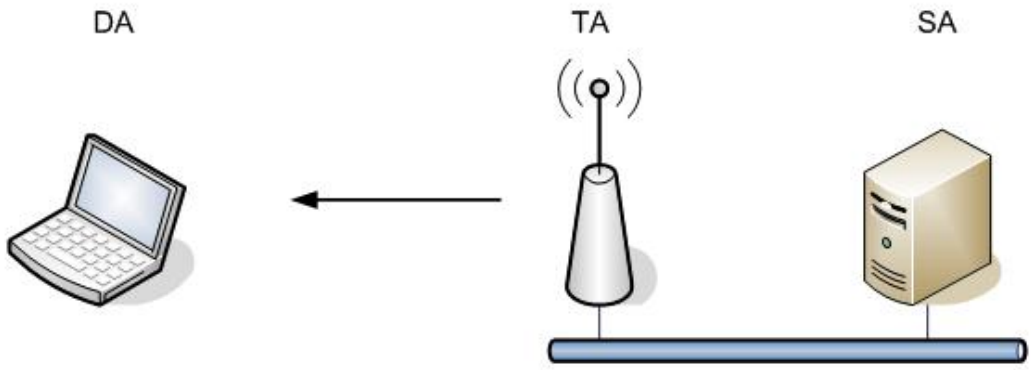
Adresse 1	Adresse 2	Adresse 3	Adresse 4
RA	SA	DA	Non utilisée



Communication d'un point d'accès vers une station

Là encore, le point d'accès servira de relais, émettant une trame 802.11 remise en forme et possédant l'adresse de l'émetteur initial en tant que SA. Les bits ToDS, positionné à 0 et FromDS à 1, viennent compléter les indications.

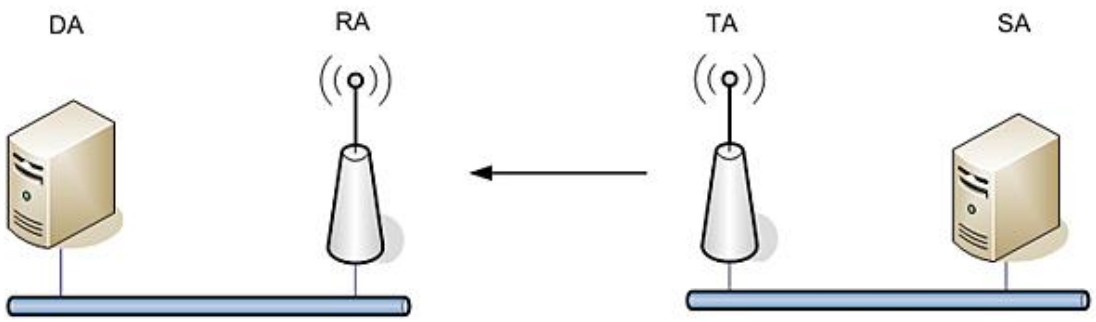
Adresse 1	Adresse 2	Adresse 3	Adresse 4
DA	TA	SA	Non utilisée



Transmission de communication entre deux points d'accès

Le seul cas utilisant le quatrième champ d'adresse est qualifié de Wireless Distribution System (WDS). Ici, les champs ToDS et FromDS ont pour valeur 1. Le WDS permet une transmission entre deux points d'accès, ou deux ponts, associés par le canal radio.

Adresse 1	Adresse 2	Adresse 3	Adresse 4
RA	TA	DA	SA



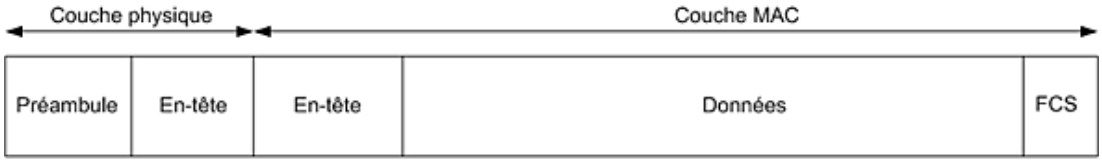
6. Améliorations du 802.11n draft

Afin d'optimiser le contenu des trames en couche MAC, les spécifications 802.11n, actuellement en version non définitives, apportent différents compléments.

a. L'agrégation de trames

L'efficacité globale est d'abord améliorée par la possibilité d'agréger les trames.

En effet, beaucoup de trames 802.11 sont constituées à partir de trames Ethernet traduites. Prenons l'exemple d'un point d'accès qui reçoit sur son interface Ethernet une trame destinée à un client Wi-Fi. La partie donnée de cette trame, qui n'excède pas 1518 octets est d'abord extraite. Elle vient constituer la partie données de la trame 802.11, à laquelle sont ajoutés un préambule et un en-tête radio (couche physique). Puis l'en-tête de couche MAC et enfin le FCS, voire l'accusé de réception ACK, sont ajoutés.



Rappel : la trame Wi-Fi (simplifiée)

On conçoit que si plusieurs trames Ethernet doivent être envoyées à un même client 802.11, elles peuvent être agrégées, en n'ajoutant qu'une seule fois les champs ne contenant pas les données.

Les trames peuvent désormais atteindre 64 kilo-octets.

Agrégation MSDU

L'agrégation MSDU collecte d'un coup une série de trames Ethernet dont la destination est commune et n'en fait qu'une seule trame 802.11.

Comme ce sont les trames vers une seule destination qui sont regroupées, le chiffrement peut être réalisé normalement. Par contre, si la qualité de service est utilisée, il n'est pas question d'agréger des trames de priorités différentes.

Agrégation MPDU

Cette seconde méthode travaille d'abord unitairement les trames. Par exemple, elle traduit une à une les trames Ethernet, en y ajoutant l'en-tête MAC 802.11. Ce n'est qu'ensuite qu'elle regroupe les informations dont la destination est commune. Dans ce cas, l'en-tête de couche MAC n'est donc pas agrégée.

L'avantage de cette solution est que plusieurs chiffrements distincts peuvent être mis en œuvre au sein d'une même trame Wi-Fi agrégée. Par contre, l'efficacité est moindre que dans la solution précédente.

b. Accusé de réception par bloc

Normalement l'émetteur de chaque trame de type unicast se voit individuellement confirmer la bonne réception de celle-ci (ACK - *Acknowledgement*). Ce fonctionnement n'est pas remis en cause avec l'agrégation MSDU. Par contre, l'agrégation MPDU regroupe des trames individuelles. Il serait donc nécessaire de confirmer la réception de chacune des trames constituantes. Le mécanisme d'accusé de réception par bloc (*block acknowledgement*), déjà utilisé en 802.11e permet de répondre au problème posé. L'ensemble des confirmations individuelles attendues est regroupé dans une seule réponse, beaucoup plus rapide et utilisant moins de bande passante. Dans des environnements entraînant des forts taux d'erreurs, ce mécanisme est très appréciable.

c. Intervalle de temps réduit

Lorsque l'agrégation de trames ne peut être entendue, il est quand même possible d'optimiser les transmissions en utilisant le mécanisme TXOP (*Transmission opportunity*) issu de l'amendement 802.11e. En effet, celui-ci autorise l'envoie d'une rafale de trames. 802.11n augmente encore l'efficacité de ce système en réduisant l'intervalle de temps Short Inter Frame Space (SIFS). Ce nouveau temps d'attente baptisé Reduced Inter Frame Space (RIFS) ne peut pas être utilisé en mode de compatibilité.

d. Mode de compatibilité

La compatibilité avec les spécifications 802.11a, b et g est possible en 802.11n draft. Dans ce cas, une trame compatible avec cette dernière contient à la fois des en-têtes et préambules communs et d'autres spécifiques.

S'affranchir d'une telle possibilité améliore énormément les débits, mais nécessite que l'ensemble des matériels soient conformes avec les derniers amendements.

Ce mode n'est pas encore figé. Il est actuellement appelé Greenfield Mode.

Sécurité du réseau local

Le système d'information (SI), regroupant l'ensemble des éléments attachés aux réseaux de l'entreprise, est devenu, avec le temps, une véritable nébuleuse. De nombreux utilisateurs doivent y avoir accès, qu'ils soient employés, partenaires ou clients. Il est utopique de penser contrôler leurs actions.

Dans le même temps, le SI a adopté un grand nombre de standards, de fait ou issus de normes, au lieu de solutions propriétaires. Mais il est ainsi devenu ouvert.

La prise de conscience de la problématique de sécurité est récente. Beaucoup des protocoles utilisés, par exemple, n'ont pas été conçus à l'origine pour être sécurisés. On peut citer, parmi ceux-ci, la plupart de ceux de la suite TCP/IP. Les interconnexions entre les systèmes se sont multipliées, particulièrement à travers le réseau public Internet. Là encore, de nombreuses failles sont apparues.

L'exploitation du système d'information actuel est donc fortement perfectible en terme de sécurité. Nous ne pouvons penser éliminer tout risque, mais il peut être réduit en le connaissant et en adoptant des solutions adéquates.

1. Compréhension de la menace

a. Les garanties exigées

La sécurité d'un système d'information (SSI), et plus particulièrement d'un réseau, s'appuie sur quatre thèmes clés :

- l'authentification, permettant de s'assurer de l'identité et connaître ainsi l'origine des opérations ;
- la confidentialité, qui a pour but d'éviter toute divulgation d'informations ;
- l'intégrité, pour interdire ou connaître les modifications et se préserver des pertes d'information ;
- la disponibilité, qui permet d'assurer un service en toutes circonstances.

À cela, nous pouvons ajouter une cinquième nécessité, de plus en plus d'actualité : la non répudiation. Elle permet d'être certain, en toutes circonstances, de l'origine d'une communication ou d'un transfert d'informations. La non répudiation reprend un concept familier de notre vie quotidienne, la signature, ici sous forme électronique.

Afin de s'assurer du niveau de garantie offert par le système d'information, des analyses peuvent être effectuées. Elles permettront d'évaluer le niveau de menace qui pèse sur celui-ci, afin d'adopter des parades proportionnées aux risques. Des méthodes d'analyse, comme MEHARI, du club de la sécurité des systèmes d'information français (Clusif), permettent de s'appuyer sur des référentiels existants pour mener à bien cette étude.

Site Web du club de la sécurité des systèmes d'information français : http://www.clusif.asso.fr

Les actions adoptées le sont ensuite en toute connaissance de cause. Le risque évalué peut être :

- assumé, c'est-à-dire que ces conséquences sont connues, mais que le choix est fait de ne pas s'en protéger ;
- évité, et donc, après sa mise en évidence, le SI est protégé à ce niveau ;
- limité, en le réduisant ou diminuant ses causes ;
- transféré, et il est déporté à un autre niveau.

Le niveau de protection offert peut être lui-même évalué. Pour cela, il existe également des référentiels. Les critères communs, par exemple, permettent l'évaluation et la certification des fonctions de sécurité de produits et de systèmes. Leur version 2.1 a même été normalisée par l'ISO en 1999, sous le numéro 15408.

L'analyse et l'évaluation des risques permettent ainsi d'adopter des niveaux de sécurité appropriés, en fonction des garanties souhaitées pour le système d'information.

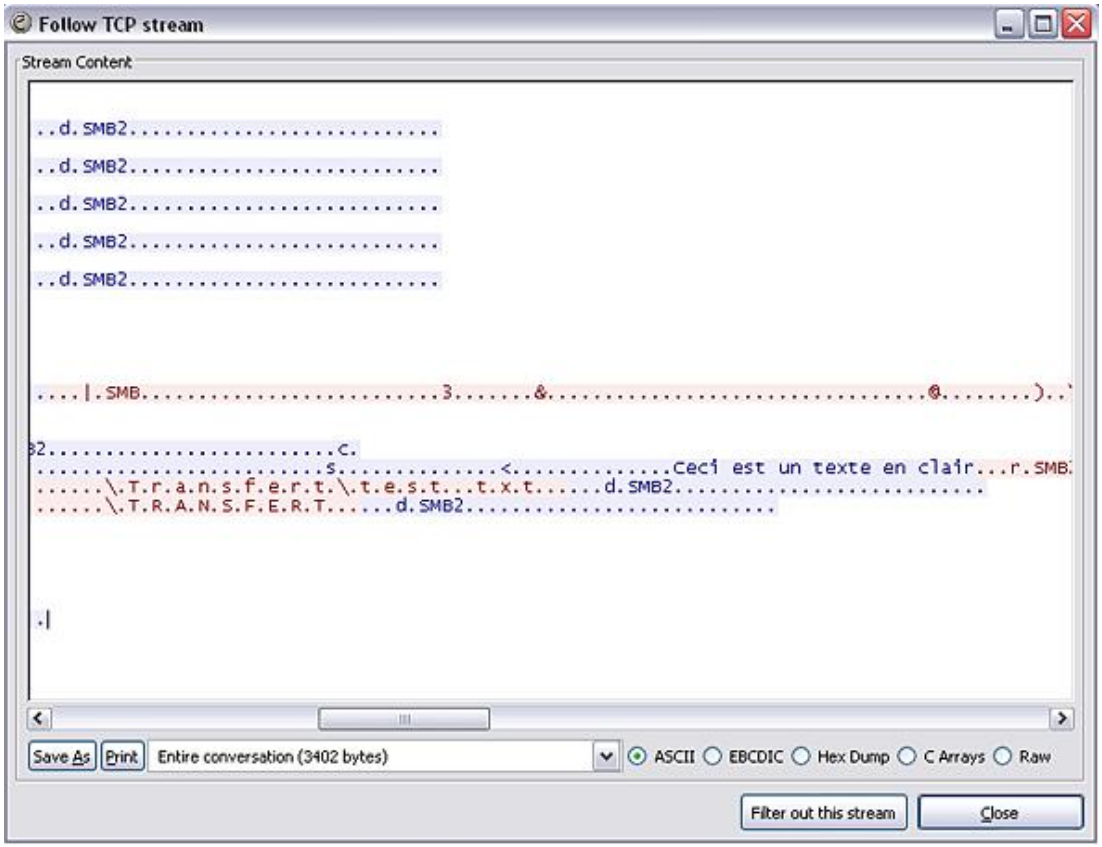
b. Les dangers encourus

Il peut être important, avant de vouloir gérer les risques, de connaître les dangers potentiels encourus par le SI. Ceux-ci portent d'abord sur les communications et le système lui-même, au niveau matériel comme logiciel.

Nous nous focaliserons ici uniquement sur l'aspect circulation des informations.

Risques sur la circulation des données

Dans beaucoup de réseaux, l'essentiel, voire la totalité des communications transportées transite en clair. Les contenus sont donc lisibles par n'importe qui.



Résultat d'une écoute réseau, le texte du fichier transmis est visible

L'analyse de trame précédente correspond à une demande d'ouverture d'un fichier stocké sur un serveur, à partir d'un poste de travail. Nous pouvons voir que son contenu, "Ceci est un texte en clair", a été reconstitué lors de la communication réseau.

Risques au niveau des protocoles Réseau et Transport

Les protocoles de communication réseau, faillibles, peuvent être la cible d'attaques portant sur leurs spécificités, c'est-à-dire leurs en-têtes.

De nombreuses méthodes sont connues pour cela. Beaucoup ont exploité les différentes couches d'un modèle comme TCP/IP, dont les deux niveaux Réseau et Transport cumulent les faiblesses.

Par exemple, sur Internet Protocol (IP), l'adressage logique peut être usurpé. Les opérations de fragmentation/défragmentation peuvent également être exploitées.

Internet Control error Message Protocol (ICMP) et l'usage des commandes "ping", ont été la source de nombreuses attaques.

La poignée de main (3-way handshake) d'établissement de connexion du protocole Transmission Control Protocol (TCP) peut être exploitée pour détourner des communications.

Ce ne sont que quelques exploitations, il en existe de nombreuses autres. Heureusement, les évolutions ont rendu ces protocoles plus fiables. En effet, les logiciels qui pilotent cette pile tiennent compte désormais de l'historique des nombreuses attaques tentées.

Ce n'est pas pour autant qu'elles sont à l'abri de tentatives nouvelles, mais les risques tendent à sérieusement se réduire.

Risques au niveau des protocoles applicatifs standard

La quasi-totalité des dangers récents exploite cette couche. Des protocoles applicatifs standard, comme HyperText Transfer Protocol (HTTP), Simple Mail Transfer Protocole (SMTP), File Transfer Protocol (FTP), Domain Name System (DNS), sont particulièrement visés. Ils sont, en effet, d'usage tellement courant, que trouver une nouvelle vulnérabilité est devenu très payant.

Ces protocoles applicatifs présentent, comme ceux de niveau inférieur, des failles, dont beaucoup sont dues à leur conception, plutôt ancienne. Là encore, c'est leur interprétation logicielle qui entraînera les principaux problèmes.

Par exemple, l'exploitation, toujours plus avancée, des pages Web dynamiques et des logiciels additionnels complémentaires, implique des programmations toujours plus complexes des interpréteurs que sont les navigateurs Web. Régulièrement, de nouvelles failles sont découvertes et doivent être corrigées.

Les pièces jointes des messages électroniques sont devenues les vecteurs privilégiés des attaques virales, diffusant logiciels malveillants et vers.

Risques au niveau des protocoles de couches basses

Au niveau le plus bas, un protocole comme 802.11, nous le verrons bientôt, n'est pas exempt de failles, loin s'en faut.

La généralisation des commutateurs pour l'interconnexion entre ordinateurs par Ethernet a considérablement amélioré la sécurisation de ce niveau.

Risques au niveau logiciel

Les équipements, sur le réseau, sont devenus plus complexes. Les commutateurs, comme les routeurs, doivent offrir des fonctions très importantes. Ils sont désormais très souvent pilotés par de véritables systèmes d'exploitation.

Il est nécessaire de protéger leurs moyens d'administration et les comptes associés.

Ces logiciels peuvent comporter des failles. Il est recommandé de s'informer sur les mises à jour correctives et, si nécessaire, de les appliquer. C'est particulièrement le cas pour les systèmes d'exploitation des serveurs et postes de travail.

Là encore, connaître l'existence de ces dangers et comprendre la nécessité de s'en protéger est crucial.

c. Le degré d'intensité de la menace

Bien sûr, toutes les entreprises n'ont pas le même degré de sensibilité aux attaques. En fonction de leur taille et des données traitées, les risques sont plus ou moins sérieux. En complément de l'identification des cibles à protéger, et de leurs vulnérabilités, une prise en compte des niveaux de menace permet d'affiner l'analyse.

Trois niveaux sont ainsi répertoriés :

- l'écoute ;
- l'intrusion ;
- la prise de contrôle.

Écoute des communications

L'écoute passive est très difficilement détectable. Elle consiste juste à intercepter les signaux circulant. La reconstitution de l'information est facilitée si elle circule en clair. Un logiciel d'écoute et d'analyse de trames, ou sniffer, suffit pour cela. L'usage des ondes radio facilite grandement de telles attaques.

La capture de signaux parasites compromettants (SPC) est également une méthode d'écoute passive. Elle peut être réalisée sur tout matériel transmettant des informations électriques, comme les câbles réseaux ou un simple écran. Il suffit d'écouter les variations du signal, qui "déborde" du matériel, comme ondes électromagnétiques ou courants de conduction.

L'écoute active est moins discrète. Consistant à solliciter un équipement pour obtenir des informations, elle peut être repérée plus facilement. En contrepartie, il est plus facile d'obtenir les informations recherchées.

Intrusion et prise de contrôle

Une intrusion est un accès illicite à un système. Le pirate accède ainsi à l'information elle-même ou aux services informatiques.

Il peut ensuite prendre le contrôle d'un système pour l'administrer à distance.

Nous pouvons comprendre que ces trois menaces ne présentent pas le même danger pour le réseau. Par contre, elles se complètent les unes par rapport aux autres, l'écoute facilitant l'intrusion, qui elle-même permet la prise de contrôle.

2. Techniques d'attaques et d'intrusions

a. Les différents acteurs

Une connaissance des agresseurs potentiels et de leurs capacités permet d'affiner le niveau de protection souhaitable. Une menace peut être une attaque volontaire ou une simple négligence, voire une fausse manipulation.

Une altération du système d'information peut avoir pour origine des personnes présentant des profils très différents. Ceux que l'on peut qualifier de pirates sont désormais attirés par l'argent.

Employés de l'entreprise

Les utilisateurs eux-mêmes sont la cause d'un certain nombre d'incidents. Ils ne sont pas à l'abri d'erreurs de manipulation, particulièrement si les droits et permissions dont ils disposent ne sont pas en relation avec leurs tâches. Ces utilisateurs peuvent être à l'origine de l'exécution de codes malveillants ou de vers joints à un message électronique.

Le non respect de la confidentialité des mots de passe, ou le non verrouillage des postes de travail, facilite les opérations illicites.

L'utilisation non parcimonieuse des comptes d'administration est une faille importante. Beaucoup d'administrateurs utilisent de tels comptes au quotidien, ce qui augmente fortement les risques sur le système d'information.

De simples actions de sensibilisation et d'information peuvent être suffisantes pour réduire fortement ces dangers.

Utilisateurs d'Internet

Avec la démocratisation de l'Internet haut débit sont arrivées de nouvelles menaces pour l'entreprise. Un grand nombre de particuliers sont désormais connectés de manière semi-permanente, voire permanente, au même interréseaux que celles-ci.

Peu sensibilisés aux dangers de l'Internet, ces utilisateurs sont les relais privilégiés d'attaques vers les installations professionnelles.

L'usage de logiciels pair à pair (peer to peer) et de messageries électroniques ou instantanées, sans précautions, facilite la promulgation des logiciels malveillants.

La non mise à jour des signatures de virus et des correctifs de sécurité, ainsi que l'absence d'utilisation de pare-feu personnel rendent ces ordinateurs très vulnérables. Ils peuvent ensuite servir de relais pour des attaques à destination des entreprises.

Par exemple, une action de déni de service distribué (DDoS - *Distributed Denial of Service*) consiste à faire envoyer simultanément une requête depuis de multiples postes vers une cible. Celle-ci peut être un site Web qui, submergé, s'écroule et ne répond plus aux demandes légitimes. L'impact, pour un serveur de commerce électronique mal protégé, est sérieux. Une telle agression est grandement facilitée par la présence permanente sur l'Internet de machines peu, ou pas, protégées : le pirate a pu y installer le logiciel qui sera ensuite source de l'attaque.

Acteurs expérimentés

Ces informaticiens connaissent très bien les systèmes et la programmation. Ils sont capables d'utiliser des techniques avancées, telles que le retro-engineering, ou décompilation. Ils ont la compétence pour mettrent en œuvre leurs propres logiciels, qu'ils ont développés.

Ils sont qualifiés par des termes anglais, généralement non traduit.

Le Hacker, ou White Hat, cherche avant tout à approfondir son savoir. Expert du réseau, il n'est pas malintentionné et utilise ses compétences pour l'amélioration du système. Fondamentalement, il s'agit du profil le moins dangereux pour les réseaux d'entreprise.

Le Cracker, ou Black Hat, est véritablement malveillant. Il cherche à s'introduire dans les systèmes informatiques, ayant pour seul but d'effectuer des actions nuisibles. Il utilise ses connaissances pour détruire ou voler l'information, planter les systèmes... Auparavant, il était captivé par le jeu que représente le défit. Ce pirate est désormais de plus en plus souvent attiré par l'appât du gain.

Acteurs inexpérimentés

Ces simples utilisateurs de logiciels peuvent être dangereux pour les systèmes d'information. Leurs qualificatifs sont également des termes anglais, tels que :

- Newbies, les novices ;
- Scripts kiddies, les débutants ;
- Lamers, littéralement boiteux, expression méprisable donnée par les acteurs plus compétents.

Ces différents profils ont pour point commun le manque de compétences réelles. Les deux premiers, en phase d'apprentissage, s'attaquent ainsi généralement à des proies faciles. Et la difficulté d'attaquer un réseau d'entreprise peut les rebuter.

Le lamer trouve ses ressources sur Internet, ou dans certaines publications grand public. Sans avoir véritablement la conscience qu'il peut provoquer une nuisance, il exploite ainsi des logiciels qu'il ne contrôle pas. Ses actions non maîtrisées peuvent avoir un impact sur son ordinateur : altération, installation de logiciels malveillants... Là encore, la propagation d'un problème peut être forte si cette machine est connectée à l'interréseaux.

Nous retrouverons typiquement de tels profils chez beaucoup de passionnés du Wi-Fi.

b. Le scénario d'une attaque type

Une attaque volontaire d'un système d'information est un processus complet, qui peut être typiquement décomposé en six actions élémentaires :

- la recherche de renseignements ;
- la préparation ;
- l'intrusion ;
- l'installation ;
- le camouflage ;
- la propagation.

Elle peut être provoquée depuis le réseau local lui-même, ou à partir du réseau d'un partenaire, avec lequel une liaison privilégiée a été mise en place. Les accès distants depuis des clients de réseaux privés virtuels (VPN - *Virtual Private Network*) peuvent également être utilisés. Mais les accès à partir d'un réseau public, tel qu'Internet, restent des moyens très simples d'atteindre un système.

Les tentatives à partir d'accès locaux sont les plus dangereuses : l'accès physique aux matériels les rend encore plus vulnérables. Le simple branchement sur une prise réseau, non utilisée et active, permet déjà un accès privilégié.

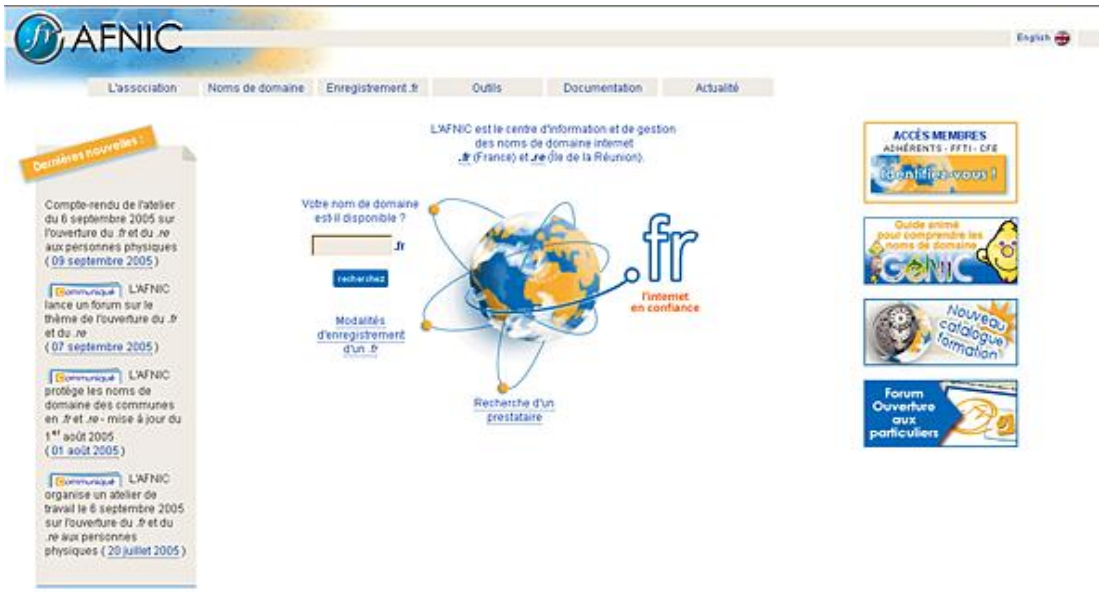
La recherche de renseignements

Le premier but est l'identification précise de la cible. La recherche peut porter sur :

- le plan d'adressage IP ;
- les logiciels utilisés, ainsi que leur version ;
- les comptes, particulièrement ceux administratifs ;
- les matériels.

Les investigations peuvent inclure un travail sur des informations publiques, comme les plages d'adresses IP Internet allouées à l'entreprise, ses noms de domaines, les noms des responsables...

Par exemple, le site de l'association française pour le nommage Internet en coopération (AFNIC) maintient une base d'informations publiques d'affectation des noms de domaine .fr. De premiers renseignements sont disponibles sur leur site.



Site Web de l'AFNIC : http://www.afnic.fr

La lecture de blogs ou de forums peut apporter son lot d'informations. Certains contributeurs dévoilent quantités d'informations sur leur entreprise.

Des écoutes, actives ou passives peuvent être mises en œuvre. Elles vont déjà permettre de trouver quelques fichiers mal protégés, de reconnaître quelques logiciels utilisés...

La préparation

Après avoir collecté suffisamment d'informations, le pirate peut rechercher les moyens d'attaquer la cible.

Par exemple, s'il a reconnu la version du serveur Web ou de messagerie SMTP, il peut rechercher sur Internet quelles sont les failles répertoriées. Il peut ainsi essayer de se procurer des logiciels permettant de les exploiter.

Différents tests directs permettent au pirate de vérifier l'état des configurations. Il peut être très facile de retrouver certains mots de passe. Parfois, des valeurs de configuration par défaut, rendant le système plus ouvert, ont été laissées...

L'intrusion

Une fois obtenus les renseignements utiles et les outils adéquats, le pirate peut envisager l'action en tant que telle.

Pour cela, il va compromettre le système, en exploitant les bugs, failles de sécurité et mauvaises configurations repérées précédemment.

Cette action peut également prendre la forme de branchements pirates, qui le mettront au cœur du système d'information visé.

L'installation

Pour pénétrer dans le système, l'intrus a utilisé une faille, qui doit être considérée comme temporaire. Pour pallier à cela, l'installation d'un logiciel, qui créera une connexion permanente avec son poste, est un bon moyen.

Le camouflage

La discrétion étant impérative, toute trace des actions précédentes doit être effacée. Au besoin, les journaux sont réinitialisés. Les programmes installés se font très discrets, placés dans des arborescences où ils seront difficiles à retrouver.

La propagation

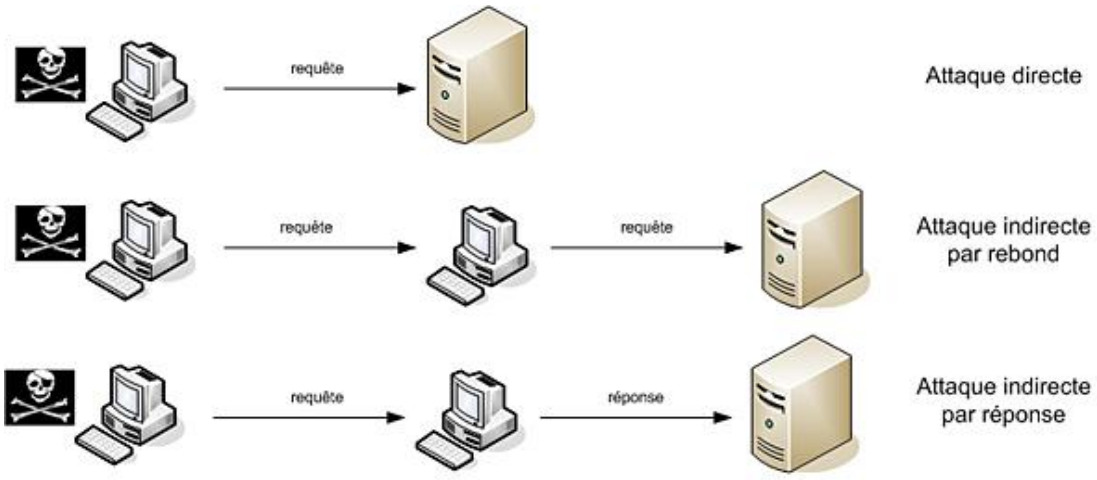
Une fois installé sur une machine, le pirate peut chercher à s'en servir comme base, pour aller plus loin. Cette nouvelle vague d'attaques reprend les étapes précédentes, dans une démarche itérative.

c. Les outils et types d'attaques

Trois familles d'attaques sont répertoriées. La plus simple consiste à tenter une intrusion directe sur la machine visée. Dans ce cas, la source de l'action est uniquement la machine de l'attaquant.

L'attaque indirecte par rebond exploite un ordinateur intermédiaire, qui a pu être compromis précédemment. Masquant la source réelle du piratage, cet intermédiaire relaie les paquets envoyés de celle-ci.

Le dernier moyen est un dérivé de l'attaque précédente, procurant les mêmes avantages. Dans cette attaque indirecte par réponse, le pirate envoie juste une requête, dont la réponse est envoyée à l'ordinateur victime. Une usurpation d'adresse source peut avoir été effectuée pour cela. Et il est très difficile de remonter à l'origine de l'attaque.



Les familles d'attaques

Hormis la pénétration d'un système, les attaques par déni de service (DoS - *Denial of Service*) sont très prisées. Elles visent à solliciter tellement un service réseau qu'il ne répond plus aux demandes légitimes, voire s'arrête. Pour encore plus d'efficacité, des milliers de machines peuvent attaquer simultanément. On parle de déni de service distribué (DDoS - *Distributed Denial of Service*). Là encore, l'aspect mercantile gagne ce type d'attaque, qui peut être précédée d'une extorsion de fond. Par exemple, une entreprise peut désormais se voir menacée d'un envoi massif de mails, évitable par versement d'une somme d'argent.

Les différentes présentations ci-dessous n'ont pas pour but l'exhaustivité. Mais elles reflètent des moyens courants et simples de profiter des faiblesses d'un système.

Ingénierie sociale

Cette technique, appelée en anglais "social engineering", consiste à manipuler des personnes pour contourner les dispositifs de sécurité. Considérant que l'être humain est le maillon faible du système d'information de l'entreprise, l'ignorance ou la crédulité des employés est exploitée.

Cette discipline est particulièrement utile dans les étapes de recherche de renseignements et d'intrusion.

La force de persuasion peut être utilisée pour entrer physiquement dans les locaux, en se faisant passer pour une personne d'un autre site, un technicien intervenant... Très rapidement, différentes informations peuvent être glanées, parmi lesquelles :

- des mots de passe, inscrits sur un post-it collé sur l'écran, sous un clavier... ;
- des informations confidentielles, sur des documents présents sur les bureaux...

De plus, un intrus se promenant dans les locaux de l'entreprise peut utiliser des sessions non verrouillées ou autres facilités offertes.

Un simple coup de téléphone suffit parfois pour obtenir un mot de passe, ou des informations qui seront exploitables ensuite. Sous une certaine pression, beaucoup d'utilisateurs n'hésiteront pas à communiquer oralement leur mot de passe, sans être certains de l'identité de leur interlocuteur.

Une autre technique consiste à demander des informations par mail, en se faisant passer pour quelqu'un d'autre. L'utilisateur ira-t-il vérifier l'adresse de l'expéditeur, dont le nom de domaine est très proche de celui de l'entreprise ?

L'escroquerie par "phishing", issu des mots anglais "phreaking", désignant le piratage de lignes téléphoniques et "fishing" (pêche), en est une variante très efficace. Cette arnaque complète l'envoi de mail par une usurpation de charte graphique de site Web. Elle incite un individu à transmettre des données confidentielles, bancaires par exemple. Un message électronique est d'abord envoyé. Il contient un lien redirigeant vers un faux site aux couleurs de l'entité usurpée. Un numéro comme celui de la carte bancaire sera facilement obtenu.

Le courrier ci-dessous a été publié par la banque de France et se retrouve à l'adresse : http://www.banque-france.fr/fr/instit/telechar/discours/20050620.pdf

BANQUE DE FRANCE
EUROSYSTÈME

Paris, le 20 juin 2005

Mise en garde de la Banque de France

La Banque de France voit son nom et son logo utilisés sans son accord dans un courrier électronique vantant un « nouveau système de paiement par Internet » où elle est citée comme partenaire. La Banque de France ne connaît pas ce système appelé "Global Private Banking" et n'a rien à voir avec lui. Aucun crédit ne doit être accordé à ce courrier reçu par de nombreux internautes français, et qui cherche visiblement à les abuser.

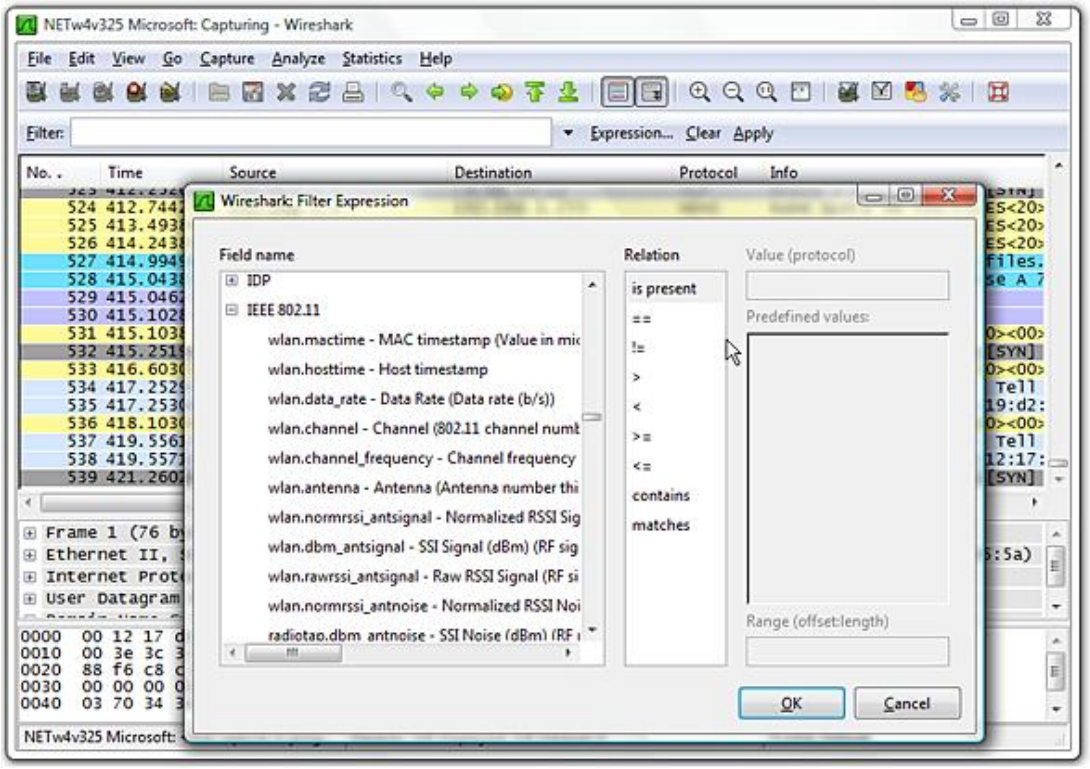
L'utilisateur est au cœur des problèmes de sécurité des réseaux. Sa formation et sa sensibilisation sont nécessaires pour réduire les risques d'ingénierie sociale. L'application de quelques règles de bon sens suffisent parfois.

Écoute réseau

Pour tenter de pénétrer un système, un pirate peut rechercher des renseignements en détournant des outils normalement utilisés dans l'administration des systèmes.

Ainsi, un analyseur de trames est utile pour reconnaître les flux circulant et, le cas, échéant, retrouver les communications qui ralentissent un réseau. Comme il sert à la lecture et l'interprétation des trames capturées, on peut comprendre que toute information en clair diffusée par Ethernet peut être facilement lue.

Dans le monde, des logiciels libres de nombreux projets sont actifs. Parmi ceux-ci, le très célèbre Ethereal a évolué en WireShark. Ce logiciel est capable de reconstituer une session TCP. Cette fonction a d'ailleurs été utilisée lors de la capture de trame présentée dans le point A.1.b de ce chapitre. Gratuit et sous licence GPL, il peut être téléchargé à partir du site : www.wireshark.org.



Le logiciel d'écoute réseau WireShark

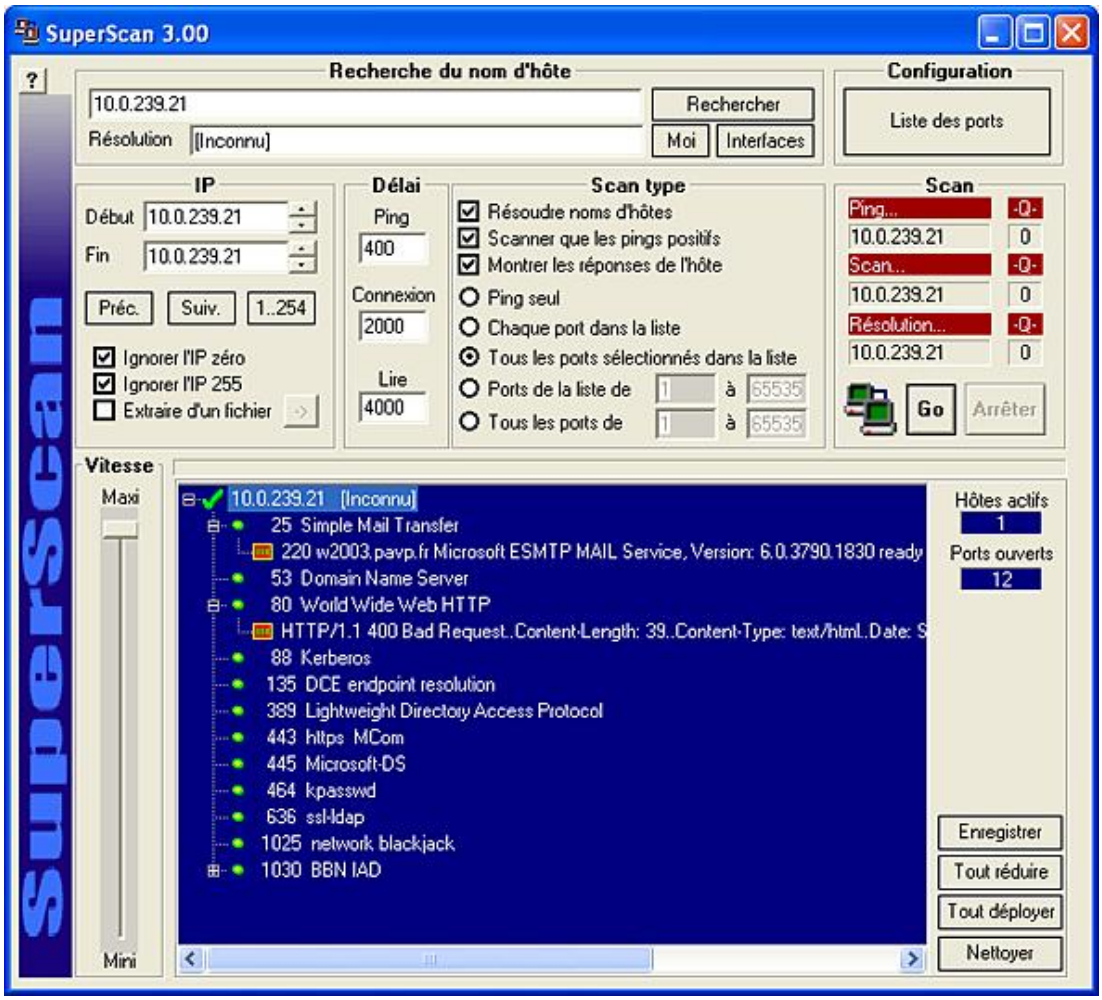
L'écoute réseau, ou sniffing, est avant tout une affaire de connaisseurs, car les outils ne remplacent pas des capacités d'interprétation. Cette technique d'écoute passive est très difficile à détecter. Mais sa portée tend à se réduire sur les réseaux Ethernet, avec l'usage de commutateurs par exemple. L'usage du Wi-Fi relance l'utilisation de l'écoute réseau.

Analyse des ports

Dans un réseau de type TCP/IP, un service serveur écoute sur un port, TCP ou UDP, qui lui est propre. À chacun correspond un numéro, entre 0 et 65 535. La première série, jusqu'à 1024, comprend les ports bien connus (well known port) des applicatifs standard. Parmi ceux-ci, on peut citer :

- 80, pour HTTP ;
- 25, pour SMTP ;
- 53, pour DNS ;
- 21, pour FTP...

L'analyse de ports consiste à les balayer successivement. On parle de "scan". Lorsqu'un port en écoute est sollicité, il répond. Parfois, il renvoie beaucoup d'informations, comme dans la copie d'écran suivante. Ce serveur MS Windows 2003, de test heureusement, cumule, entre autres, les services d'annuaire Active Directory, donc LDAP, et les fonctions de serveur HTTP et SMTP de Internet Informations Server (IIS). Le scanner de ports utilisé est gratuit et extrêmement simple d'emploi.



Résultat de scan, sur un serveur Microsoft Windows 2003, avec le logiciel Superscan

De nombreux logiciels non payants sont disponibles sur Internet, tels que Nmap (*Network mapper*), qui existe pour différents systèmes d'exploitation. Il propose différentes techniques de balayage, plus ou moins discrètes, qui permettent de rendre l'écoute moins active.

Nmap peut être téléchargé à partir de nombreux sites, dont celui de Insecure.

Téléchargement de Nmap sur le site Web de Insecure : http://www.nmap.org

L'outil d'analyse de ports n'est utilisé que dans une phase de recherche de renseignements.

Codes malveillants

De tels logiciels peuvent être composés de deux fonctions distinctes :

- une possibilité de reproduction ;
- une capacité d'attaque, avec une charge nocive.

Souvent désignés sous le terme générique de virus, on peut en réalité les différencier. Cette appellation est clairement définie dans la RFC 1135, qui peut être retrouvé à l'adresse http://www.ietf.org/rfc/rfc1135.txt.

Un virus est donc un bloc de code qui est introduit dans un hôte pour s'y propager, mais nécessite l'exécution de celui-ci pour s'activer. On le différencie du ver (worm), qui se propage par la messagerie ou les failles réseaux et ne contient pas obligatoirement de charge nocive. La bombe logique, à déclenchement conditionnel, par exemple une date, est une troisième variation sur ce thème.

De nombreuses attaques sont provoquées par ces codes malveillants. Leur impact est devenu tel que désormais les grands médias relatent les principales invasions.

Les codes malveillants disposent de deux moyens importants de propagation. Le premier est de continuer d'utiliser la crédulité des utilisateurs, par l'ingénierie sociale. En effet, beaucoup ne résisteront pas à l'intitulé alléchant d'une pièce jointe reçue d'un émetteur pourtant inconnu.

L'exploitation de vulnérabilités des applications est un deuxième vecteur courant de transmission. Les systèmes d'exploitation ne sont pas les seuls touchés. Les navigateurs Web, Internet Explorer et Mozilla Firefox en tête, sont également très vulnérables.

Programmes furtifs

Le cheval de Troie (Troyan horse), ou Troyen, pourrait entrer dans la catégorie des codes malveillants. Mais il n'en contient pas les deux fonctions. Par contre, un ver peut l'installer sur un ordinateur.

Une fois installé, ce programme reste dissimulé. Il peut simplement ouvrir un port réseau, pour être utilisé comme serveur. Le pirate a ainsi pris possession de la machine.

Les logiciels espions, ou spywares, sont une sous-catégorie du cheval de Troie. Ils peuvent être :

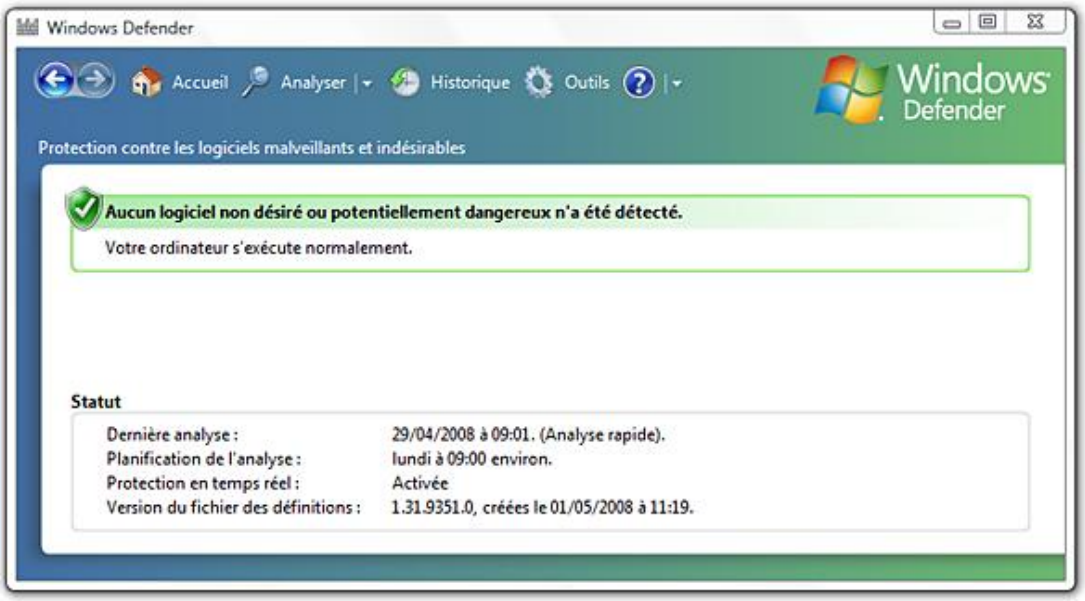
- À vocation commerciale, collectant des données pour cibler des bannières publicitaires ;
- Mouchards, par lesquelles l'information collectée est discrètement renvoyée.

Dans cette dernière catégorie de logiciels espions, les programmes "keyloggers" sont chargés de renvoyer les informations saisies au clavier, comme des mots de passe ou numéros confidentiels.

Les bots, diminutif de robots, sont des logiciels qui permettent de contrôler des machines distantes. Elles deviennent ainsi des "zombies", qui peuvent être utilisées pour lancer une attaque programmée ou servir de relais pour les attaques par spam. Un bot permet également de ne déclencher un mouchard que pour une durée précise, ou d'exécuter un cheval de Troie serveur à la demande.

Dans tous les cas, ces logiciels travaillent à l'insu de l'utilisateur, mais également des informaticiens de l'entreprise.

Microsoft inclut désormais Windows Defender dans ces systèmes d'exploitation, avec une mise à jour de signature mensuelle. Parmi les autres utilitaires semblables, nous pouvons citer celui de la société Lavasoft (www.lavasoft.fr), Ad-aware, ou Spybot search and destroy (www.safer-networking.org).



Microsoft Windows Defender

3. Principes de sécurisation

a. Les services de la sécurité

Répondant aux demandes de garanties nécessaires en terme de sécurité d'un système d'information (SSI), ces services doivent tenir compte des connaissances et analyses effectuées.

Les différents services de sécurité à maintenir sont donc :

- Contrôle d'accès au système ;
- Gestion des habilitations ;
- Intégrité ;
- Non répudiation ;
- Authentification ;
- Confidentialité.

Ces protections s'appliquent à l'information comme aux systèmes supports. Il est indispensable qu'aucune protection ne soit forcée, ni oubliée. Nous traiterons spécifiquement les deux principales à maintenir sur un réseau, l'authentification et la confidentialité.

Contrôle d'accès au système

Il s'agit ici de protéger physiquement les matériels. Il est nécessaire de verrouiller les salles serveurs, mais également désormais les bureaux. En effet, quantité de matériels mobiles, contenant des informations importantes peuvent être subtilisés.

Les systèmes d'exploitation et autres logiciels doivent être sécurisés, par paramétrages et installations régulières des correctifs de failles logiciels.

Les réseaux peuvent être isolés les uns par rapport aux autres, et les communications doivent être filtrées.

Des logiciels antivirus doivent également être installés et maintenus. Des outils de détection d'intrusion (IDS - *Intrusion Detection System*) peuvent compléter les protections nécessaires.

Gestion des habilitations

Avec les logiciels utilisant leur propre système d'habilitation, des failles peuvent vite apparaître. Il est, de toute façon, crucial de ne pas donner plus de permissions que nécessaire aux différents employés et autres utilisateurs du SI.

Grâce aux systèmes d'annuaires, certains systèmes d'information centralisent quelque peu cette gestion. On constate malheureusement que toute la problématique n'est pas résolue.

De plus, l'attribution de permissions est très souvent perfectible dans le temps, où les consignes finissent par être oubliées, sous le flot des exceptions.

Intégrité

Lors des transferts, vérifier l'intégrité, c'est s'assurer qu'aucune modification n'a eu lieu entre l'émetteur et le destinataire (homme ou machine). Elle peut être un très bon complément à la confidentialité. Nous avons vu, par exemple, que les différentes couches du 802.11 emploient pour cela un contrôle de redondance cyclique (CRC - *Cyclic Redundancy Code*).

Le CRC demeure faillible, et peut être retravaillé discrètement par un pirate. Il convient tout de même très bien pour pallier aux problèmes de transmission. Des mécanismes de hachage, calculant une empreinte numérique, demeurent plus fiables.

Une fonction de hachage utilise un algorithme de cryptographie générant un texte de longueur fixe, quelle que soit la taille de celui d'entrée. Le résultat de ce calcul est appelé condensé, empreinte ou haché. Cette fonction est dite à sens unique, puisqu'il n'est en aucune façon possible de retrouver le texte d'origine à partir de l'empreinte, qui est communiquée au destinataire. Celui-ci peut effectuer le même calcul à partir du contenu de la trame envoyée. Il suffit d'une seule modification pour ne pas retrouver le même résultat et considérer que le contenu est altéré. Les deux principaux algorithmes utilisés sont :

- Message Digest 5 (MD5), générant des empreintes de 128 bits ;
- Secure Hash Algorithm 1 (SHA ou SHA1), produisant des résultats sur 160 bits.

Le service d'intégrité, en terme de stockage et d'administration des systèmes, peut être fourni par la journalisation et les audits.

Non répudiation

Ce service est apporté par la notion de signature, qui n'est pas l'authentification. Elle peut nécessiter, pour être valide, la confiance d'un tiers. La signature électronique allie à cette validation d'identité, un calcul d'intégrité par hachage.

Un système d'accusé de réception est utilisé par différentes couches réseaux. Une application comme la messagerie peut l'utiliser.

b. L'authentification

Ce service de sécurité est particulièrement important quand un matériel est connecté à un réseau, donc quand il donne accès à d'autres machines. Il inclut en fait deux fonctions. La première est l'identification, c'est-à-dire la reconnaissance de l'identité. L'authentification elle-même, prouve l'identité déclarée.

Quatre formes de vérification peuvent être exploitées :

- "Ce que je connais", comme un mot de passe ;
- "Ce que je possède", tel un support physique ;
- "Ce que je suis", examinant une caractéristique humaine ;
- "Ce que je sais faire", comme une signature manuscrite.

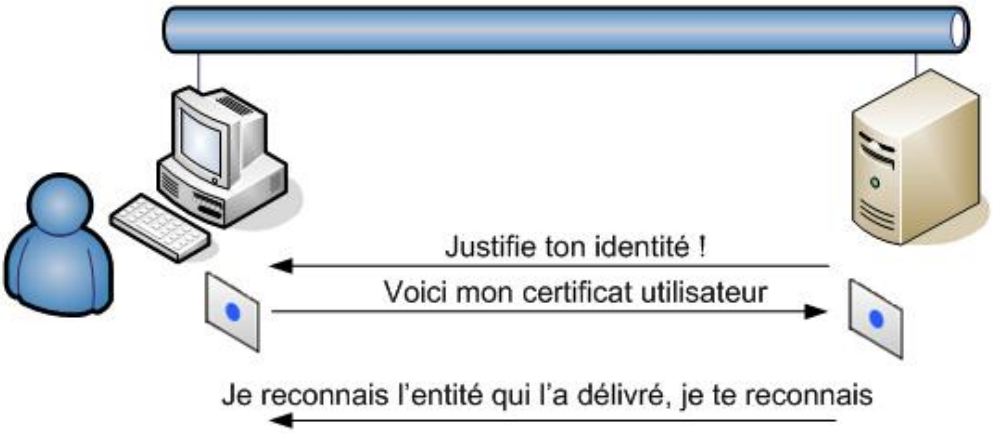
Dans l'authentification informatique, ce dernier cas nécessite un écran tactile. Nous ne le traiterons pas dans la suite.

Quand la portée d'un réseau va au-delà des bâtiments contrôlés, à travers Internet ou par les ondes hertziennes, une réflexion particulière sur le choix du moyen d'authentification est importante. Des solutions, plus élaborées que le mot de passe, sont disponibles, à moindre coût, qui réduisent les risques d'usurpation de l'identité.

Identification

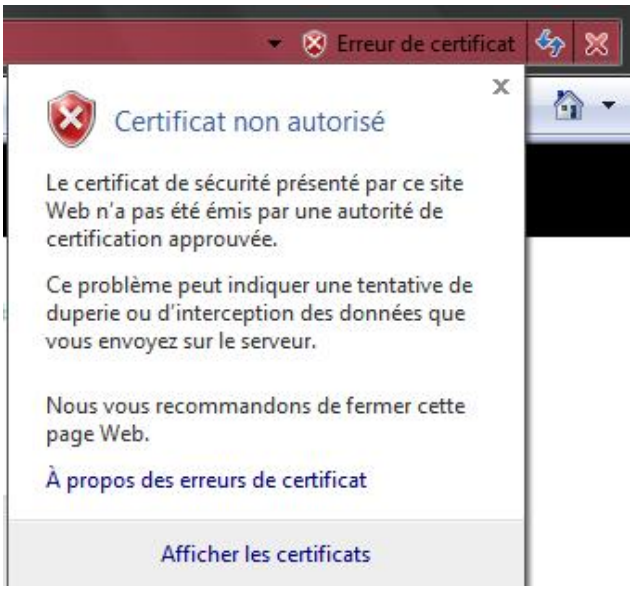
Le principal moyen d'identification prend la forme d'un "login". Saisi par l'utilisateur, son existence est contrôlée dans une base de données ou un fichier.

L'informatique permet, comme dans la vie courante, l'usage d'une sorte de carte d'identité, le certificat électronique. Il doit être reconnu par tous les systèmes, et donc son format est standard. Celui actuel est X509, dans sa version 3.



Processus de reconnaissance d'un certificat électronique

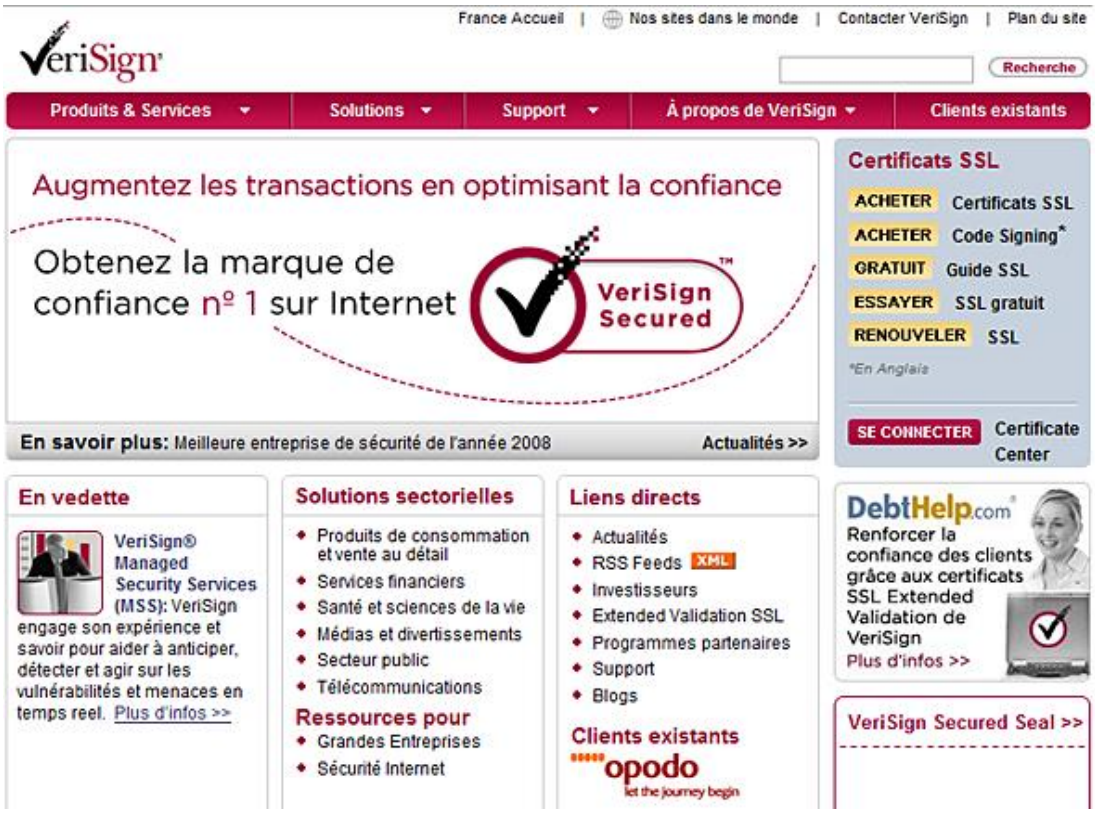
Un certificat électronique est délivré par une entité, l'autorité de certification (CA - *Certificate Authority*), ou l'une de ses délégations. Elle doit être connue de l'ordinateur demandant vérification. Elle est tiers de confiance.



Message d'erreur indiquant la non reconnaissance de l'autorité de certification du certificat

Une entreprise peut mettre en œuvre ses propres serveurs de délivrance et de gestion des certificats. Un tel système est qualifié d'infrastructure de gestion des clés (PKI - *Public Key Infrastructure*), car, et nous le verrons plus loin, la gestion des identités n'est qu'un de ses buts.

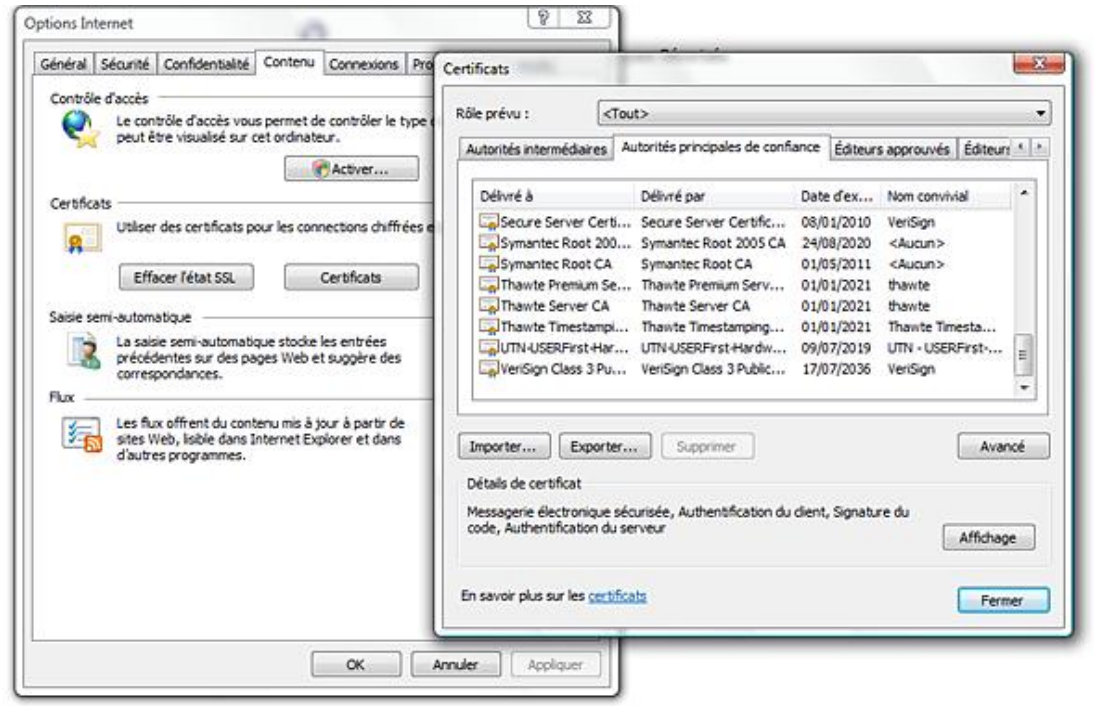
Pour éviter le déploiement et l'administration d'une telle infrastructure, les certificats peuvent être achetés auprès de sociétés spécialisées. Elles sont reconnues et validées au niveau mondial.



Site Web de la société Verisign : http://www.verisign.fr

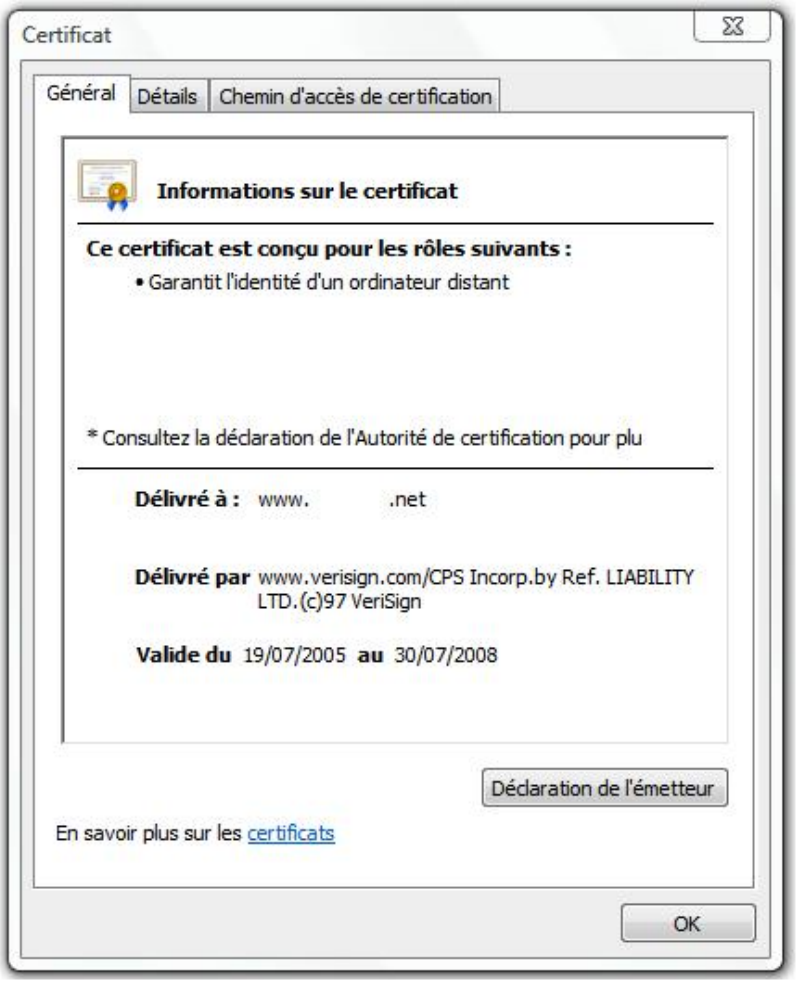
L'identité justifiée par le certificat doit être reconnue. Pour cela, il faut, avant tout, que l'autorité de délivrance soit connue du système qui la vérifie. Sur les systèmes Windows, par exemple, elles sont listées dans les propriétés de l'Internet Explorer, onglet **Contenu**.

Si une infrastructure de gestion des clés a été déployée pour l'entreprise, il est nécessaire de la faire reconnaître sur tous les postes et serveurs concernés.



Liste des autorités principales de confiance du navigateur Internet Explorer

Les certificats électroniques peuvent justifier de l'identité d'un utilisateur ou d'un serveur. Ils ont également de nombreuses autres applications.



Un certificat électronique garantissant l'identité du serveur d'un site Web

Authentification par mot de passe

Le mot de passe représente actuellement le moyen le plus courant d'authentification.

La première catégorie en est le mot de passe statique. Il s'agit d'une simple suite de caractères alphanumériques et spéciaux, choisis par un être humain, pour une durée illimitée ou non. Pour vérifier sa saisie, il est stocké dans un fichier ou une base de données, sur l'ordinateur ou un serveur.

Un tel mot de passe peut être la cible d'attaques diverses, par ingénierie sociale, dictionnaire ou force brute, pour tenter de le retrouver.

L'usage de mots de passe dynamiques réduit la faiblesse d'une telle authentification. Parmi les techniques utilisées, la plus courante allie la connaissance du code d'authentification à un support physique. Chaque mot de passe, appelé également jeton (Token), a un usage unique (OTP - *One Time Password*). Il est proposé à l'utilisateur par un générateur, la carte à jeton, qui le calcule aléatoirement. Un facteur temporel est inclus, pour son unicité. Un composant logiciel correspondant est nécessaire sur le serveur qui validera ce mot de passe. La plus célèbre solution de ce type est le RSA Secure ID.

Modèle de carte à jeton de la solution

Une telle solution est un peu plus complexe à mettre en œuvre que la précédente. De plus, elle nécessite la synchronisation régulière de la carte à jeton avec le serveur. Elle est très difficile à mettre en défaut, tant que le composant physique n'est pas perdu ou volé. L'accès à ce dernier peut être protégé par un code.

Authentification avec support physique

Nous avons vu que les solutions à mots de passe dynamiques peuvent faire appel à un support physique. Mais un tel matériel peut être utilisé seul dans une solution d'authentification. Dans ce cas, la reconnaissance de l'objet, à distance ou par insertion dans un lecteur est nécessaire. Ce moyen est réputé plus sûr que l'usage d'un mot de passe statique. Il peut être plus simple qu'une solution à mots de passe dynamiques.

Le support physique peut être une carte à puce. Son accessibilité logique nécessite complémentairement la connaissance d'un code Personal Identity Number (PIN). Elle est devenue courante avec les cartes bleues, vitales ou Subscriber Identity Module (SIM) de téléphonie mobile.

Une carte à puce nécessite un lecteur spécifique. Elle propose une capacité mémoire et peut ainsi contenir des mots de passe, voire le certificat d'identité de son possesseur.

Un deuxième support peut être une clé USB spéciale. Contrairement à la solution précédente, un connecteur, permettant de lire son contenu, est présent sur tous les ordinateurs modernes. Ce moyen propose également une capacité mémoire pour le stockage d'informations personnelles. Son accès peut être protégé par un code, voire par une reconnaissance d'empreinte digitale.

Authentification par caractéristique humaine

Une empreinte digitale est une caractéristique biométrique. Elle permet de vérifier directement l'identité de la personne et ne nécessite pas de secret complémentaire, code PIN ou mot de passe. Il s'agit du moyen le plus simple pour l'utilisateur et il est très sécurisé. En effet, l'utilisateur porte toujours son identifiant avec lui et il est très difficile de lui voler !

En contrepartie, l'accès à la biométrie est un peu plus complexe, nécessitant des matériels plus onéreux. L'utilisation de l'empreinte digitale est la solution la plus simple, très souvent préférée à d'autres, comme la reconnaissance vocale ou le test de l'iris de l'œil.

La vérification de l'unicité des caractéristiques d'un doigt est désormais très accessible, par l'exploitation de lecteurs spécifiques ou incorporés au clavier, à l'ordinateur portable ou au périphérique mobile. Les nouvelles générations de lecteurs d'empreintes digitales privilégient un passage du doigt en mouvement au lieu de sa pose. Ainsi, l'empreinte digitale ne peut être récupérée suite à l'appui.

Par contre, cette authentification ne permet pas une disponibilité permanente de certaines informations, qui sont stockées dans les cartes à puce et clés USB.

Exemples de lecteur d'empreintes digitales

c. La confidentialité

Rendre secret un message est la première des utilisations des systèmes de cryptographie. Pour cela, une transformation, appelée chiffrement, est réalisée sur l'information, le texte en clair. Le résultat est un texte chiffré, ou cryptogramme. Le texte original est retrouvé normalement par une opération de déchiffrement.

L'expression cryptage est parfois utilisée au lieu du terme chiffrement.

En informatique, des fonctions mathématiques, les algorithmes cryptographiques, génèrent des clés, qui peuvent servir aux calculs de chiffrement et/ou de déchiffrement.

Effectuer un décryptage, c'est tenter de retrouver le texte en clair à partir d'un cryptogramme, sans connaître la clé de déchiffrement. Une telle action est cataloguée comme cryptanalyse.

La nécessité de confidentialité des échanges est encore plus importante sur les réseaux ouverts. Si le paquet ne doit pas être lu entre l'émetteur et le destinataire, il est nécessaire de le chiffrer, afin qu'il ne circule pas en clair. Cela peut être effectué sur les couches basses, moyennes ou hautes du modèle réseau.

En terme de stockage, si une information est considérée confidentielle, le fichier qui la contient doit être chiffré. Une telle action de chiffrement est particulièrement recommandée sur des périphériques portables et mobiles.

Deux familles de systèmes cryptographiques sont utilisées pour rendre confidentiel des communications réseaux. Elles mettent en œuvre :

- des clés symétriques, utilisées à la fois pour le chiffrement et le déchiffrement ;
- des clés asymétriques (privées/publiques), utilisée chacune pour une seule des deux tâches.

Chiffrements à clés symétriques

Cette méthode est la plus ancienne. Une seule et unique clé, générée par un algorithme, est utilisée. Elle est nécessaire pour l'opération de chiffrement comme celle de déchiffrement.

Cette clé, qui doit rester secrète, doit circuler entre l'émetteur et le destinataire. Il s'agit là du principal problème d'usage de ce système.

La fiabilité des échanges de messages chiffrés par clé symétrique dépend de deux facteurs :

- la taille des clés ;
- leur fréquence de renouvellement.

Un juste compromis est nécessaire entre la longueur de clé et la puissance de calcul demandée. En effet, si la clé est trop petite, elle pourra être retrouvée facilement et les paquets perdront leur confidentialité. Si elle est trop importante, les calculs de chiffrement/déchiffrement pourraient demander une capacité processeur incompatible avec les besoins de nombreuses communications simultanées ou l'exploitation de périphériques peu puissants (PDA, smartphone...).

Une clé, dite statique, est saisie manuellement sur les matériels émetteur et destinataire. On peut concevoir que, dans ce cas, le renouvellement de la clé est rare. Ceci augmente d'autant les chances, pour un pirate, de la retrouver. L'usage de méthodes exploitant des clés dynamiques, c'est-à-dire renouvelées régulièrement, est préférable.

Les algorithmes de chiffrement symétrique les plus utilisés sont :

- Rivest's Cipher n°4 (RC4), utilisant différentes tailles de clés, couramment jusqu'à 256 bits ;
- Data Encryption Standard (DES), dont les clés mesurent 56 bits ;
- Triple DES, variante de l'algorithme précédent, chiffrant successivement avec trois clés DES, dont deux différentes ;
- Advanced Encryption Standard (AES), le plus récent, avec des clés atteignant 256 bits.

Chiffrements à clés asymétriques

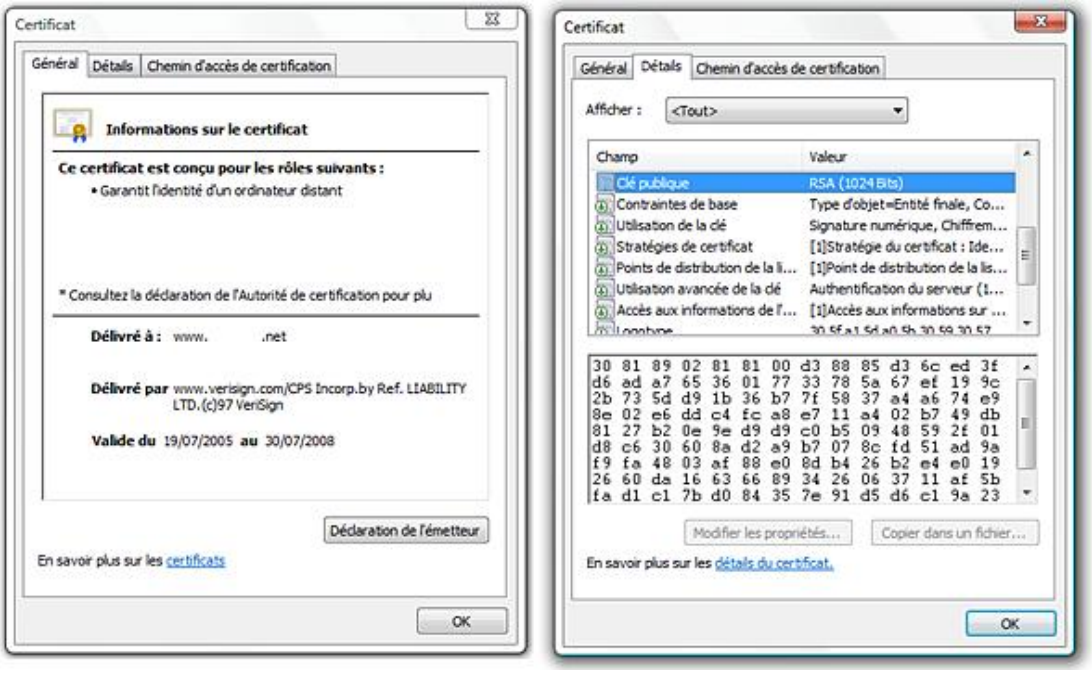
Complémentaires de la technique à clés symétriques, celle-ci utilise deux clés distinctes :

- la première est qualifiée de privée, possession exclusive de son propriétaire ;
- la seconde est publique et circule.

Ces deux clés sont mathématiquement liées. Ce que fait l'une, seule la seconde peut le défaire. Par contre, il n'est pas possible de retrouver l'une avec l'autre. Si un chiffrement est réalisé avec la clé publique, seule la clé privée correspondante, qui reste protégée en permanence, peut déchiffrer le message.

Cette méthode asymétrique implique de ne pas devoir générer systématiquement une nouvelle paire de clés. Cela entraînerait des complications d'administration et de gestion de celles-ci. Une durée de vie plus longue est donc privilégiée, ce qui impose des clés de taille plus conséquente que précédemment.

L'utilisation de chiffrements asymétriques nécessite généralement la mise en œuvre d'une infrastructure de gestion de clés (PKI - *Public Key Infrastructure*), comme celle qui est utilisée pour l'identification. En effet, il est nécessaire d'identifier le possesseur de la clé publique qui circule. Ainsi, ses caractéristiques sont ajoutées au certificat électronique, qui présente également la clé publique à utiliser.



Certificat serveur d'un site Web et clé publique correspondante

Les clés privées sont stockées dans une partie du certificat qui ne circule pas.

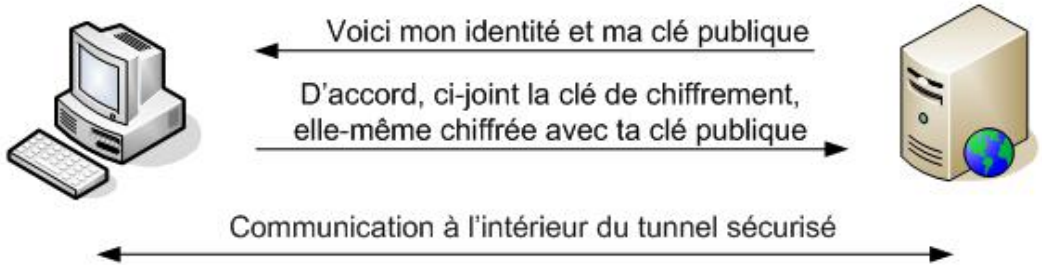
Les certificats électroniques fournissent également, dans leur partie publique, l'algorithme de hachage utilisé pour vérifier l'intégrité des paquets délivrés.

L'algorithme de chiffrement asymétrique le plus utilisé est celui Rivest, Shamir and Adelman (RSA), du nom des trois concepteurs. Il est concurrencé par celui Diffie-Hellman. Les clés utilisées ont couramment des tailles de 1024 ou 2048 bits, voire supérieures.

Pour les communications réseaux, le chiffrement de tous les messages avec de telles clés impliqueraient des puissances de calcul très importantes. C'est donc plutôt la clé symétrique de chiffrement qui est protégée, lors de son transport, par un système asymétrique. À partir du moment où chaque entité possède une clé, un tunnel de chiffrement peut être mis en œuvre. En effet, la communication deviendra incompréhensible pour tout autre système.

Secure Socket Layer (SSL), dont la version 3 est standardisée comme Transport Layer Security (TLS), fonctionne ainsi. Ce protocole de sécurisation des transactions est utilisé, par exemple, dans les communications Web prises en charge par Hyper Text Transfer Protocol over TLS (HTTPS). La mise en place d'une telle sécurité se déroule comme suit.

Le serveur Web fournit d'abord son certificat, qui doit être reconnu par le client. Ce dernier génère une clé de chiffrement symétrique, elle-même chiffrée avec la clé publique fournie avec le certificat. Cette information est ensuite renvoyée au serveur, qui peut retrouver la clé symétrique, grâce à la sienne privée. Ensuite, toute la communication est chiffrée, à l'intérieur d'un tunnel sécurisé.



Processus de mise en œuvre d'un tunnel SSL

Attaques d'un réseau Wi-Fi

Ce réseau local peut être la cible d'attaques indépendantes de la technologie. Toutes les tentatives de récupération de mot de passe, d'usurpation d'adresse IP, d'exploitation de trous de sécurité et autres techniques décrites précédemment sont exploitables.

En plus, un réseau hertzien est faillible à des violations spécifiques. Et parmi celles-ci, le réseau 802.11 présente quelques faiblesses qui lui sont propres. Comme précédemment, la connaissance de celles-ci et des moyens de protection permet de limiter les incidents.

Il est nécessaire de considérer que l'installation d'un périmètre Wi-Fi représente une ouverture du réseau local filaire. L'interconnexion avec celui-ci doit donc être protégée.

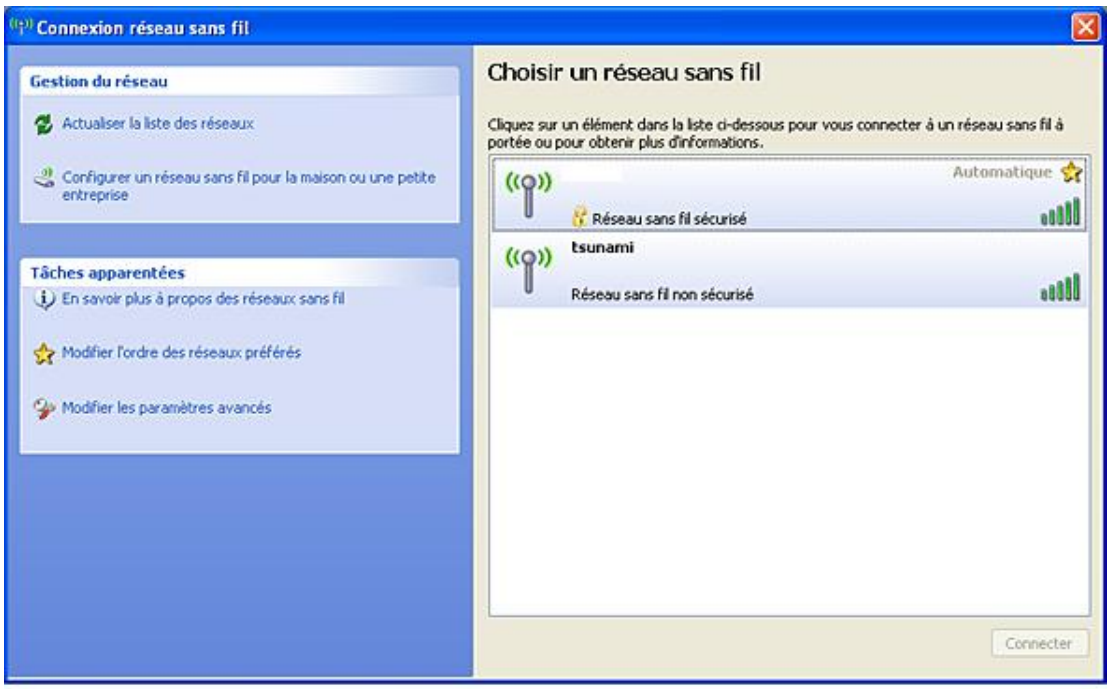
La réflexion sur la sécurité, qui doit précéder l'installation d'un réseau de type Wi-Fi, peut amener à mettre en évidence les failles du réseau filaire déjà en usage. Si la sécurité de l'existant se révèle perfectible, elle devra d'abord être renforcée.

1. Vulnérabilité du 802.11

La première faiblesse des réseaux 802.11 est due à leur rayonnement dans, et en dehors, des locaux. Celui-ci peut être limité, par un choix adéquat d'antenne et un réglage de la puissance des points d'accès. Mais, dans un immeuble, par exemple, on ne peut penser limiter le réseau Wi-Fi à son étage. De même, si l'ensemble, d'un bâtiment doit être couvert par un tel réseau, les ondes radio sortiront des murs et donc les informations circulant également.

L'accès au réseau de l'entreprise ne s'effectue donc pas dans un cadre fermé. Les écoutes, passives ou actives, et l'interception des données depuis l'extérieur, sont concevables.

La connexion d'un poste de travail intrus à un réseau Wi-Fi trop ouvert est très discrète, et parfois même automatique. En effet, nombreux sont les points d'accès qui distribuent également les paramètres IP, en plus de permettre une association facilitée. Souvent, une fois connecté ainsi de manière illicite au réseau d'entreprise, l'intrus accède à Internet en toute discrétion. Cette connexion peut être le point de départ d'actions répréhensibles sur ce réseau public, en tout anonymat. L'entreprise pourrait être tenue pour responsable de celles-ci.



Détection de présence par Windows d'un point d'accès de marque Cisco, non protégé, repérable par son SSID "tsunami"

Un signal radio peut être brouillé et le Wi-Fi n'est pas lui-même conçu pour se protéger de telles attaques de déni de service. D'autres faiblesses sont directement imputables au fonctionnement de la couche MAC, par exemple en utilisant de manière pernicieuse certaines trames de gestion.

Les spécifications 802.11 ne prévoient pas de processus d'authentification du point d'accès. La borne légitime peut donc être supplantée par une autre, pirate. Les postes de travail client pourraient se connecter à cette dernière en toute transparence.

La reconfiguration distante de points d'accès mal sécurisés est un autre danger. En effet, une borne est potentiellement paramétrable de l'extérieur de l'entreprise, en fonction de la portée du réseau hertzien. Il suffit ensuite de connaître un compte d'administration et son mot de passe. Ces derniers doivent donc être discrets et protégés par des moyens forts.

Il est, de plus, nécessaire de protéger physiquement les équipements Wi-Fi d'infrastructure. Le vol d'une borne permet de s'attarder sur ses protections et de répertorier des caractéristiques du réseau.

2. Attaques

a. L'écoute du réseau

Recherche de réseaux sans fil

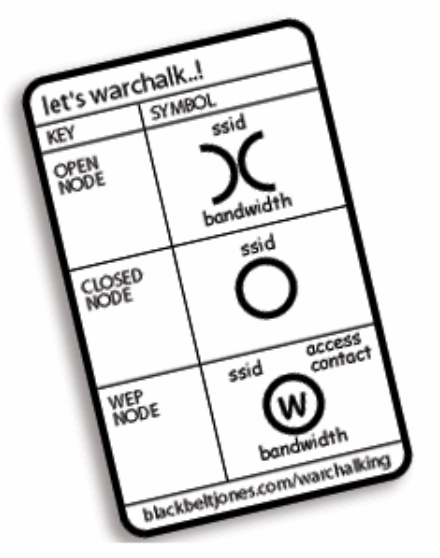
Nous avons vu précédemment que le Wi-Fi est très bavard, particulièrement avec les configurations par défaut, annonçant également le SSID. La recherche de réseaux Wi-Fi détectables sur la voie publique est nommée Wardriving.

La cartographie des réseaux, à l'aide d'un ordinateur portable ou d'un assistant personnel, nécessite juste une carte réseau Wi-Fi et un logiciel d'écoute, comme NetStumbler, également utilisé par l'administrateur du réseau.

Le logiciel MiniStumbler, version pour PocketPC de NetStumbler

Un tel logiciel d'écoute peut être associé à un système de Global Positioning System (GPS), permettant de positionner le point d'accès sur une carte.

La personne ayant détecté le réseau peut simplement noter sur place, à la craie, son emplacement et son niveau de protection. Cette action porte le nom de Warchalking. Deux étudiants londoniens ont inventé un code simple pour ce repérage, qui a été très prisé.



Carte des sigles de Warchalking

Il faut noter que de telles actions deviennent vites répréhensibles, puisqu'elles peuvent être assimilées à une écoute des informations du réseau de l'entreprise. De plus, elles peuvent être le point de départ d'une attaque plus précise.

Recherche d'informations

Une fois le réseau Wi-Fi trouvé, une écoute passive, par collecte des trames peut être réalisée. Des outils, comme kismet, téléchargeable sur www.kismetwireless.net, peuvent, là encore, être détournés de leur exploitation légale.

L'analyse de ces trames, permet la reconstitution des informations et données circulant. Une telle intrusion passive peut également fournir des renseignements stratégiques sur le réseau de l'entreprise, comme les adresses IP des serveurs, les protocoles utilisés...

b. Le déni de service

Sur un réseau Wi-Fi, la première possibilité d'attaque par déni de service est l'utilisation des interférences radio. En pratique, cela nécessite au brouilleur d'être proche physiquement et d'avoir une réelle volonté de faire tomber ce réseau, ce qui limite quand même le risque.

Différentes méthodes utilisent les trames de gestion de la couche MAC. Elles nécessitent généralement la mise en œuvre d'un point d'accès pirate, ou Fake AP.

Une telle borne peut servir, par exemple, à envoyer des trames de balises ciblées. Elle empêche ainsi les connexions des utilisateurs au point d'accès de l'entreprise.

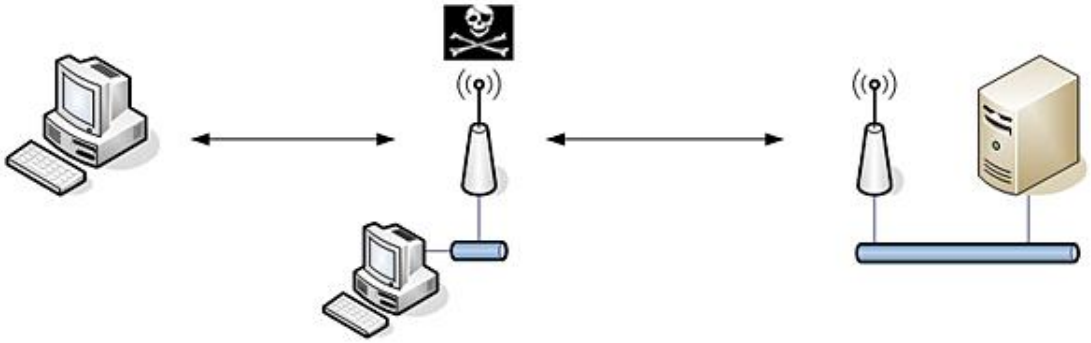
Une autre solution consiste en l'envoi, par ce point d'accès illicite, de trames de désassociation, à destination de stations connectées. Celles-ci chercheront ensuite à se connecter à nouveau au point d'accès. Il tentera ainsi en permanence de réassocier les clients. Pendant ce temps, il ne peut plus transporter les trames de données.

D'autres attaques DOS sont possibles, y compris sur les couches applicatives. Mais pour ces dernières, cela ne concerne plus directement le Wi-Fi.

c. L'intrusion active dans le système

Un intrus peut exploiter un réseau Wi-Fi, comme il le ferait d'un réseau filaire, pour atteindre les serveurs et les emplacements de stockage.

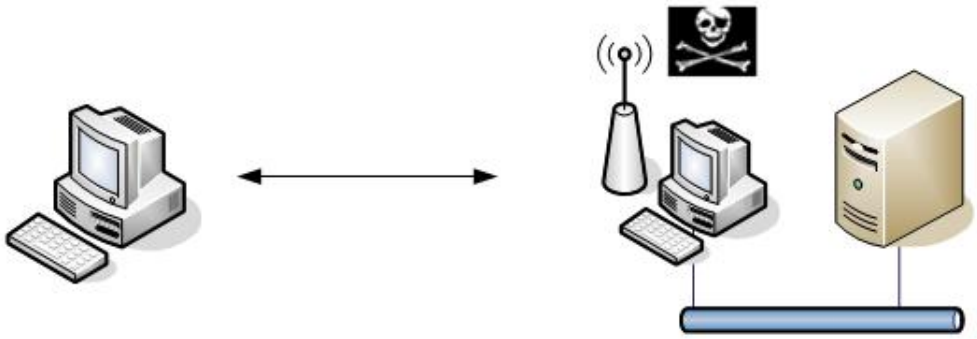
Son action consiste d'abord à la simple interception des trames qui transitent. Leur modification pourrait être possible. Pour cela, le pirate doit s'interposer entre la station et le point d'accès. Une telle situation d'attaque porte le nom de Man in the Middle (MiM).



Placement d'un point d'accès Man in the Middle

Une première solution pour réaliser une attaque MiM consiste à mettre en œuvre un point d'accès illicite, ou fake, afin de capter les demandes d'association des stations. Ensuite, un travail doit être réalisé au niveau des informations transmises, pour donner l'illusion d'une communication normale. Pour cela, les techniques d'usurpation d'adresse MAC peuvent être exploitées. Ainsi, par exemple, la borne pirate se fait ensuite passer pour une station légitime auprès du point d'accès de l'entreprise.

Si le pirate a obtenu un accès physique au réseau filaire pour son installation, il sert lui-même directement d'intermédiaire entre les réseaux Wi-Fi et Ethernet.



Placement MiM, borne illicite connectée physiquement au réseau

Cette dernière situation est très profitable pour l'intrus, qui peut écouter les communications. Mais rien ne l'empêche, avant retransmission, de modifier discrètement les contenus de trames. L'attaque MiM autorise toutes les actions répréhensibles, jusqu'au déni de service.

3. Solutions de protection

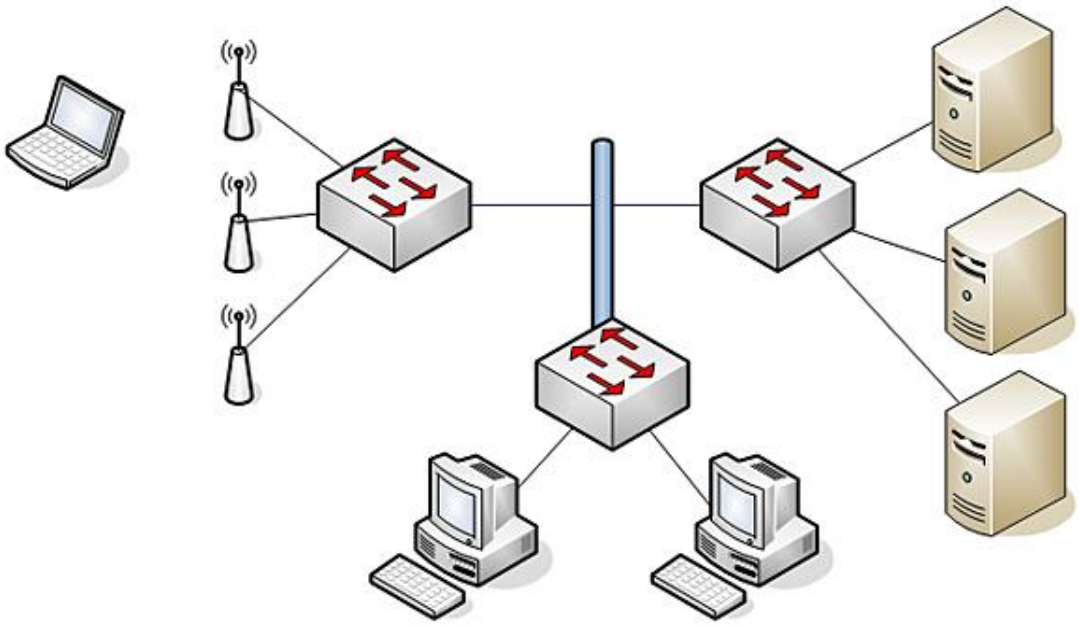
Nous avons vu précédemment qu'un certain nombre de moyens permettent d'attaquer un réseau de type 802.11.

Il n'est pas vraiment possible de protéger les communications contre des dénis de service. Par contre, la position d'un équipement réalisant du DOS se retrouve. Pour cela, des solutions de supervision peuvent être utilisées. Certains points d'accès sont capables de diagnostiquer des états anormaux, au niveau radio et de remonter l'information à des équipements dédiés. Des solutions, utilisant des sondes d'analyses de trames, sont un autre moyen de détection.

Si la portée du réseau reste limitée et ne déborde pas trop à l'extérieur des murs, les risques d'attaques se réduisent.

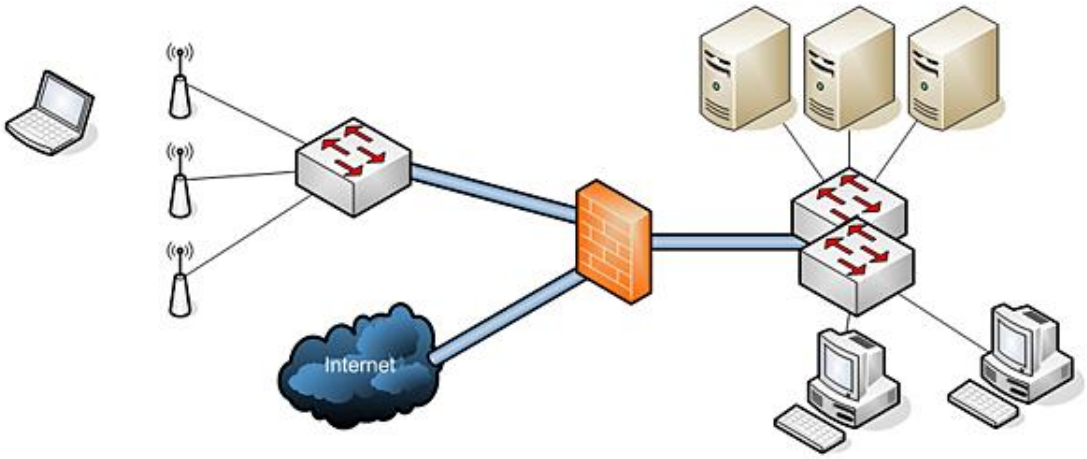
Afin de ne pas provoquer certains des déboires cités précédemment, il est fortement recommandé d'empêcher tout branchement parasite sur le réseau Ethernet, comme celui d'une borne illicite. La protection de ce réseau filaire et des prises de connexion sur les commutateurs, sont donc nécessaires.

En fait, il est recommandé de considérer le réseau Wi-Fi comme étant une possibilité d'accès externe au réseau de l'entreprise. Il doit donc être isolé de tous les autres réseaux.



Isolation physique du réseau Wi-Fi, par commutateur dédié

Mais la compartimentation peut être réalisée sur les niveaux supérieurs. Un pare-feu de niveau 3, voire applicatif, peut être mis en place, afin d'analyser les trafics et d'empêcher ceux anormaux.



Isolation physique puis filtrage des communications Wi-Fi avec un pare-feu

Ces protections architecturelles, doivent ensuite être complétées de solutions d'authentification et de chiffrement. Elles permettent d'éviter les écoutes, les intrusions, les attaques de type MiM...

Les spécifications 802.11 proposent des solutions d'authentification très basiques, utilisant un filtrage des adresses MAC ou un secret partagé. Nous verrons dans le chapitre suivant que de telles protections peuvent être rapidement insuffisantes dans un environnement professionnel.

La méthode Wired Equivalent Privacy (WEP), expression qui peut être traduite par privatisation équivalente au réseau filaire, a montré un certain nombre d'insuffisances. Un simple calcul CRC est chargé de la vérification d'intégrité.

Une seconde génération de sécurisation a succédé à WEP. La solution Wi-Fi Protected Access (WPA) différencie même le niveau de protection recommandé pour la maison, de celui nécessaire dans l'entreprise. Elle allie authentification et méthode de chiffrement. Dans le premier cas, la connaissance d'une clé partagée par la station et le point d'accès, suffit pour mettre en œuvre la communication. Dans un milieu professionnel, l'authentification est prise en charge par le standard IEEE 802.1x. Le protocole Temporal Key Integrity Protocol (TKIP) permet l'exploitation de clés changeantes, donc dynamiques. Un calcul d'intégrité plus fiable, Message Integrity Code (MIC), est également mis en œuvre.

WPA2 est l'appellation commerciale du standard IEEE 802.11i. Cette troisième solution vient compléter les capacités de la précédente, avec un chiffrement encore plus fort. Ici l'algorithme Advanced Encryption Standard (AES) est utilisé. Le calcul d'intégrité lui-même est renforcé.

Solution	Protocole	Authentification	Chiffrement
WEP	WEP	Optionnelle	RC4
WPA pour la maison	TKIP	Clé partagéee	RC4
WPA pour l'entreprise	TKIP	802.1x	RC4
WPA2 pour la maison	CCMP	Clé partagéee	AES
WPA2 pour l'entreprise	CCMP	802.1x	AES

Les différentes méthodes d'authentification et chiffrement du Wi-Fi

Les propositions WPA et WPA2 pour l'entreprise peuvent être considérées comme sûres. Leur niveau de chiffrement permet une confidentialité évitant écoute et intrusion. Leur niveau d'authentification permet également d'éviter l'insertion d'un point d'accès pirate.

Ces différentes solutions seront développées dans les chapitres suivants.

Protections complémentaires

Les spécifications 802.11 couvrent les couches basses du modèle OSI. Les protections qui peuvent être directement associées au Wi-Fi correspondent donc aux niveaux Physique et Liaison de données.

Il est possible de considérer des solutions plus génériques, portant sur ces mêmes couches, voire celles de niveau supérieur. Elles peuvent venir compléter ou remplacer les solutions spécifiques au réseau radio.

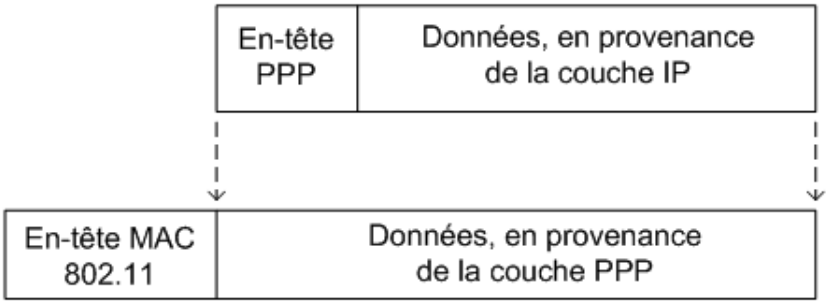
Ainsi, considérant que Wi-Fi est un réseau externe, comme Internet, la communication peut traverser un réseau privé virtuel (RPV), en anglais Virtual Private Network (VPN). Les points clés, au niveau de la sécurité, restent l'authentification, le chiffrement et les calculs d'intégrité.

Enfin, une isolation forte des communications hertziennes, physiquement ou logiquement, peut être appliquée entre elles ou par rapport au réseau filaire Ethernet.

1. Réseaux privés virtuels

a. Le fonctionnement

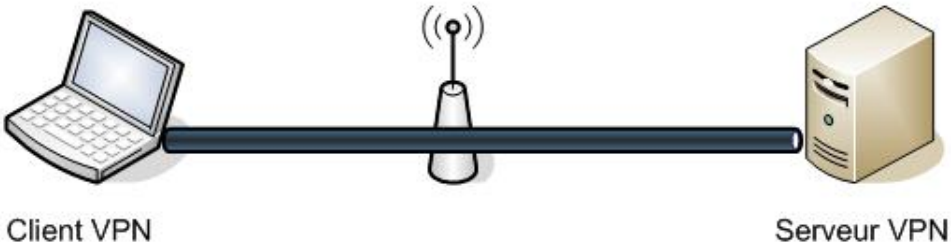
Les mécanismes de réseaux privés virtuels, ont pour but de privatiser une infrastructure réseau publique. Ils sont particulièrement utilisés à travers Internet. Un tunnel d'isolation virtuel est ainsi monté, entre deux terminaisons. Cette communication est de type point à point, entre un client et son serveur. Le transport des données est assuré par un protocole spécifique : Point to Point Protocol (PPP).



Encapsulation du protocole PPP dans Wi-Fi

Pour mettre en œuvre la session VPN, une connexion au réseau doit d'abord être établie. Ainsi, dans un réseau Wi-Fi, l'association de la station au point d'accès est d'abord effectuée. Cette étape n'est pas nécessairement sécurisée.

Ensuite, pour avoir accès au réseau local Ethernet, par l'intermédiaire de la borne, l'utilisateur doit établir une connexion à l'aide d'un logiciel client VPN. Le tunnel est ainsi créé, avec un serveur VPN placé de l'autre côté.



Tunnel sécurisé VPN traversant le point d'accès

Le point d'accès reste traducteur entre les trames 802.11 et Ethernet. Il traite ainsi les en-têtes du premier protocole, encapsulant ensuite les paquets PPP dans l'autre et réciproquement.

Les garanties d'authentification, de chiffrement et de vérification d'intégrité, peuvent être à la charge exclusive du réseau privé virtuel. Il est quand même possible de renforcer certaines protections sur le point d'accès lui-même. Certains modèles sont même capables d'assurer eux-mêmes les fonctions de serveur VPN.

b. L'authentification

Lorsque le client VPN demande accès à son serveur, l'authentification de l'utilisateur est, avant tout, exigée.

Le transfert des informations d'identification et de mot de passe, peut être pris en charge, de manière plus ou moins sécurisée, par un certain nombre de protocoles standardisés, à travers PPP :

- Password Authentication Protocol (PAP), peu recommandable car le mot de passe circule en clair ;
- Challenge Handshake Authentication Protocol (CHAP), ne transmettant qu'un hachage du mot de passe, mais encore très perfectible en terme de sécurité ;
- Microsoft CHAP version 1 (MS-CHAPv1) et version 2 (MS-CHAPv2), versions améliorées de la précédente.

Une véritable assurance de sécurité est apportée par le mécanisme Extensible Authentication Protocol (EAP), qui permet différents moyens d'authentification, y compris l'usage d'un support physique ou de la biométrie.

Le couplage d'EAP avec les standards IEEE 802.1x et RADIUS forme une solution qui peut être très sécurisée.

C'est d'ailleurs celle qui a été retenue pour WPA et WPA2 en environnement professionnel. Nous en reparlerons dans les chapitres suivants.

c. Le chiffrement

Une fois l'étape d'authentification passée, le tunnel de communication peut être mis en place, à différents niveaux du modèle OSI :

- Couche 2, avec Layer 2 Transport Protocol (L2TP) ;
- Couche 3, avec Point to Point Tunneling Protocol (PPTP) ou IP Security (IPSec) ;
- Couches supérieures avec, par exemple, SSL/TLS.

Les deux protocoles PPTP et L2TP utilisent PPP pour transporter les données. L2TP allège les en-têtes, avec une compression possible à 4 octets au lieu de 6.

Le chiffrement, dans PPTP, est fourni par le protocole Microsoft Point to Point Encryption (MPPE), utilisant l'algorithme RC4. Des clés de 40, 56 ou 128 bits peuvent être exploitées. L'authentification peut être assurée par MS-CHAP1 ou MS-CHAPv2, par exemple.

Si la confidentialité des informations transmises par L2TP est nécessaire, elle est assurée par le standard IPSec.

Un filtrage des communications peut être effectué, sur le point d'accès lui-même ou juste après, sur le réseau Ethernet, afin de ne laisser passer que les paquets VPN souhaités. Pour PPTP, le transit du protocole Generic Routing Encapsulation (GRE), numéroté 47 dans l'en-tête IP, doit être autorisé. L2TP utilise le port UDP numéroté 1701. L'usage de IPSec nécessite la transmission des trafics à travers le port UDP 500, pour l'échange de clés.

Filtrage PPTP avec un pare-feu

Il est recommandé de privilégier l'usage du couple L2TP/IPSec, plus que PPTP/MPPE, pour la réalisation d'un tunnel VPN sur les couches 2 et 3. Le protocole IPSec fournit différents services qui sont détaillés ci-dessous.

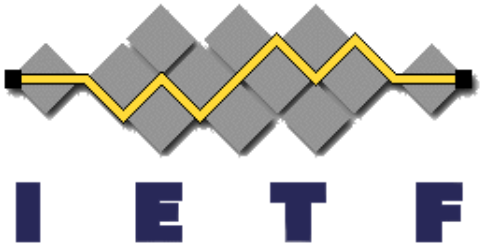
De nouveaux types de réseaux VPN sont apparus récemment. Considérant que tous les postes utilisateurs sont

capables d'interpréter les trames SSL/TLS, grâce aux navigateurs par exemple, VPN-SSL privilégie une solution sans déploiement ni installation de client (client less). De plus, les trafics sécurisés par ce moyen utilisent un port potentiellement plus couramment ouvert sur les pare-feu, le TCP 443, correspondant à HTTPS.

2. IPSec

a. Les services

Le but de l'organisme Internet Engineering Task Force (IETF) est l'amélioration du fonctionnement du réseau Internet. Comme pour l'IEEE, des groupes de travail définissent des standards, qui sont ici documentés dans des publications Request For Comments (RFC).



Site Web de l'IETF : http://www.ietf.org

Une RFC est repérée par un numéro unique. Chaque évolution fait l'objet d'une nouvelle documentation, qui peut compléter ou rendre obsolète la précédente. Il n'y a pas de mise à jour de RFC.

Les différents usages de IPSec ont été défini par l'IETF, dans plusieurs RFC, numérotées 2401 (http://www.ietf.org/rfc/rfc2401.txt), 2402, 2406 et 2408. Cette solution est disponible de façon optionnelle avec IP version 4, avant d'incorporer la version 6 de ce protocole.

La suite IPSec est conçue pour assurer plusieurs types de sécurisation :

- Confidentialité et protection contre l'analyse du trafic, par le chiffrement ;
- Authenticité des données et contrôle d'accès, par une authentification mutuelle des deux extrémités de la communication, la signature, ainsi que des calculs d'intégrité ;
- Protection contre l'injection de paquets, l'anti-rejeu.

Le rejeu (replay) est une technique, utilisable par un intrus, qui consiste à renvoyer des paquets capturés lors d'une communication réseau légitime. Le serveur reçoit ainsi à répétition la même information. Il doit systématiquement la retraiter et peut mal interpréter ces paquets tous identiques. Pour éviter cette relecture, une fonction d'anti-rejeu ajoute un numéro de séquence aux informations. Ainsi le serveur est capable de distinguer des paquets déjà reçus, et évitera leur traitement.

Comme la sécurisation IPSec agit au niveau de la couche IP, elle est indépendante des couches basses. Peu lui importe que les paquets IP sécurisés soient transportés par Ethernet, Wi-Fi ou tout autre protocole de ce niveau. De même, tous les types de données, indépendamment des applications, peuvent être sécurisés par ce moyen.

IPSec distingue deux niveaux de protection, à travers deux protocoles :

- Authentication Header (AH), qui ne prend en charge que l'authentification, le contrôle d'intégrité et l'anti-rejeu ;
- Encapsulating Security Payload (ESP) qui ajoute la fonction de confidentialité.

AH et ESP peuvent être utilisés ensemble ou séparément, en fonction du niveau de protection souhaité.

Le processus complet IPSec comporte, au préalable, une phase de négociation du niveau de sécurité souhaité entre les deux extrémités. Cette association de sécurité (SA - *Security Association*) est unidirectionnelle et dépendante de chaque protocole. Jusqu'à quatre SA peuvent donc être mis en œuvre, chacune précisant :

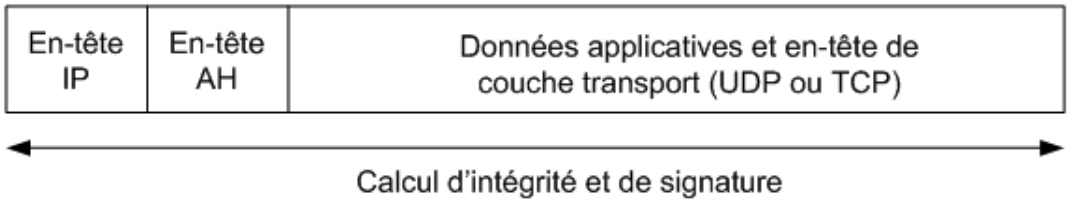
- un identifiant unique d'association, le Security Parameters Index (SPI) ;
- le type de trafic IP qui doit être sécurisé ;
- le protocole utilisé ;
- les algorithmes de hachage, voire de chiffrement retenus.

Si des clés de chiffrement sont nécessaires, la négociation s'effectue également à ce moment. Un tunnel est d'abord créé, sous la forme d'une SA, par le protocole standard dédié à cet usage, Internet Security Association Key Management Protocol (ISAKMP). L'échange de clés est ensuite pris en charge par Internet Key Exchange (IKE), utilisant le port UDP 500. IKE est également utilisé lors d'un renouvellement de clé durant une session.

b. Le mode transport

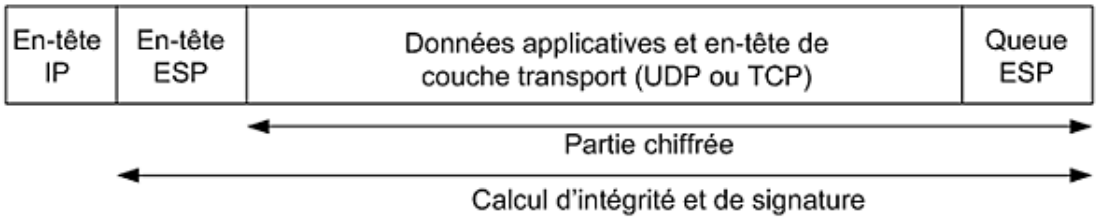
Le mode transport protège une communication spécifique entre deux entités. Ainsi, les paquets de communication d'une application, correspondant à un port TCP donné, peuvent être sécurisés, sans que cela n'influe sur l'ensemble des trafics.

Si une encapsulation par Authentication Header a été négociée, un contrôle d'intégrité est réalisé sur tout le paquet, incluant les adresses IP source et destination. La provenance des données, comme leur authenticité, est donc garantie. Ce calcul d'intégrité utilise les algorithmes MD5 ou SHA.



La trame AH en mode transport

Le contrôle d'intégrité réalisé par Encapsulating Payload Protocol ne prend pas en compte l'en-tête IP. En revanche, la communication est chiffrée, par DES ou 3DES.



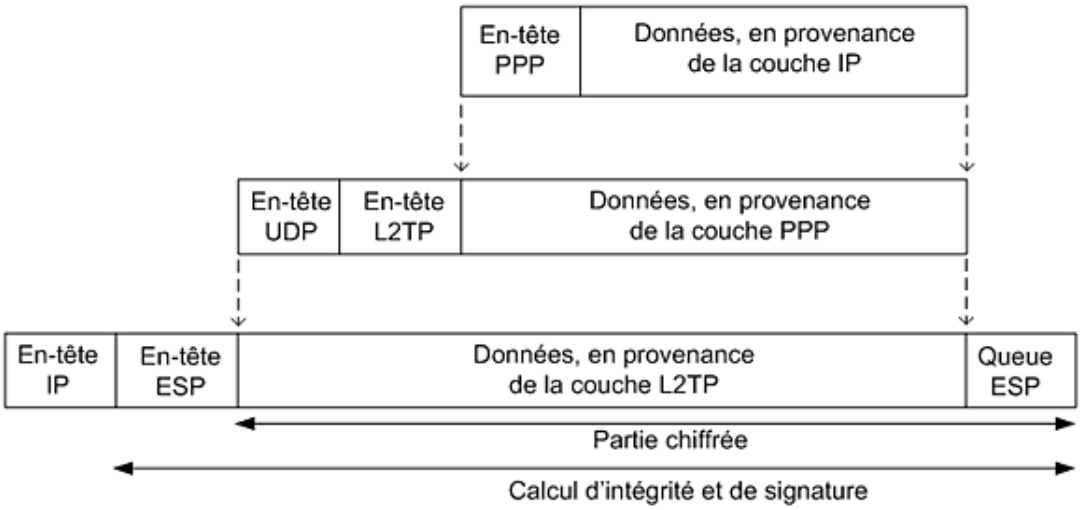
La trame ESP en mode transport

L'encapsulation des paquets ESP dans AH permet à la fois un contrôle d'intégrité sur l'ensemble de la trame et son chiffrement.

c. Le mode tunnel

Le mode tunnel est utilisé pour protéger l'ensemble des communications entre deux entités. Il s'agit typiquement de la configuration d'IPSec utilisée avec L2TP, dans le cadre d'un VPN.

Là encore, les protocoles AH et ESP peuvent être utilisés.



La trame ESP en mode tunnel

L'encapsulation de la totalité des paquets dans un tunnel ESP apporte les mêmes sécurisations que dans le mode transport, pour toutes les applications. Comme précédemment, l'intégrité peut être renforcée avec AH, qui la calculera en incluant les adresses IP source et de destination.

Un VPN L2TP, avec IPSec en mode tunnel, offre une alternative avec une solution de sécurité dédiée au protocole 802.11.

3. Isolation du réseau

a. Les VLAN

L'interconnexion des hôtes Ethernet par l'intermédiaire de commutateurs (switchs), plutôt que par des concentrateurs (hubs), a eu pour premier effet de supprimer la diffusion, par l'équipement centralisateur, de l'ensemble des trames reçues. Cette aptitude est apportée par un traitement au niveau de la couche 2, Liaison de données, du modèle OSI.

Les capacités d'administration des commutateurs ont permis l'apport de fonctionnalités avancées, comme les Virtual Local Area Network (VLAN), autorisant une segmentation logique du réseau. Ainsi, il devient possible de contrôler, voire d'empêcher tout dialogue entre équipements interconnectés sur un même commutateur.

La compartimentation logique peut être effectuée de plusieurs manières. Un VLAN, qualifié d'implicite, peut être réalisé à partir de différents critères :

- les numéros de ports du commutateur, sur la couche 1 OSI ;
- les adresses MAC des matériels qui y sont reliés, sur la couche 2 OSI ;
- le protocole utilisé, sur la couche 3 OSI.

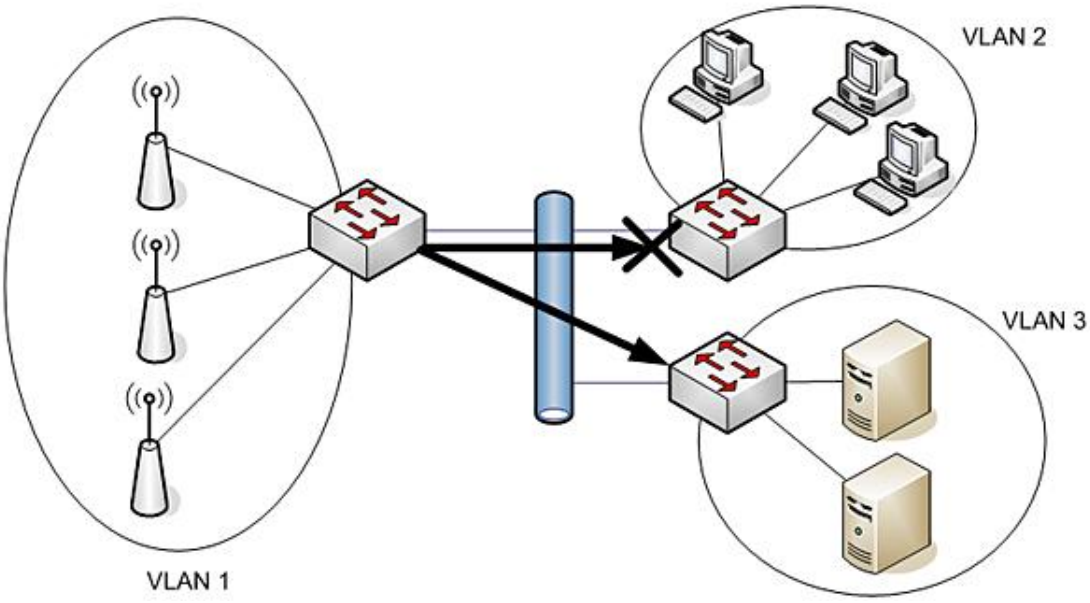
Les commutateurs capables de traiter les en-têtes de niveau IP peuvent également utiliser les adressages logiques de ce protocole comme critère d'isolation. Par exemple, des sous-réseaux IP peuvent correspondre à des VLAN distincts.

Si les clients des points d'accès sont tous membres d'un même sous- réseau IP, une telle compartimentation peut présenter un grand intérêt.

L'IEEE, avec le standard 802.1q, a complété les capacités des réseaux locaux virtuels en définissant une étiquette de VLAN (VLAN tag), qui complète la trame Ethernet. Les VLAN explicites permettent ainsi la segmentation au travers de plusieurs commutateurs. Prenons exemple d'un cœur de réseau, commutateur de niveau 3, contenant la déclaration des différents VLAN utilisés, associant pour chacun un sous-réseau et un identifiant de VLAN. Les différents commutateurs associés à ce cœur connaissent et utilisent ces VLAN.

La virtualisation des réseaux locaux, donc le découpage logique, peut présenter un très grand intérêt dans une interconnexion de réseaux hertzien avec celui local filaire. Elle permet de distinguer les communications en

provenance de stations Wi-Fi et de les isoler en conséquence.

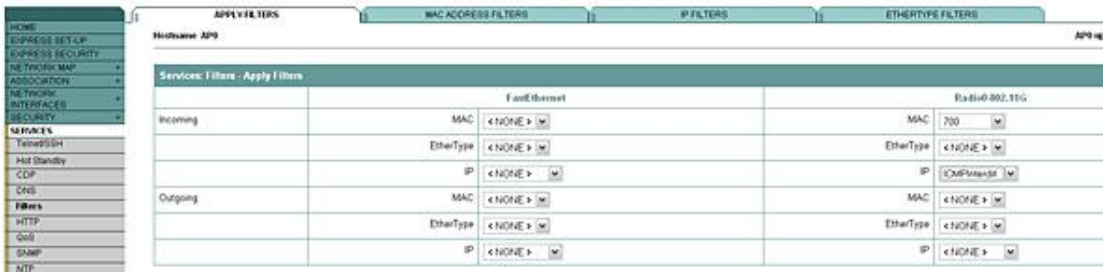


Exemple de VLAN évolué, blocage des communications du Wi-Fi vers les postes de travail LAN

b. Les réseaux indépendants

Une indépendance réelle entre réseaux peut être apportée par la mise en œuvre d'un pare-feu. Celui-ci peut être placé derrière le commutateur regroupant les bornes.

Certains point d'accès eux-mêmes proposent des fonctionnalités de filtrage entre les interfaces filaires et non filaires.

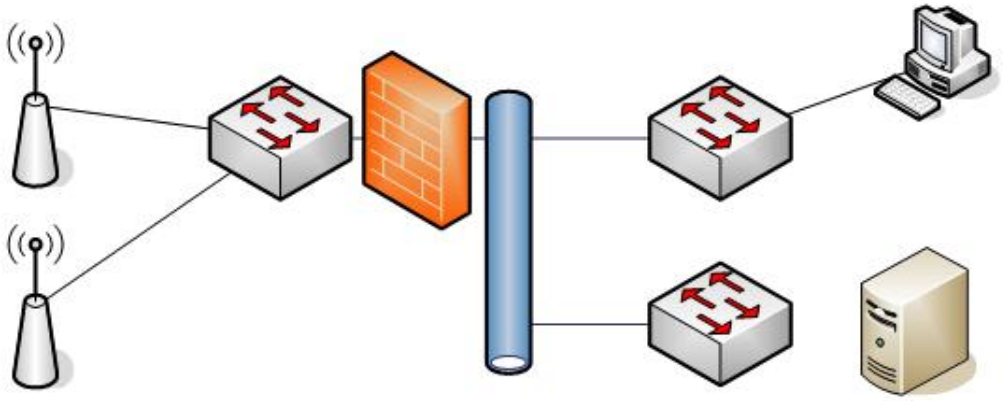


Possibilité de filtrage des communications sur un point d'accès de marque Cisco

Une segmentation par pare-feu est complémentaire de l'usage d'un VPN ou d'un VLAN et n'empêche pas leur usage. Ici, il s'agit de vérifier que le trafic est bien conforme à ce qu'il doit être.

Ainsi, un pare-feu analyse les en-têtes des couches moyennes, 3 et 4 du modèle OSI, afin de bloquer les paquets sur des conditions telles que :

- le type de protocole ;
- les adresse IP, source comme destination ;
- les numéros de port TCP et UDP...



Exemple de positionnement d'un pare-feu derrière le réseau hertzien

La nouvelle génération de pare-feu, dite applicative, devient capable d'analyser certains corps de paquets, tels que ceux des protocoles Simple Mail Transport Protocol (SMTP), Hyper Text Transfer Protocol (HTTP)... Un tel niveau d'analyse permet de pallier les nouvelles formes d'attaques, qui profitent de failles sur ces applicatifs standard.

Protection intégrée du 802.11

La sécurisation du réseau n'a pas été une véritable préoccupation lors de la rédaction des spécifications 802.11. Avant ce standard, les différentes solutions propriétaires ne mettaient que peu souvent en avant des solutions de renfort de sécurité et il semble que cela ait eu une incidence.

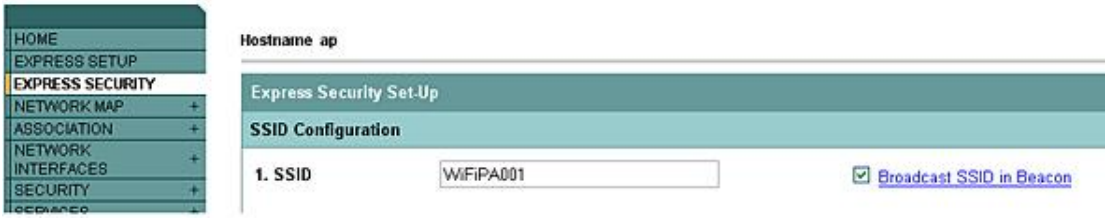
Les deux critères de confidentialité et de protection de l'accès au réseau sont quand même applicables, à travers quelques options. Mais la protection intégrée reste de faible niveau.

Les solutions qui sont présentées ci-dessous avaient pour but d'éviter l'association abusive au réseau. Elles ne s'appliquent que dans des infrastructures Basic Service Set (BSS) et Extended Service Set (ESS). L'utilisation d'un point d'accès est donc nécessaire.

1. Non diffusion du SSID

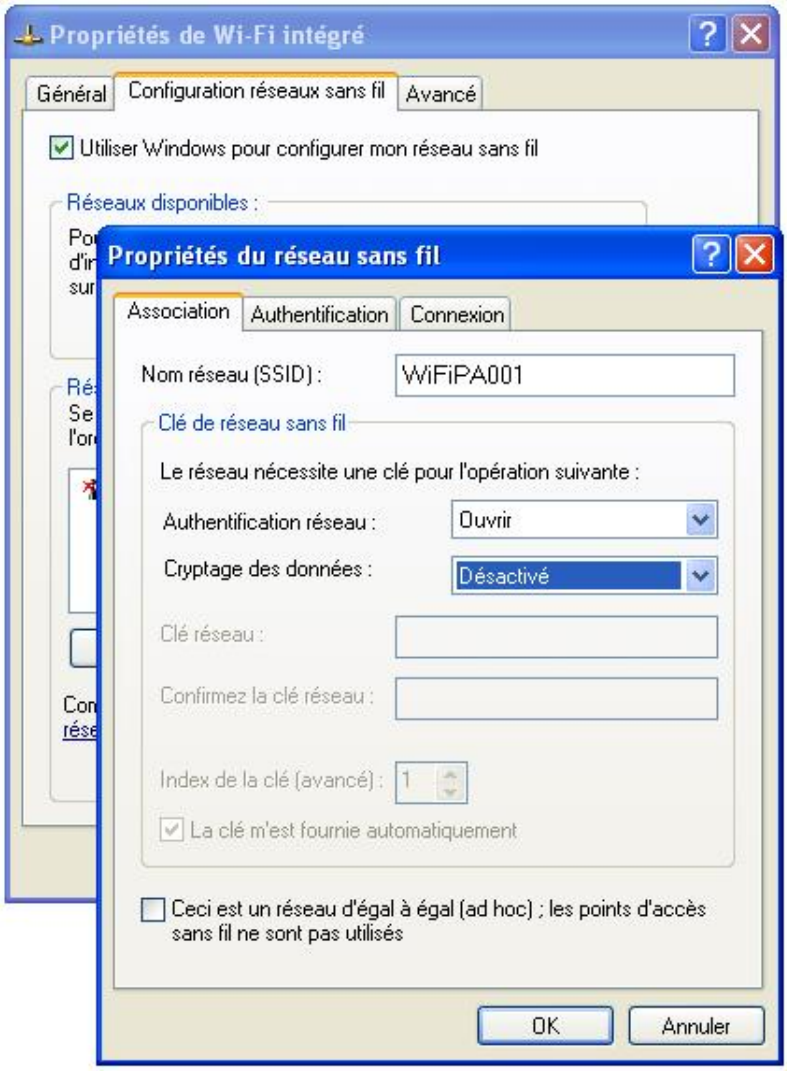
Si une borne ne diffuse pas le nom de son réseau, un client qui ne le connaît pas, ne pourra pas s'y connecter directement.

Dans l'interface d'administration du point d'accès, une simple case à cocher ou un bouton radio d'activation, suffisent pour ne plus joindre le nom du Service Set IDentifier (SSID) aux trames de balises.

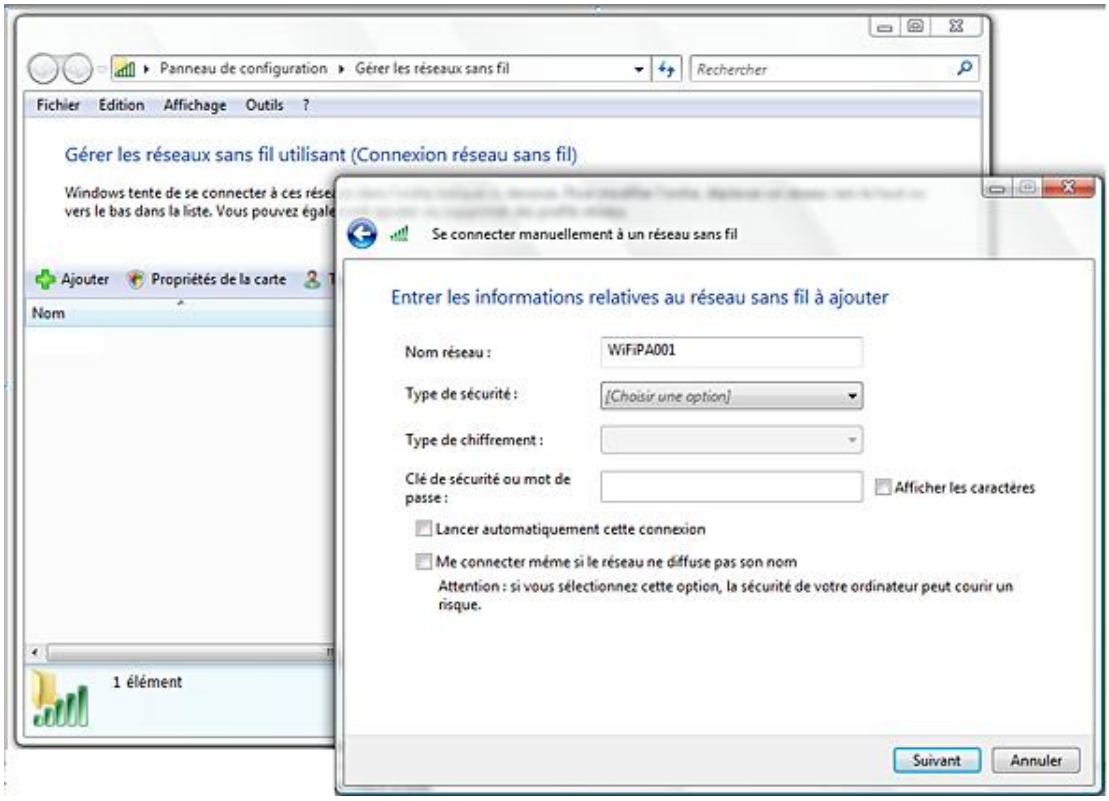


Choix du SSID et de sa diffusion (broadcast), sur un point d'accès de marque Cisco

Sur le poste client, il suffira de saisir manuellement ce paramètre, en ajoutant un nouveau réseau sans fil, puis en saisissant le nom de celui-ci.



Saisie du SSID d'un nouveau réseau Wi-Fi (interface MS Windows XP SP2)



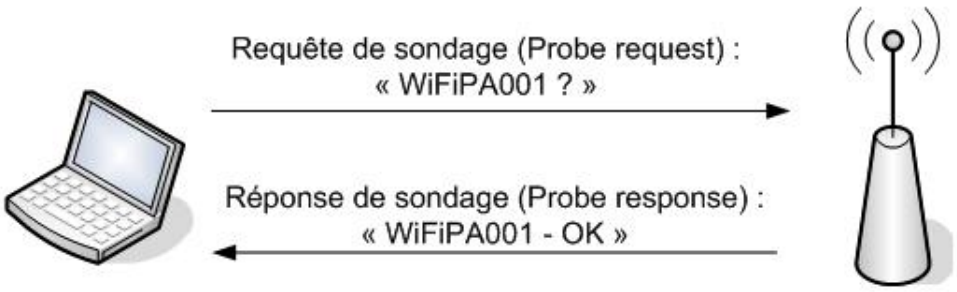
Saisie du SSID d'un nouveau réseau Wi-Fi (interface MS Windows Vista)

Dans Vista, la configuration de la connexion Wi-Fi s'effectue désormais à partir du **Centre Réseau et partage**, puis en demandant à **Gérer les réseaux sans fil**.

Cette action doit juste être considérée comme un camouflage, et non une réelle méthode de sécurisation. En effet, la station, pour connaître le nom de réseau de la borne, annoncera successivement les SSID qu'elle connaît, lors de requêtes de sondage. Une écoute des trames circulant permet d'intercepter l'interrogation, puis la réponse du point d'accès. L'information est ainsi reconstituée.

De plus, il est fortement recommandé de systématiquement changer le nom de SSID par défaut. En effet, celui-ci est le même pour l'ensemble des modèles d'une marque. La discrétion est donc préférable, même si la non divulgation du nom de fabricant d'un point d'accès n'est qu'un artifice. En effet, un usager averti peut, grâce aux premiers octets de l'adresse MAC de la borne, en déduire également cette information.

Le choix de nom de réseau est également important. Il ne devrait pas pouvoir être retrouvé par simple déduction.



SSID non diffusé, le dialogue de découverte

2. Filtrage par adresse MAC

Lorsqu'une station s'adresse à un point d'accès, elle lui fournit son adresse MAC, en tant que source de la trame. Une possibilité d'authentification, par cette information, a donc été ajoutée aux bornes.

Par saisie manuelle, il est donc possible de lister les clients dont la demande de connexion est autorisée.

Listage des adresses MAC authentifiées

On peut concevoir la difficulté de maintenance d'un tel filtrage, dans une entreprise équipée de multiples points d'accès. Chaque client qui est autorisé doit être ajouté dans toutes les listes. Il est possible, avec certains modèles, de déporter et centraliser ces informations sur un serveur, afin d'éviter ce désagrément.

L'écoute des communications permet de retrouver une adresse acceptée. L'usurpation de celle-ci, ou MAC spoofing, permet ensuite de se connecter de manière illicite au point d'accès. Une telle action peut être facilitée par le fait que le client, mobile, peut ne pas être connecté régulièrement.

3. WEP et authentification associée

Le système précédent, utilisant la reconnaissance de l'adresse physique, est destiné à identifier un ordinateur client auprès d'une borne. Un autre type d'authentification autorise une identification mutuelle des deux extrémités.

Cette procédure s'effectue après prise de connaissance des deux entités, à travers le processus de sondage, ou bien une diffusion de SSID entendue par une station.

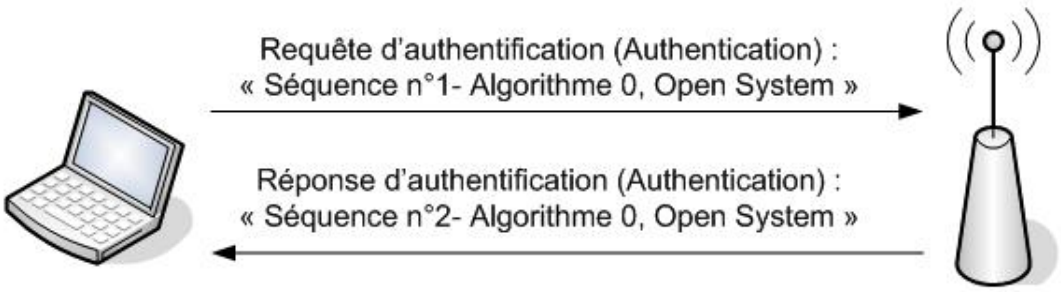
Open System authentication

Cette première méthode proposée par les spécifications 802.11, est la plus basique. Qualifiée d'ouverte, elle ne nécessite aucun pré-requis et peut être considérée comme une authentification nulle. Il s'agit de celle utilisée par défaut.

L'authentification ouverte s'effectue en deux temps :

- Une des parties envoie une trame de gestion, de sous-type authentification, précisant le numéro d'algorithme d'authentification souhaité, ici 0 ;

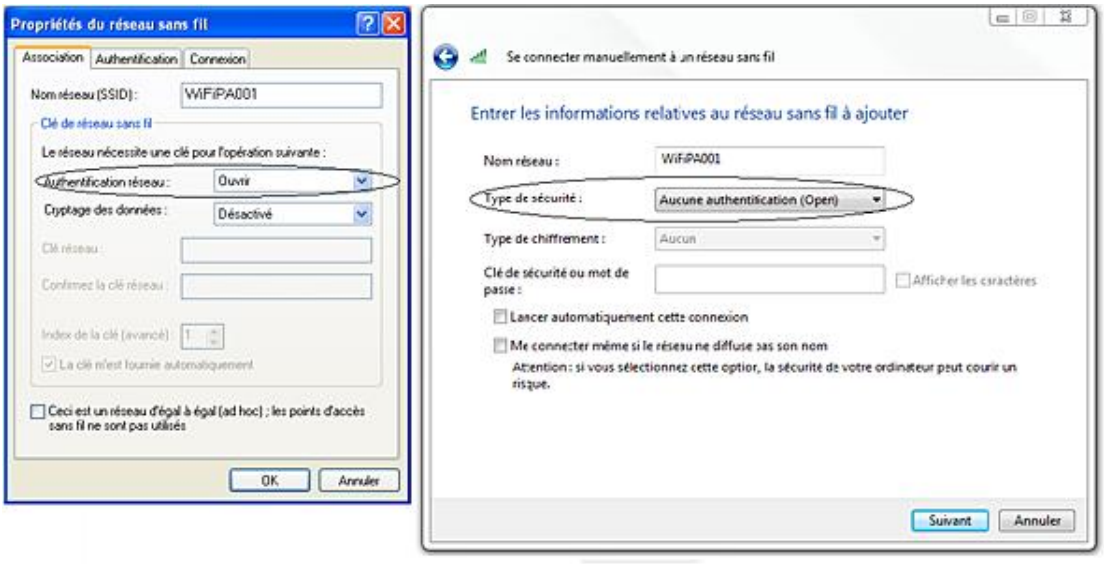
- En retour, lui est fourni l'acceptation ou le refus, toujours dans une trame de sous-type authentification.



Processus d'authentification ouverte

Dans le cas où une sécurisation ouverte avec clé WEP est mise en œuvre, le processus est chiffré, puisque les informations sont contenues dans le corps de trame. Ainsi, il est nécessaire que la clé utilisée soit la même sur le point d'accès et le client.

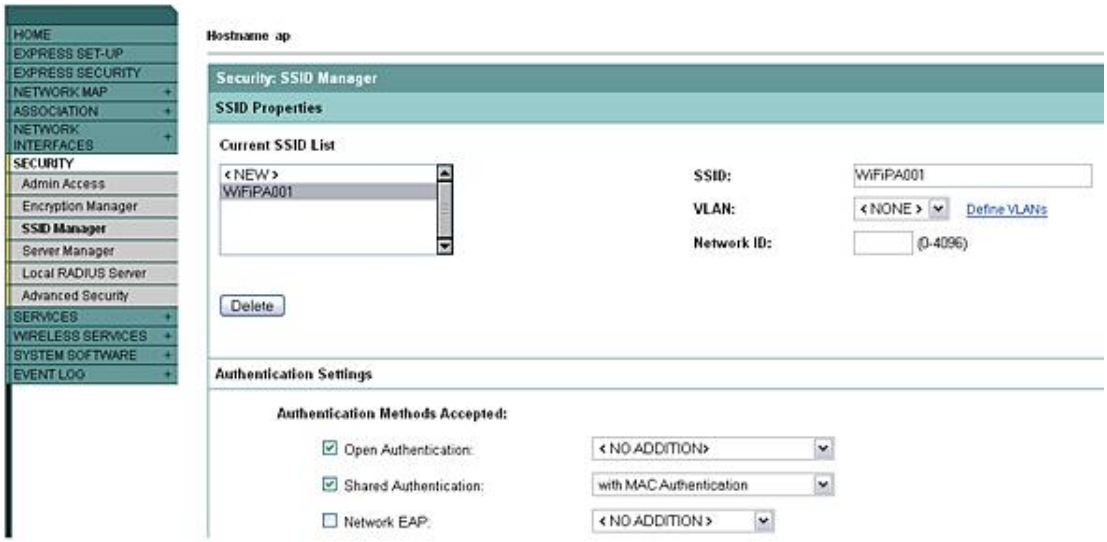
Sur le client, la configuration manuelle du réseau Wi-Fi, nécessaire si le SSID n'est pas diffusé, permet ce choix.



Choix du mode d'authentification sur le client (à gauche XP SP2, à droite Vista)

Shared Key authentication

Cette deuxième méthode nécessite la possession d'une clé de chiffrement communautaire, partagée par les deux extrémités.

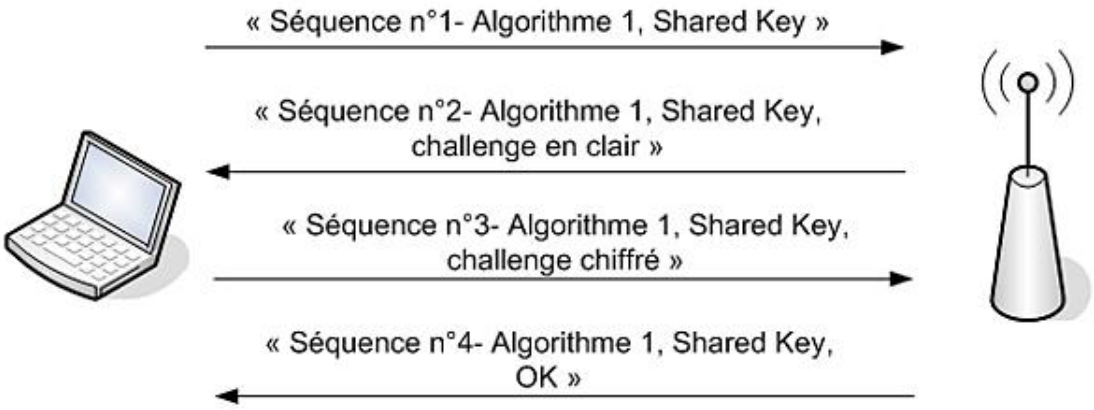


Choix du mode d'authentification sur le point d'accès

Pour vérifier cette possession de clé, un texte de défi, ou challenge, est utilisé. Pour cela, un programme, nommé WEP Pseudo-Random Number Generator (PRNG), produit une suite de 128 octets aléatoires, qui formeront ce challenge.

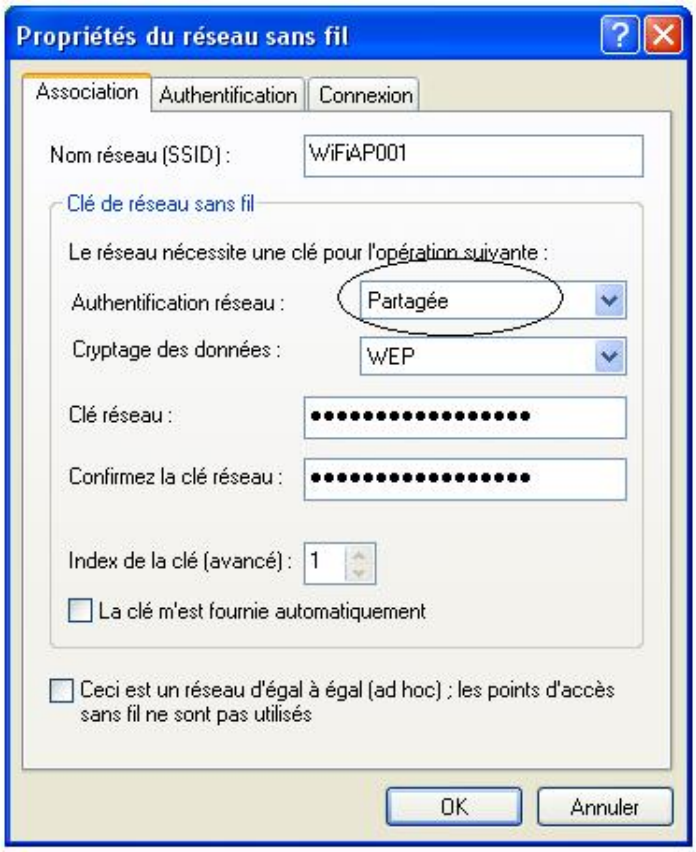
Quatre trames successives sont utilisées. Celle d'authentification initiale précise que le mode clé partagée est demandé. Si l'autre entité n'est pas configurée pour cela, le processus s'arrête. Sinon, le texte de challenge est généré et renvoyé en clair au demandeur. Celui-ci le chiffre avec sa clé WEP et transmet cette nouvelle information.

Finalement, le texte est déchiffré et comparé à celui d'origine. S'il est identique, l'authentification est réalisée et l'étape d'association peut être entamée.



Processus d'authentification à clé partagée

Sur le poste de travail, la configuration manuelle du réseau Wi-Fi permet le choix de ce mode partagé.



Choix du mode d'authentification sur le client

Prévue à l'origine pour renforcer l'authentification, cette méthode peut être considérée comme moins sécurisée que la précédente. En effet, le double transit du message, d'abord en clair, puis chiffré, facilite la découverte de la clé WEP, qui est ensuite utilisée dans toute la communication.

De plus, ce processus ne protège pas d'une attaque de type Man in the Middle (MiM). Si la station pirate est configurée comme point d'accès, utilisant le même SSID que l'entreprise, elle peut intercepter la demande de défi. Celle-ci est ensuite prolongée jusqu'à la borne de l'entreprise, qui authentifie donc l'installation illicite. Le processus initial avec la station est interrompue. Celle-ci reprendra donc une recherche complète de point d'accès, ce qui est transparent pour l'utilisateur.

La recherche de méthodes d'authentification plus solides que celle-ci est donc recommandée.

Chiffrement WEP

1. Fonctionnement

Pour éviter les écoutes clandestines (eavesdropping), l'usage de la solution Wired Equivalent Privacy (WEP) a été proposé avec les spécifications 802.11.

Utilisant une solution à clé symétrique, cette proposition ne précise pas de mécanisme de gestion des clés d'origine. Elles doivent donc être saisies manuellement sur les stations et points d'accès qui doivent communiquer.

Pensée comme solution équivalente au réseau filaire, WEP n'est pas prévu pour être fortement sécurisé. La simplicité d'usage a été privilégiée, afin d'encourager la mise en œuvre de cette solution. La découverte de différentes failles relativise son usage.

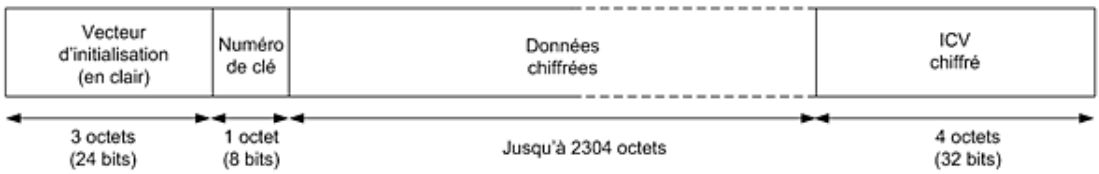
C'est dans le champ de contrôle (FC - *Frame Control*) des trames de données et de gestion d'authentification, qu'est précisée l'utilisation du chiffrement WEP. Ce bit, positionné à 1, précise que le corps de trame est crypté. Un tel chiffrement n'est pas possible dans les autres types de trames de gestion, ainsi que dans celles de contrôle.

a. Le vecteur d'initialisation

Le vecteur d'initialisation (IV - *Initialisation Vector*), est une séquence de bits qui change régulièrement. Combiné à la clé statique, il introduit une notion aléatoire au chiffrement. Ainsi, deux messages identiques ne donneront pas le même contenu chiffré, puisqu'ils ne seront pas issus d'une même clé.

La longueur du vecteur d'initialisation est de 24 bits, soit 16 777 216 valeurs possibles. Une telle taille de variable autorise à penser que le numéro utilisé est unique et ne sera pas réutilisé.

Comme la clé, le vecteur d'initialisation doit être connu à la fois de l'émetteur et du récepteur. La solution d'un mécanisme de génération automatique qui devrait être présent sur tous les équipements, n'a pas été retenue. Le vecteur d'initialisation est donc transporté en clair dans les trames non fragmentées MSDU (*MAC Service Data Unit*) ou fragmentées MPDU (*MAC Protocol Data Unit*).



Le corps de trame chiffré

b. L'algorithme RC4 dans WEP

L'algorithme de chiffrement RC4 a été développé par l'un des grands noms de la cryptographie, Ronald Rivest, en 1987. Le nom de son inventeur est inclus dans celui-ci : Rivest Cipher n°4. Il est utilisé dans de nombreuses applications, dont Secure Socket Layer (SSL), donc dans le commerce électronique sur Internet.

RC4 ne nécessite pas de puissance de calcul conséquente. Des logiciels simples peuvent prendre en charge les étapes de chiffrement et de déchiffrement, sans l'aide de matériels spécialisés. Il est considéré comme fiable, mais son interprétation peut entraîner des faiblesses d'usage.

Deux étapes sont nécessaires pour l'opération de chiffrement complète :

- L'initialisation de la clé ;
- La réalisation du cryptogramme, le texte chiffré.

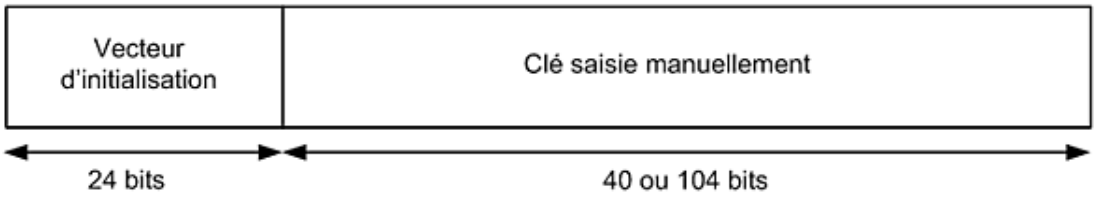
Initialisation de la clé

Deux longueurs de clé WEP peuvent être choisies sur les équipements Wi-Fi :

- 40 bits, soit 5 octets ;

- 104 bits, soit 13 octets.

Le vecteur d'initialisation y est systématiquement ajouté comme préambule. Ainsi, les constructeurs annoncent parfois des tailles de clé de 64 bits (8 octets) et 128 bits (16 octets), ce qui n'est pas tout à fait vrai.



Clé d'origine

Un tableau de 256 octets, soit autant de cellules, est d'abord formé. Il est initialisé en y ajoutant les 8 ou 16 octets du binôme clé + IV. Le report de ces valeurs est répété autant de fois que nécessaire.

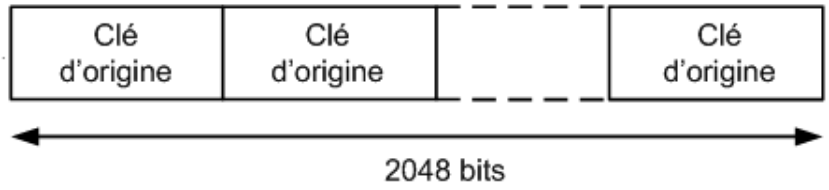


Table initialisée

Par permutation et autres manipulations, les cellules sont ensuite mélangées. Ce procédé porte le nom de Key Scheduling Algorithm (KSA). Il représente le cœur du mécanisme de chiffrement.

Après cette phase d'initialisation, chaque case est remplie d'une valeur qui semble aléatoire. La table elle-même se trouve dans un des 256 états possibles, soit dans l'une des 2^{1700} combinaisons autorisées.

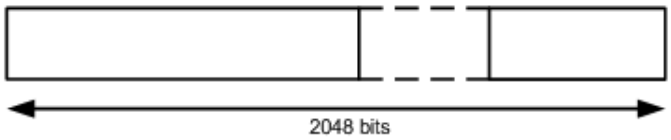


Table aléatoire résultante

La clé de chiffrement réellement utilisée est une séquence de bits extraite de cette table.

Comme le temps de génération de celle-ci est très court, elle peut évoluer en cours de chiffrement, par exemple en utilisant un autre vecteur d'initialisation. Ainsi, la cryptanalyse en recherche de clé est fortement ralentie.

Le chiffrement du texte

Il a été mathématiquement démontré, par Claude Shannon, dans les années 40, qu'un chiffrement n'est fiable que si la longueur de clé est au moins égale à celle du message à chiffrer.

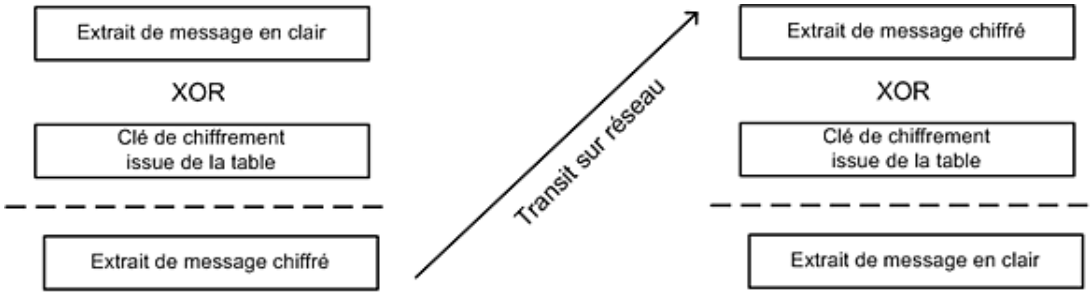
Ainsi, dans le chiffrement RC4, chaque bit du texte en clair est chiffré, en flux continu, par un bit de la table. Un artifice est nécessaire, afin d'éviter que deux mêmes textes donnent le même résultat chiffré. Ceci permettrait, en effet, de retrouver la clé de chiffrement. Ce changement systématique est la raison d'être du vecteur d'initialisation.

L'opération de cryptage utilise donc l'une des clés aléatoires, générée précédemment, combinée avec le même nombre de bits de données à chiffrer. Une opération XOR, bit à bit, est réalisée entre ces deux éléments.

Opération	Résultat
0 XOR 0	0
0 XOR 1	1
1 XOR 0	1
1 XOR 1	0

L'opérateur XOR présente l'avantage de produire le même résultat avec l'opération inverse, ce qui est indispensable dans le cadre d'un chiffrement symétrique.

Ainsi, si la clé utilisée pour déchiffrer le message est la même que celle qui a servi à chiffrer, l'opération XOR sur le cryptogramme permet de retrouver le texte initial.



Opérations de chiffrement et de déchiffrement

c. Le contrôle d'intégrité

Le code CRC des trames MAC est prévu pour pallier aux erreurs de transmission. Il ne peut être suffisant pour lutter contre des actions illicites. En effet, un pirate peut parfaitement modifier le contenu de la trame et insérer le code CRC correspondant.

WEP défini un mécanisme, nommé Integrity Check Value (ICV), destiné à contrôler l'intégrité du message chiffré transmis. Pour cela, un code équivalent au CRC précédent, sur 32 bits, est calculé. Il résulte du message en clair et non du contenu chiffré.

Le résultat du calcul ICV est ensuite ajouté à la fin du message, puis le tout est crypté. La clé WEP est donc nécessaire pour l'interpréter.

Inclusion de l'ICV dans la trame

La modification discrète de cette trame chiffrée sans en connaître la clé semble inconcevable, puisque le résultat de l'ICV serait différent.

2. Mise en œuvre de clé

a. La distribution des clés

La clé WEP utilisée par le point d'accès et tous ses clients est la même. Statique, elle ne sera pas changée lors des différentes communications. Seul le vecteur d'initialisation, incrémenté régulièrement, circule dans les trames.

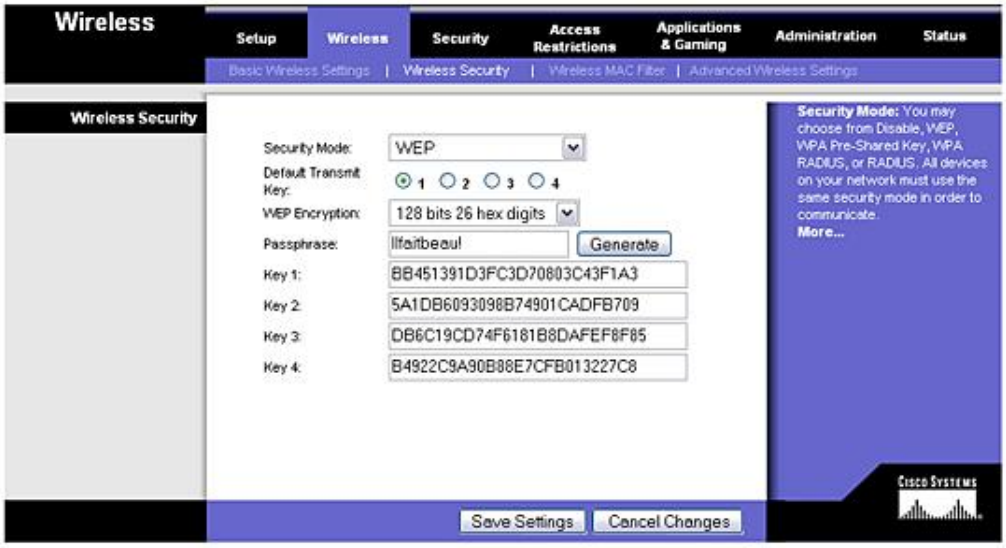
La distribution des clés WEP consiste donc en des opérations manuelles de saisie sur toutes les entités. En fonction des équipements et de leur interface d'administration, différents moyens sont proposés par les constructeurs.

Par exemple, la clé peut être saisie au format hexadécimal, avec les caractères 0 à 9, puis A à F. Un caractère hexadécimal est codé sur 4 bits. Le nombre de signes demandés dépend de la longueur de la clé :

- 10 pour une clé de 40 bits (5 octets) ;
- 26 pour une clé de 104 bits (13 octets).

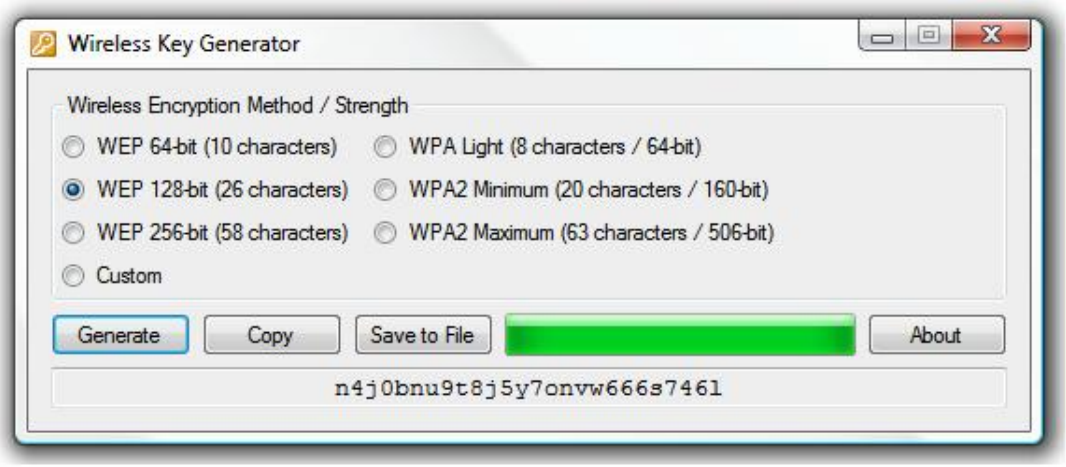
Une autre méthode consiste à saisir la clé sous forme de caractères, spéciaux ou non, codés sur 1 octet chacun. Ils seront ensuite traduits en valeurs binaires correspondant à la table ASCII.

D'autres points d'accès autorisent la saisie d'un mot de passe quelconque, qui sert de variable d'entrée à un programme de génération automatique de clé WEP. En sortie, une, voire plusieurs clés WEP de 40 ou 104 bits sont générées. Il suffira ensuite de recopier ces dernières sur les clients.



Génération automatique de clé à partir d'une phrase (passphrase), sur un point d'accès de marque Linksys

Le choix d'une clé WEP peut être simplifié par des programmes ou des sites Web, de générateurs de clés. Ci-dessous est présenté une copie d'écran du logiciel Wireless Key Generator, téléchargé gratuitement depuis Internet.



Logiciel Wireless Key Generator

Si la solution WEP est choisie, la clé peut être changée régulièrement. Chaque renouvellement implique la ressaisie de cette information sur toutes les entités qui devront communiquer par cryptogrammes.

b. Le renouvellement de clé

Le changement régulier de la clé statique WEP est nécessaire : elle peut être divulguée ou retrouvée. Cette opération implique une saisie manuelle de la nouvelle clé sur toutes les entités.

Une étape de transition, durant laquelle deux clés sont utilisées, doit donc être mise en œuvre. Elle est possible, car un équipement peut recevoir des paquets chiffrés par l'une des clés qu'il connaît. Le numéro de la clé utilisée est ajouté dans les trames.

Une seule clé, dite active, est utilisée pour les émissions de cryptogrammes.

Pour débuter le processus de renouvellement, une nouvelle clé est saisie sur les points d'accès, par exemple à la deuxième position.

Saisie d'une deuxième clé WEP sur un point d'accès

Cette deuxième clé est ensuite ajoutée et activée sur tous les clients, qui gardent en mémoire la précédente. Ainsi, les stations chiffreront les trames avec la clé active, la deuxième, tout en étant capables de déchiffrer celles en provenance des points d'accès avec la première.

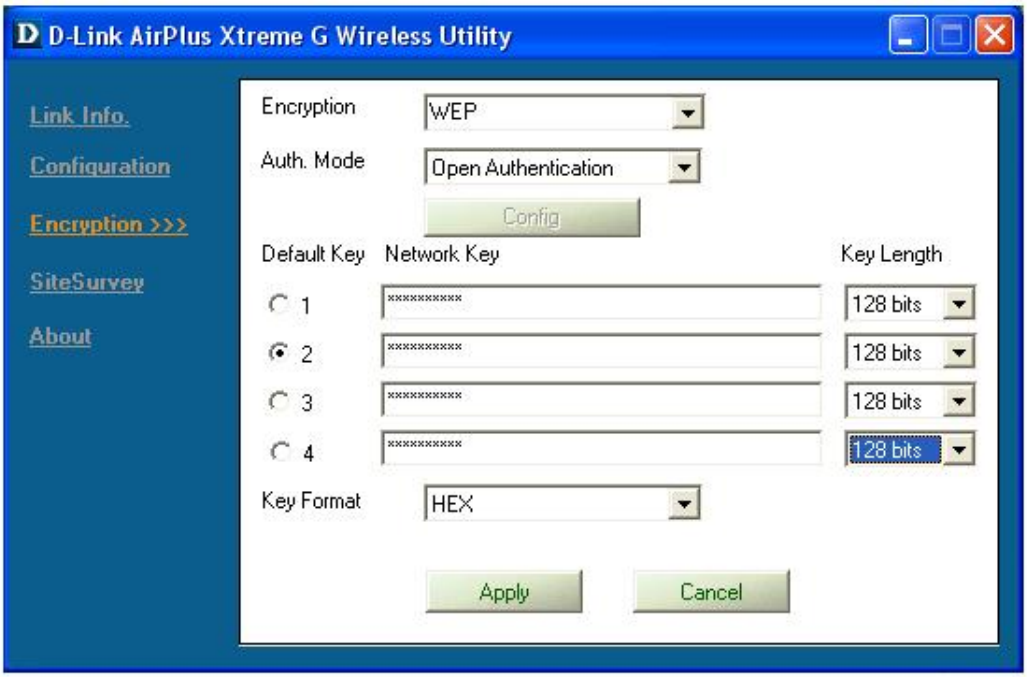
Finalement, lorsque tous les postes connaissent cette deuxième clé, elle peut être activée sur les points d'accès. Puisqu'elle ne sert plus, la première doit être effacée.

c. Les clés individuelles

Deux types de clés WEP sont définis. Lorsqu'une seule est en usage, elle est partagée par tous et sert pour l'ensemble des communications au sein de l'infrastructure.

Une deuxième clé, qualifiée d'individuelle, peut être utilisée. Elle permet de réduire l'exploitation de la première dans les communications de type unicast, depuis les stations vers les points d'accès.

Nous avons vu précédemment qu'un équipement peut stocker plusieurs clés. Parmi elles, une seule, celle active, sert pour le chiffrement. Les autres peuvent être utilisées pour le déchiffrement des trames reçues. Si les stations utilisent des clés actives différentes, les points d'accès doivent donc les connaître.



Les quatre champs de saisie de clé, sur un client de marque D-Link

Dans un réseau d'infrastructure, les trafics de type multicast ou broadcast ont tous pour origine le point d'accès.

Une clé commune doit donc être connue sur tous les équipements.

Ainsi, les points d'accès peuvent exploiter plusieurs clés individuelles et une partagée. Les stations ne connaissent que leur propre clé et celle commune. Lorsqu'un renouvellement de clé avec transition est décidé, quatre champs de saisie sont nécessaires.

3. Failles du WEP

Nous avons vu précédemment que les protections intégrées au 802.11, non diffusion du SSID, filtrage des adresses MAC et authentification partagée, ont vite démontré leurs faiblesses.

La lourdeur de la distribution des clés et de leur changement complique les renouvellements, qui ne sont pas aussi réguliers qu'ils devraient l'être. Dès l'année 2000, plusieurs publications démontrent la faiblesse des clés WEP. Elles peuvent désormais être retrouvées en quelques minutes. Il est donc reconnu, depuis, qu'elles ne sont pas sûres. Leur usage dans un réseau d'entreprise n'est pas recommandé.

a. Les faiblesses du vecteur d'initialisation

Le vecteur d'initialisation est censé fournir une information aléatoire qui rend une clé unique dans le temps. Sa longueur de 24 bits, soit moins de 17 millions de combinaisons, est trop courte.

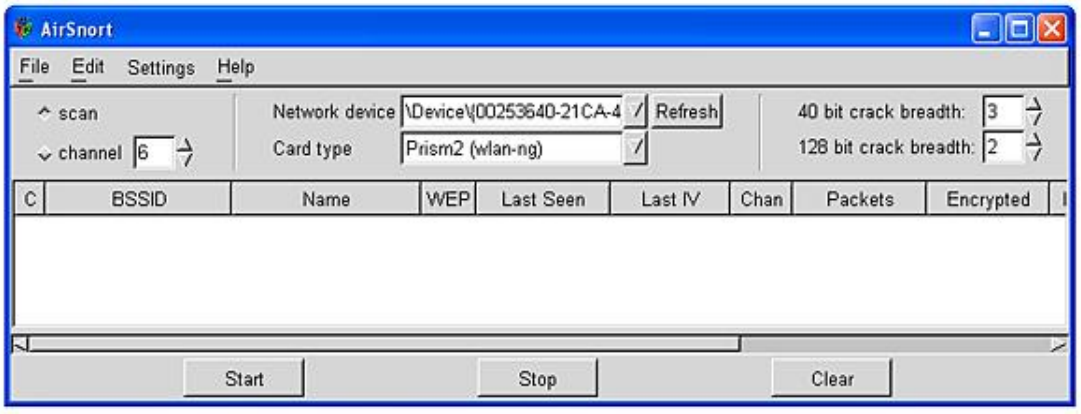
Dans une communication réseau d'entreprise quelconque, 5 à 8 heures de trafic peuvent suffir à transmettre un tel nombre de trames. Ce temps peut être réduit à quelques dizaines de minutes dans un réseau fortement exploité. Ainsi, en réalité, le vecteur d'initialisation se répète. L'information de chiffrement perd son caractère aléatoire et des cryptogrammes chiffrés avec une même clé circulent à intervalles réguliers.

Une écoute passive des communications permet de capturer les trames. Dans celles-ci, le vecteur d'initialisation circule en clair, donc il est facile d'en retrouver deux identiques. Comme il est utilisé avec la même clé statique d'origine, cette dernière pourrait être déduite des trames chiffrées également capturées.

Par exemple, un logiciel comme Kismet, conçu pour l'écoute passive en administration de réseaux, comprend les trames Wi-Fi. Très prisé, ce logiciel gratuit sous UNIX/LINUX peut être obtenu sur le site www.kismetwireless.net.

C'est en 2001 qu'une première attaque sur les vecteurs d'initialisation est publiée, par Scott Flurher, Itsik Mantin et Adi Shamir. Son nom correspond d'ailleurs à leurs initiales : FMS. Ces spécialistes de la cryptographie démontrent même qu'un certain nombre de vecteurs, dit faibles, simplifient encore le piratage.

Dans les jours suivants, deux développeurs mettent à disposition sur Internet un logiciel, AirSnort, capable de casser une clé WEP selon la technique FMS. Téléchargeable sur airsnort.shmoo.com, il est destiné à sensibiliser contre ce danger et démontrer que l'attaque décrite peut être facilement mise en œuvre.



Logiciel AirSnort

Afin d'accélérer la recherche, des outils apparaissent, permettant de réinjecter des paquets capturés, pour augmenter artificiellement le trafic.

En 2004, un pirate du nom de Korek, diffuse un logiciel qui permet de casser la clé WEP, en capturant un nombre réduit de vecteurs d'initialisation, faibles ou non. Il suffit désormais d'environ 150 000 trames pour retrouver une clé de 64 bits et de 500 000 pour une clé de 128 bits.

Rapidement, l'outil Aircrack apparaît, combinant l'attaque FMS et celle de Korek. Il est le premier d'une longue série de logiciels démontrant les failles dues aux collisions des vecteurs d'initialisation. Une dizaine de minutes suffisent actuellement pour retrouver une clé WEP par ces moyens.

b. Les problèmes des clés de chiffrement

Le vecteur d'initialisation présente une telle faille que la quasi-totalité des attaques le sollicitent.

La première des faiblesses de la clé WEP reste son caractère statique. Il est très facile de la compromettre, puisqu'elle est présente sur de nombreux postes de travail, ainsi que sur tous les points d'accès. De plus, il s'avère souvent que de nombreux utilisateurs la connaissent.

Certaines clés choisies sont très simples. Des attaques par dictionnaire peuvent, comme pour les mots de passe, retrouver l'information.

c. L'exploitation du contrôle d'intégrité

Le calcul de type Cyclic Redundancy Code (CRC), utilisé par Integrity Check Value (ICV) ne devrait servir qu'à vérifier si la trame reçue n'a pas été altérée lors de la communication. Une telle technique n'est pas fiable contre un piratage volontaire.

En effet, il est parfaitement possible de modifier le contenu de la trame de manière à retrouver le même résultat de calcul.

Ainsi, si une trame a été capturée puis modifiée par un intrus, elle peut être réinjectée et interprétée, comme si rien ne s'était passé.

Chiffrement WPA

Dès les spécifications IEEE 802.11 d'origine, il était prévu de proposer des moyens de sécurisation plus conséquents que ceux intégrés, dans une autre publication.

Malheureusement, les failles ont été trop rapidement mises en évidence. La standardisation d'une sécurité forte, prévue avec 802.11i, tardait à arriver. Le risque de remise en cause de la technologie Wi-Fi devenait important.

En 2002, la Wi-Fi alliance annonce sa propre solution intermédiaire, le Wi-Fi Protected Access (WPA), qu'elle certifiera dès 2003.

1. Présentation

À sa sortie, WPA est compatible avec les équipements existants. Une simple mise à jour des firmwares, logiciels pilotes, suffit pour ajouter cette option. WPA représente donc un compromis exploitable facilement, puisque les matériels ne doivent pas être changés.

Le but principal de WPA est de pallier les différentes failles du WEP.

Ainsi, le vecteur d'initialisation a désormais une longueur de 48 bits, au lieu de 24. La non réutilisation devient concrète, puisque plusieurs milliers d'années pourrait être nécessaires pour utiliser toutes les séquences possibles, dans une communication normale.

WPA continue d'utiliser l'algorithme de chiffrement RC4, qui n'est pas remis en cause. Par contre, il évite l'usage des clés faibles. De plus désormais, la clé d'origine n'est plus statique et est changée régulièrement. Ces propriétés reposent sur le système Temporal Key Integrity Protocol (TKIP).

Le contrôle d'intégrité lui-même est retravaillé.

La coexistence avec des équipements utilisant WEP reste possible.

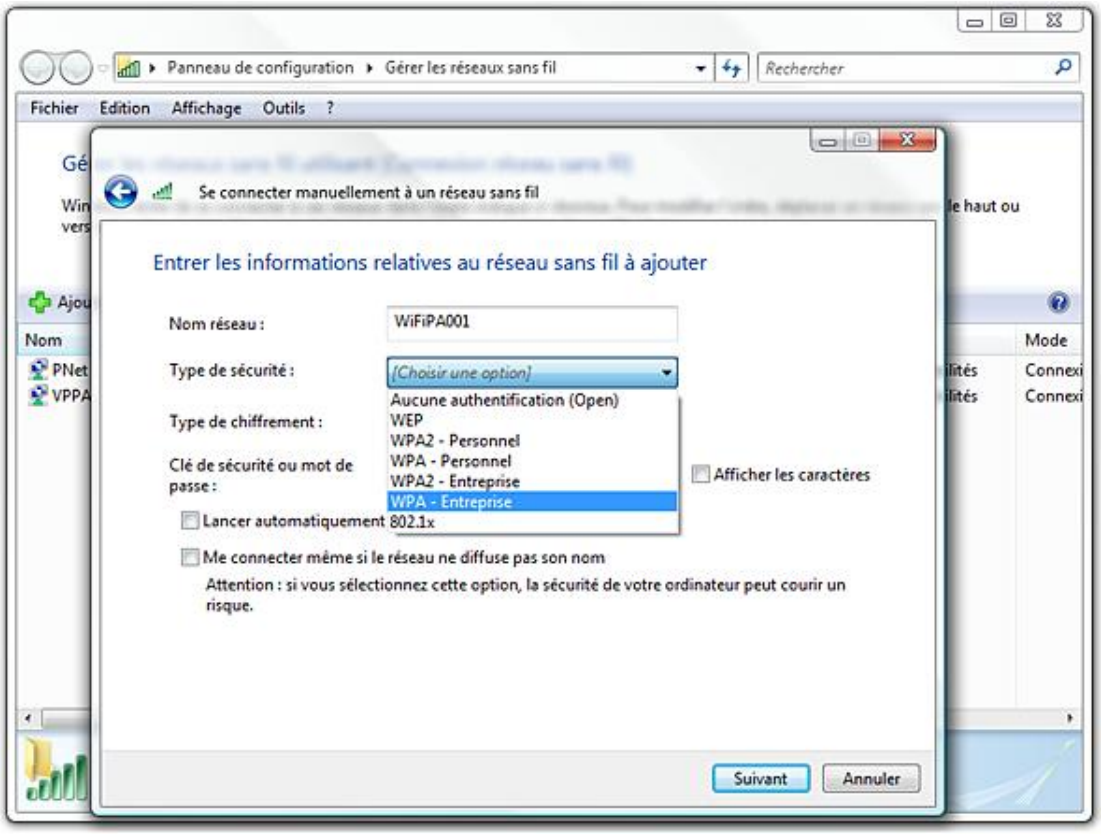
2. Authentification

Indépendamment de la volonté de corriger les failles de la méthode précédente, WPA introduit une différenciation des usages.

Deux implémentations distinctes de l'authentification sont proposées :

- Pour la maison, Personnel (Personal) ;
- Pour les professionnels, Entreprise (Entrerprise).

Ces deux modèles gardent le même moyen de chiffrement, avec TKIP.



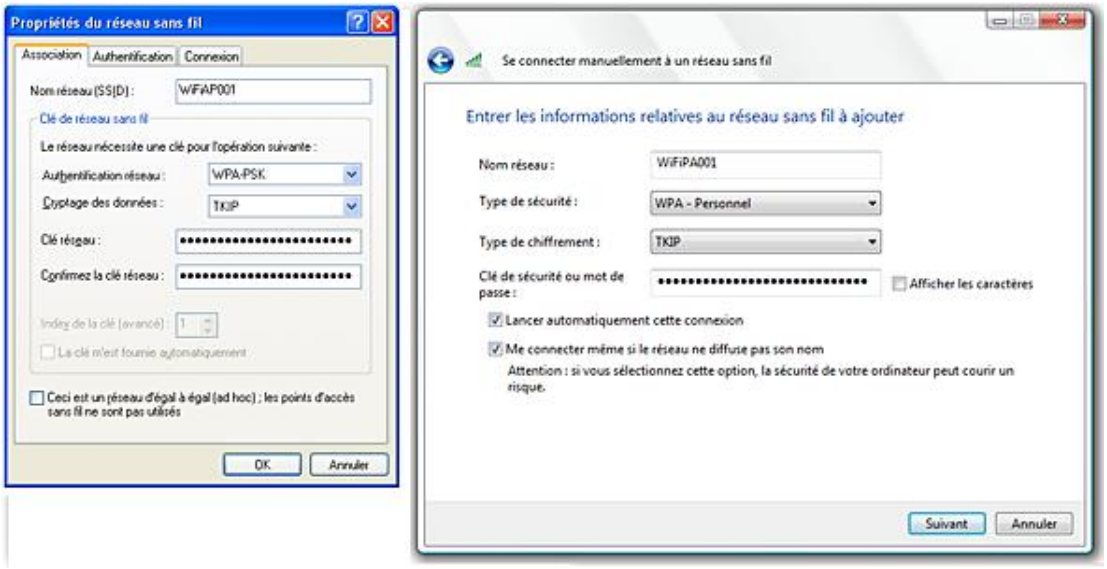
Les niveaux de sécurité proposés avec Windows Vista

Windows Vista a adopté les dénominations "standard". Dans la copie d'écran ci-avant, nous distinguons bien la possibilité de configurer WPA-Entreprise ou WPA-Personnel. Par contre, chaque mode peut utiliser TKIP ou AES, ce qui n'était pas disponible à l'arrivée de WPA. Nous reparlerons des autres moyens de sécurisation dans les chapitres suivants.

Pour une utilisation personnelle de Wi-Fi, un mécanisme simple est utilisé. On retrouve la nécessité de présence d'une clé identique sur les deux extrémités. Ce mode est appelé Pre-Shared Key (PSK).

Saisie des informations WPA-PSK sur un point d'accès

Toutefois, une méthode de saisie de la clé est exploitée, contrairement au WEP. Ainsi, un mot de passe (passphrase), le plus long possible entre 8 et 63 caractères, est choisi. Un générateur standard calculera une clé maîtresse (PMK - *Pairwise Master Key*) de 256 bits.



Saisie de la clé WPA-PSK sur le client (à gauche XP SP2, à droite Vista)

Si le mot de passe est trop court, une attaque par tests successifs, avec dictionnaire par exemple, permettra de le retrouver facilement. Une vingtaine de caractères est un minimum recommandé. Ce mot de passe reste faillible, puisqu'il doit être distribué sur tous les postes et points d'accès.

Cette solution simple demeure quand même une très bonne réponse aux failles du WEP, sur des petites infrastructures (SOHO - *Small Office Home Office*) ou des réseaux ad hoc. Elle est certifiée par la Wi-Fi alliance depuis avril 2003.

Wi-Fi® Interoperability Certificate — **Certification ID: WFA5991**

bg WiFi n DRAFT CERTIFIED®

This certificate indicates the capabilities and features that successfully completed interoperability testing by the Wi-Fi Alliance. You may find detailed descriptions of these features at www.wi-fi.org/certification_programs.php.

Certificate Date:	February 20, 2008
Category:	External Wi-Fi Adapter Card
Company:	3Com
Product:	3Com Wireless 11n USB Adapter
Model/SKU#:	WL-600

This product has passed Wi-Fi certification testing for the following standards:

IEEE Standard	Security	Multimedia	Special Features
802.11b	WPA™ - Personal	WMM®	Wi-Fi Protected Setup™
802.11g	WPA™ - Enterprise		PIN
802.11n draft 2.0	WPA2™ - Personal		PBC
	WPA2™ - Enterprise		
	EAP Type(s)		
	EAP-TLS		
	EAP-TTLS/MSCHAPv2		
	PEAPv0/EAP-MSCHAPv2		
	PEAPv1/EAP-GTC		
	EAP-SIM		

Certification d'un point d'accès, incluant WPA

Dans des environnements plus conséquents, la Wi-Fi Alliance propose l'usage d'une authentification plus poussée, utilisant le standard IEEE 802.1x avec EAP. Sa description et son exploitation font l'objet du chapitre suivant.

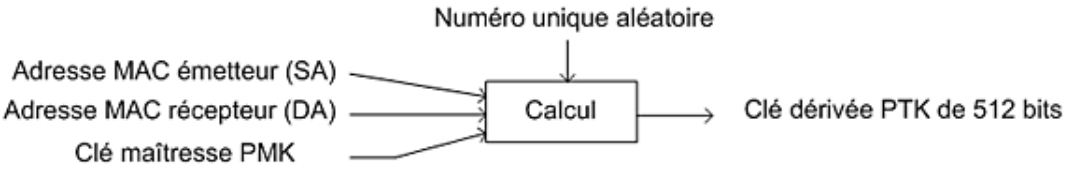
3. Chiffrement

a. Le protocole TKIP

Les différentes clés

Nous avons vu que la passphrase saisie génère une clé partagée (PSK - *Pre Shared Key*) utilisée pour l'authentification, comme clé maîtresse (PMK - *Pairwise Master Key*), sur 256 bits.

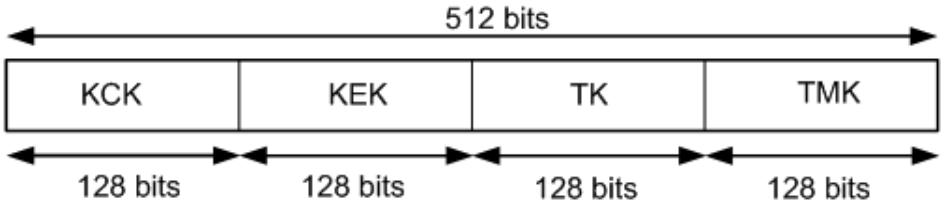
Par calcul, des clés temporaires (PTK - *Pairwise Transient Key*) de 512 bits de longueur, sont dérivées de cette PMK. La fonction utilisée est basée sur celle de hachage à sens unique keyed-Hashing for Message Authentication (HMAC) définie dans la RFC 2104. Ce calcul prend en compte les adresses MAC source et destination.



Le calcul des clés temporaires PTK

Les 512 bits de la PTK sont ensuite divisés en quatre clés de 128 bits chacune :

- Key Confirmation Key (KCK), utilisée dans le dialogue 802.1x ;
- Key Encryption Key (KEK), utilisée également en 802.1x ;
- Temporal Key (TK), assurant le chiffrement ;
- Temporal MIC Key (TMK), utilisée dans le calcul d'intégrité.

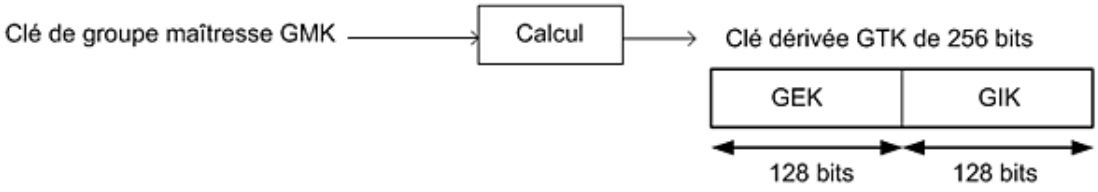


Composition des clés temporaires PTK

Les clés précédentes sont utilisées lors des transmissions de type unicast, dans lesquelles le récepteur est unique. Pour les trames multicast et broadcast, des clés de groupe sont utilisées. Ainsi, une clé de groupe maîtresse (GMK - *Group Master Key*), aléatoire et de 128 bits, sert d'entrée à la même fonction de calcul que précédemment. En résultat, une clé de groupe temporaire (GTK - *Group Temporal Key*) de 256 bits est générée. Elle est renouvelée lorsqu'un client quitte le réseau.

Les clés GTK contiennent :

- Group Encryption Key (GEK), sur 128 bits, pour le chiffrement ;
- Group Integrity Key (GIK), sur 128 bits pour l'intégrité.

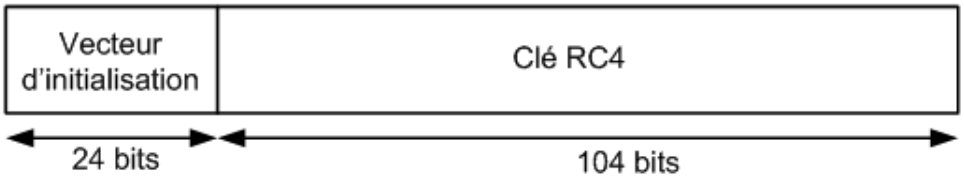


Calcul des clés de groupe

Fonctionnement de TKIP

Cette méthode de changement de clé est exigée avec WPA, que ce soit pour l'entreprise ou personnellement. Supprimant les failles majeures du WEP, TKIP reste peu complexe.

Ainsi, l'algorithme de chiffrement utilisé demeure RC4. Les clés utilisées, comprenant toujours un vecteur d'initialisation, ont une longueur de 128 bits exclusivement.

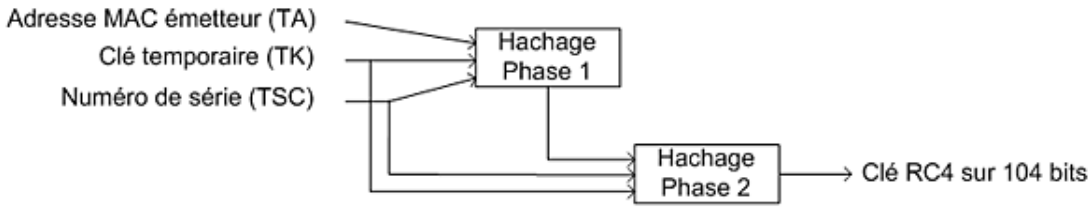


Clé sur 128 bits générée par TKIP

Avant d'être initialisés par le calcul de l'algorithme RC4, les 104 bits de la clé résultent d'un double hachage, qui va mixer les entrées. La première phase met en œuvre :

- L'adresse MAC de l'émetteur (TA - *Transmitter Address*) ;
- Une clé temporaire (TK - *Temporal Key*) dérivée de la clé d'origine ;
- Un numéro de série unique, sur 48 bits, alloué à chaque trame (TSC - *TKIP Sequence Counter*).

Le résultat de ce premier calcul est à nouveau mélangé à la clé temporaire et au numéro de série pour donner la clé effective.



Génération d'une clé RC4

L'inclusion de l'adresse MAC source évite que deux stations puissent avoir la même clé de chiffrement. La clé temporaire change à chaque trame, impliquant la non réutilisation de clés. La méthode de gestion de clés TKIP permet à la fois de supprimer celles qui sont reconnues simples et les doublons.

Le compteur TSC est incrémentiel. Il identifie l'âge des trames et permet d'éviter les attaques par rejeu. En effet, un récepteur n'acceptera pas de recevoir de multiples fois la même trame, reconnue par ce numéro.

Distribution des clés

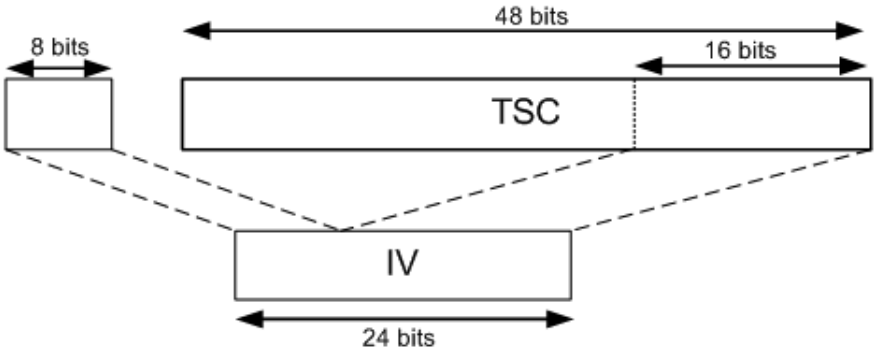
La méthode de chiffrement/déchiffrement utilisée est toujours symétrique. Ces opérations doivent donc être réalisées avec des clés identiques, qui doivent être connues sur les deux extrémités.

La première clé utilisée, la PMK, est connue à la fois de l'émetteur et du récepteur et a servi à l'authentification. Elle sert également à mettre en œuvre un tunnel sécurisé entre ces entités, dans lequel circuleront les clés temporaires de chiffrement/déchiffrement.

b. Le vecteur d'initialisation

Le champ du vecteur d'initialisation reste sur 24 bits, pour garder une compatibilité avec le WEP. Cette longueur devient ici moins problématique, étant donnée que la clé RC4 est changée régulièrement par TKIP.

Les 16 derniers bits du compteur TKIP Sequence Counter (TSC), sont combinés avec une valeur sur 8 bits, choisie de telle manière que la séquence évite l'usage des vecteurs réputés faibles.



Constitution du vecteur d'initialisation

Les 32 bits du TSC non utilisés dans le vecteur d'initialisation sont insérés dans le corps de trame. Ils constituent l'IV étendu (Extended IV), qui est placé avant les données. La fonction d'anti-rejeu se basera sur ces valeurs.

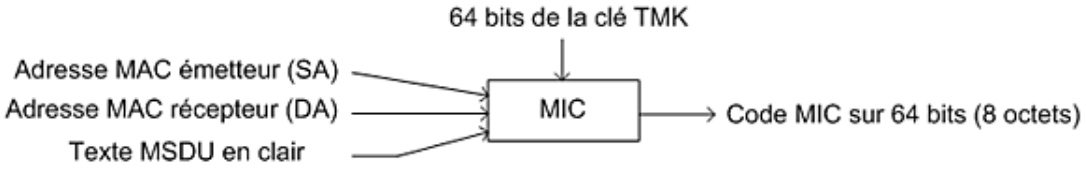
C'est dans le champ ID qu'est indiqué l'usage de WPA et donc de l'IV étendu. WEP n'utilise, dans cet octet, que deux bits, indiquant l'une des 4 clés utilisées. Le positionnement à 1 du troisième bit, dans ce cas seul significatif, indique que WPA est utilisé dans cette trame.

Le corps de trame WPA

c. Le contrôle d'intégrité MIC

Afin que le récepteur puisse s'assurer que la trame n'a pas été modifiée depuis l'émission, un protocole portant le nom de Michael est exploité. Conçu spécialement pour le WPA, il reste simple et rapide.

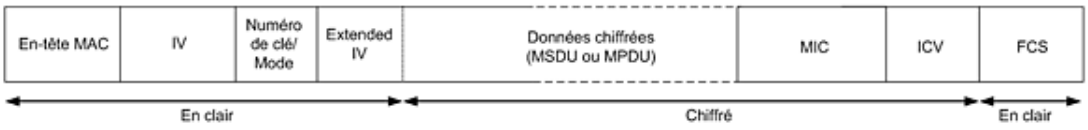
Ce protocole calcule un code d'intégrité (MIC - *Message Integrity Code*) non linéaire, contrairement à la fonction de type CRC du WEP. MIC résulte d'une série d'opérations XOR, décalages de bits et d'additions, réalisés à partir de différents éléments d'entrée. Parmi ceux-ci, on retrouve la clé Temporal MIC Key (TMK). En fait, ces 128 bits sont divisés en deux parts égales, et seuls 64 bits sont insérés ici.



Le calcul du MIC

Le code MIC est calculé à partir du contenu non fragmenté de la trame, le MSDU. À réception, il sera donc nécessaire de reconstituer complètement les trames fragmentées pour vérifier l'intégrité. Ainsi, un fragment illicite ne peut être ajouté.

Les 8 octets du MIC sont chiffrés avant d'être insérés entre la partie de données et le champ ICV. Finalement, le résultat d'un calcul CRC entre le code MIC et le texte en clair est ajouté dans le champ Integrity Check Value (ICV), afin de garder une compatibilité avec WEP.



La trame 802.11 chiffrée par WPA

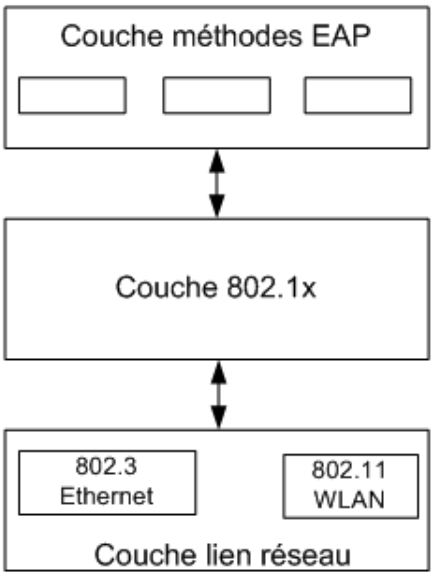
Principes du standard IEEE 802.1x

L'organisme Wi-Fi Alliance recommande, dans la configuration WPA d'entreprise, l'usage d'une architecture d'authentification standard 802.1x.

Le premier avantage de cette méthode est qu'elle est conçue pour la famille de protocoles de couches basses IEEE 802. Elle est donc indépendante du contexte.

Couplée avec certains des mécanismes Extensible Authentication Protocol (EAP), une telle solution autorise la distribution automatique des clés de chiffrement. Celles-ci seront propres à chaque utilisateur et leur durée de vie limitée à la session.

1. Fonctionnement

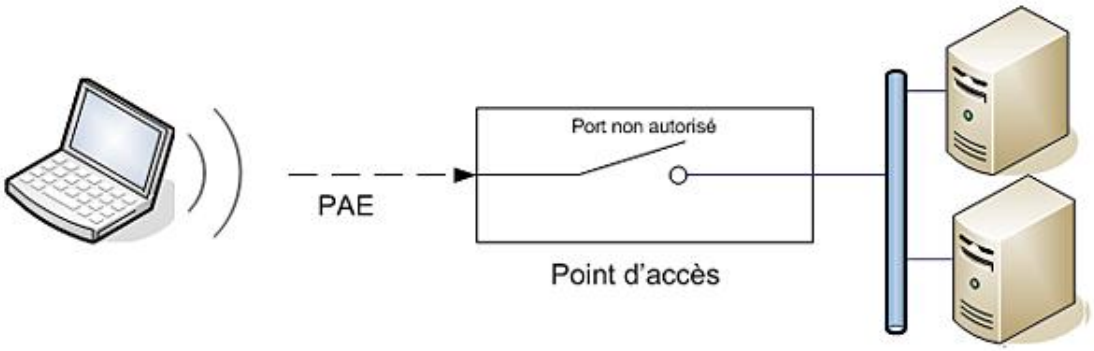


Le modèle 802.1x, sur les couches basses du modèle OSI

802.1x porte l'appellation de "Port Based Network Access Control", littéralement contrôle de l'accès réseau par port. Il travaille au niveau des couches basses du modèle OSI. Son but est d'autoriser ou non l'accès physique à un réseau local, après authentification du demandeur.

Ainsi, sur un réseau Ethernet, 802.1x est utilisé par un commutateur (switch). L'association entre le port d'entrée du client et le port de sortie demandé n'est effective qu'après la validation de l'authentification. L'entrée logique gérée par 802.1x est nommée Port Access Entity (PAE).

Dans le cadre d'un réseau Wi-Fi, le point d'accès va gérer la commutation entre la demande sur le réseau hertzien et l'association du port Ethernet de sortie.



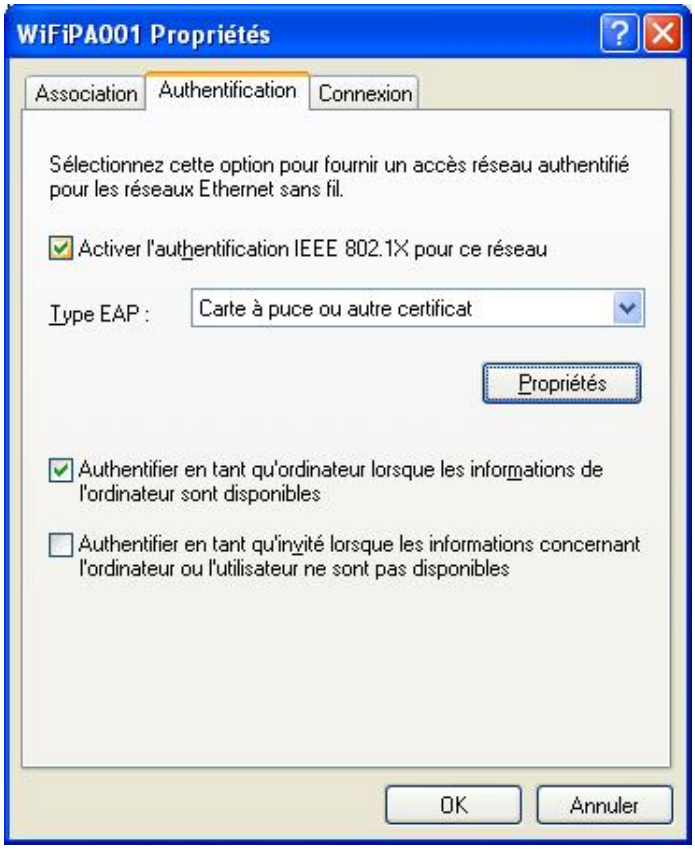
Contrôle du port par 802.1x

2. Acteurs

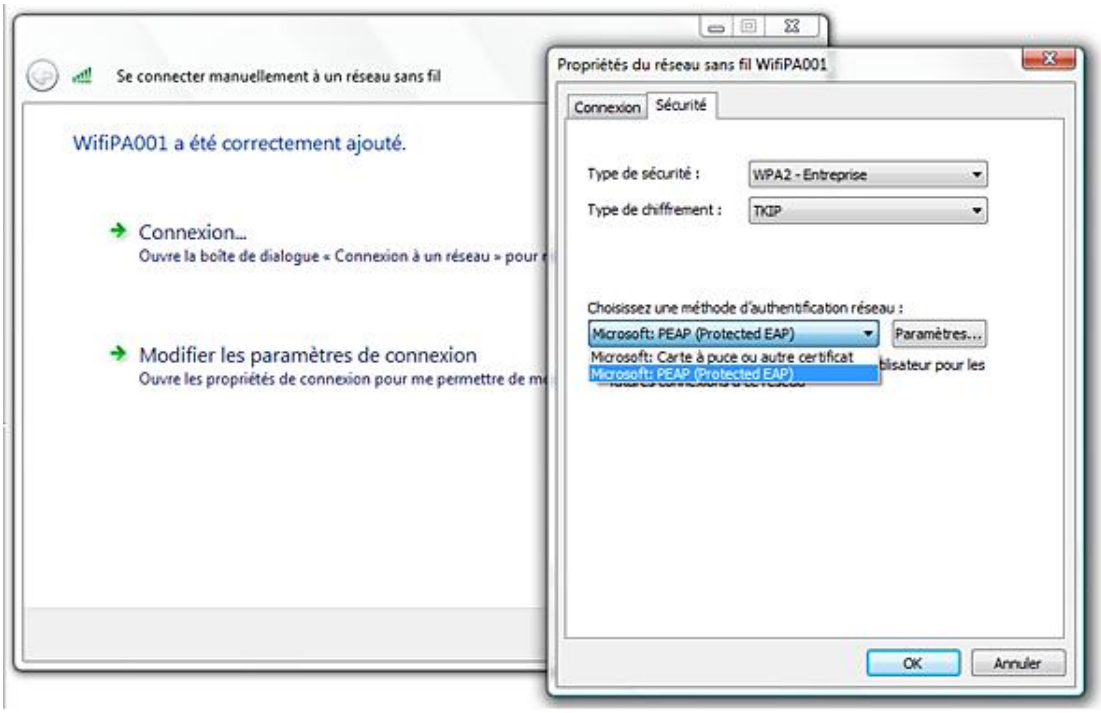
Trois participants sont définis, dans l'architecture 802.1x, pour mener à bien le processus.

Le premier composant est le système à authentifier (Supplicant). Ce client est généralement le poste de travail de l'utilisateur qui souhaite se connecter au réseau.

Sur un système d'exploitation MS Windows 2000, XP, voire 2003, il suffit d'associer le mode d'authentification dans les propriétés de l'interface réseau ou du réseau favori sans fil.



Activation de l'authentification 802.1x sur un client Windows XP SP2



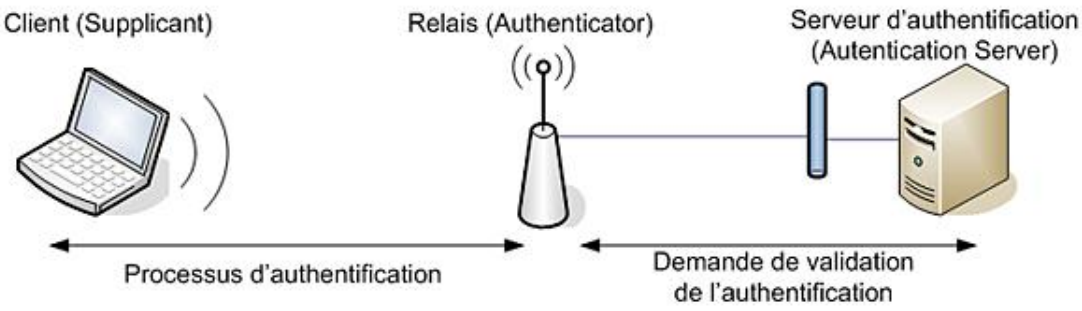
Activation de l'authentification 802.1 sur un client Windows Vista

---

Pour fixer le niveau d'authentification dans une configuration Wi-Fi de Windows Vista, il est nécessaire, après avoir ajouté la connexion sans fil, d'en modifier les paramètres de connexion ou les propriétés.

Le point d'accès au réseau, borne Wi-Fi ou commutateur, sert de relais. C'est de ce composant, nommé Authenticator, que part la demande auprès d'un serveur d'authentification (*Authentication server*).

Le dialogue entre le client et l'intermédiaire utilise une méthode EAP. 802.1x propose, pour la seconde phase, une communication selon le protocole Remote Authentication Dial In User Service (RADIUS).



Les composants du processus 802.1x

Serveur RADIUS

Le protocole Remote Authentication Dial In User Service (RADIUS) a été conçu pour prendre en charge la gestion des connexions des utilisateurs distants au réseau. Ses capacités sont résumées par l'acronyme AAA qui lui est souvent associé. Cette expression résume les trois fonctions prises en charge : identification et authentification (Authentication), gestion des autorisations d'accès (Authorization) et comptabilisation des connexions (Accounting).

Son utilisation est préconisée, mais non obligatoire, avec 802.1x.

1. Standard RADIUS

a. Les origines

Le protocole RADIUS a été conçu par l'entreprise Livingston, puis standardisé par l'IETF. Ces spécifications ont été publiées en 1997, dans la RFC numérotée 2058. La RFC 2138 l'a remplacée, elle-même rendue obsolète par la RFC 2865 (http://www.ietf.org/rfc/rfc2865.txt). Les publications numérotées 2548, 2809, 2866, 2867, 2868 et 2869 définissent des compléments. D'autres seront ajoutées en fonction des besoins d'évolution.

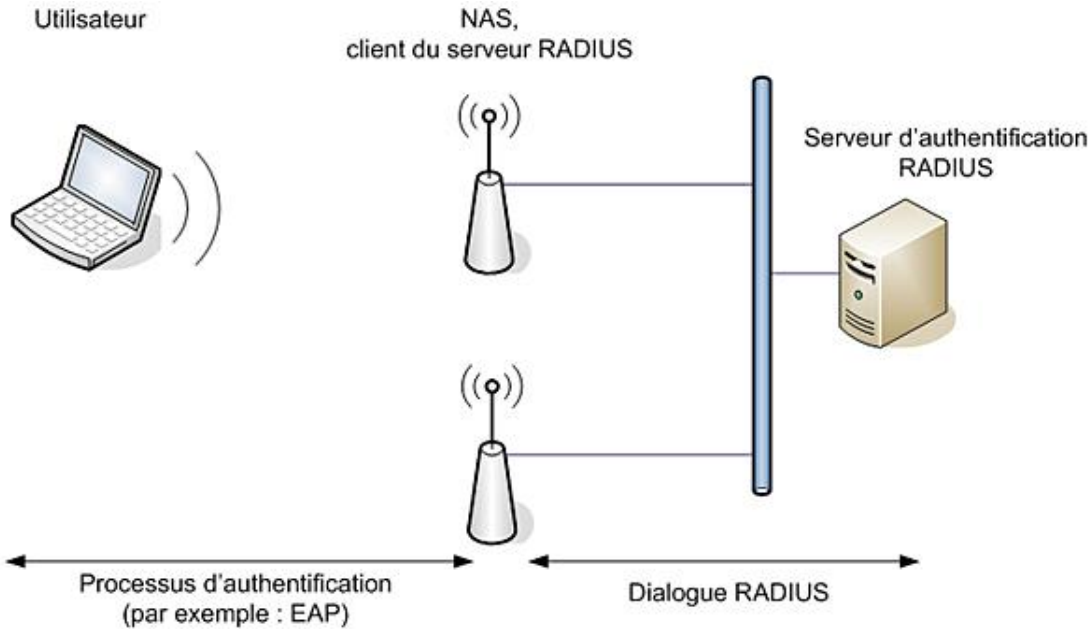
b. L'architecture

RADIUS décrit une architecture similaire à celle du IEEE 802.1x. En effet, on y retrouve également trois éléments :

- un utilisateur, effectuant la demande d'authentification ;
- un élément relais, le serveur d'accès réseau (NAS - *Network Access Server*), client RADIUS ;
- le serveur RADIUS lui-même, qui reçoit et interprète les demandes.

Le NAS, un point d'accès Wi-Fi par exemple, est contacté par l'usager lors d'une demande d'authentification. Un certain nombre de mécanismes standard peuvent être utilisés dans ce processus, dont ceux de type EAP. Cette particularité est traitée dans la RFC 2869.

Le protocole RADIUS entame ensuite un dialogue de type client/serveur, à partir du NAS vers le serveur RADIUS. Au besoin, ce dernier centralise les demandes issues de plusieurs clients.



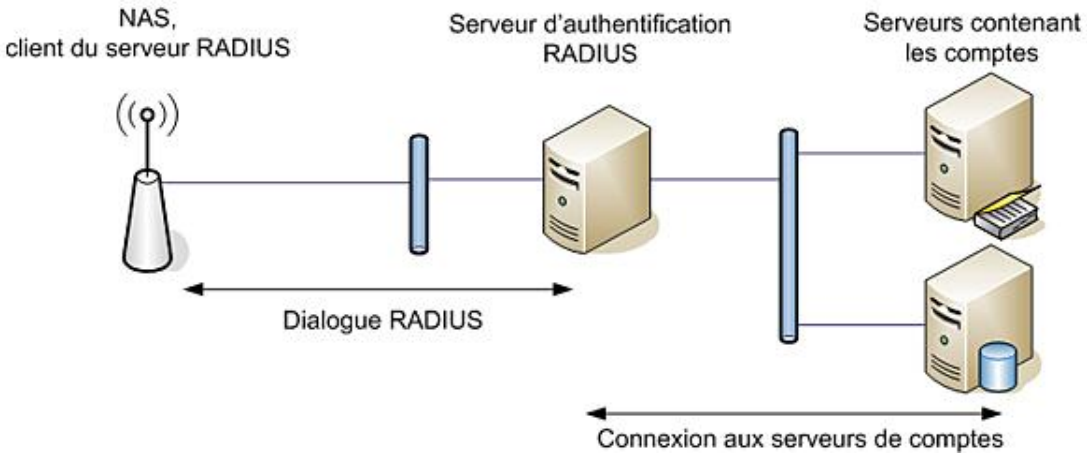
L'architecture RADIUS

Dans des infrastructures importantes, il est possible de cascader plusieurs serveurs RADIUS, l'un tenant le rôle de proxy pour le suivant, en relayant les demandes.

Le serveur RADIUS lui-même ne contient pas la liste des comptes à authentifier. Des connecteurs logiciels permettent la transmission de la demande à des entités dédiées à cet usage :

- serveurs de base de compte ;
- serveurs d'annuaires (contrôleurs de domaine MS Windows, LDAP...) ;
- serveurs de base de données...

Ces derniers valideront la demande ou non et la réponse sera transmise au NAS.



Transmission de la demande d'authentification

Cette architecture peut paraître quelque peu complexe au premier abord, mais elle présente de nombreux avantages. Tout d'abord, la configuration sur les points d'accès est très simple, puisqu'il suffit de paramétrer la liaison avec le serveur RADIUS. Aucune information sur les comptes utilisateurs n'est contenue dans ces bornes. De plus, le dialogue entre le serveur RADIUS et son client est sécurisé.

Enfin, au lieu de déclarer à nouveau des comptes qui sont déjà utilisés sur le réseau interne, l'architecture RADIUS permet l'interconnexion avec les différentes bases existantes.

c. Les attributs

Les communications entre le serveur RADIUS et son client NAS véhiculent différents paramètres, les attributs, qui sont caractérisés par un numéro d'identification et une valeur. Un dictionnaire, présent sur les différents éléments en communication, met en rapport ce numéro, l'intitulé de l'attribut et son type.

Ces paires attribut/valeur (AVP - *Attribute/Value Pair*) permettent la transmission des informations d'authentification vers le serveur RADIUS. En retour, les caractéristiques précises de l'autorisation ou des demandes diverses, sont délivrées.

Une soixantaine d'attributs standard sont définis dans la RFC 2865, dont un certain nombre sont utilisables dans 802.1x. Il est possible d'utiliser des attributs supplémentaires (VSA - *Vendor Specific Attribute*), encapsulés dans celui numéroté 26.

N° attribut	Nom d'attribut	Caractéristique
1	User-Name	Identifiant du demandeur
2	User-Password	Mot de passe du demandeur, ou plutôt le hachage correspondant
4	NAS-IP-Address	Adresse IP du NAS
5	NAS-Port	Numéro de port client du NAS
26	Vendor-Specific	Réservé à l'usage de caractéristiques propriétaires
27	Sesssion-Timeout	Temps maximum de la session
28	Idle-Timeout	Temps d'inactivité avant déconnexion forcée
30	Called-Station-Id	Adresse du NAS, par exemple MAC
31	Calling-Station-Id	Adresse du demandeur, par exemple MAC
32	NAS-Identifier	Numéro d'identification du NAS

Différentes RFC définissent des attributs supplémentaires :

- 2866 précise la comptabilisation des connexions utilisateur (Accounting) ;
- 2868 décrit ceux pour l'établissement d'un tunnel chiffré ;
- 2869 propose des extensions au niveau de l'authentification ;
- 2548 spécifie ceux de type Vendor Specific de Microsoft.

La RFC 2869 inclut une proposition de RADIUS pour le support du protocole EAP, et donc de l'authentification 802.1x. Cette possibilité est confirmée dans les RFC 3579 et 3580, traitant spécifiquement de ce dialogue. Les échanges "EAP over Radius" utilisent deux attributs supplémentaires, Message-Authenticator et EAP Message, sur lesquels nous reviendrons.

2. Dialogue client/serveur RADIUS

a. Les différents paquets

Le protocole RADIUS définit principalement six types de requêtes entre le NAS et le serveur RADIUS.

La première, Access-request, est envoyée par le NAS, pour transmettre la demande d'authentification. Elle contient les attributs d'identité de l'utilisateur et de mot de passe.

En retour, le paquet Access-accept peut être envoyé, afin d'accepter la demande précédente, après validation auprès d'un serveur de compte. Il contient différents attributs de service.

Si la demande n'a pas été acceptée, la requête Access-reject est émise par le serveur RADIUS. Elle peut transporter, comme attribut, un message d'erreur pour l'afficher sur l'écran de l'utilisateur.

L'envoi par le NAS d'un paquet Accounting-request indique le début ou la fin d'une session.

L'accusé de réception du paquet précédent est le Accounting-response.

Access-challenge est un paquet contenant un défi, qui peut être renvoyé après un Access-request. Par cette requête, le serveur RADIUS demande le renvoi d'une réponse au message. Des informations complémentaires peuvent être demandées par ce biais.

Ces requêtes sont encapsulées dans des paquets IP. Le protocole de transport utilisé est User Datagram Protocol (UDP). Il a été privilégié pour son usage simple et sa rapidité. Le serveur RADIUS écoute donc par défaut sur les ports :

- UDP 1812 (anciennement 1645), pour les services d'authentification et d'autorisation ;
- UDP 1813 (anciennement 1646), pour le service de comptabilisation.

b. Le contenu des paquets

L'en-tête RADIUS est fixe et mesure 20 octets. La première information communiquée est un numéro de code, précisant le type de paquet RADIUS transporté.

Numéro de code	Type de paquet
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (expérimental)
13	Status-Client (expérimental)
255	Réservé

Les différents numéros de code

Les quatre champs de l'en-tête sont :

- le numéro de code ;
- un identifiant, compteur permettant d'associer les requêtes et les réponses ;
- la longueur complète de la requête ;
- un contrôle d'intégrité (Authenticator) entre le client et le serveur.

Le corps de ce paquet est constitué des attributs, placés simplement les uns après les autres.

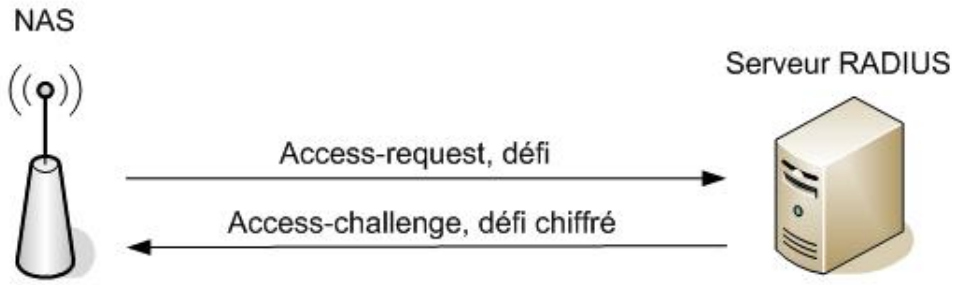
Le paquet RADIUS

c. La communication complète

Authentification des entités

La transaction entre le NAS et le serveur RADIUS débute par leur authentification mutuelle. Pour cela, un mécanisme de secret partagé est mis en œuvre. Ce mot de passe (passphrase) doit être aussi complexe que possible. Il est recommandé également qu'il soit dépendant de chaque NAS.

Le premier paquet envoyé, un Access-request, propose un message de défi. En utilisant cette information et sa propre clé, le serveur calcule une nouvelle valeur et l'insère dans la réponse. Un calcul similaire a été effectué sur le NAS, qui a conservé le résultat en mémoire et le compare à celui du serveur RADIUS.



Authentification des entités

Si la vérification est concluante, la communication peut continuer.

Calculs d'intégrité

Après l'étape d'authentification, ce secret partagé sert à la vérification d'intégrité et de provenance de chaque paquet provenant du serveur RADIUS.

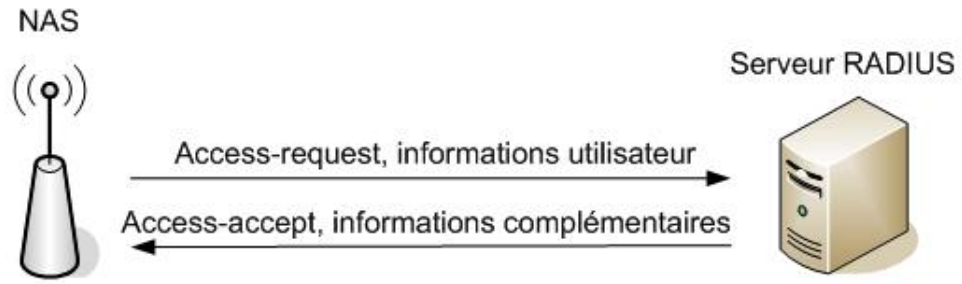
Dans un Access-request, le NAS inclut un nombre aléatoire, au sein du champ Authenticator de l'en-tête. Quel que soit le type de paquet de retour, il contiendra dans ce même champ une empreinte unique, issue d'un calcul de hachage MD5, combinant :

- le code de la requête ;
- l'identifiant d'association entre les requêtes et les réponses ;
- la longueur du paquet ;
- l'information Authenticator envoyée précédemment ;
- le secret partagé ;
- la requête elle-même, ou 16 octets nuls dans un paquet de comptabilisation.

Ainsi, le NAS est assuré de la provenance effective de l'information et de sa non altération durant le transport.

Exemple de dialogue

Après l'authentification, les communications entre le serveur et son client sont simples. Le secret partagé peut être utilisé pour chiffrer certains attributs, mais la plupart circulent en clair.



Une transaction autorisant connexion utilisateur

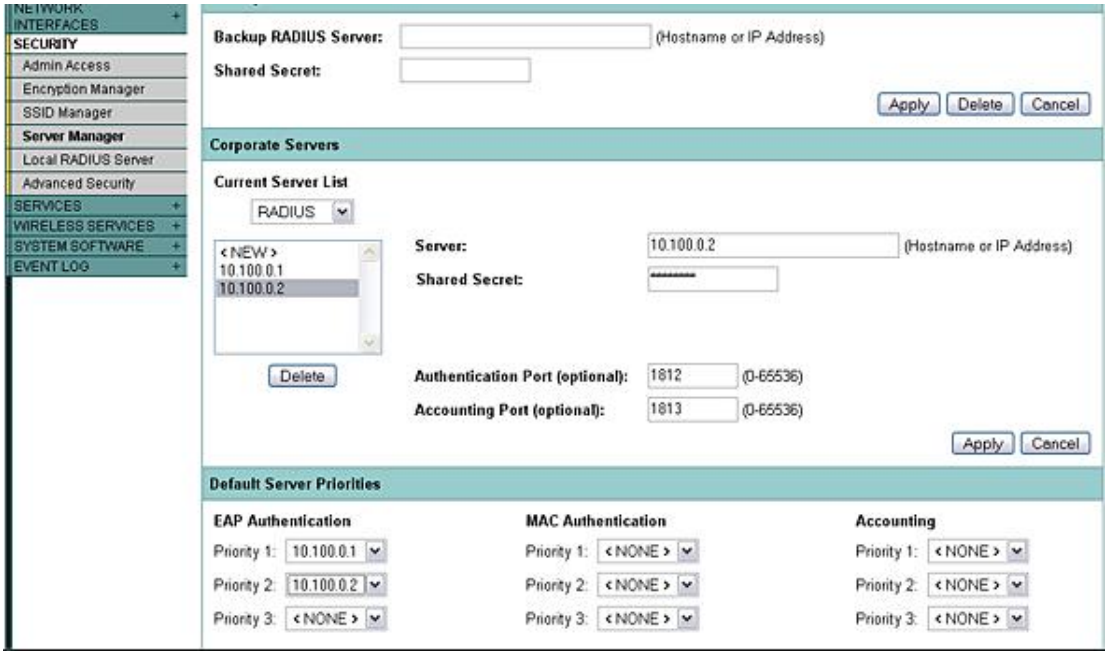
Après cette validation, le poste de travail est autorisé à se connecter au réseau par le protocole 802.1x.

3. Configuration de l'architecture RADIUS

a. Sur un point d'accès

La configuration d'une borne Wi-Fi comme serveur NAS est une opération simple. Les paramètres à saisir sont généralement :

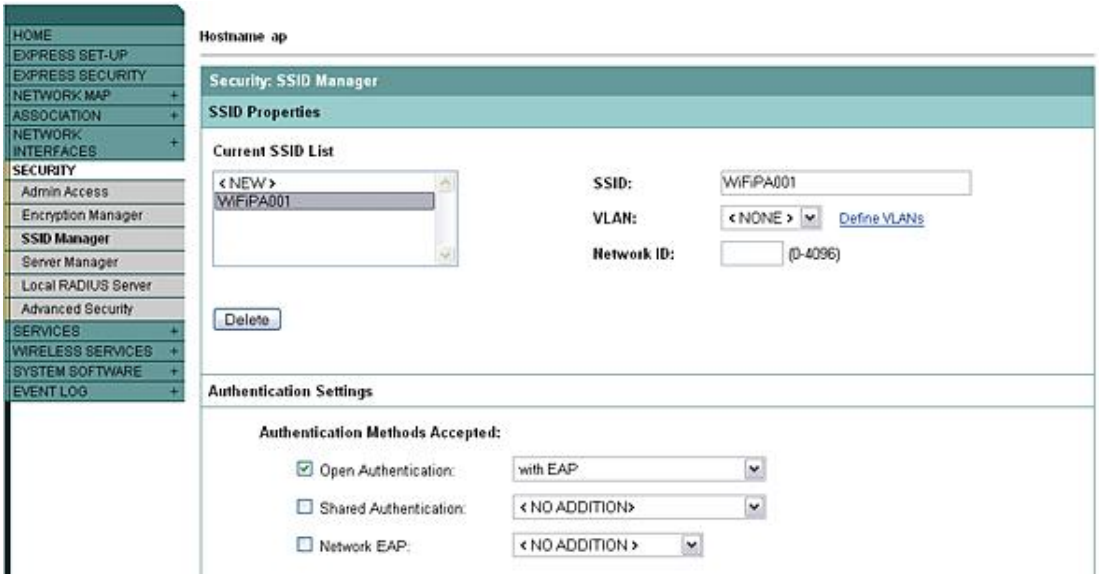
- l'adresse IP du serveur RADIUS ;
- le secret partagé ;
- les numéros de port d'authentification et de comptabilité.



Configuration des paramètres NAS sur un point d'accès

En fonction des modèles de points d'accès, il peut être possible de configurer les connexions à plusieurs serveurs RADIUS. Ces derniers peuvent être interrogés pour valider un compte utilisateur ou bien l'adresse MAC du poste client.

Il peut être nécessaire de préciser ensuite le mode d'authentification. S'il est EAP, la connexion avec un serveur RADIUS est nécessaire.



Choix de la méthode d'authentification EAP sur un point d'accès

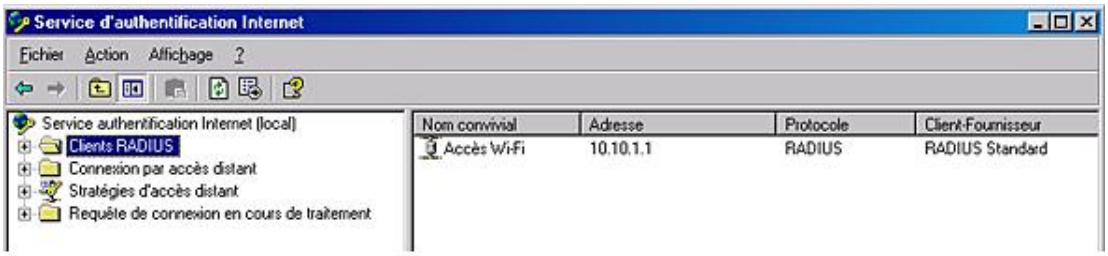
b. Sur un serveur RADIUS

De nombreuses solutions existent sur le marché. Nous n'en citerons que quatre :

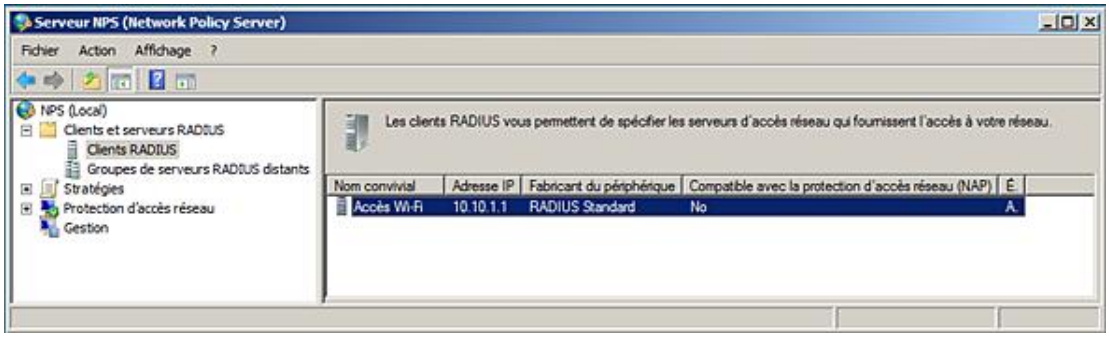
- FreeRADIUS sous Linux, proposition du monde des logiciels libres (http://www.freeradius.org) ;
- le produit Cisco Access Control Server (ACS), fonctionnant sur système d'exploitation Microsoft Windows ;
- le service d'authentification Internet (IAS - *Internet Authentication Server*) composant intégré aux serveurs MS Windows 2000 et 2003.

- Le service de règles de réseaux (NPS - *Network Policy Server*) intégré à MS Windows 2008.

La configuration d'un serveur RADIUS nécessite au moins deux étapes. La première phase, liaison avec le serveur NAS, nécessite de connaître le secret partagé et l'adresse IP de celui-ci. La connexion avec au moins un serveur de compte ne doit pas être oubliée.



Exemple de configuration du client RADIUS sur le serveur IAS Windows 2003



Exemple de configuration du client RADIUS sur le serveur NPS Windows 2008

Méthodes d'authentification EAP

Le but des méthodes Extensible Authentication Protocol (EAP) est d'authentifier les utilisateurs, avant de les laisser rentrer sur le réseau. Elles gèrent ainsi le transport de ces informations d'authentification, dans l'architecture 802.1x/ RADIUS présentée précédemment.

En fait, un certain nombre de méthodes sont basées sur EAP, autorisant l'usage de moyens aussi divers que les login/mots de passe, les certificats électroniques, les cartes à puce, la biométrie...

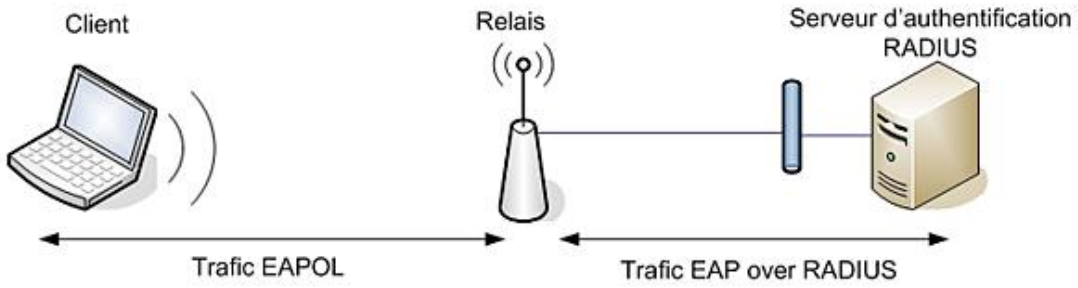
Certaines de ces méthodes sont dites génératrices de clés (*Key Generating*), venant ainsi fournir également la solution de chiffrement.

1. Fonctionnement

a. Les principes

L'organisme IETF a également standardisé EAP, à travers les publications RFC 2284, puis 3748 (http://www.ietf.org/rfc/rfc3748.txt), qui a rendu la première obsolète.

Le standard 802.1x propose l'utilisation d'EAP entre le système à authentifier et le relais, ici un point d'accès. Ce transport des informations sur les médias de la famille IEEE 802 est appelé EAP over LAN (EAPoL). Nous avons vu précédemment que RADIUS a été étendu, pour prolonger ce trafic, entre le relais et le serveur d'authentification. Ce trafic est EAP over RADIUS.



Les deux types de trafic EAP

Ainsi, le contrôleur d'accès, en l'occurrence la borne Wi-Fi à laquelle est associé le client, transmet les demandes jusqu'au serveur RADIUS. En attendant la validation de l'authentification, il bloque toute autre tentative de communication.

b. Les paquets EAP

Les quatre types de paquets EAP ressemblent à ceux utilisés dans les communications RADIUS.

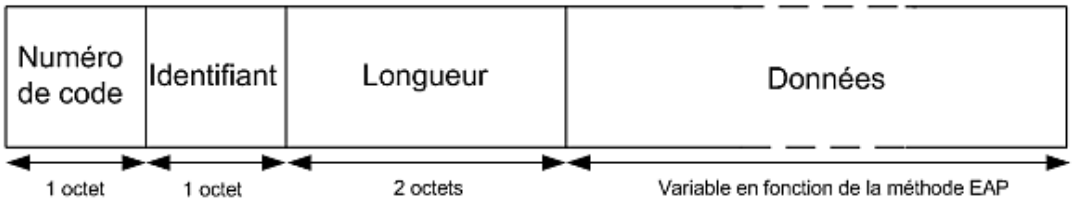
Le premier paquet est celui de requête. Il est envoyé par le relais d'authentification, demandant au client la fourniture de ses informations d'authentification. Elles lui sont fournies en réponse. Le champ de données de ce dernier paquet dépend de la méthode EAP utilisée.

Les deux autres paquets précisent la réponse du serveur d'authentification, indiquant un succès ou un échec.

Numéro de code	Type de paquet
1	Requête (Request)
2	Réponse (Response)
3	Succès (Sucess)
4	Echec (Failure)

Les différents numéros de code

L'en-tête de ces paquets EAP ne comporte que trois champs. Ils contiennent les numéros de code du paquet, son identifiant et sa longueur.



Le paquet EAP

L'extension EAPoL a été définie pour 802.1x sur des réseaux locaux. D'autres types de messages sont ajoutés, dont :

- EAPoL-Start, demande initiale du client ;
- EAPoL-Packet, qui encapsule les paquets EAP ;
- EAPoL-Key, pour l'échange de clé de chiffrement ;
- EAPol-Logoff, demande de fin de session.

Le format du paquet EAPoL évolue quelque peu. Son contenu exact dépend également du type de protocole LAN dans lequel il sera encapsulé. Dans les différents champs de l'en-tête sont précisés, en plus, la version et le type de paquets.

c. Le dialogue complet

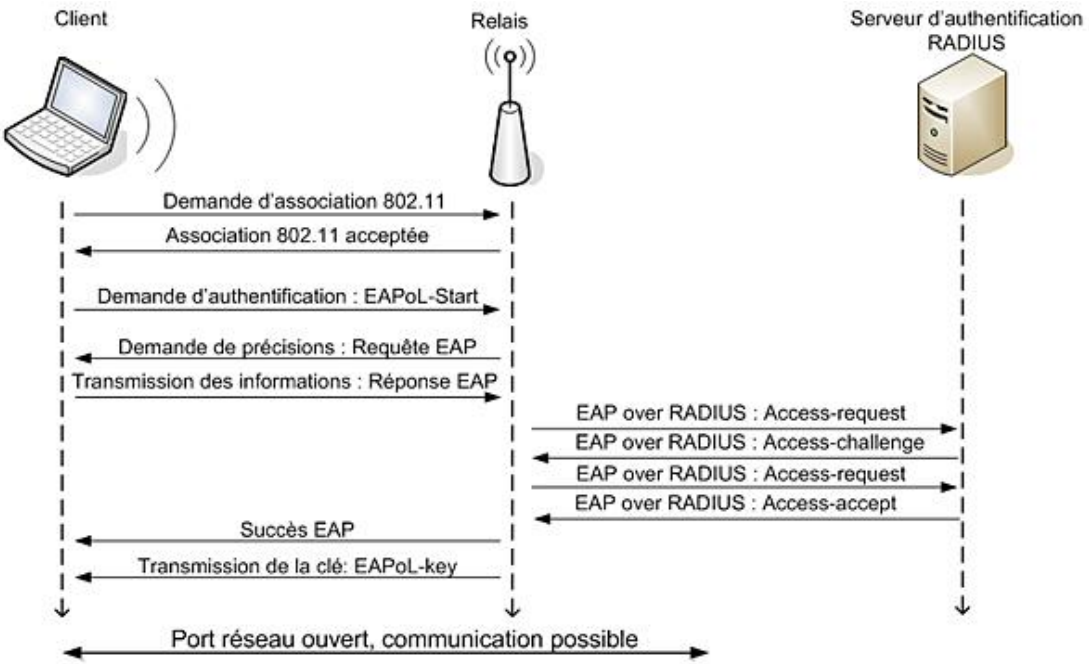
La première étape du processus complet est indépendante de EAP. Il s'agit de l'association entre le client Wi-Fi et le point d'accès. Pour la suite, les paquets EAPoL seront encapsulés dans ceux 802.11.

Ensuite, le client peut entamer la phase d'authentification. Elle démarre par le paquet EAPoL-Start. En réponse, le point d'accès demande les informations d'identité, selon une méthode précise. Si le client utilise cette même méthode, il répond et ce paquet est transmis au serveur RADIUS, entamant un second dialogue.

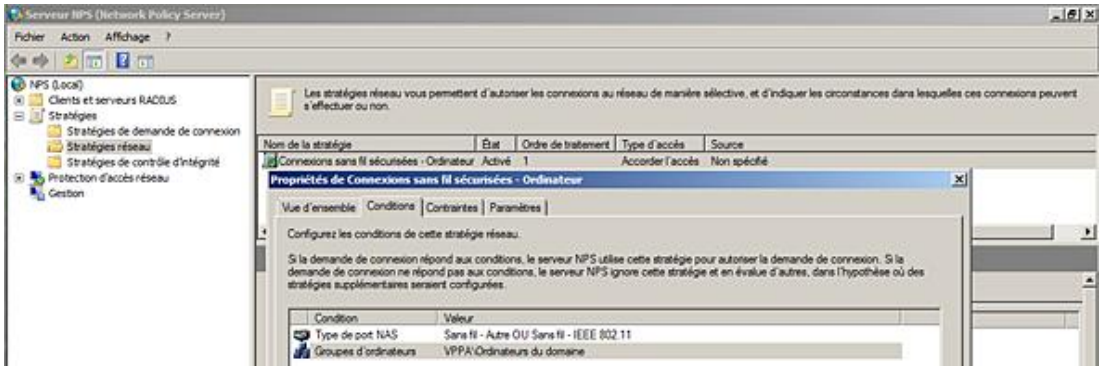
La communication de défi est entamée, avant l'échange de paquets Access-request de demande d'authentification et sa réponse, ici Access-accept.

Finalement, l'acquiescement est prolongé jusqu'au client. À ce moment peut être fournie la clé de session.

Le processus d'authentification terminé, les communications peuvent être prolongées au-delà du point d'accès.



Les serveurs d'authentification Windows IAS (Windows 2000 et 2003) et NPS (Windows 2008) proposent, en complément à l'authentification, des stratégies réseaux. Ainsi, pour accorder l'accès, des conditions doivent être vérifiées, en plus de l'authentification. Une stratégie intéressante, dans une architecture Active Directory, peut être d'authentifier d'abord l'ordinateur, en vérifiant son appartenance au groupe Ordinateur du domaine, puis de forcer une nouvelle authentification de l'utilisateur, avec appartenance à un groupe autorisé à se connecter en Wi-Fi.



Exemple de stratégies réseau sur un serveur NPS

2. Solutions d'authentification EAP

a. Les principales méthodes

Extensible Authentication Protocol propose un canevas sur lequel viennent s'apposer différentes solutions d'entrée des informations d'authentification, englobant l'identification. Il est donc possible d'envisager différentes méthodes reposant sur ce modèle. Plus ou moins sécurisées, elles seront surtout adaptées aux besoins.

Les trois formes que sont mot de passe, support physique et caractéristique humaine peuvent ainsi être utilisées distinctement ou de manière combinée.

La RFC 3748, qui définit EAP, propose plusieurs méthodes. La première est basée sur un système One Time Password, mot de passe à usage unique. EAP-OTP utilise un défi aléatoire envoyé au client. Un générateur l'utilise avec une "passphrase" partagée pour générer le mot de passe. Quelque peu complexe d'usage, cette méthode a montré des failles. De plus, elle ne demande pas d'authentification mutuelle entre le client final et le serveur d'authentification RADIUS.

L'usage d'une carte à jeton générique (GTC - *Generic Token Card*), est également présenté dans la RFC 3748. Cette méthode EAP-GTC, très sure, nécessite la possession par l'utilisateur d'un boîtier de génération de clé, le jeton. Cet utilisateur répond au défi envoyé par le serveur en saisissant le code présenté par la carte à jeton. En fonction du type et de la marque de celle-ci, les processus peuvent changer légèrement.

Dernière méthode de la série, EAP-Message Digest (EAP-MD5) ne réclame pas non plus d'authentification mutuelle entre le client final et le serveur RADIUS. Elle demande la saisie d'un identifiant et du mot de passe correspondant. Ce dernier est transmis comme empreinte, hachée par MD5. Des failles importantes lui ont été trouvées.

Sur les réseaux distants, la société Microsoft recommande l'usage de son protocole d'authentification dérivé du Challenge Handshake Authentication Protocol (CHAP), MS-CHAPv2, défini dans la RFC 2759. Il était donc normal qu'ils étendent leur solution en EAP-MSCHAPv2. Cette méthode, incluse dans Windows, nécessite transmission de l'identifiant et d'un mot de passe, haché par un algorithme propriétaire.

La société Cisco propose également sa propre méthode, Lightweight EAP (LEAP), basée sur login/mot de passe. Cet EAP propriétaire nécessite la mise en œuvre d'une solution complète l'appliquant.

Trois autres méthodes montrent de très intéressantes capacités dans le contexte d'authentification sur un réseau sans fil 802.11. Fiables, elles permettent également la distribution automatique de clés de chiffrement.

EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS) et EAP-Protected EAP (EAP-PEAP) sont détaillées ci-dessous.

Seules les méthodes les plus connues ont été citées, d'autres existent ou sont en cours d'élaboration.

b. La méthode EAP-TLS

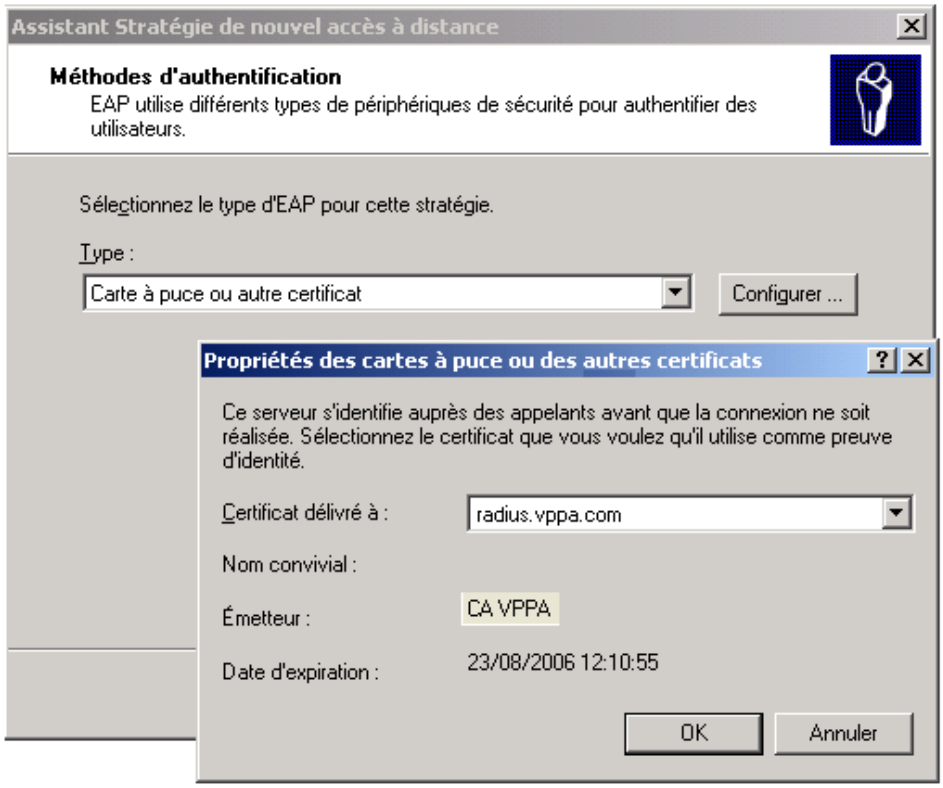
Elle est définie dans la RFC 2716. Elle s'appuie sur le protocole Transport Layer Security (TLS), lui-même décrit dans la RFC 2246. Elle est reconnue comme très sécurisée.

EAP-TLS utilise les certificats électroniques pour une authentification mutuelle entre le client et le serveur. Un tunnel sécurisé est également mis en place pour la distribution des clés de chiffrement.

La mise en œuvre d'une infrastructure de gestion des clés et donc d'une autorité de certification (CA - *Certificate Authority*) est recommandée. En effet, tous les serveurs RADIUS et tous les utilisateurs qui doivent être authentifiés par ce moyen, doivent posséder un certificat électronique. Leur achat auprès d'une société spécialisée pourrait coûter très cher.

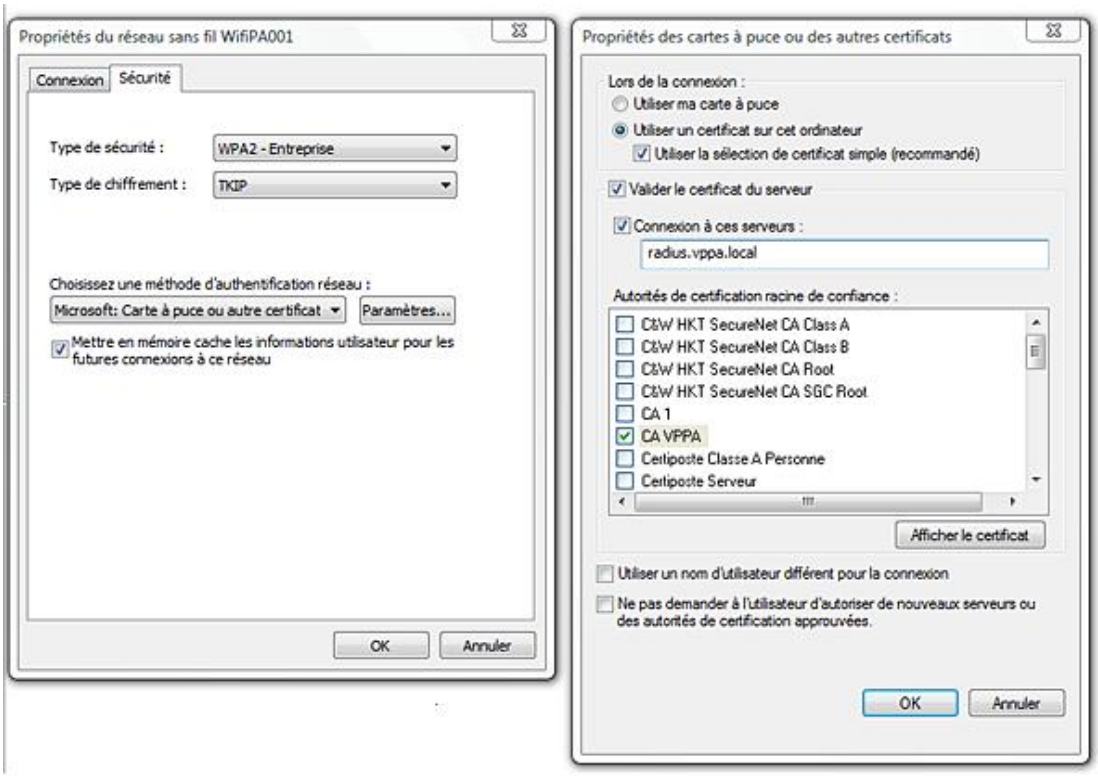
Ce dispositif d'identification est utilisé sur les serveurs pour :

- être reconnu par le client demandant connexion ;
- mettre en œuvre le tunnel chiffré initial.



Paramétrage d'un serveur RADIUS Microsoft (IAS) pour EAP-TLS

L'utilisateur lui-même doit être en possession d'un certificat validant son identité, puisque celui-ci lui sera demandé par le serveur RADIUS avec lequel il communiquera. Si le certificat électronique est stocké sur le poste de travail, il n'est accessible qu'après l'ouverture de session du système d'exploitation. La saisie d'informations d'identification (login) et de mot de passe est donc nécessaire. Le stockage de ce certificat sur un support physique, carte à puce ou clé USB est également possible.



Configuration d'un client Windows Vista pour EAP-TLS

Le dialogue d'authentification reste basé sur celui présenté précédemment. Le paquet EAPoL-Start contient un message TLS-Start, auquel le client répond. Ensuite, le serveur renvoie son certificat, auquel est joint sa clé publique. Il demande également par ce même paquet celui du client.

Le dialogue EAP-TLS (simplifié)

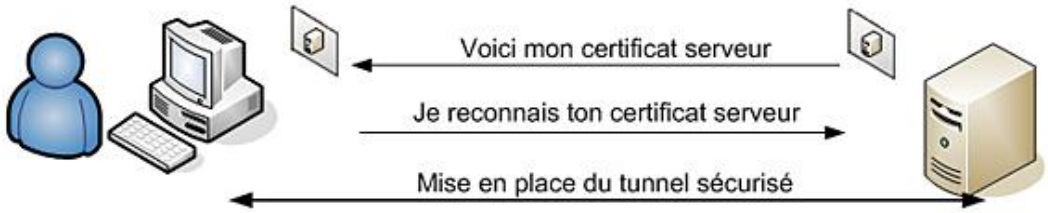
Si cette authentification mutuelle est validée, le processus de distribution des clés de chiffrement peut être entamé.

c. Les méthodes EAP-PEAP et EAP-TTLS

Les méthodes EAP-Tunneled Transport Layer Security (EAP-TTLS) et EAP-Protected EAP (EAP-PEAP) sont très proches.

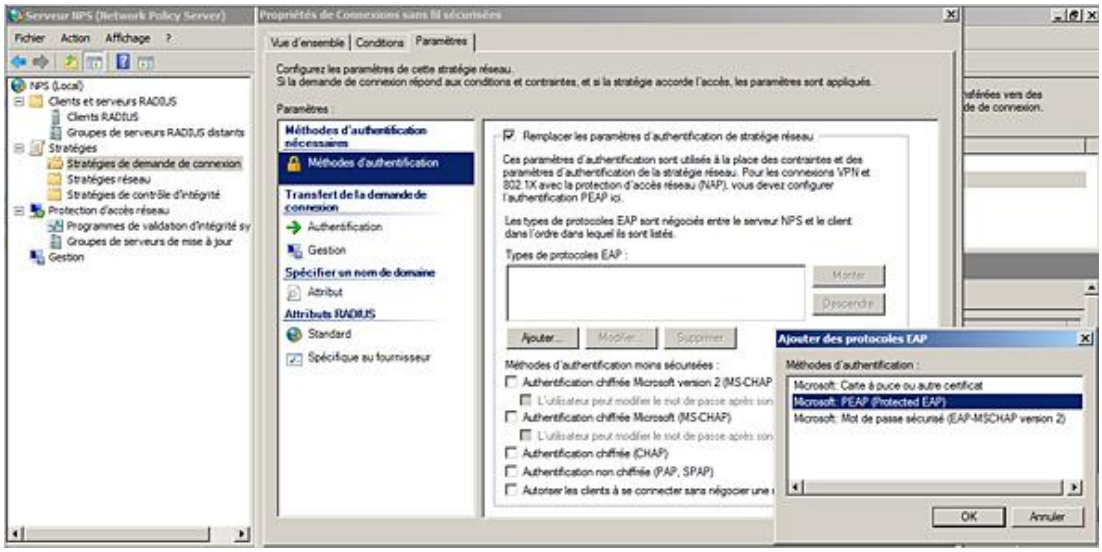
Toutes deux proposent l'authentification du serveur RADIUS par le client, grâce à un certificat électronique, dont l'autorité de délivrance est reconnue. Avec EAP-PEAP comme avec EAP-TTLS, les utilisateurs n'ont pas besoin de posséder un certificat.

Grâce au certificat serveur et à la clé publique qui y est attachée, un tunnel sécurisé TLS est mis en place. La saisie des informations d'authentification utilisateur, identifiant et mot de passe, peut maintenant être réalisée. Le traitement entre ces deux méthodes devient, à partir de ce moment, différent.

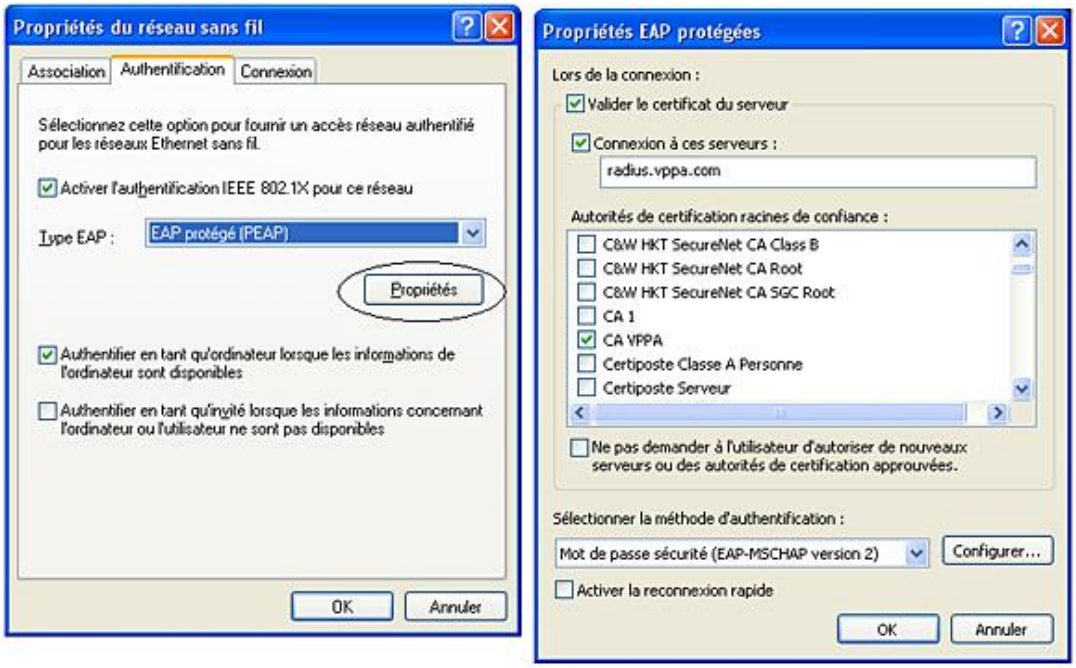


La mise en place du tunnel dans EAP-PEAP et EAP-TTLS

La méthode EAP-PEAP, développée par Cisco et Microsoft, encapsule ce dialogue dans des paquets EAP, ce qui nécessite un serveur RADIUS compatible. À l'intérieur du tunnel et de manière transparente pour l'extérieur, le mode d'envoi de ces informations peut être MD5, OTP, MS-CHAPv2... En effet, le transfert est sécurisé par le tunnel et il suffit juste que le serveur RADIUS puisse vérifier ces informations.



Mise en œuvre de la méthode d'authentification sur le serveur NPS (Windows 2008)



Configuration d'un client Windows pour EAP-PEAP

EAP-TTLS utilise directement les attributs RADIUS pour transférer les informations d'identification et d'authentification. Elles sont encapsulées dans les Attribute Values Pairs (AVP), l'échange est donc plus standardisé.

Le mode d'identification interne est, là encore, transparent. Une circulation des mots de passe en clair est même possible.

Ces méthodes présentent toutes deux l'avantage de simplifier l'obtention d'informations utilisateur, en ne demandant pas de gestion de certificat. Comme toujours, la faiblesse des mots de passe est à prendre en compte.

EAP-PEAP est une solution moins standardisée, mais elle bénéficie de deux soutiens de choix, avec Cisco et Microsoft. Le client correspondant est installé sur les postes MS Windows. EAP-TTLS, plus flexible, par son utilisation des AVP, exige l'installation d'un client spécifique.

3. Distribution des clés de chiffrement

En plus des vérifications d'authentification, le couplage de 802.1x avec certaines méthodes EAP permet l'automatisation de délivrance des clés de chiffrement.

Une clé maîtresse (PMK - *Pairwise Master Key*) de 256 bits est générée par le serveur RADIUS et renvoyée au point d'accès dans un message EAP over RADIUS. Elle est contenue dans un Vendor Specific Attribute (VSA) défini par Microsoft. Cet attribut porte le numéro 17 et s'intitule MS-MPPE-Recv-Key. En effet, la Wi-Fi Alliance s'est servie de cette caractéristique déjà existante, la seule dédiée au transfert de clé.

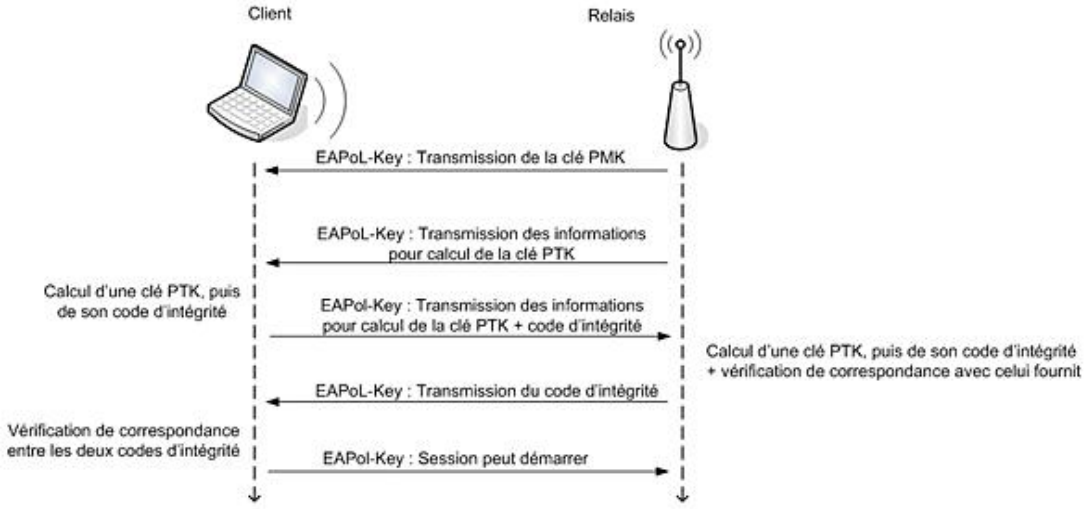
Ainsi, après authentification mutuelle et mise en place du tunnel sécurisé, la clé est fournie au client.

Même si cette solution n'est pas standardisée, une clé WEP statique peut être délivrée par ce processus.

Comme dans le système WPA-PSK, la solution WPA Enterprise, n'utilise pas cette clé PMK pour le chiffrement. Une clé Pairwise Transient Key (PTK) de 512 bits, dérivée de la précédente est calculée sur chaque entité, à partir :

- de la clé PMK ;
- de numéros aléatoires générés sur le point d'accès et le client ;
- des adresses MAC du point d'accès et du client.

Le processus d'échange complet est nommé poignée de main à quatre étapes (Four-way handshake). Il est réalisé dans des paquets EAPol-Key et permet de s'assurer que les mêmes clés seront utilisées des deux côtés.



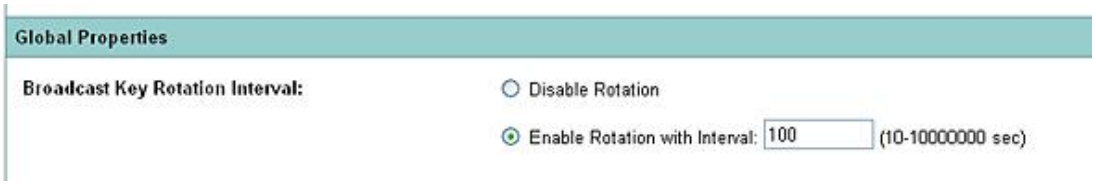
Le processus "four-way handshake"

Nous rappelons que les 512 bits de la clé PTK sont divisés en quatre clés de 128 bits, dont les deux premières seront ici utilisées :

- Key Confirmation Key (KCK), pour les calculs d'intégrité ;
- Key Encryption Key (KEK), pour le chiffrement.

La première utilisation de ce chiffrement par la clé temporaire, est la délivrance, à partir du point d'accès, de la clé de

groupe temporaire (GTK - *Group Temporal Key*) de 256 bits. Durant la session, le point d'accès peut changer de clé de groupe à intervalles réguliers. Pour faciliter la transition, l'usage temporaire de deux clés est prévu.



Paramètre de renouvellement de clés de groupe sur un point d'accès

Généralités

Le standard 802.11i est finalisé par l'IEEE en juin 2004. Ratifié trois mois après, il est estampillé WPA2 par la Wi-Fi Alliance.

802.11i ouvre de nouvelles perspectives en officialisant une nouvelle manière de considérer la sécurité des réseaux 802.11. La refonte par rapport aux premières spécifications est très conséquente.

WPA était bien une transition vers cette troisième génération, qui prolonge les principes déjà décrits en terme d'authentification.

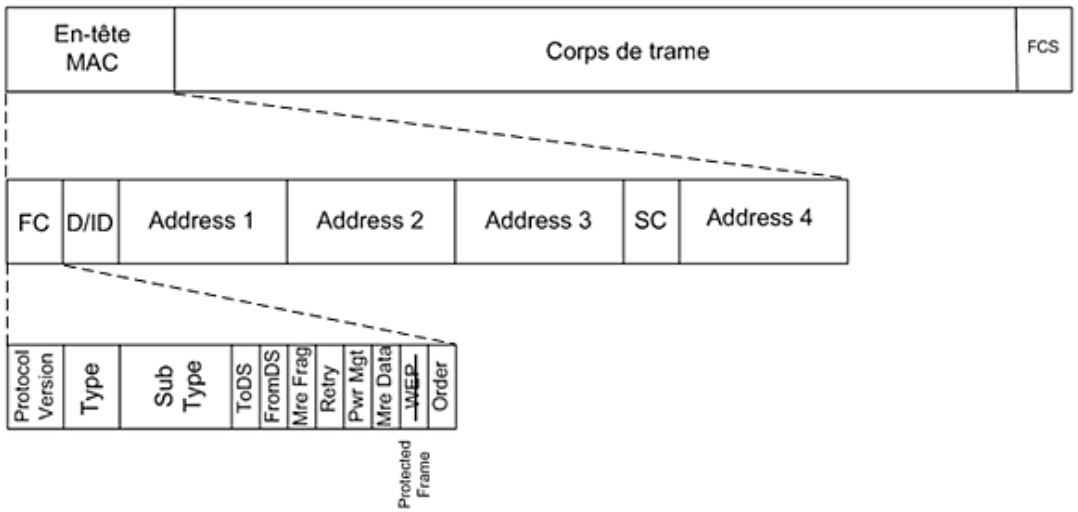
1. Points clés

802.11i définit avant tout un réseau de sécurité forte (RSN - *Robust Security Network*) utilisant, pour les professionnels, les moyens d'authentification du protocole IEEE 802.1x<$I802.1x> (RSNA - *Robust Security Network Association*).

La compatibilité avec les modèles de sécurisation précédents est possible, dans un réseau qualifié de transition (TSN - *Transition Security Network*). Elle permet de conserver les usages des moyens décrits dans le standard 802.11 :

- Open System authentication/ Shared Key authentication ;
- WEP...

Les spécifications 802.11i complètent et étendent la couche MAC 802.11. Ainsi, sans modifier la structure de l'en-tête décrite dans le chapitre 5, le champ de clé WEP est renommé en "Protected Frame". Il reste positionné à 1 si un chiffrement quelconque est demandé.



Le renommage du champ WEP dans l'en-tête MAC 802.11i

Quelques trames de gestion sont également modifiées, avec l'insertion possible dans le corps de trame, partie éléments d'informations (IE - *Information Element*), d'une signalétique RSN détaillant les capacités. Ainsi, un point d'accès peut désormais annoncer la possibilité d'utiliser 802.11i/WPA2 dans ses trames de balises ou de réponse de sondage. Cette information circule également, depuis les stations, dans les trames de requête d'association et de réassociation.

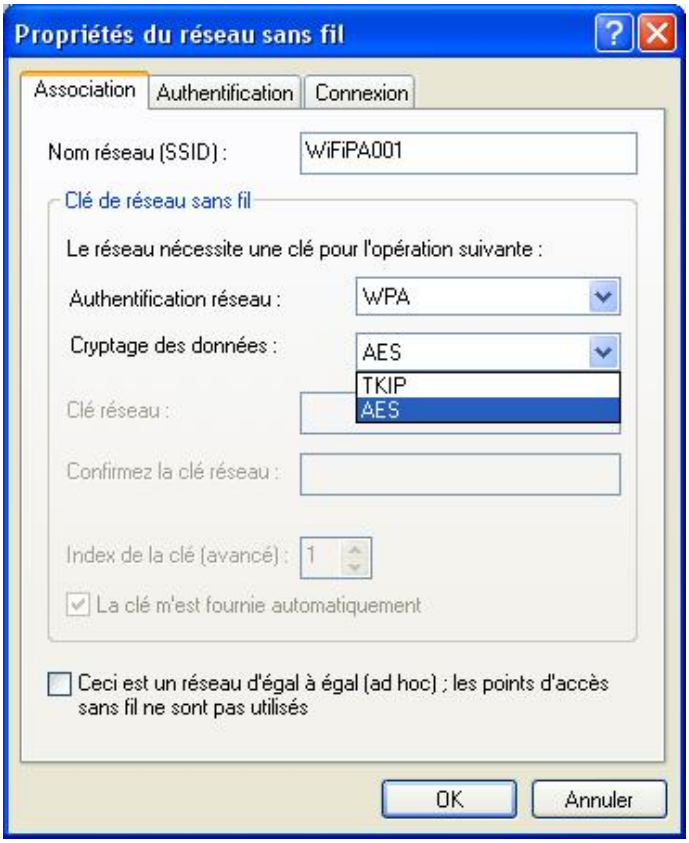
Des codes de justification supplémentaires ont été ajoutés aux trames de désassociation, pour tenir compte des processus 802.1x et de leur mise en échec.

2. Chiffrement

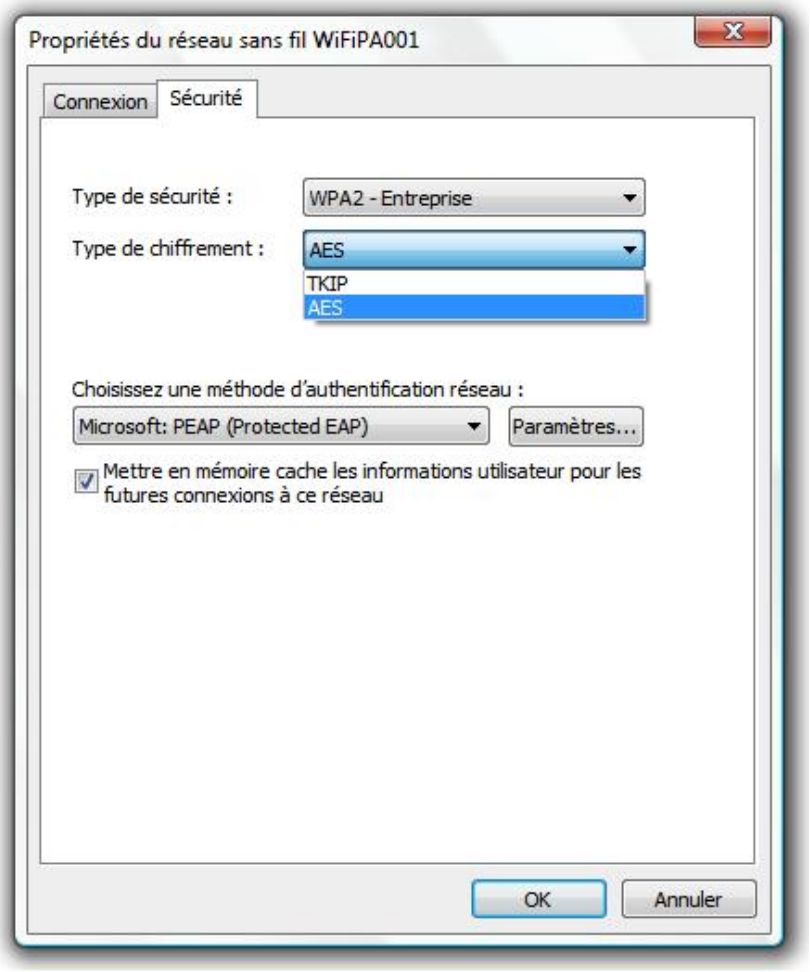
Tout en gardant compatibilité avec les modèles de sécurisations précédents, 802.11i rompt avec l'usage de l'algorithme RC4.

Ainsi, le chiffrement, dans une structure RSN, est assuré par le protocole CTR with CBC-MAC Protocol (CCMP), basé sur l'algorithme Advanced Encryption Standard (AES). Dans certains menus de configuration logicielle, le sigle WPA/AES, au

lieu de WPA2, est utilisé, par opposition à WPA/TKIP.



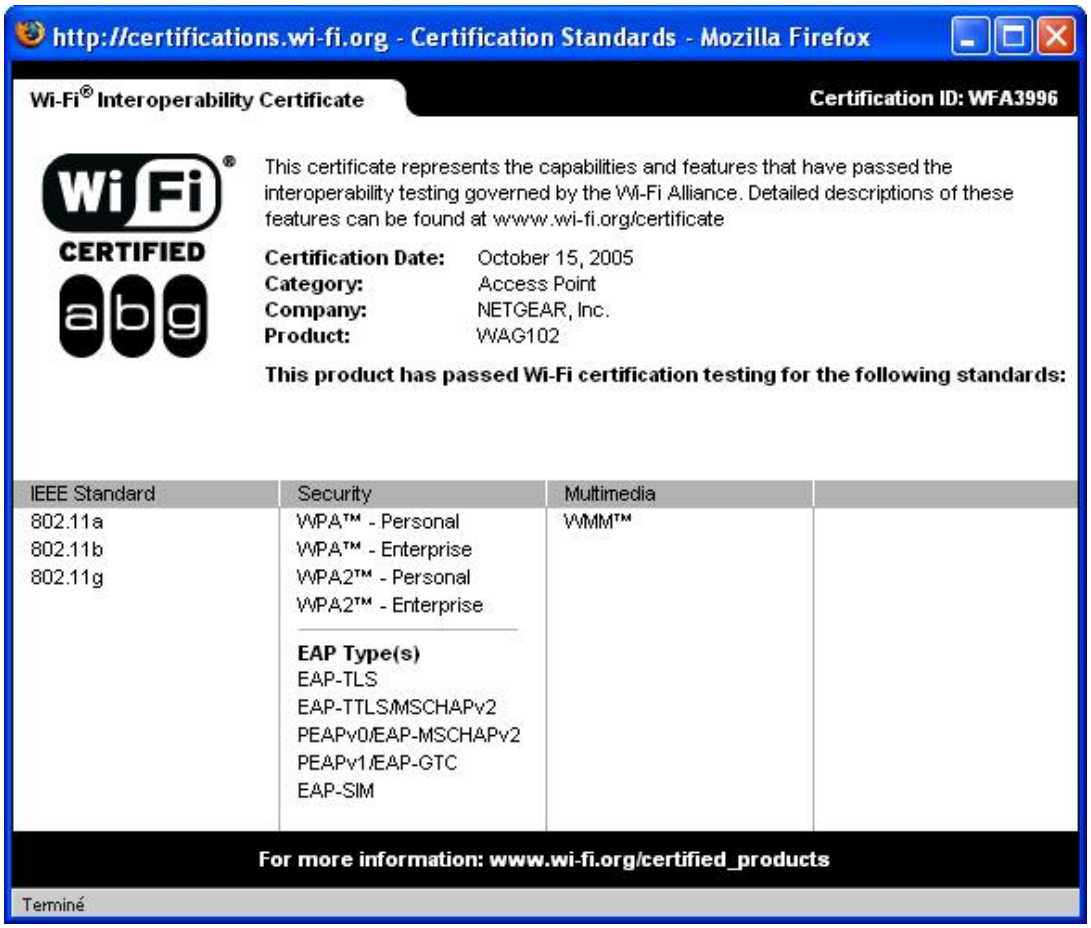
Prise en charge du chiffrement CCMP-AES par Windows XP SP2



Prise en charge du chiffrement CCMP-AES par Windows Vista

Au début, cette rupture a rendu incompatible bon nombre de matériels existants, non prévus pour supporter 802.11i. Une simple mise à jour des pilotes ne suffisait plus, contrairement au passage à WPA. Les matériels récents sont généralement compatibles, mais il est fortement recommandé de vérifier leur certification en WPA2 par la Wi-Fi Alliance.

Windows XP SP2 nécessite le téléchargement d'un correctif pour la prise en charge de WPA2. Cette mise à jour porte le numéro KB893357.



Certification d'un point d'accès pour WPA2

Sur les points d'accès, il est recommandé de vérifier la présence d'un composant de calcul dédié au chiffrement AES. En effet, l'usage de cet algorithme peut ralentir les transmissions, si plusieurs postes de travail sont associés.

3. Authentification et distribution des clés

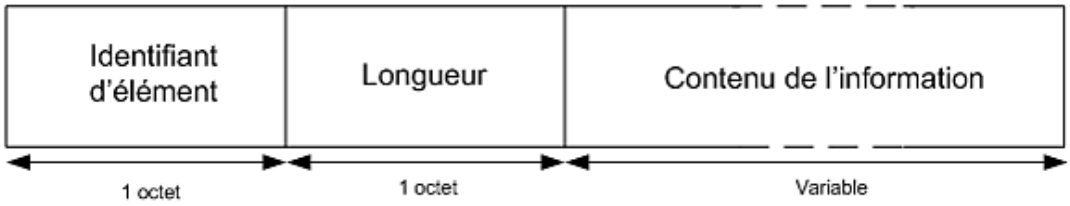
Comme pour WPA, deux niveaux d'authentification sont autorisés :

- Personnel (Personal), utilisant une clé partagée ;
- Entreprise (Enterprise), exploitant les capacités du 802.1x.

L'architecture professionnelle d'authentification, qualifiée de Robust Security Network Association (RSNA), doit distribuer automatiquement les clés. Les processus décrits dans le chapitre précédent sont ici conservés. Ainsi, l'échange de la clé Pairwise Transient Key (PTK) reste celui nommé "four way handshake". Il est également suivi de celui de transmission de la clé de multicast et broadcast, Group Temporal Key (GTK).

Les formats de clés autorisés par 802.11i sont :

- WEP 40 bits, exclusivement pour GTK ;
- WEP 104 bits, exclusivement pour GTK ;
- TKIP, pour PTK et GTK ;
- CCMP, pour PTK et GTK.



Rappel : le format du champ Information Element (IE)

La politique RSN, dans une trame de balises, de réponse de sondage, de requête d'association ou de réassociation est précisée dans un champ d'éléments d'informations (IE). Ce nouveau contenu, ajouté au corps de trame, a pour identifiant le numéro 48.

Version	Informations de clé de groupe (Group Cipher Suite)	Informations de clé individuelle (Pairwise Cipher Suite)	Gestion d'authentification (Authenticated Key Mgmt)

Extrait du contenu de l'information, dans le champ IE (simplifié)

La version est celle du protocole RSNA. Sa valeur reste, pour l'instant, positionné à 1, ce qui indique :

- Que la méthode "Open System authentication" est supportée ;
- Que l'ex-champ de clé WEP, renommé en "Protected Frame", est géré ;
- Que le RSN IE est disponible ;
- Que le protocole CCMP est supporté ;
- Que la mise à jour des clés peut être réalisée à travers EAPoL-Key.

Les paramètres "Group Cipher Suite" indiquent le type de clé de groupe, pour les trafic broadcast et multicast. Ils contiennent deux informations :

- un identifiant, Organizationnally Unique Identifier (OUI), sur 3 octets ;
- une valeur, Suite Type, sur 1 octet.

OUI	Valeur	Signification
00-0F-AC	0	Pas d'usage de ce champ
00-0F-AC	1	WEP 40 bits
00-0F-AC	2	TKIP
00-0F-AC	3	Réservé
00-0F-AC	4	CCMP
00-0F-AC	5	WEP 104 bits
00-0F-AC	6-255	Réservé
OUI fabricant	Autre	Propre au constructeur
Autre	Toutes	Réservé

Détail des valeurs "Group Cipher Suite"

Les champs suivants servent pour le transfert d'informations sur les clés individuelles. Dans ceux "Authenticated Key Management" est indiqué le mode d'authentification, donc de gestion de clé :

- Valeur 1, pour utilisation de 802.1x ;

- Valeur 2, pour Pre-Shared Key (PSK) ;
- Autres, réservé ou pour usage constructeur.

Détails de fonctionnement

Les spécifications 802.11i définissent précisément trois fonctions de sécurisation.

La première assure la confidentialité, intégrant un système d'anti-rejeu. Nous avons vu que ce protocole CTR with CBC-MAC Protocol (CCMP) utilise l'algorithme de chiffrement Advanced Encryption Standard (AES). La compatibilité avec les systèmes précédents, WEP et TKIP est quand même précisée.

L'authentification forte, avec 802.1x a déjà été abordée.

La troisième fonction est un contrôle d'intégrité puissant.

1. Algorithme AES

a. La naissance

L'algorithme de chiffrement à clés symétriques Data Encryption Standard (DES) est très utilisé, encore plus que Rivest's Cipher 4 (RC4). Malheureusement il aurait dû être renouvelé depuis longtemps, puisque les clés utilisées, dont la taille est de 56 bits, sont insuffisantes. Faute d'adoption d'un nouveau standard, la vie de ce système a été prolongée avec la variante Triple DES (3DES).

En 1998, le National Institute of Standards and Technologies (NIST), service du ministère américain de l'économie, lance un appel pour définir un nouveau standard de chiffrement. Dans leur cahier des charges, ils précisent les caractéristiques de celui-ci :

- la méthode doit être à clés symétriques et chiffrement par blocs ;
- la logique utilisée doit être plus solide que celle du Triple DES, avec des tailles de clé de 128, 192 et 256 bits ;
- cette logique doit être publique et de propriété intellectuelle libre dans le monde entier.

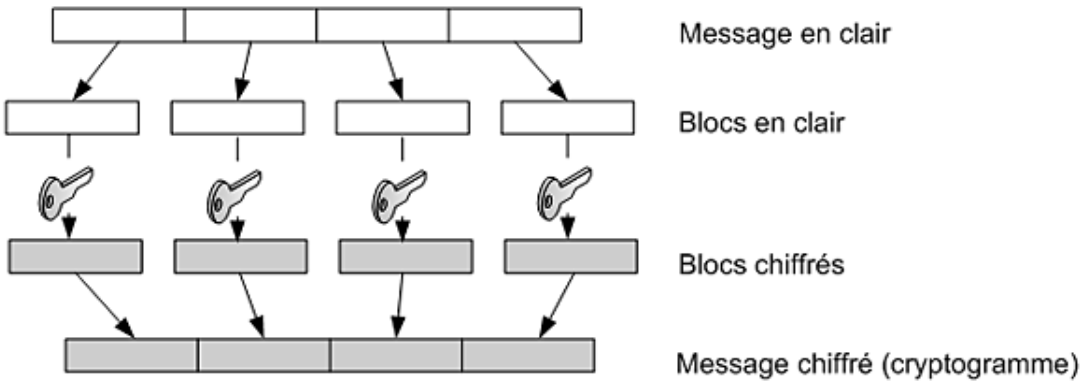
Finalement, c'est la proposition appelée RIJNDAEL, des belges Joan Daemen et Vincent Rijmen qui est retenue en octobre 2000. Elle sera renommée AES. Au jour où sont écrites ses lignes, aucune faille exploitable n'a encore été trouvée.

b. Le chiffrement par blocs

AES ne travaille pas sur un flux de bits, comme RC4, mais sur des bouts de texte. Un découpage de l'information à chiffrer est donc effectué. Chaque partie est transformée en blocs de même taille. Du bourrage (padding) peut être ajouté à la dernière pour obtenir la taille souhaitée.

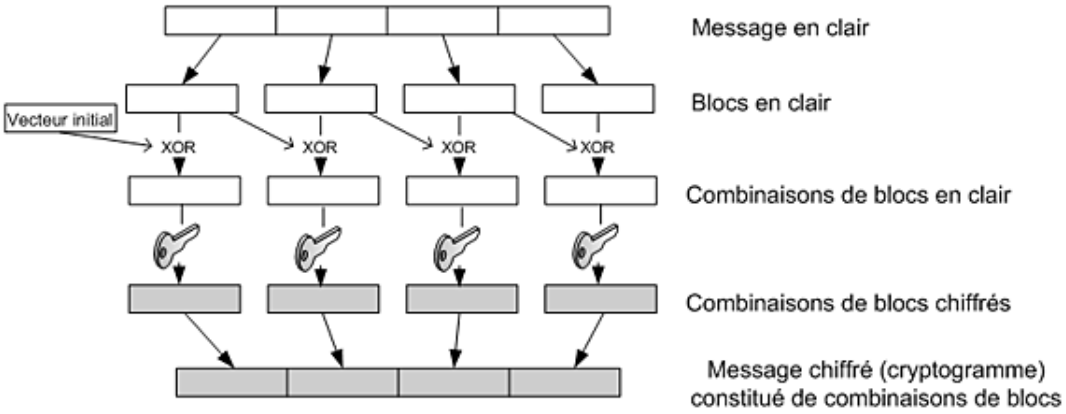
Quatre principales méthodes de découpage de blocs peuvent être utilisées.

Le catalogue électronique de codes (ECB - *Electronic Code Book*) est la méthode la plus simple, qui chiffre indépendamment chaque bloc. Elle ne protège pas des redondances, puisque deux chiffrements d'un bloc identique avec la même clé donneront le même cryptogramme.



Principe du découpage en blocs ECB

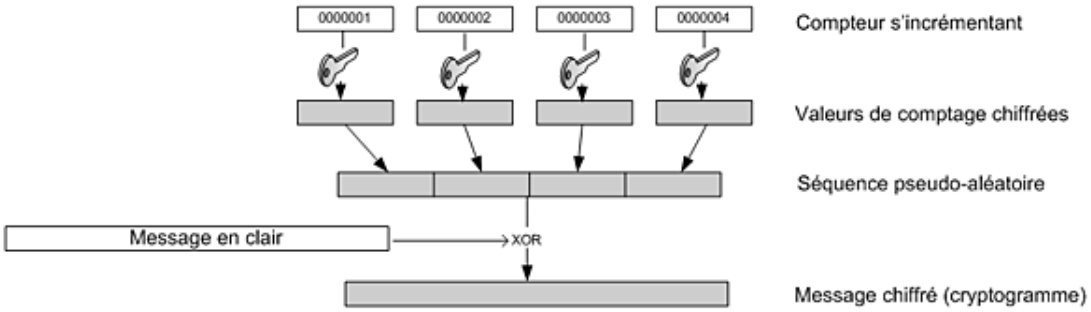
La réponse à ce problème est fournie dans le cryptogramme à blocs chaînés (CBC - *Cipher Bloc Chaining*). Un calcul OU exclusif (XOR) est réalisé entre chaque bloc et son précédent, créant une dépendance des uns par rapport aux autres. Pour chiffrer le premier bloc, un vecteur initial aléatoire est calculé.



Principe du découpage en blocs CBC

Le chiffrement à rétroaction (CFB - *Cipher Feed Back*) nécessite également un vecteur initial. Dans cette méthode, une clé partielle est construite en utilisant le bloc précédent. Un dernier moyen d'utilisation des blocs est le chiffrement à rétroaction de sortie (OFB - *Output Feed Back*) qui résiste même aux erreurs de transmissions.

Le mode compteur (CM - *Counter Mode*) est une variante, découlant de la méthode ECB. Ici, les blocs issus du message restent indépendants les uns des autres. Mais pour protéger d'une redondance, un compteur est utilisé, dont les valeurs sont chiffrées et combinées avec le message lui-même. Finalement, le résultat tient plus d'un chiffrement par flux.



Principe de blocs en Counter Mode (CM)

c. Le calcul

AES est indépendant du mode de découpage en blocs. Chacun subit une série de transformations combinées, avec la clé. Le nombre de répétitions de ces transformations dépend de la taille du bloc et de celle de la clé. Au minimum, cette séquence est répétée 10 fois, avec une taille de 128 bits pour chacun.

Avant tout, ces deux éléments, bloc et clé, sont positionnés dans deux tableaux de 4 lignes chacun. Le nombre de colonnes dépend des tailles. Il est de 4 colonnes pour 128 bits.

Après cette répartition non linéaire, un mélange des tableaux est effectué, par des combinaisons d'opérations simples sur les différents éléments :

- Décalage des lignes, par une fonction nommée ShiftRow ;
- Brouillage des colonnes, par fonction MixColumn.

Le déchiffrement est simple, par l'opération inverse.

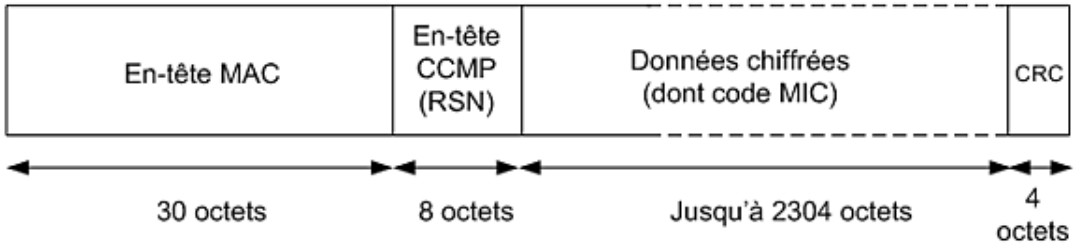
2. Protocole CCMP

L'IEEE propose, dans l'implémentation RSN du 802.11i, l'utilisation des découpages par blocs, à travers le protocole CTR with CBC-MAC Protocol (CCMP). Les fonctions assurées sont :

- la confidentialité et l'anti-rejeu, avec l'exploitation du mode compteur (CM) dans CTR et le chiffrement AES ;
- l'intégrité et l'authentification des extrémités, par une évolution du mode CBC, nommée Cipher Bloc Chaining with Message Authentication Code (CBC-MAC), utilisant, là encore, AES.

CCM est un mode général, défini dans la RFC 3610. Son implémentation nécessite de préciser la taille du champ Message Integrity Code (MIC), ici 8 octets et celui de longueur de trame, sur 2 octets. Les clés de chiffrement temporaires (TK - *Temporal Key*), propres à chaque session, ont une longueur de 128 bits, soit 16 octets.

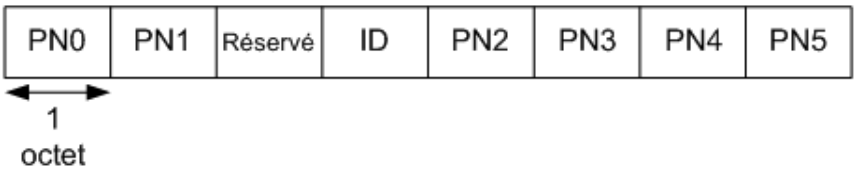
À l'en-tête MAC est ajouté un en-tête CCMP. Il contient un numéro de paquet (PN - *Packet Number*), codé sur 48 bits, soit 6 octets. Le chiffrement porte à la fois sur les données de couche MAC, fragmentées ou non, et sur le MIC.



Trame MAC de type RSN

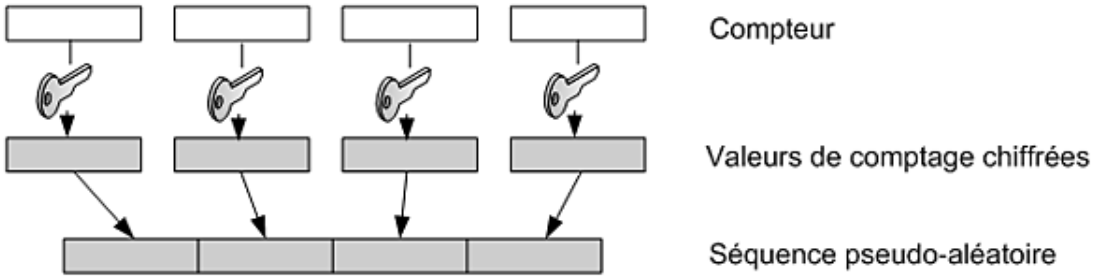
Afin de garder compatibilité de structure avec TKIP, le champ PN est éclaté en 6 parties non contiguës. Le troisième octet, ID, est découpé en trois parties :

- 5 bits restant à 0 pour un espace réservé ;
- L'Extended IV, positionné à 1 ;
- Le numéro de clé (Key ID), sur 2 bits positionnés à 0.



L'en-tête CCMP

Le processus d'encapsulation CCM introduit un certain nombre de données aléatoires, avant l'opération de chiffrement par AES, puis le calcul XOR avec le message à chiffrer. La séquence pseudo aléatoire du Counter Mode (CM) est enrichie, dans le processus CTR.



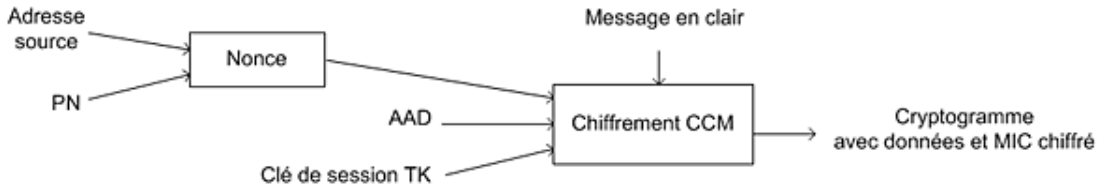
Rappel : génération de la séquence pseudo aléatoire du CM

En effet, le compteur est constitué à partir de plusieurs valeurs :

- le numéro de paquet PN, qui est systématiquement incrémenté ;
- un code Additional Authentication Data (AAD), issu de l'en-tête MAC de la trame ;
- une valeur "nonce" aléatoire.

Pour obtenir le code AAD, beaucoup de bits de l'en-tête MAC sont positionnés à 0, afin de les camoufler. Les quatre champs d'adressage sont utilisés.

Le nonce est constitué à partir de l'adresse d'émission et du numéro PN. Une troisième entrée serait un octet de priorité, pour l'instant bloqué à 0.



Les entrées du chiffrement CCM

Le mécanisme d'anti-rejeu est assuré par la transmission dans la trame du numéro PN séquentiel.

Le destinataire peut réaliser l'étape de déchiffrement à partir de l'en-tête CCMP contenant le PN en clair et de la clé TK, qu'il connaît déjà.

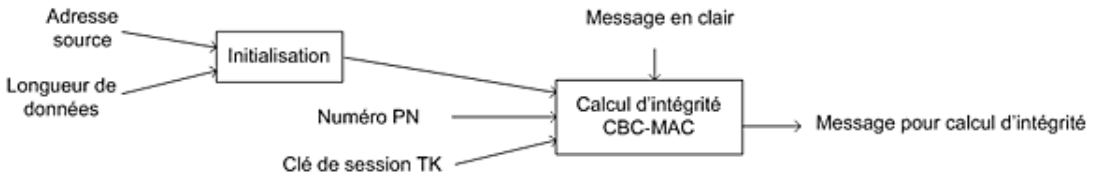
3. Contrôle d'intégrité CBC-MAC

L'authentification des extrémités et la vérification de l'intégrité sont assurées par Cipher Bloc Chaining with Message Authentication Code (CBC-MAC), autre partie de CCMP.

Ce calcul utilise en entrée un découpage du message en blocs. Pour fixer la taille du dernier à 128 bits, un complément de bourrage (padding) peut être ajouté.

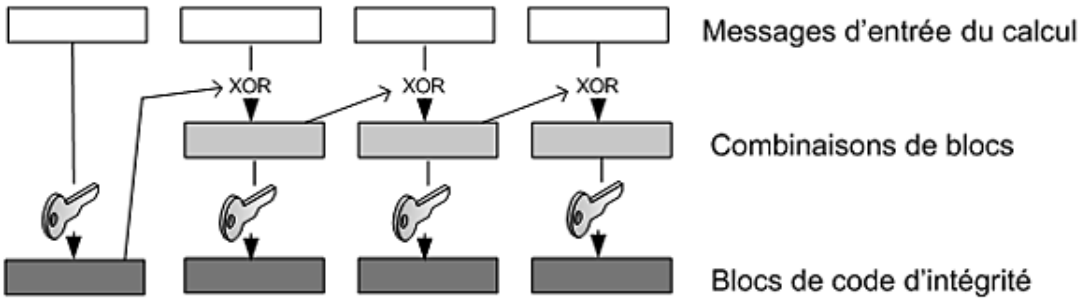
L'entrée du calcul d'intégrité est constituée :

- du message en clair ;
- de l'en-tête CCMP, incluant le numéro PN ;
- d'informations extraites de l'en-tête MAC ;
- de bourrage si besoin.



Le message d'entrée du calcul d'intégrité

Le premier bloc ainsi constitué est d'abord chiffré par l'algorithme AES et la clé de session. Il est ensuite combiné au deuxième par un XOR et ainsi de suite.



Calcul d'intégrité avec CBC

Un tel mécanisme, très fiable, nécessite quand même une puissance de calcul importante. Par contre, il présente l'avantage de tenir compte à la fois du message en clair et de son cryptogramme.

Le résultat de l'opération d'intégrité de chaque trame est finalement découpé en deux, puis inséré dans les 64 bits du champ MIC.

Critères de choix

Dans son implémentation de plus haut niveau, 802.11i présente une méthode fiable et complète de sécurisation. Cette capacité se paye par la puissance de calcul nécessaire sur les équipements.

L'authentification professionnelle avec 802.1x, EAP et RADIUS est recommandée, dès que le réseau Wi-Fi est utilisé régulièrement.

La compatibilité de 802.11i, certifié WPA2, avec la génération précédente TKIP est assurée. Ce dernier mode peut être suffisant dans bien des cas. D'autant plus que la mixité est permise, afin de gérer simultanément plusieurs niveaux de sécurité.

WPA2 fonctionne à la fois dans une infrastructure gérée par des points d'accès et en mode ad hoc. La méthode WPA ne peut être exploitée dans ce dernier cas.

Nous retiendrons également que WEP apporte une sécurité très insuffisante, et son usage n'est pas recommandé.

L'alternative est possible avec des méthodes de sécurisation qui ne sont pas propres à ce réseau, en construisant des réseaux privés virtuels.

Possédant enfin un standard de sécurisation, le Wi-Fi peut désormais progresser en débit et en qualité de service.

Solution	Protocole	Chiffrement	Intégrité
WEP	WEP	RC4	CRC
WPA	TKIP	RC4	MIC
WPA2	TKIP	RC4	MIC
WPA2	CCMP	AES	CBC-MAC

Tableau récapitulatif des méthodes de chiffrement et d'intégrité

Évaluation des besoins

Si le réseau Wi-Fi est un prolongement de celui Ethernet de l'entreprise, la réalisation d'une étude complète est un impératif. Profiter de la flexibilité d'un réseau local radio impose une démarche qui ne doit pas être précipitée.

Il est nécessaire, avant tout, de bien définir quel sera l'usage du réseau sans fil. Bien sûr, une interconnexion maillée entre interfaces, par un réseau ad hoc, peut se faire dans l'instant. Ce ne doit pas être le cas pour la mise en service de points d'accès dans un réseau d'infrastructure interne, ou de ponts, pour interconnecter deux réseaux privés.

La réflexion ne sera pas non plus la même, s'il s'agit d'offrir un accès dans une salle de réunion, de prolonger le réseau Ethernet ou de proposer une alternative à celui-ci dans l'ensemble d'un bâtiment.

Les contraintes à prendre en compte pour l'exploitation sont variées. Les prestations hertziennes doivent d'abord fournir une couverture adéquate, et les matériels correspondre aux besoins. Les éléments informatiques couvriront les réglages d'optimisation et des moyens de sécurisation.

1. Paramètres

a. Le choix des standards

802.11b fait désormais figure de standard historique et n'est plus exploité qu'exceptionnellement, par exemple dans des environnements industriels où son faible débit n'est pas pénalisant.

En cas de fortes contraintes d'interférences sur la bande des 2.4 GHz, le 802.11a peut être adopté, d'autant plus que la largeur de bande passante désormais autorisée l'avantage. Par contre, l'utilisation de ce standard est peu courante en France et relativement peu de matériels le prennent en charge.

L'adoption du 802.11g s'impose donc, en vérifiant pour les nouveaux équipements, particulièrement les points d'accès, la compatibilité 802.11n draft.

Au niveau de la sécurité, il est recommandé de vérifier les certifications, par la Wi-Fi Alliance. Dans un environnement professionnel, la possibilité d'application du standard 802.11i (WPA2) est indispensable. La Wi-Fi Alliance signale également quels modes EAP sont disponibles pour l'authentification.

La capacité, par les bornes, à prendre en charge le standard IEEE 802.3af, Power over Ethernet (PoE) permet de s'affranchir d'un branchement au courant électrique. Dans ce cas, le réseau Ethernet transmet également une tension suffisante pour l'alimentation de l'équipement, à travers les deux paires non utilisées pour les transmissions.

b. La couverture radio

Lorsque le service que devra apporter le réseau sans fil est déterminé, par exemple une alternative au réseau Ethernet, les zones de couverture doivent être précisées.

En intérieur, quelques questions basiques sont à poser, telles que :

- Dans quelle partie exacte du bâtiment doit-on utiliser le réseau ?
- Quelles pièces nécessitent un accès ?
- Dans ces pièces, quelles zones d'ombres pourraient être tolérées ?

Cette première analyse des besoins permet, sans le figer, de rapprocher le réseau Wi-Fi de sa future réalité. Il paraît important de fixer cette couverture géographique au plus large, afin d'éviter des déboires dans l'évolution du réseau.

Une fois ces besoins précisés, l'étude permet également d'avoir une première idée des cellules à mettre en œuvre. Ces caractéristiques de couverture sont dépendantes des dispositions de pièces. Si l'espace est constitué de nombreuses salles fermées, comme dans des hôpitaux et cliniques, voire comme certains environnements de bureau, les zones doivent être plus petites. Les cellules seront de tailles plus importantes dans des espaces ouverts, comme des entrepôts ou des magasins. En revanche, dans de tels bâtiments, les rayonnages, dont le contenu est très changeant, sont à prendre en compte.

Cette étude de couverture sera complétée par un bilan radio, afin de préciser la position et le type des antennes à utiliser.

c. Le service aux utilisateurs

D'autres critères importants de l'étude sont le nombre et la densité des utilisateurs qui feront appel au réseau Wi-Fi. Leurs besoins moyens en bande passante sont également à prendre en compte dans le service.

Sachant que le débit utile est partagé entre les différents postes associés au point d'accès, la permanence de connexion est également un facteur. En effet, des utilisateurs ponctuels ne seront pas comptabilisés de la même façon que des usagers réguliers.

De plus, les exigences en débit d'un poste de travail peuvent être très variées, dépendant des applications réseaux exploitant le canal radio. Des fonctionnalités bureautiques, générant des transferts avec des serveurs de fichiers ou de données, ne requièrent pas le même taux moyen de bande passante que la consultation de sites Web. Les exigences réseaux sont encore différentes avec des périphériques, vidéo-projecteurs ou imprimantes par exemple, intégrés au réseau sans fil.

À partir d'un point d'accès émettant en 802.11g, il faut considérer que le débit utile n'excède pas 23 Mbps, à cause des en-têtes de trames. Les mécanismes de chiffrement ne réduisent que très peu cette valeur. Par contre, la fragmentation fait chuter fortement le débit. Avec la mise en œuvre des options d'économie d'énergie, il ne faut pas s'attendre à excéder une douzaine de mégabits par seconde. Il ne faut pas oublier que ces valeurs diminuent en éloignant l'interface cliente du point d'accès.

Là encore, les perspectives d'évolution doivent être prises en compte, tant au niveau applicatif que de localisation, en retenant les facteurs les plus contraignant.

d. Le niveau de sécurisation

Après la couverture radio et le service, la réflexion doit prendre en compte les niveaux de sécurité souhaitables sur le réseau hertzien.

Le cloisonnement, recommandé entre Wi-Fi et Ethernet, implique une séparation logique (VLAN) voire physique, ainsi qu'un filtrage des trafics. Les points d'accès peuvent même être traités comme source d'entrée externe au Système d'Information, avec des contrôles d'accès renforcés par pare-feu, et la mise en place de zone démilitarisée (DMZ - *Demilitarized Zone*). Des sondes de détection d'intrusion (IDS - *Intrusion Detection Sytem*) peuvent être mises en œuvre, afin de remonter des alertes en cas d'attaque sur le réseau.

Si le service est destiné à des utilisateurs ayant des niveaux d'accès distincts au Système d'Informations, les niveaux d'authentification, et surtout de chiffrement peuvent être adaptés. Par exemple, la sécurité nécessaire n'est pas la même s'il s'agit de proposer un simple accès à Internet ou bien aux serveurs de l'entreprise. Ces moyens pourront également être complétés au niveau du filtrage, pour interdire l'accès à certains serveurs par des canaux peu sécurisés.

Sur le réseau lui-même, le choix est permis entre une sécurisation de niveau 2, utilisant les capacités de WPA ou WPA2, ou de niveau supérieur, avec un système VPN.

Trop souvent, la sécurité des postes utilisateurs est négligée, particulièrement dans le cas d'ordinateurs portables, voire de périphériques nomades. Pour ceux-ci, la sécurisation des stockages par chiffrement est encouragée. Elle pourrait être couplée avec un moyen d'authentification fort, pour l'accès logique au poste.

Enfin, l'intégrité physique des équipements doit être assurée par fixation anti-vol sur les supports. La tolérance de panne des points d'accès peut même être étudiée. Pour cela les bornes sont doublées, avec une première restant active et une deuxième qui prend le relais au besoin.

e. Le choix du matériel

Les équipements retenus sont certifiés pour les standards souhaités. De plus, ils doivent être conçus pour l'environnement d'entreprise, offrant ainsi des capacités plus appropriées que leur pendant pour la maison.

Si l'ensemble d'un bâtiment doit être couvert par le réseau Wi-Fi, il peut être intéressant de privilégier une architecture agrégée des points d'accès. Dans ce cas, des contrôleurs centralisent la gestion du RLAN, en ajoutant des fonctions complémentaires, qui ne sont pas concevables sur des bornes autonomes, telle que la détection de bornes pirates ou l'adaptation dynamique à l'environnement.

L'intérêt de fonctions ajoutées par les constructeurs, telles que la possibilité de constituer des VLAN radio, n'est pas à négliger.

Un pont de liaison entre deux réseaux peut être placé à l'extérieur. Si ce choix est retenu, non seulement le modèle doit être approprié, mais une alimentation électrique par PoE est préférable.

2. Organisation du réseau Wi-Fi

a. Le bilan radio

Le bilan de liaison radio est effectué à partir de la zone géographique à couvrir, déterminée précédemment. Son but est de définir les meilleurs emplacements des points d'accès et de leurs antennes, ainsi que les modèles de ces dernières.

Plusieurs méthodes peuvent être utilisées pour optimiser ce service.

Calcul du bilan radio

Fondamentalement, un bilan radio est le résultat de calculs prenant en compte le cheminement du signal entre l'émetteur et le récepteur.

Au sortir de l'antenne d'émission, le gain total est l'addition de celui du point d'accès et de l'antenne. À cette valeur doit être soustraite la perte occasionnée par un potentiel câble d'antenne : Gain d'émission [dBm] = gain d'émetteur-perte dans le câble + gain d'antenne.

Ce gain est affaibli en fonction de l'espace libre traversé. La formule de calcul tient compte de la distance ainsi que de la longueur d'onde l du signal : Perte de propagation [dB] = 20*log (4Π*distance /λ)

Par exemple, à 2.4 GHz, l'affaiblissement calculé est de :

- 60 dB sur 10 m ;
- 74 dB sur 50 m ;
- 80 dB sur 100 m ;
- 100 dB sur 1 000 m.

Le signal reçu a donc pour gain celui de l'émetteur auquel est retiré l'affaiblissement par la distance. À cette valeur est ajoutée le gain de l'antenne de réception, voire soustraite la perte du câble. Il est tenu compte de la sensibilité de l'interface de réception : Gain de réception [dBm] = gain d'antenne - perte dans le câble + sensibilité de récepteur.

Pour que le système soit opérationnel, l'addition du gain d'émission, de la perte de propagation et du gain de réception doit être supérieure à zéro. Une valeur de résultat donnant une marge d'environ 6 dBm est souhaitable pour espérer se rapprocher de la réalité.

Les caractéristiques techniques d'une interface client peuvent annoncer le rapport entre le débit et la sensibilité de réception, par exemple de -70 dBm pour 54 Mbps. Grâce au calcul, la distance entre le point d'accès et ce client peut être ajustée en conséquence, afin d'autoriser une telle bande passante.

La communication Wi-Fi nécessite le calcul du bilan radio dans les deux sens d'émission.

Malheureusement, la pratique, particulièrement en intérieur, s'éloigne de cette vision théorique de la communication radio. Ce calcul ne tient pas compte des contraintes de bâtiment, ni des interférences causées par d'autre réseaux Wi-Fi ou Bluetooth, voire de tout appareil utilisant la bande de fréquence 2.4 GHz. Ce bilan de liaison donne tout de même un ordre d'idée des portées de réseau Wi-Fi.

Débit (Mbps)	Portée (mètre)
54	10
48	17
36	25
24	30
18	40
12	50
9	60
6	70

Ordre d'idée des portées d'un réseau 802.11g en intérieur

Audit de site

Afin de rapprocher l'étude de bilan radio de la réalité, un audit de site (Site survey) est souvent préférable aux calculs précédents. Il peut être réalisé en situation ou par des outils de simulation.

Dans ce dernier cas, un logiciel de modélisation est utilisé, qui analysera complètement la cartographie du bâtiment et l'ensemble de ces caractéristiques, auparavant saisies. Souvent en trois dimensions, cette carte tient compte des obstacles, des matériaux de cloison et tout autre paramètre susceptible d'influer sur les cellules. Après cette configuration complète, les emplacements conseillés des points d'accès, donc également leur nombre, sont calculés. L'usage de tels logiciels est coûteux, et le résultat proposé devra généralement être validé en situation.

L'audit de site sur le terrain est réalisé grâce des outils d'analyse logiciels dédiés. Ils exploitent directement le signal radio, entre l'interface client d'un ordinateur ou d'un PDA, sur lequel ils sont installés, et le point d'accès.

Le logiciel gratuit NetStumbler (www.netstumbler.com), qui peut paraître limité pour un audit de site complet a déjà été cité. Les outils commerciaux tels que AirMagnet (www.airmagnet.com), WildPacket (www.wildpackets.com)... sont nombreux. Ils proposeront des fonctionnalités avancées, comme des transferts de données, pour tester les débits réels ou la détection d'interférences. De tels outils peuvent non seulement aider à mettre en œuvre un réseau complètement fonctionnel et répondant aux besoins exprimés, mais ils servent à faire évoluer celui-ci.

Les procédés de test peuvent être plus ou moins évolués en fonction du logiciel utilisé. Ainsi, il est possible avec certains de s'appuyer sur la cartographie du bâtiment, pour visualiser plus facilement les cellules à l'écran.

Pour que l'audit de site soit concluant, il est recommandé d'agir avec méthode. Une vue globale des secteurs qui doivent être couverts et une première idée des emplacements potentiels de points d'accès, ont été obtenues par la réflexion sur la couverture radio qui a précédée.

Comme le signal est transmis dans les trois dimensions, le test doit être réalisé en tenant compte de la hauteur à laquelle sera fixée la borne.

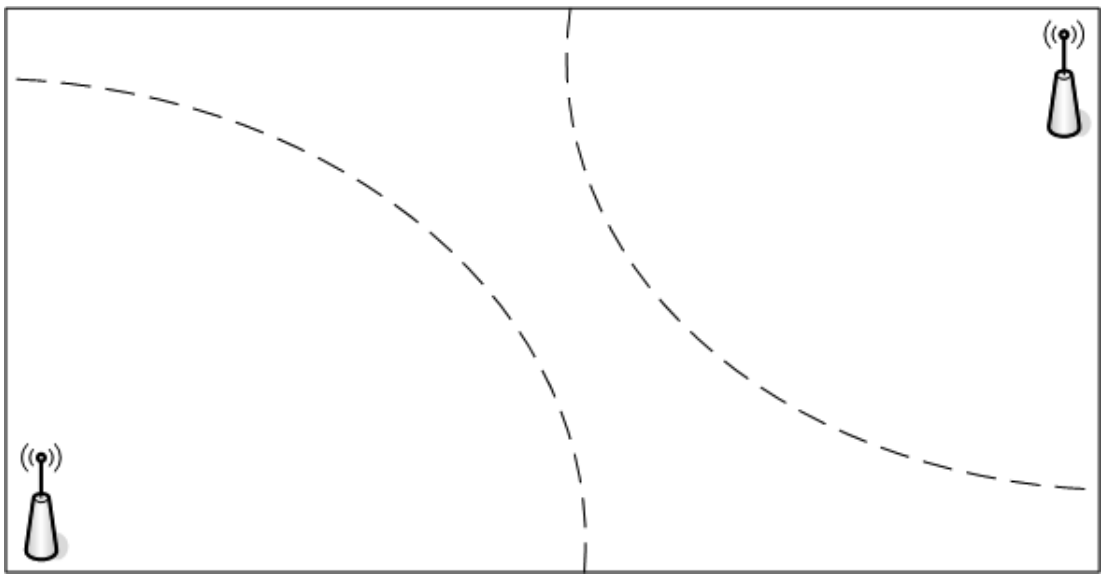
Il est recommandé, pour l'audit de site, de se munir d'un plan papier de la zone à couvrir afin de noter précisément les emplacements choisis. Si cela n'est pas possible, des rubans adhésifs de couleur marqueront les positions. Si une précision de positionnement est demandée, une roue de métrage peut être nécessaire.

Après avoir placé provisoirement l'équipement d'infrastructure, il ne reste plus qu'à mesurer la cellule réelle, en se déplaçant avec l'équipement portable sur lequel est installé le logiciel.

Non seulement l'aspect circulaire de la cellule est un idéal théorique, mais elle évolue dans le temps. Il est recommandé d'effectuer ces mesures, ou de les confirmer, dans une situation réelle, avec des être humains se déplaçant. En effet, ils peuvent influer de manière significative sur le signal, dans les conditions réelles d'utilisation.

Si la mesure n'est pas concluante, le point d'accès est déplacé, puis le nouveau positionnement testé. Ainsi, la disposition initiale est progressivement affinée.

Une autre méthode consiste à déposer d'abord les points d'accès dans les angles des pièces ou des bâtiments à couvrir. Ainsi, le périmètre sur lequel ils devraient être idéalement placés est délimité, avec une cellule atteignant ces coins. Les bornes sont ensuite repositionnées sur ce périmètre, pour peaufiner leur placement.



Exemple de test de positionnement à partir des angles

Dans certains cas, la prise de mesure peut nécessiter un changement de l'antenne des points d'accès, voire une diminution de leur puissance. Une mesure complète doit être prise à nouveau après chaque modification majeure de configuration.

Grâce à l'audit de site, la couverture radio prévue par l'étude est maintenant assurée.

Pilotage de réseaux agrégés

Si le choix s'est porté sur une architecture centralisée, pilotée par un élément commutateur propriétaire, l'audit de site peut ne pas être nécessaire.

Après avoir déployé au mieux les points d'accès, la configuration est affinée automatiquement par l'élément de gestion du réseau. Cette solution, coûteuse, permet une souplesse importante du réseau, qui peut évoluer plus facilement.

Par exemple, si la densité de population devient importante, un utilisateur peut automatiquement être associé à un autre point d'accès proche, moins chargé. Bien sûr, il est nécessaire que la cellule de ce dernier soit détectée.

b. Le placement des points d'accès multiples

Afin de finaliser les positions des points d'accès, quelques derniers critères restent à préciser.

Le réseau Wi-Fi est caractérisé par son nom de SSID, qui devra être configuré sur toutes les bornes. En fonction de l'agencement de celles-ci, leur canal sera à déterminer.

Un point d'accès est alimenté en courant et connecté au réseau filaire. Nous avons vu qu'Ethernet peut fournir l'alimentation électrique. Dans le cas où le réseau filaire est trop loin pour tendre un câble jusqu'à la borne, il est possible d'utiliser la technologie de courant porteur en ligne (CPL), voire un élément répéteur. La cellule de ce dernier devra inclure le point d'accès dont le signal est répété.

Densité des points d'accès

Avant de mettre en production les points d'accès, il peut être important de vérifier qu'ils sont bien capables de répondre à la demande, en terme de débit. Comme il est partagé entre les différents clients simultanés, la densité de placement des bornes doit être dépendante du débit total à offrir aux utilisateurs.

Ainsi, s'il s'avère qu'une cellule sert une vingtaine d'utilisateurs ayant chacun besoin de plusieurs mégabits par seconde de bande passante, une deuxième borne, proche et dont la cellule est recouvrante, sera positionnée, afin de privilégier une répartition de charge.

Problématique du roaming

Si une capacité d'itinérance sans perte de communication, ou roaming, a été prévue, la couverture réseau ne doit pas être interrompue. Un recouvrement des cellules de points d'accès doit être mis en œuvre.

Le recouvrement conseillé entre cellules est d'environ 20 %. Afin de rendre possible la réassociation avec le nouveau point d'accès, l'ancien doit pouvoir le joindre à travers le réseau filaire (DS - *Distribution System*), par une communication de type multicast.

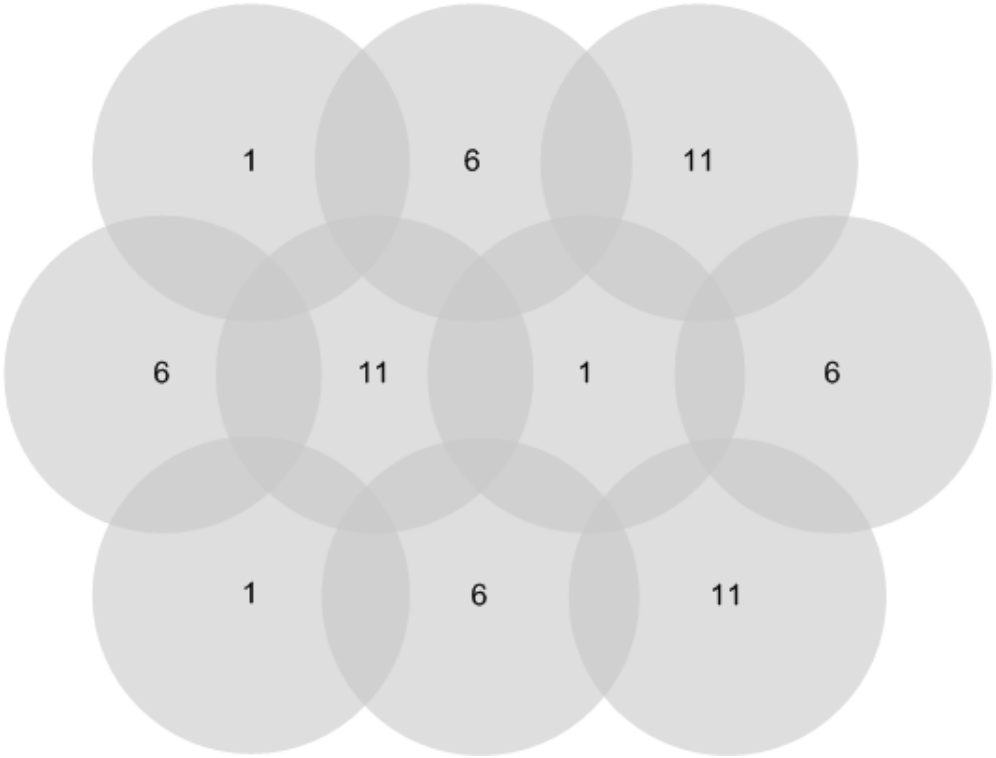
Une telle capacité sur le réseau Wi-Fi permet, par exemple, de continuer un transfert de fichier sans interruption de téléchargement. Si le réseau doit offrir un service de téléphonie sur IP sans fil, la capacité de roaming est indispensable.

Lorsque le poste de travail est client d'un serveur terminal, comme Citrix Presentation Server ou Microsoft Terminal Server, cette option peut éviter une perte de connexion brutale, gardant la session ouverte, si l'ordinateur est déplacé allumé.

Si l'authentification est déportée auprès d'un serveur RADIUS, le roaming est facilité, car cette vérification est indépendante du point d'accès.

Choix des canaux

Si cela est possible, les canaux fixés sur les points d'accès sont choisis judicieusement. Par exemple en 2.4 GHz parmi ceux 1, 6 et 11, afin d'éviter toute interférence. La dimension verticale entre étages ne doit pas être oubliée.



Exemple de choix de canaux sur des cellules recouvrantes

Comme l'espacement standard des canaux DSSS limite à trois le nombre de cellules recouvrantes sans interférence, cette situation idéale est parfois impossible. Dans ce cas, les écarts doivent être ajustés au mieux pour réduire le problème. En France, quatre cellules recouvrantes peuvent utiliser les canaux 1, 5, 9 et 13, en limitant la contrainte.

Dans le cas de ponts émettant en extérieur, les canaux 8 à 13 ne peuvent émettre légalement à plus de 10 mW. Si le PIRE est supérieur, les fréquences sont fixées dans la plage basse.

L'adoption de la bande des 5 GHz, par exemple en 802.11n draft, simplifie grandement cette problématique. En effet, le nombre de canaux non chevauchant est beaucoup plus important. De plus, l'adoption du choix de canal automatique DFS (*Dynamic Frequency Selection*) du 802.11h simplifie encore la mise en œuvre.

c. Les configurations complémentaires

Enfin, après s'être consacré à la partie radio du réseau, des besoins plus informatiques peuvent être abordés.

S'il est prévu que les points d'accès distribuent dynamiquement aux clients les adresses logiques IP, les plages sont à choisir. Si la fonctionnalité de serveur DHCP est assurée par les points d'accès eux-mêmes, la répartition doit être également pensée.

S'il a été décidé que les points d'accès servent plusieurs réseaux Wi-Fi distincts, à travers des VLAN, les noms et caractéristiques de ceux-ci sont à finaliser.

En fonction de l'étude initiale et des décisions prises, l'interconnexion avec le réseau filaire peut être réalisée et sécurisée. Au besoin, les systèmes de détection d'attaque, d'administration et de supervision sont configurés.

Lorsque toutes les configurations annexes ont été effectuées, il ne reste plus qu'à réaliser le paramétrage logiciel des points d'accès et des ordinateurs clients.

Configuration d’un point d’accès

En conclusion de cet ouvrage, nous pouvons donc résumer ce que peut être la configuration de points d’accès, puis de stations clientes. Nous considérons que tous les éléments clés sont connus et que les études exposées précédemment ont été effectuées.

Les copies d’écran présentées ci-dessous le sont pour exemple, mais les recommandations de configuration seront le plus générales possible. Une bonne prise en main du matériel avant sa mise en production est toujours préférable. En effet, chaque modèle possède ses spécificités, qui peuvent influencer de manière conséquente les paramétrages.

La centralisation de la configuration ne sera pas abordée ici. Les matériels points d’accès servant de modèles dans la suite sont de deux familles distinctes. Le premier est plutôt destiné à la maison, voire aux toutes petites entreprises. Il est de marque Linksys et son système d’exploitation est basé sur un noyau Linux. Le second cible les professionnels et peut être mis en œuvre sur des réseaux conséquents. De marque Cisco, il est piloté par une version spécifique du système propriétaire de cette marque, nommée IOS.

1. Préparation

a. Le paramétrage de base

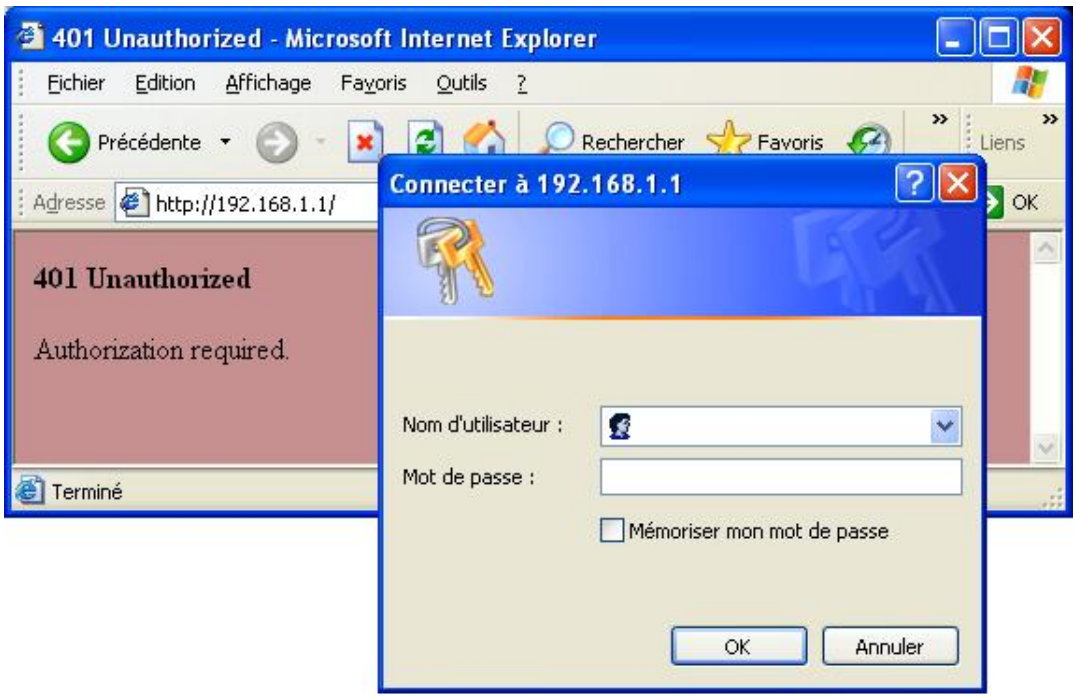
Configuration par défaut

Après branchement électrique du point d’accès, il devient opérationnel plus ou moins rapidement, le temps que son système d’exploitation se charge. Avant tout, il est nécessaire de joindre son interface de configuration. Les bornes possèdent des paramètres par défaut, configurés en usine, comme par exemple :

- les paramètres de connexion et de mot de passe du compte d’administration ;
- le nom du SSID ;
- la configuration d’adressage IP ;
- le canal radio...

Une note, voire un fascicule, fournie avec l’équipement, renseigne sur ces éléments. Ils permettent, tout d’abord, de joindre l’interface d’administration. La configuration a lieu généralement à partir d’un navigateur Internet.

Il est parfaitement possible de configurer un point d’accès par l’intermédiaire de son interface radio. Ceci n’est pas recommandé, puisque beaucoup de configurations réinitialiseront celle-ci et une reconnexion sera nécessaire. L’administration par le réseau filaire est donc préférable.

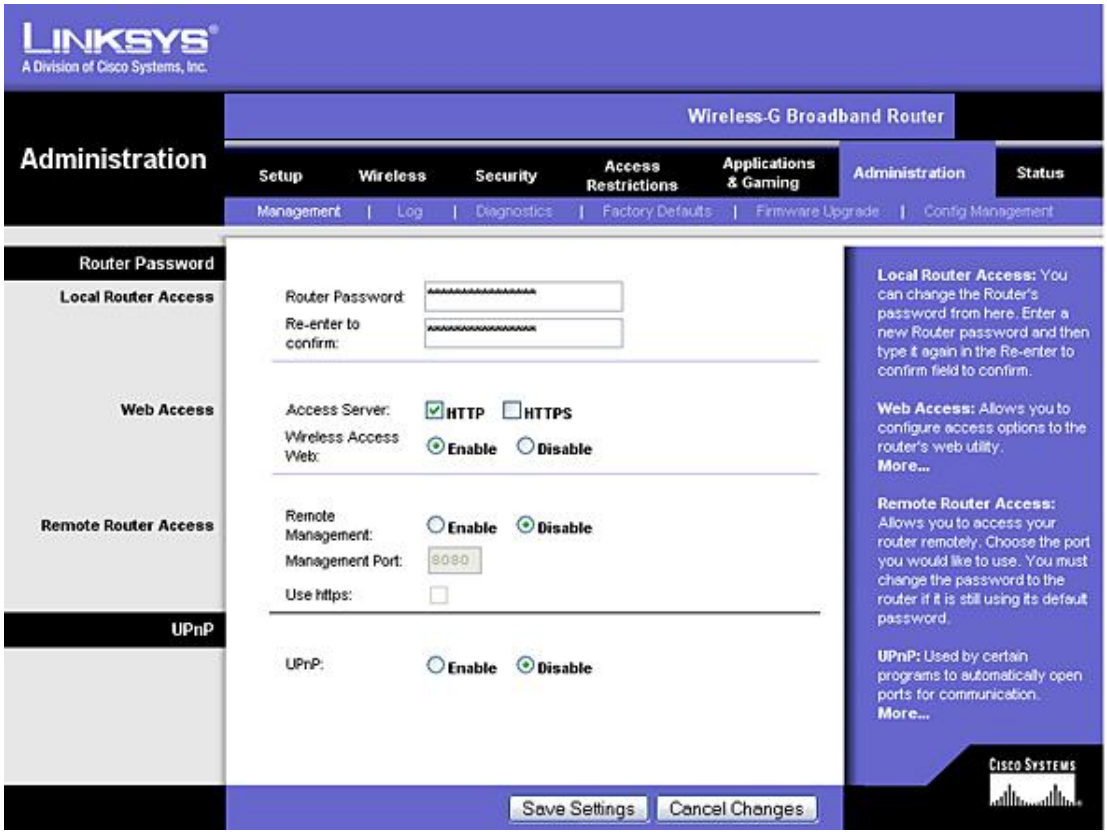


Connexion à un point d'accès de marque Linksys, sur l'adresse IPpar défaut 192.168.1.1

Compte d'administration

Avant toute autre chose, il est recommandé de changer les paramètres de compte d'administration du point d'accès. En fonction des capacités de celui-ci, plusieurs choix sont possibles :

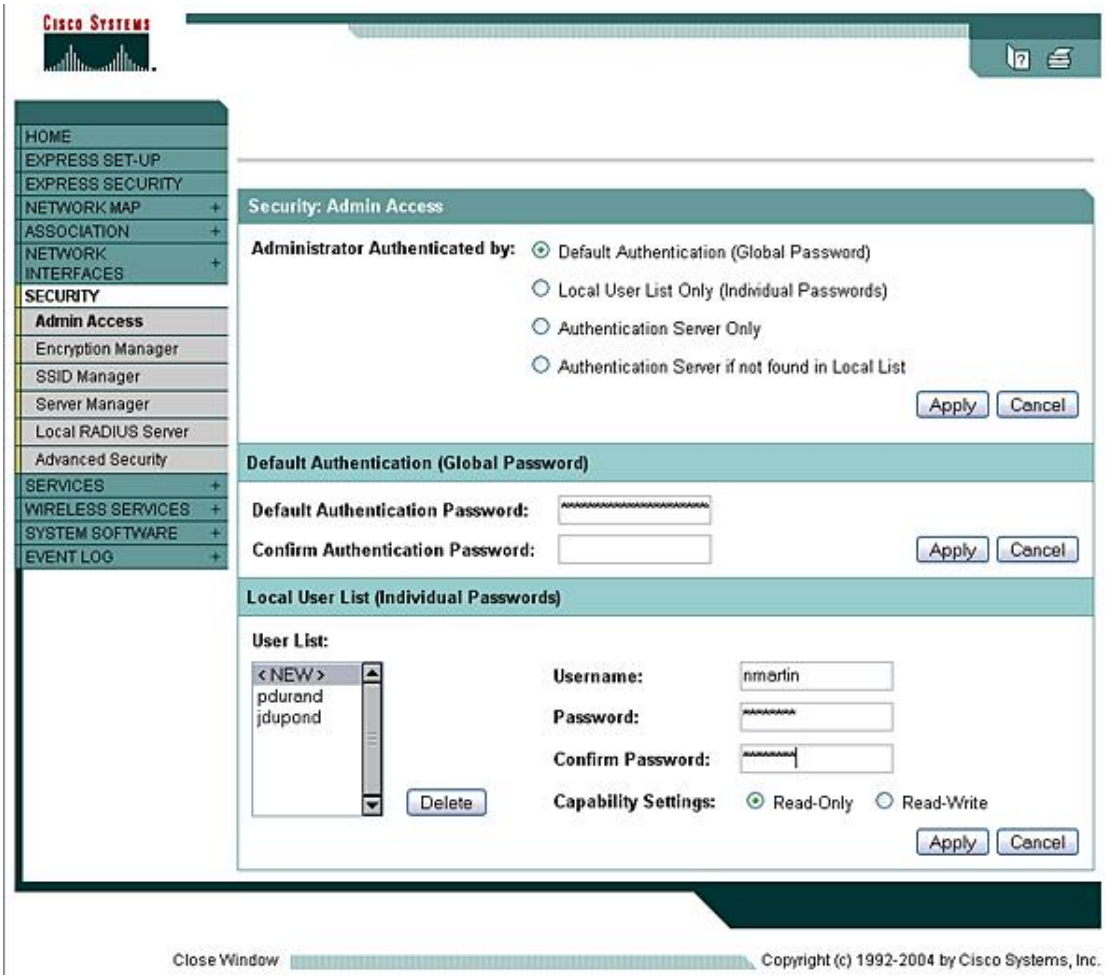
- un simple changement de mot de passe du compte intégré ;
- la modification complète du compte dans la base de la borne ;
- l'utilisation de comptes déportés sur un serveur de comptes.



Page de changement du mot de passe administrateur, point d'accès Linksys

Dans le cas de bornes évoluées, plusieurs administrateurs peuvent disposer de leur propre compte, avec des niveaux d'accès différents. Il va sans dire que cette solution est plus sécurisée.

Il faut considérer que, moins il y a d'informations sur le point d'accès, meilleure est la sécurité. Si le niveau d'authentification choisi dans l'étude retient l'usage d'un serveur RADIUS, certains modèles de bornes permettent la gestion des comptes d'administration à partir de celui-ci.

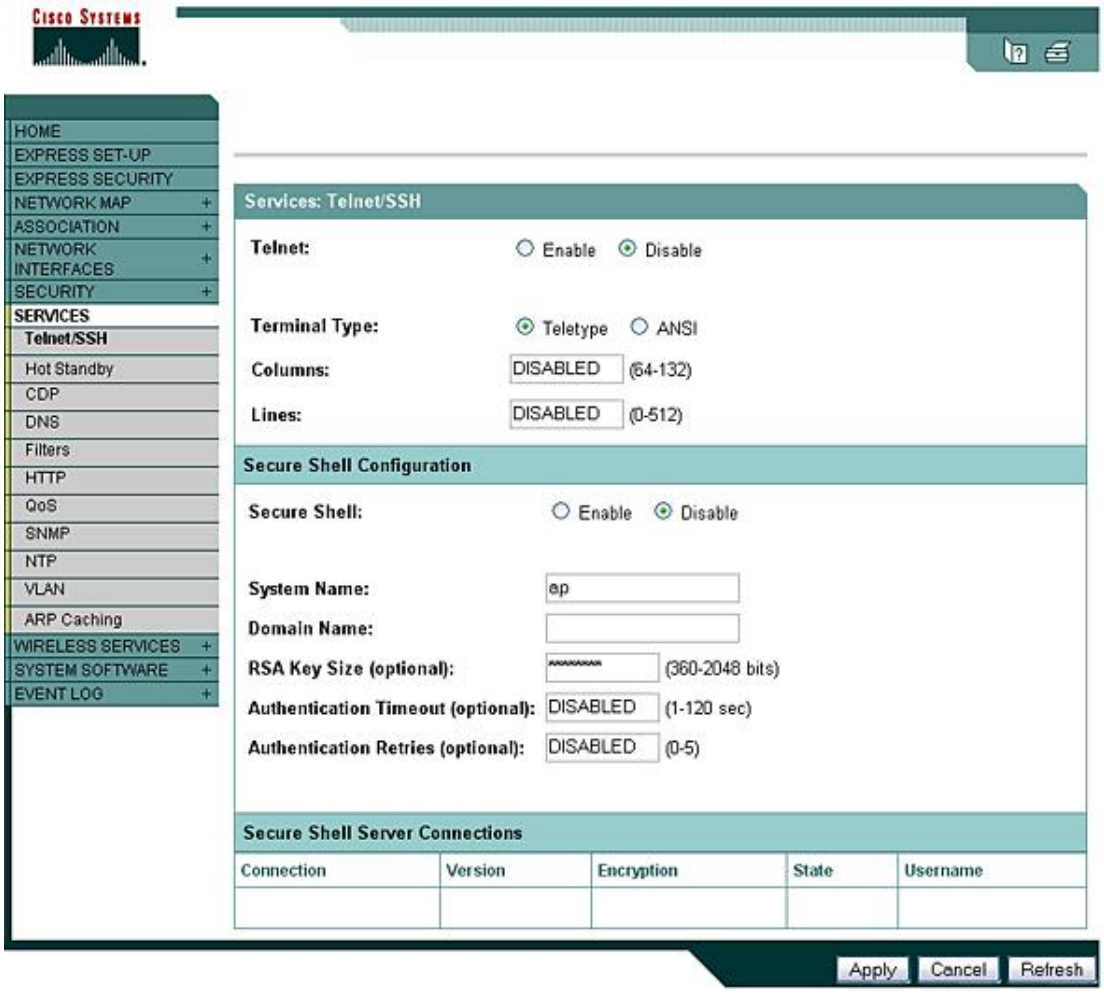


Page de gestion des comptes d'administration sur un point d'accès de marque Cisco

Environnements d'administration

Très souvent, l'interface Web n'est pas la seule disponible pour interagir avec le point d'accès. Si elle est utilisée, la communication peut être sécurisée par un chiffrement Secure Socket Layer (SSL) et le protocole Hyper Text Transfer Protocol over TLS (HTTPS).

L'usage d'interfaces alternatives est possible, par Telnet, Secure Shell Configuration (SSH) ou autres. Certaines bornes autorisent des remontées d'informations par le protocole standard Simple Network Management Protocol (SNMP).

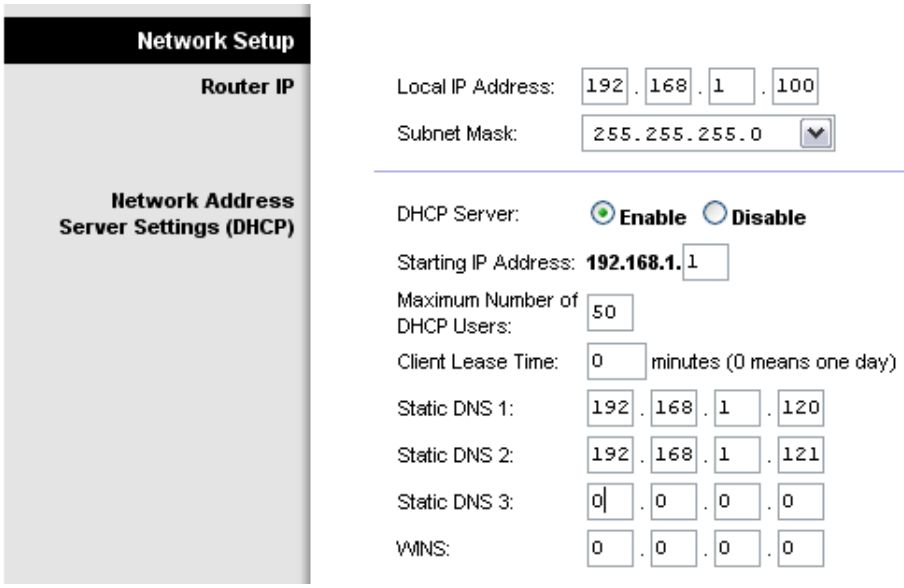


Configuration des interfaces d'administration SSH, Telnet

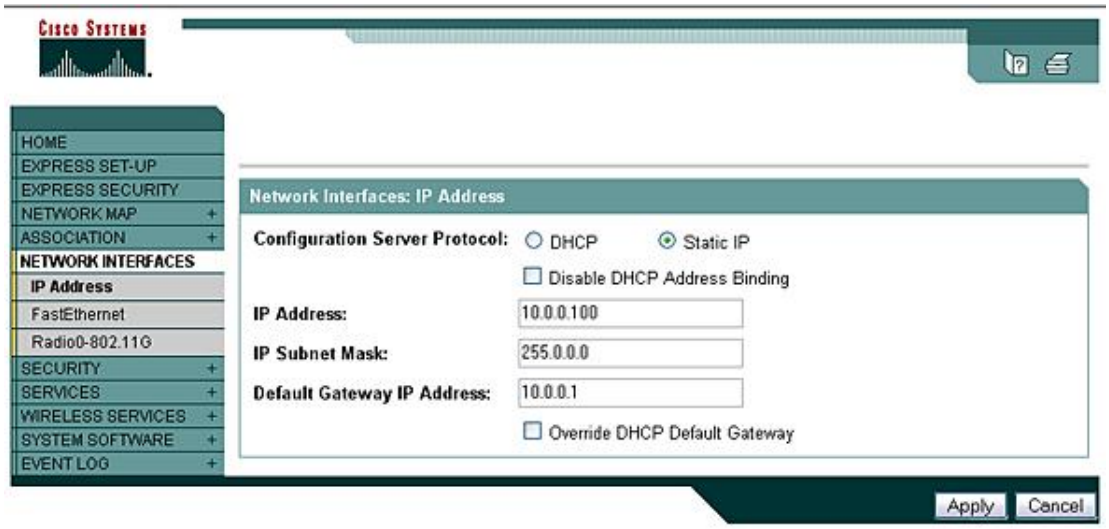
De manière générale, si un environnement d'administration n'est pas exploité, il doit être désactivé.

Adressage IP

Une fois que la sécurité d'administration du point d'accès est en place, les paramètres IP de celui-ci peuvent être modifiés. Certains acceptent de recevoir une adresse IP automatiquement, ce qui n'est pas recommandé dans une gestion décentralisée. Si la borne possède elle-même des capacités de serveur Dynamic Host Configuration Protocol (DHCP), les stations pourront recevoir automatiquement l'adresse de leur interface Wi-Fi.



La configuration des interfaces réseaux de point d'accès est très variable d'un modèle à l'autre. Parfois, les interfaces Wi-Fi et Ethernet peuvent être configurées indépendamment, chacune possédant sa propre adresse IP. Des fonctionnalités plus ou moins avancées de traduction d'adresse (NAT - *Network Address Translation*) ou de routage sont parfois disponibles.



Configuration des paramètres IP du point d'accès Cisco

Comme tout équipement adressable sur le réseau IP, un point d'accès possède un nom. Il peut être intégré dans un domaine de type Domain Name Service (DNS) et déclaré sur un service DNS.

Comme pour un serveur, la notification d'un nom facile à retenir pour chaque point d'accès est encouragée.

b. Les paramètres radio

SSID et sa diffusion

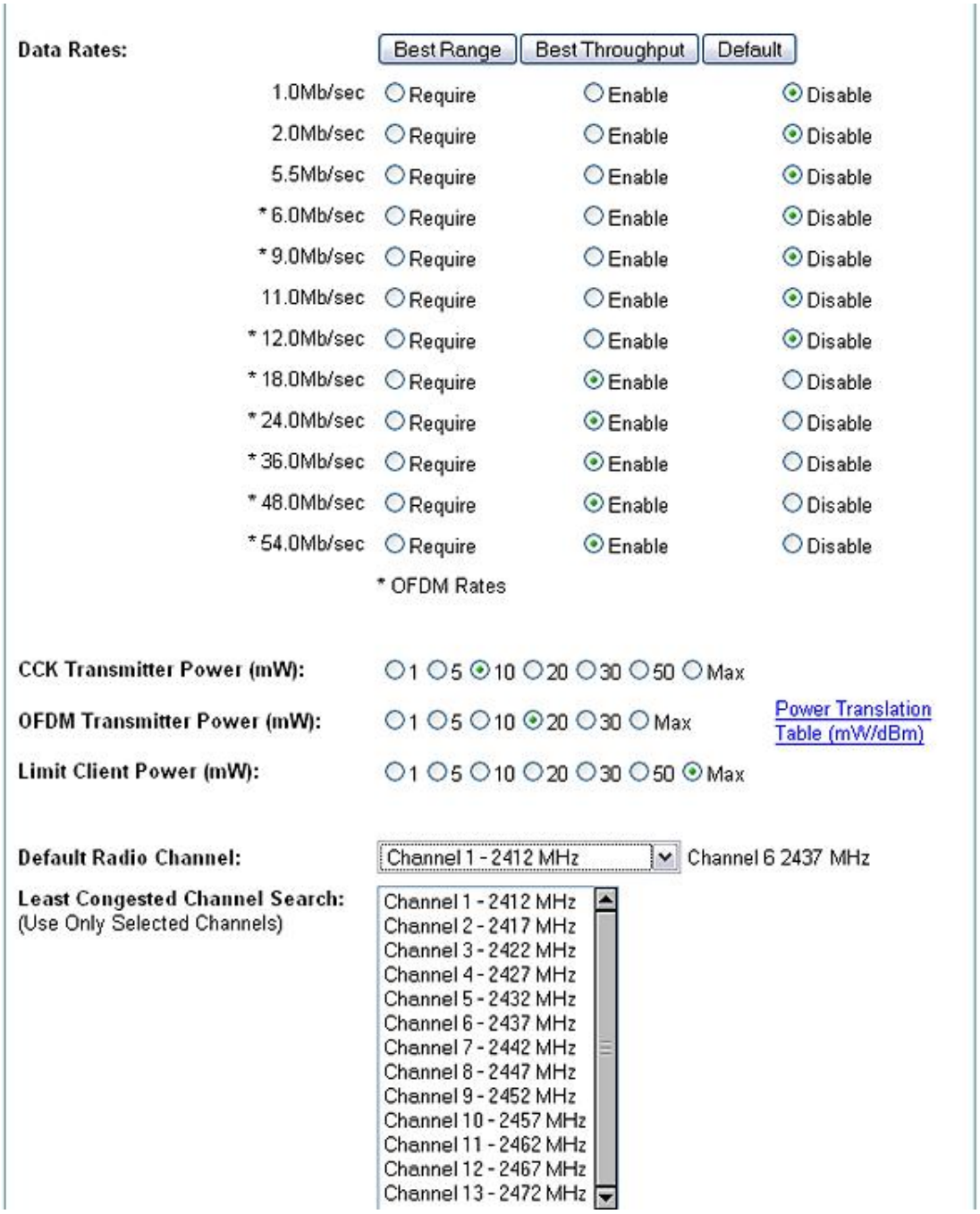
Le changement de Service Set IDentifier (SSID), nom du réseau, peut ensuite être effectué, afin de ne plus utiliser celui par défaut. Cette modification peut être l'occasion de désactiver la diffusion (broadcast) dudit SSID, à moins de vouloir rendre un service de type Hot-Spot.

Exemple de configuration simple des paramètres radio

Canal, débit et puissance

Le canal à utiliser peut être fixé dès ce moment en fonction du choix résultant de l'étude précédente.

Si le point d'accès l'autorise, le choix précis des débits possibles, ainsi que la diminution de la puissance permettent d'affiner le réglage.

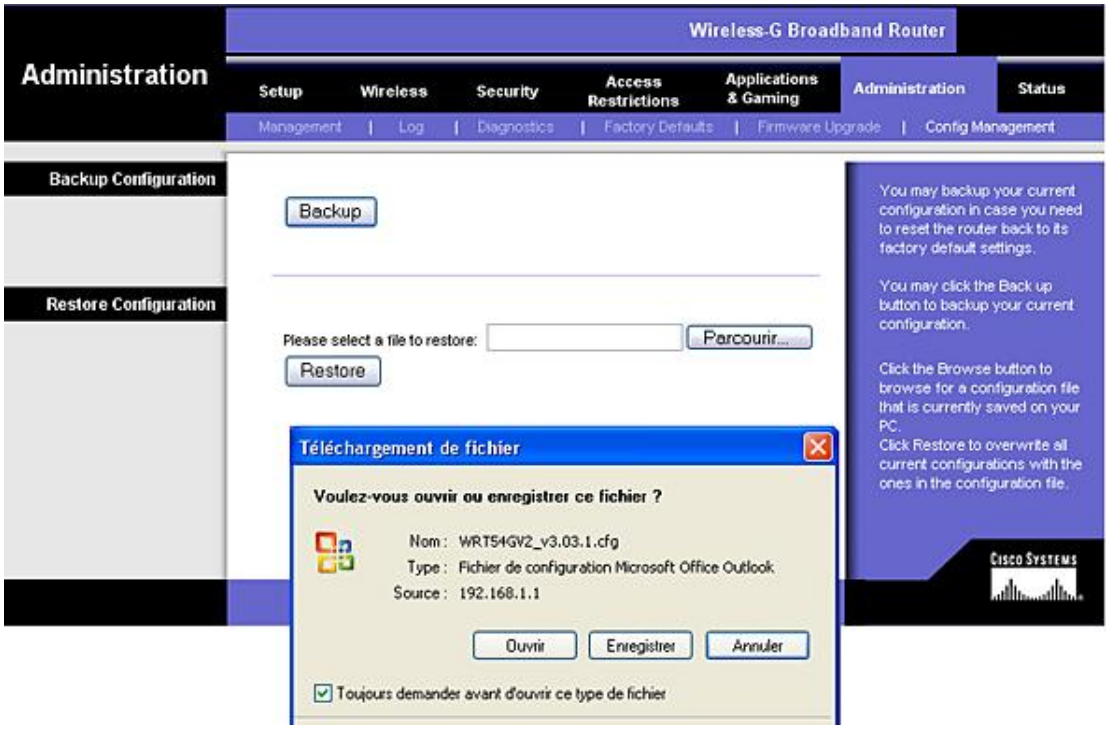


Exemple de configuration affinée des paramètres radio

Fixer ces derniers paramètres permet de disposer d'un point d'accès opérationnel, même si aucune sécurisation n'a été mise en œuvre.

c. La sauvegarde de configuration

Après toute modification de la configuration d'un point d'accès, la sauvegarde de celle-ci est recommandée. Elle permet, en cas de fausse manipulation ou de réinitialisation, de remettre rapidement la borne en opération, par restauration.



Sauvegarde de configuration, comme fichier ".cfg"

En cas de problème majeur sur un point d'accès, une réinitialisation complète en configuration usine peut être possible. Elle peut être effectuée matériellement ou bien logiciellement.

Page de sauvegarde et de réinitialisation (Reset)

La mise à jour du système d'exploitation de la borne est une opération qui peut résoudre certains problèmes, y compris de sécurité.

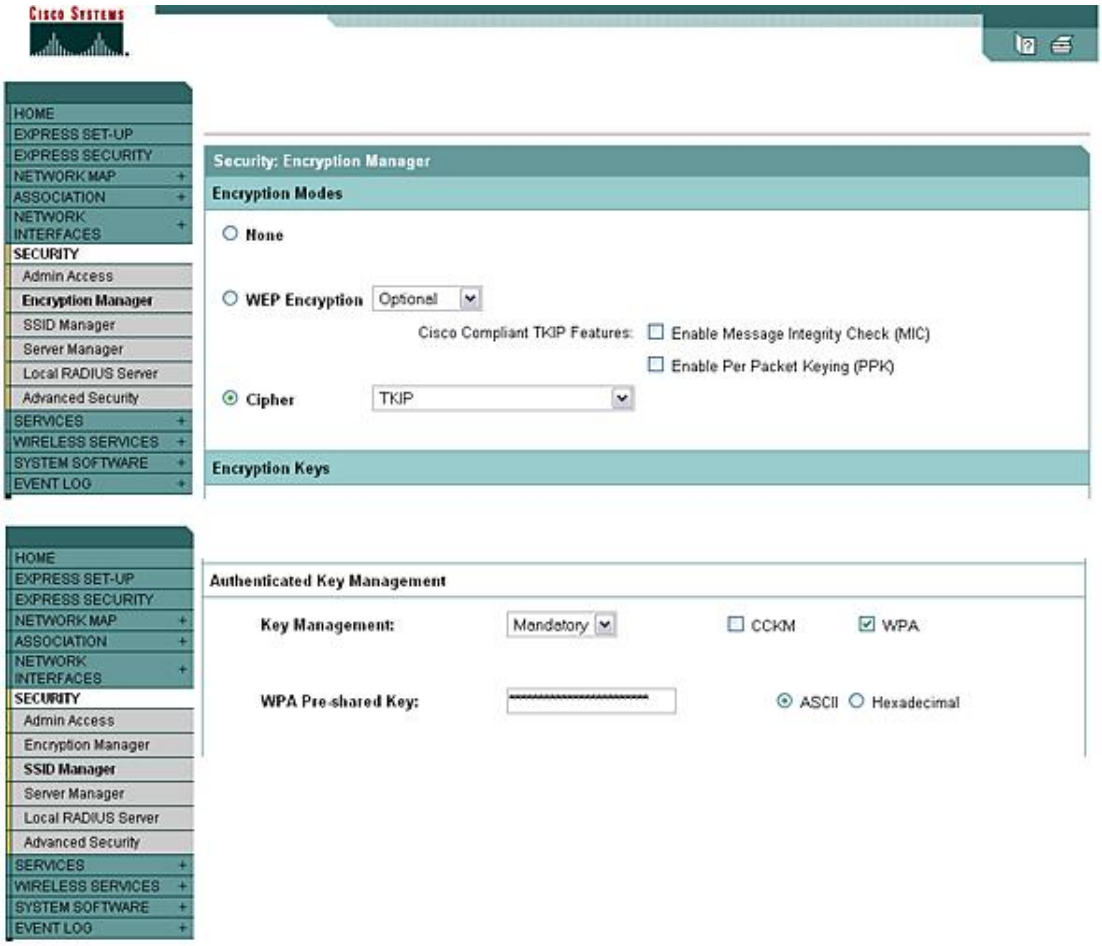
Page de mise à jour du système (Firmware)

2. Sécurisation

Certains des paramétrages basiques réalisés précédemment, comme la modification du compte administrateur ou la désactivation d'interfaces non utilisées ont renforcé la sécurité du point d'accès lui-même.

L'attachement physique du point d'accès sur son support est une solution à considérer contre le vol. En effet, les impératifs radio ne permettent pas toujours de le positionner dans un lieu sécurisé. Des systèmes utilisant des écrous anti-vol, des cadenas ou des câbles de type Kensington sont parfois utilisables.

Les méthodes de chiffrement et d'authentification ont normalement été fixées auparavant, en adéquation avec les capacités des points d'accès.



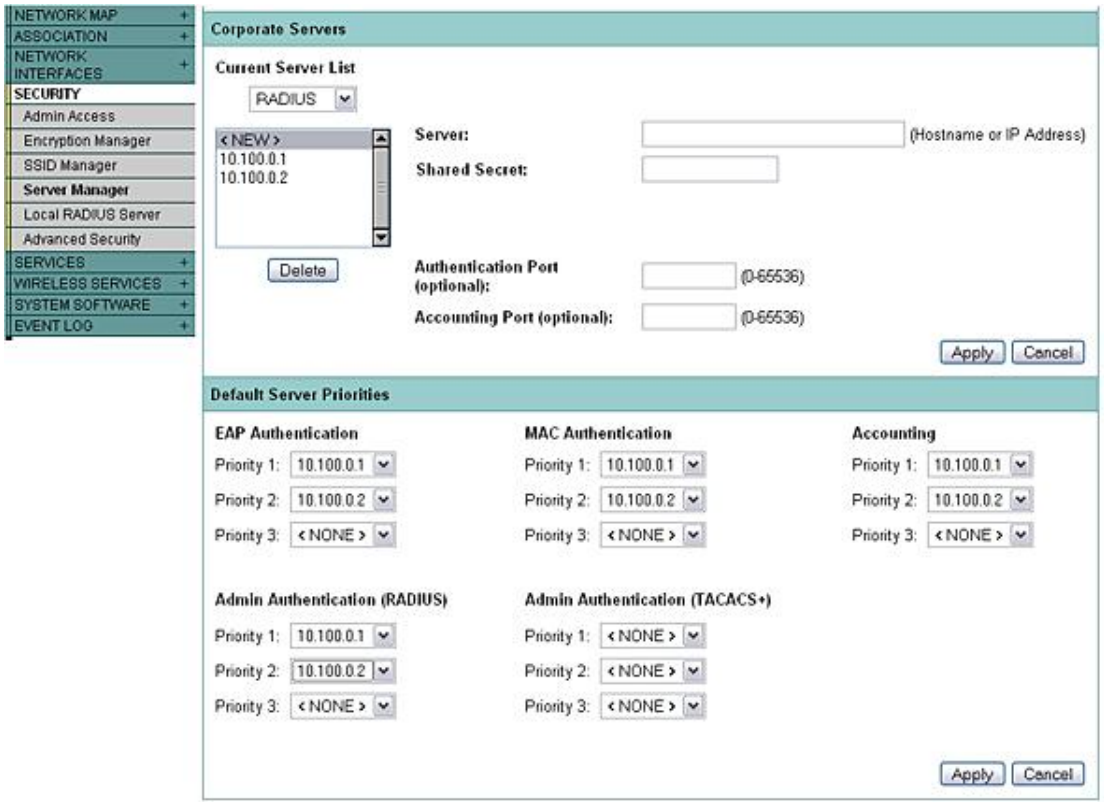
Les deux pages de configuration pour WPA-PSK, sur un point d'accès Cisco

La configuration d'une des méthodes basées sur une clé partagée (PSK - *Pre Shared Key*) reste généralement simple.

Si l'authentification RADIUS est souhaitée, les coordonnées du serveur ainsi que la clé partagée sont au moins à préciser.

Exemple de configuration de la partie client RADIUS

Sur certaines bornes, comme celle Cisco dans nos exemples, la méthode d'authentification RADIUS peut également être appliquée pour l'authentification des adresses MAC.



Différentes utilisations d'un serveur RADIUS à partir d'une borne

Ensuite, selon les modèles, d'autres protections complémentaires peuvent être mises en place, telles que des restrictions d'accès en fonction de paramètres horaires, des exigences de ré-authentification en fonction d'intervalles choisis... Souvent, des moyens de filtrage des communications plus ou moins fins sont possibles.

3. Paramétrage avancé

a. L'affinage des configurations radio

Conformément aux spécifications 802.11, d'autres choix permettent d'optimiser le fonctionnement de son réseau Wi-Fi. La diminution du seuil de fragmentation (Fragmentation threshold) peut être judicieuse dans des environnements très perturbés.

L'activation des préambules courts (*Short preamble*) permet de gagner de la bande passante. La non utilisation du système RTS/CTS peut être demandée, à travers le paramètre de seuil RTS (*RTS threshold*). D'autres paramètres dépendent directement, là encore, du modèle exploité.

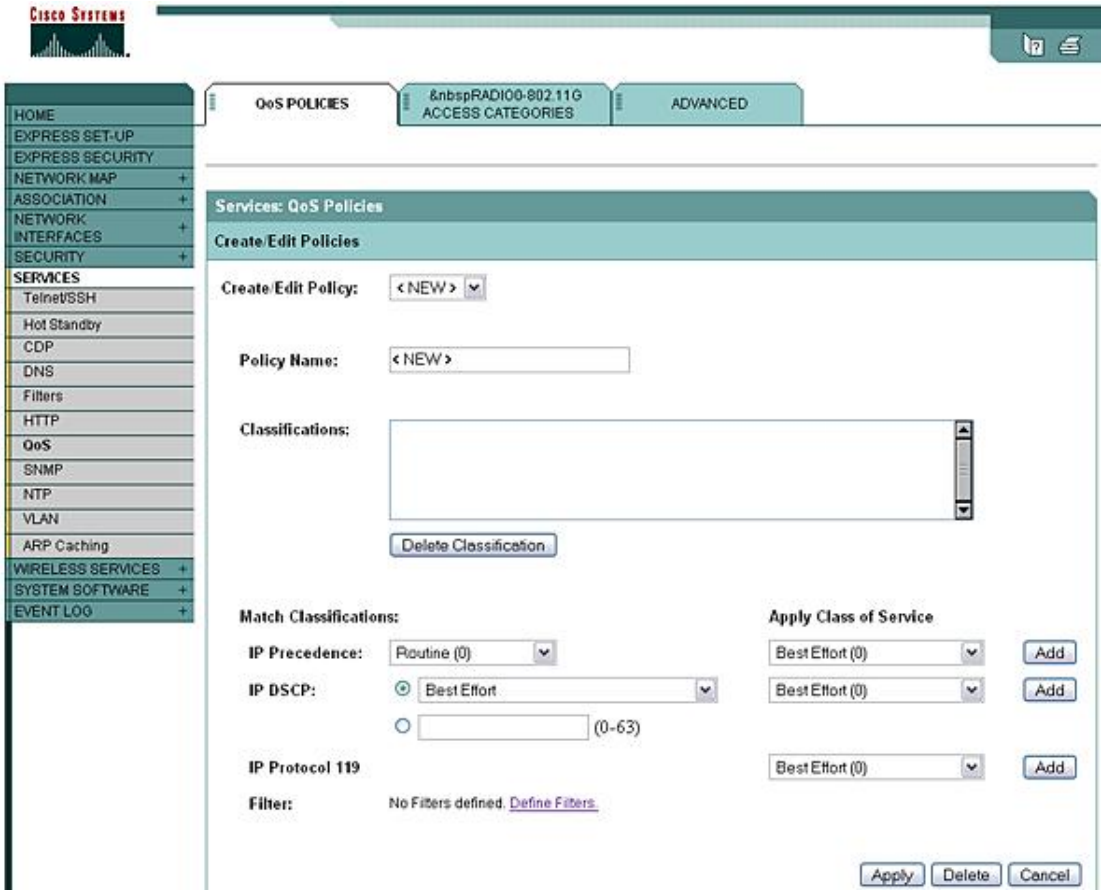
Exemple de paramétrages radio avancés

b. Les options spécifiques

Un point d'accès, professionnel particulièrement, proposera d'autres capacités qui lui sont propres. La possibilité de réaliser des réseaux virtuels (VLAN) radio permet de différencier les niveaux de service et de sécurité offerts par une même infrastructure matérielle. Ainsi, un même point d'accès pourrait servir une configuration de type Hot-spot et une autre privatisée, à travers deux VLAN associés chacun à un SSID.

La possibilité de configuration de statistiques d'exploitation et de journalisation est un point à considérer dès l'achat.

Configurer une qualité de service (QoS - *Quality of Service*) en fonction des types de flux, tels que les données ou la vidéo, peut être une option intéressante.



Page de configuration de QoS, sur point d'accès Cisco

Configuration d'ordinateurs clients

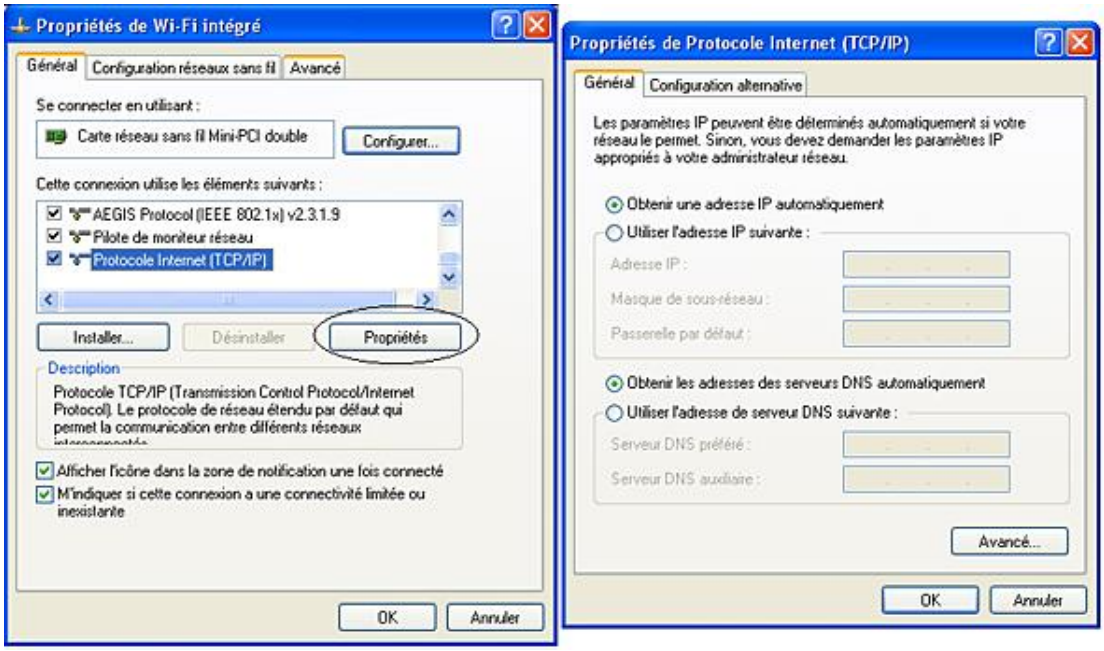
Avant l'achat d'une carte, il est recommandé de vérifier si un pilote compatible avec le système d'exploitation utilisé est disponible (Windows, Linux, MAC OS). De même, les matériels clients et pilotes devront être compatibles avec la méthode de chiffrement choisie.

Les configurations peuvent être prises en charge par l'interface logicielle du constructeur ou par le système d'exploitation.

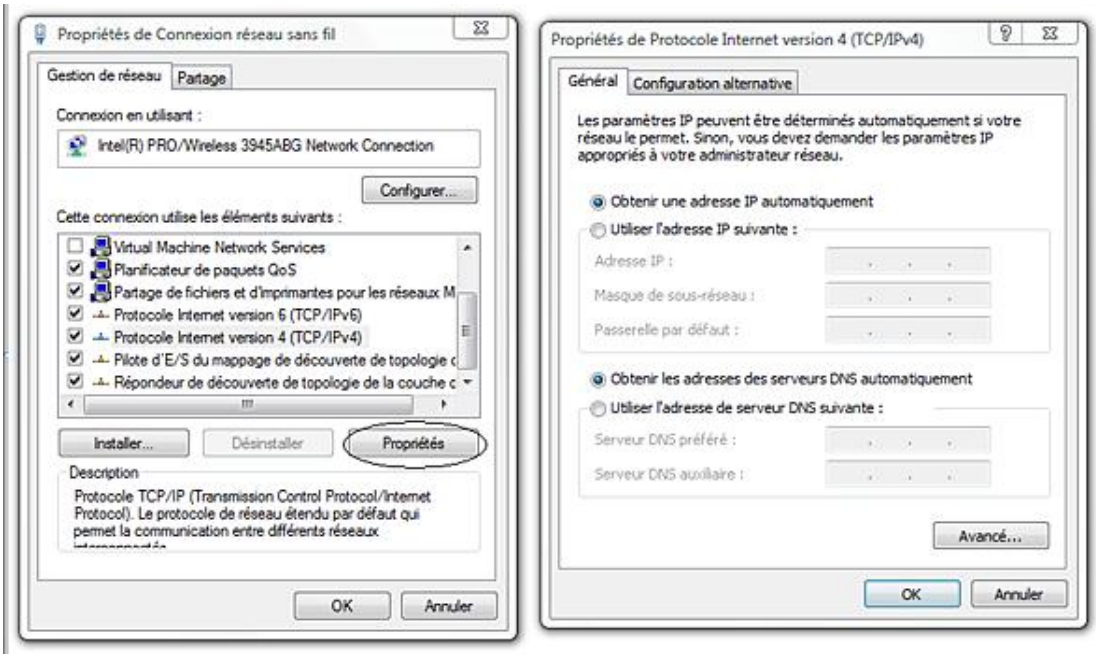
1. Paramétrage de base

a. Les généralités

Une interface réseau Wi-Fi se configure tout d'abord comme une interface Ethernet, en indiquant les paramètres du réseau IP.



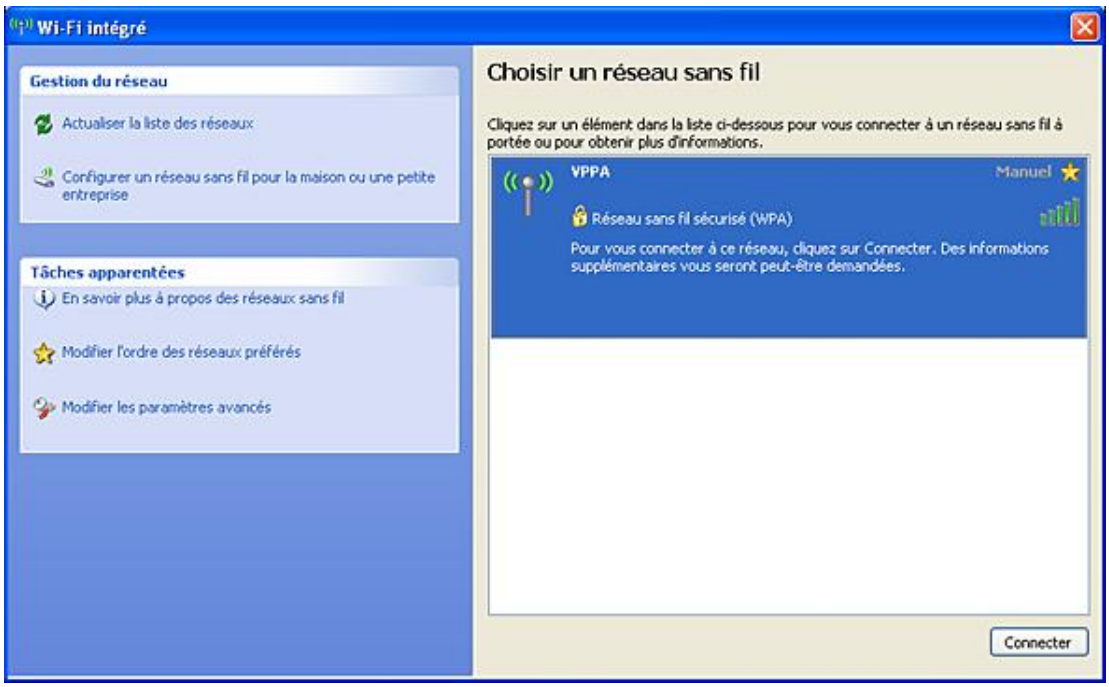
Propriétés IP sous MS Windows XP SP2



Propriétés IP sous MS Windows Vista

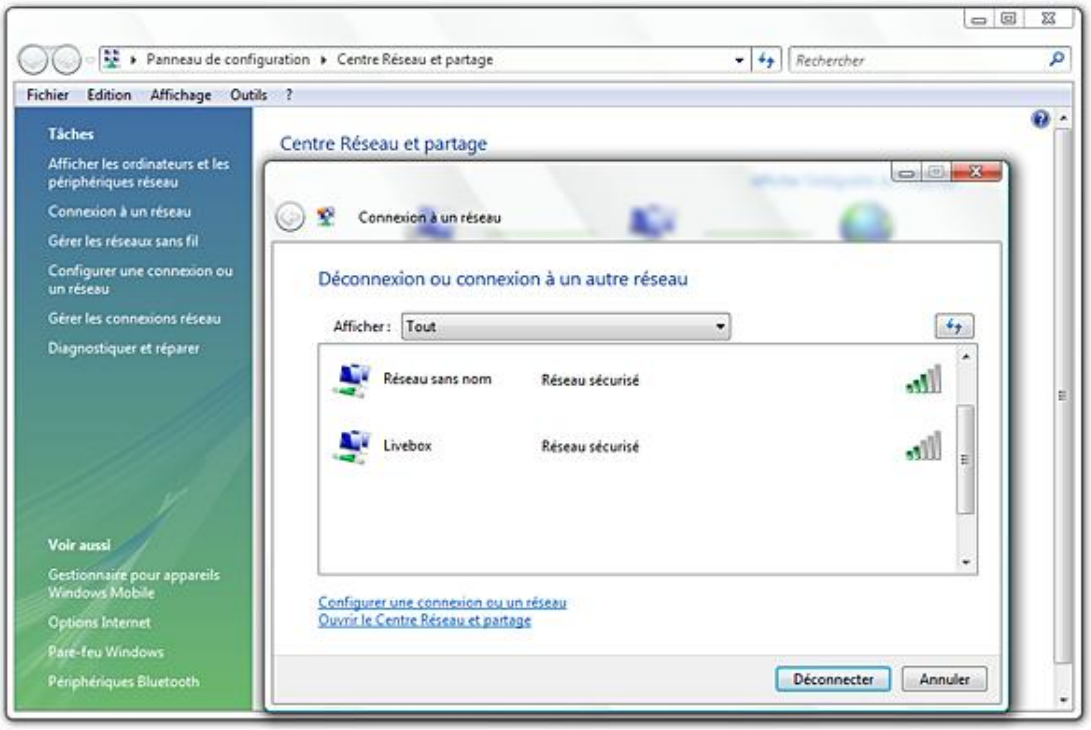
Si les capacités de MS Windows XP SP2 ont été retenues pour configurer le réseau sans fil, une fenêtre de choix de connexion à ceux détectés est disponible. Elle peut être appelée :

- à partir des propriétés de la carte réseau Wi-Fi, dans l'onglet **Configuration réseaux sans fil**, bouton **Afficher les réseaux sans fil** ;
- à partir de l'icône d'état de l'interface Wi-Fi, dans la barre de notification, à côté de l'heure.



Détection de réseaux sans fil MS Windows XP SP2

Dans MS Windows Vista la configuration est effectuée à partir du **Centre Réseau et partage**, accessible depuis le **Panneau de configuration** ou de l'icône de l'interface Wi-Fi de la barre de notification. Il est nécessaire ensuite d'appeler "**Connexion à un réseau**".

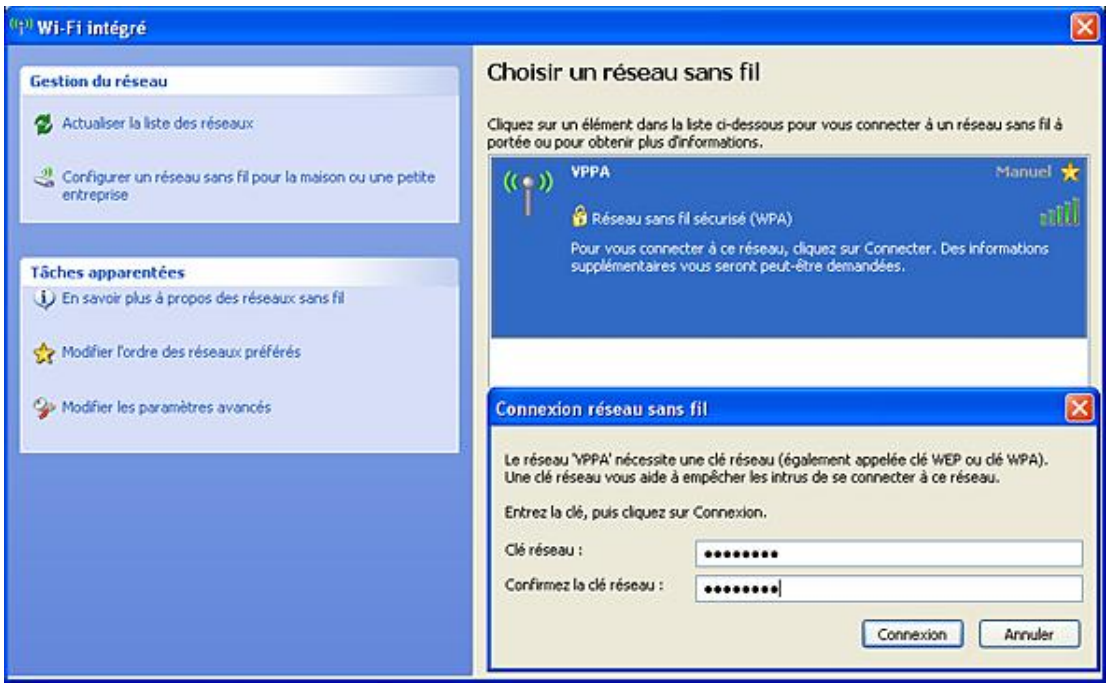


Détection de réseaux sans fil MS Windows XP Vista

Cette détection de réseau sans fil n'est possible que si l'identifiant de réseau SSID est reconnu par le poste de travail.

b. L'association automatique

Si la station a détecté le réseau, un double clic sur l'élément suffit à déclencher la demande d'association. Si des paramètres complémentaires sont à saisir, tels qu'une clé de chiffrement, ils pourront l'être à partir d'une boîte de dialogue proposée.



Connexion au réseau sans fil reconnue

Pour que l'association automatique puisse être réalisée, le SSID doit être reconnu par le poste de travail.

Dans le scénario le plus simple, de type Hot-spot, le point d'accès diffuse son SSID. Il peut même distribuer

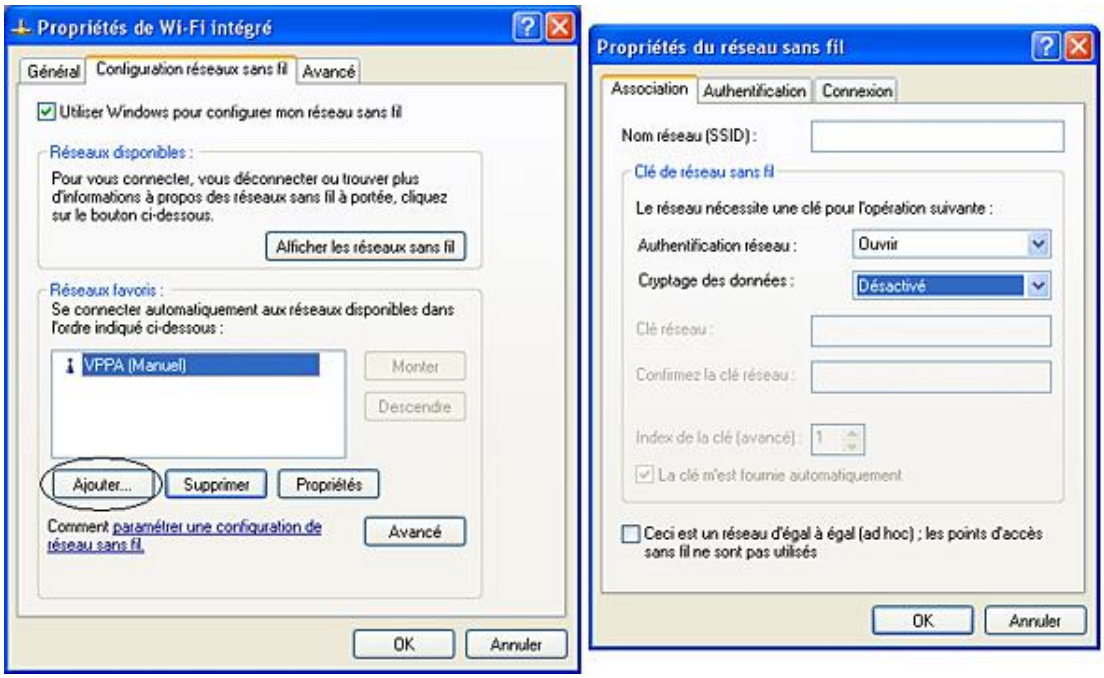
l'ensemble des paramètres IP permettant une mise en œuvre complètement automatisée de la communication, sans sécurisation. L'avantage du Wi-Fi, dans ce cas, est de permettre de se passer de configuration côté client.

Dans une application en entreprise, le SSID n'est normalement pas communiqué par le point d'accès. Le poste de travail doit donc le connaître d'avance. Dans ce cas, la station a été pré-configurée avec les paramètres du réseau.

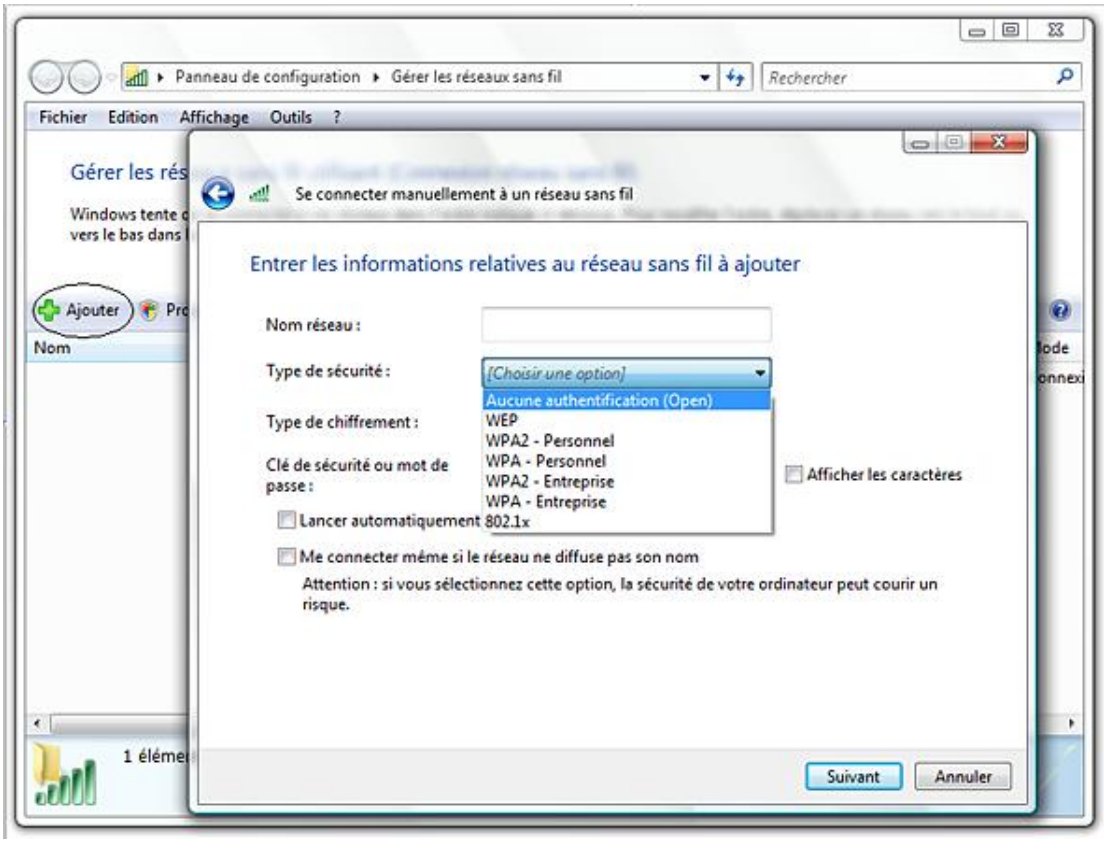
c. L'association manuelle

Quel que soit le logiciel de configuration de l'interface radio utilisé, Windows ou dépendant du constructeur de la carte, il est possible d'ajouter manuellement des caractéristiques réseaux, pour s'y associer.

Dans Windows XP SP2, cette création s'effectue à partir des propriétés de la carte réseau, onglet **Configuration réseaux sans fil**. Dans Windows Vista, cette configuration est possible à partir du **Centre Réseau et partage**, menu **Gérer les réseaux sans fil**.



Ajout d'un nouveau réseau sans fil avec MS Windows XP SP2

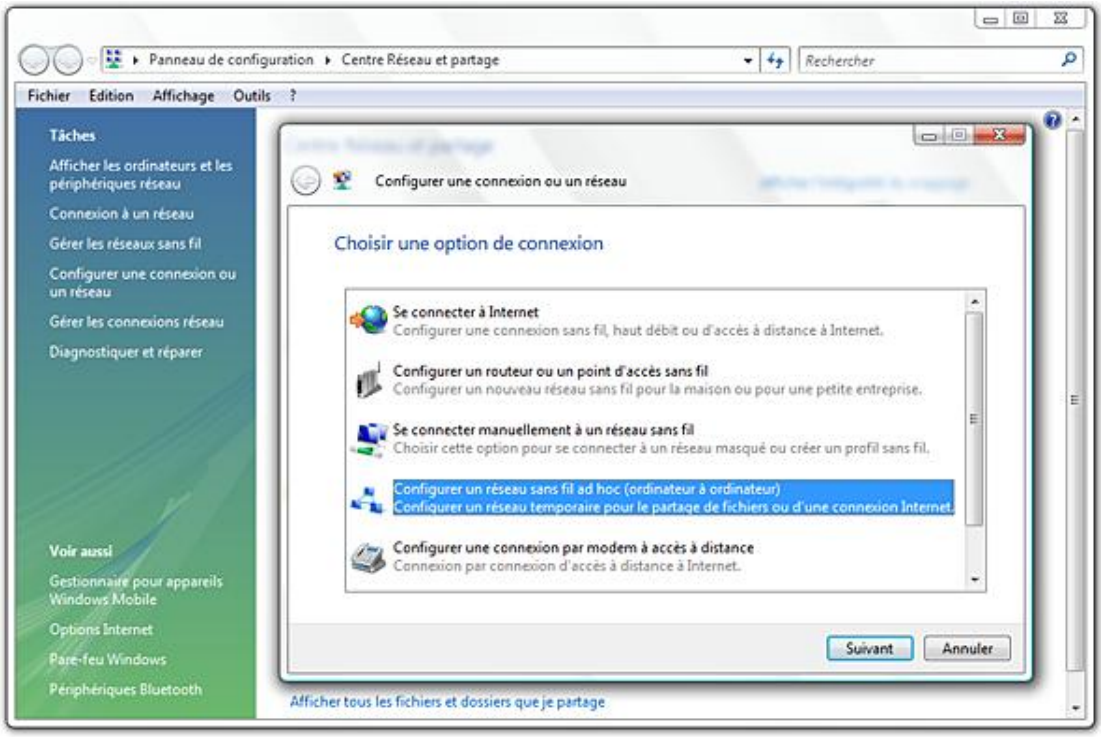


Ajout d'un nouveau réseau sans fil avec MS Windows Vista

Les paramètres à saisir concernent au moins le nom réseau SSID, le mode d'authentification et les paramètres de chiffrement. Le mode Open System Authentication est traduit, dans MS Windows XP SP2, par le terme "Ouvrir". Il reste intitulé "Open" dans Windows Vista. Il s'agit du seul cas dans lequel le cryptage des données est désactivé.

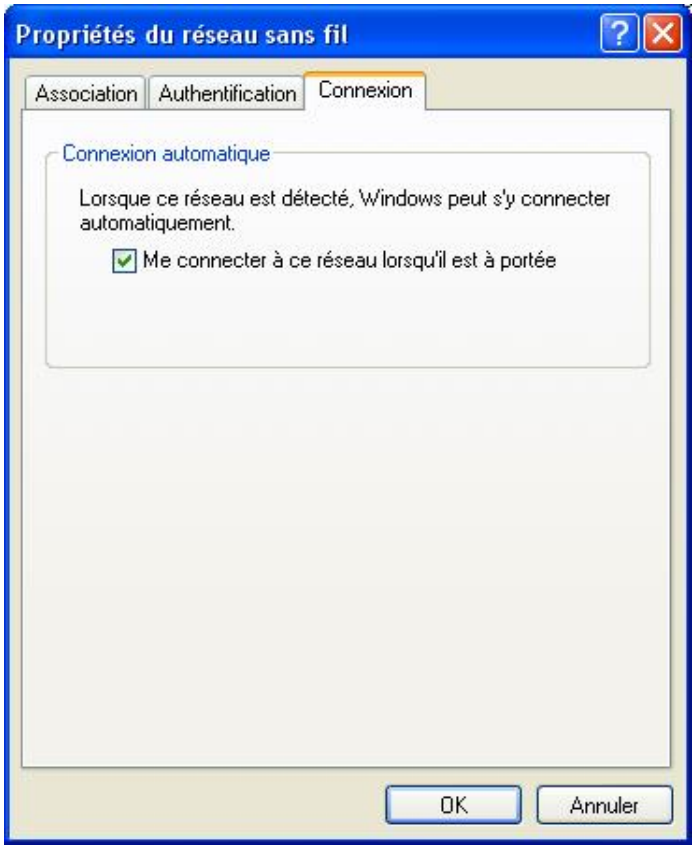
Si au moins le SSID est reconnu, le réseau pourra être détecté par Windows, qui demandera au besoin à l'utilisateur les paramètres complémentaires.

La configuration d'un réseau de type ad hoc nécessite au moins la connaissance du réseau commun, appelé également ici SSID, par l'ensemble des stations. Avec Windows XP, l'ajout d'un réseau sans fil comme précédemment suffit, en activant l'option **Ceci est un réseau d'égal à égal**. La configuration de Windows Vista est différente et s'effectue encore à partir du **Centre Réseau et partage**. La création s'effectue à partir de **Configurer une connexion ou un réseau** ou bien par l'ajout d'un réseau depuis **Gérer les réseaux sans fil**. Dans la nouvelle boîte de dialogue, demander à configurer un réseau sans fil ad hoc, puis suivre l'assistant.



Ajout d'un nouveau réseau sans fil avec MS Windows Vista

Pour chaque réseau Wi-Fi configuré, il est nécessaire de préciser si l'association automatique au réseau doit être effectuée.



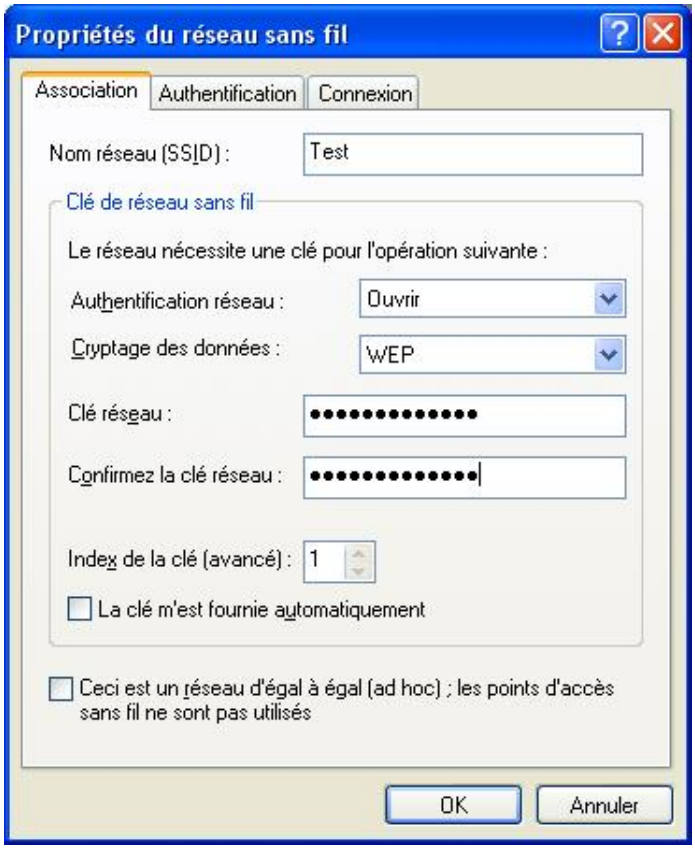
Demande d'association automatique dans l'ajout d'un réseau sans fil sur Windows XP SP2

2. Chiffrement et authentification

Le poste de travail doit s'adapter aux caractéristiques du réseau auquel il s'est associé. Pour cela, il est nécessaire de configurer manuellement les paramètres de chiffrement et d'authentification.

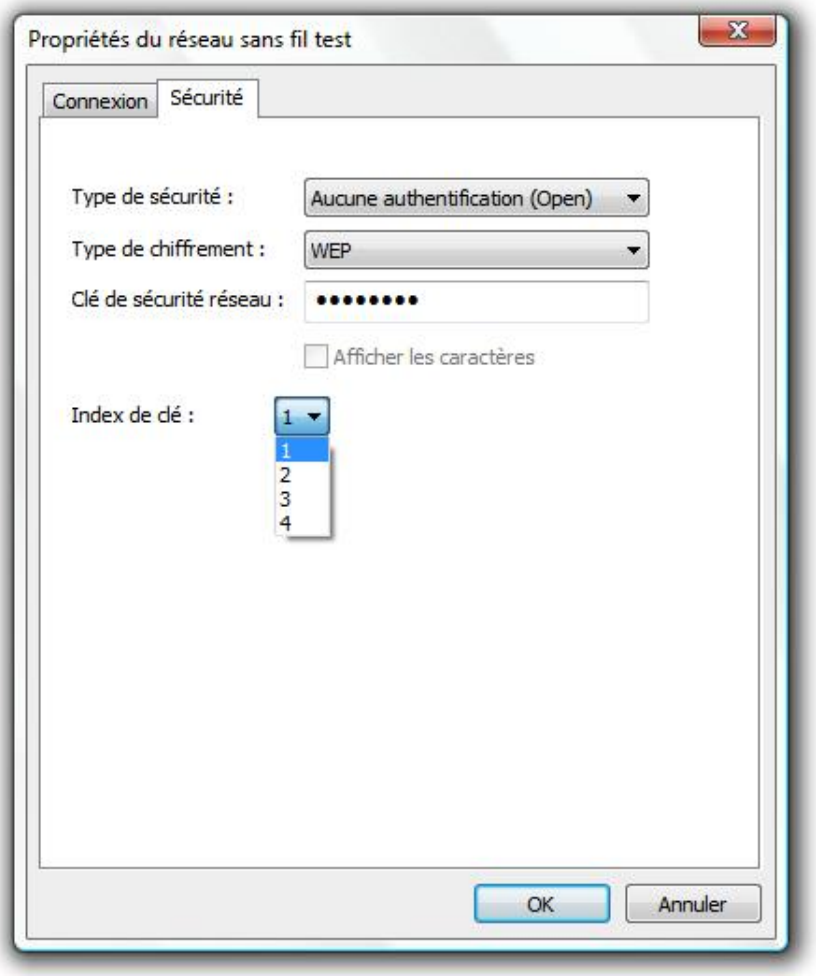
Comme nous l'avons vu précédemment, si seule une clé est à saisir, elle pourra l'être au moment de la demande d'association. Cette démarche n'est pas recommandée.

Une authentification ouverte (*Open System Authentication*) peut ne pas utiliser de chiffrement. Dans les cas de configuration chiffrée de type personnelle, une clé statique doit être saisie manuellement (WEP, WPA-PSK ou WPA/WPA2 Personnel). Cette clé sert pour l'authentification. Son numéro d'index doit correspondre à celui du point d'accès, ou dans le mode ad-hoc, à celui des autres stations.



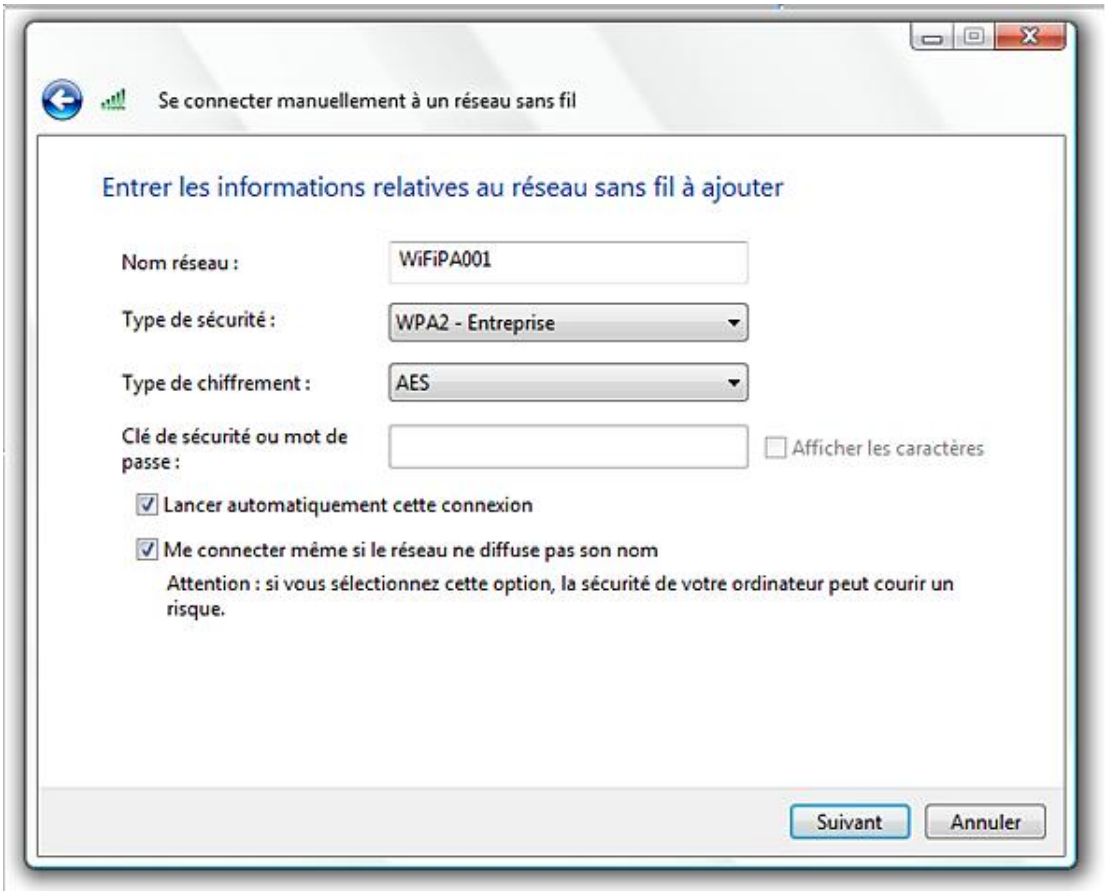
Saisie de la clé WEP sur une station

La configuration de l'index de clé dans Windows Vista s'effectue à partir des propriétés d'un réseau Wi-Fi déjà configuré, dans l'onglet **Sécurité**.



Choix de l'index de clé dans Windows Vista

Dans les modes d'authentification d'entreprise, il est nécessaire de choisir ensuite le type de chiffrement. En fonction du système d'exploitation ou du logiciel de configuration, les intitulés peuvent être différents. Un complément de paramétrage 802.1x et EAP est nécessaire.



Configuration WPA2 Entreprise avec chiffrement AES sur Windows Vista

3. Client 802.1x Windows

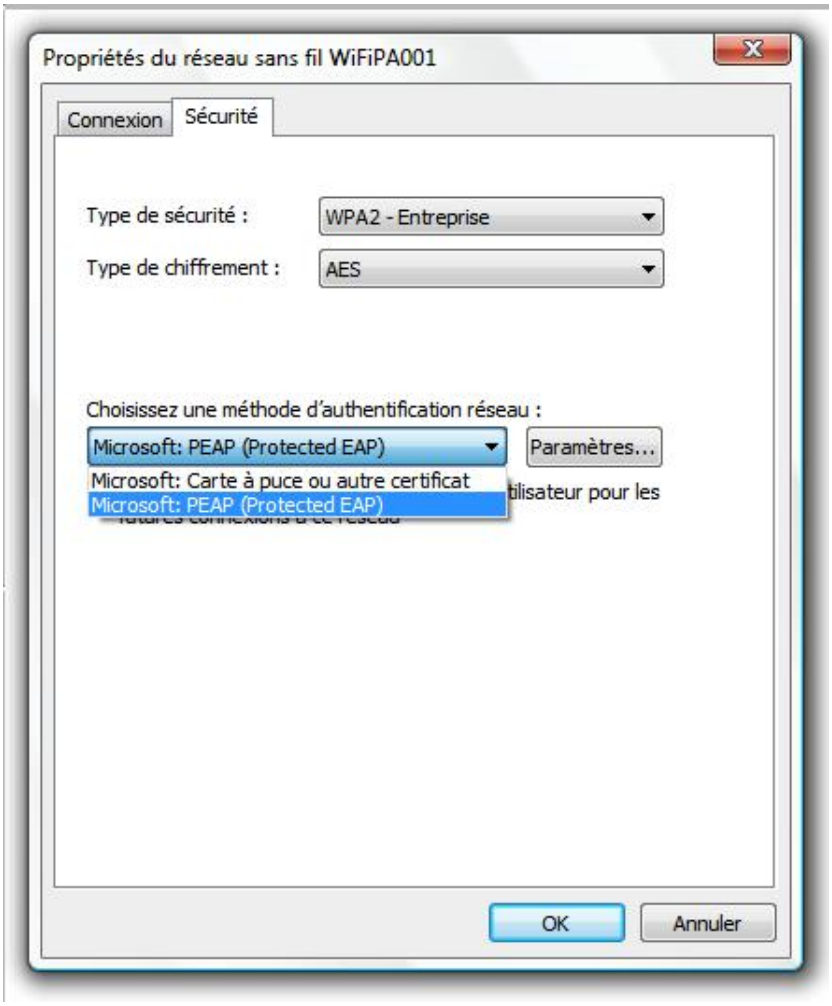
Un client d'authentification 802.1x et EAP est intégré aux systèmes d'exploitation Microsoft Windows.

Dans Windows XP, la configuration de l'authentification 802.1x s'effectue à partir de l'onglet **Authentification des propriétés** de la carte réseau. Windows Vista propose cette configuration dans les propriétés du réseau sans fil déjà configuré.

La solution d'authentification 802.1x peut même être utilisée avec un chiffrement WEP.

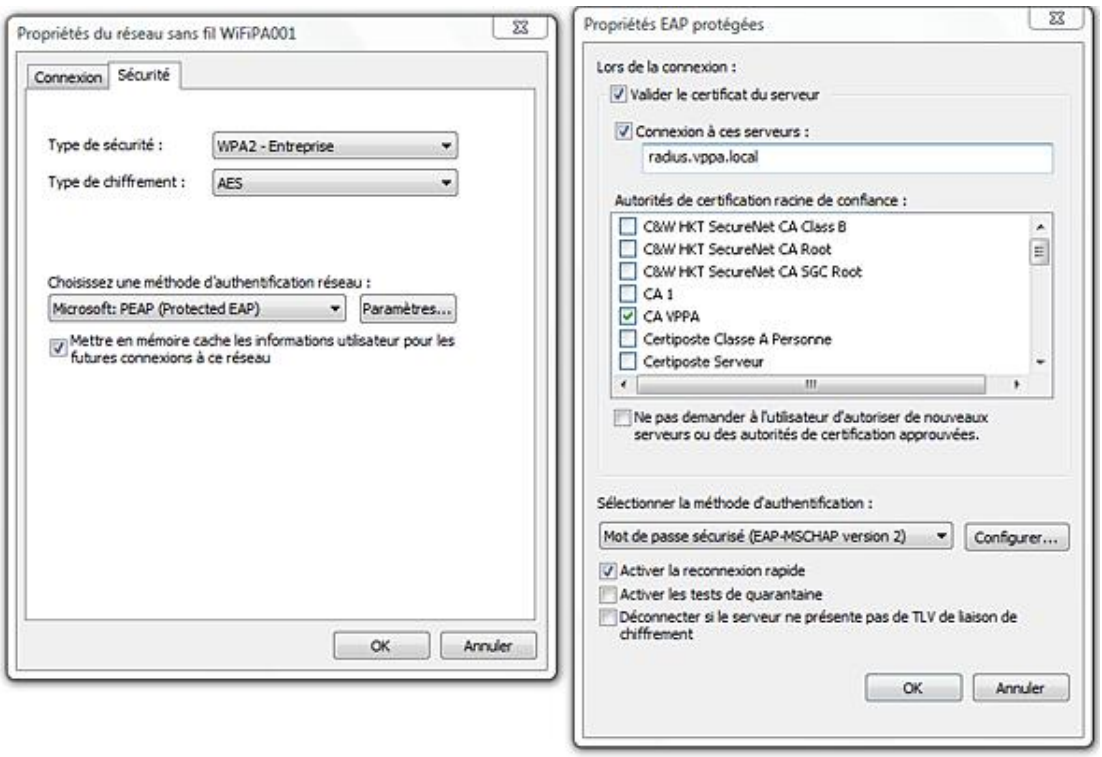
Ce client intégré autorise des connexions par deux méthodes EAP :

- EAP-PEAP, avec usage de mot de passe sécurisé par MS-Chap version 2 ou carte à puce ;
- EAP-TLS, avec stockage du certificat client sur le poste de travail ou sur une carte à puce.



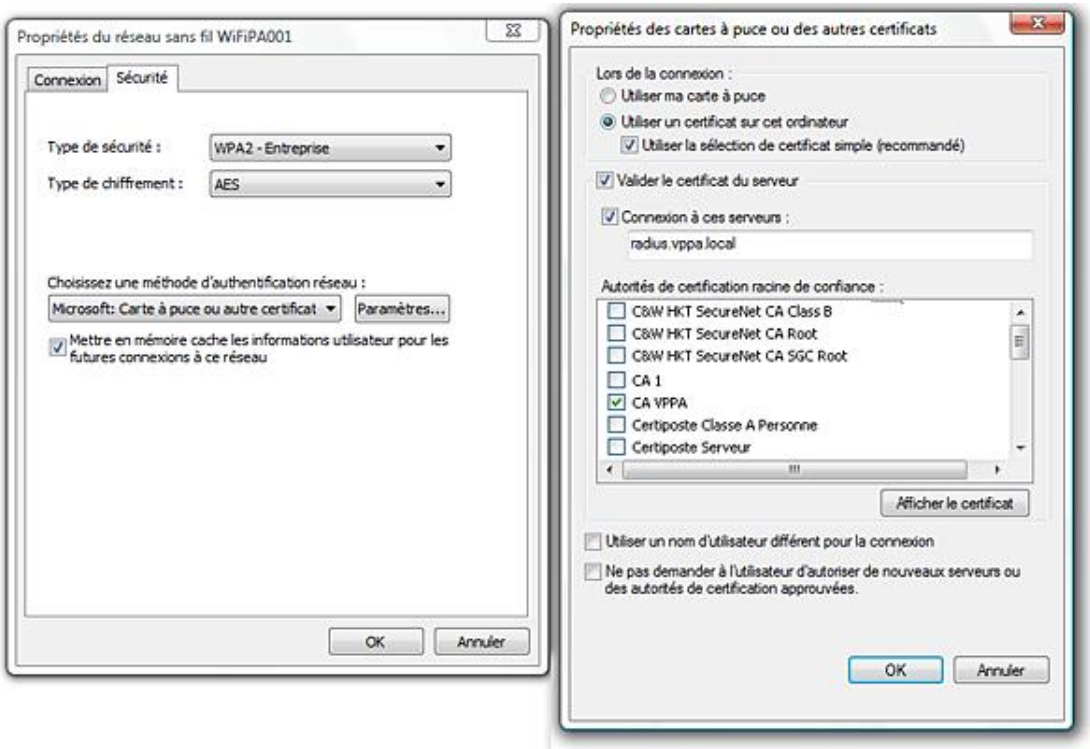
Les méthodes EAP intégrées à MS Windows Vista

Si la méthode PEAP a été retenue, il est possible de renforcer sa sécurité, par vérification du certificat du serveur RADIUS et de l'autorité de certification qui l'a délivré. Il est possible de récupérer automatiquement les identifiants d'ouverture de session, afin d'éviter à l'utilisateur une seconde saisie.



Configuration des propriétés de PEAP

Dans les propriétés d'une authentification EAP-TLS, les mêmes vérifications de certificat serveur sont recommandées. Il est nécessaire de préciser où est stocké le certificat à utiliser.



Configuration des propriétés EAP-TLS

Si ces configurations ont été correctement réalisées, l'utilisateur pourra se connecter au réseau, en fonction de la sécurité désirée et sans aucune manipulation de sa part. Pour lui, Wi-Fi représentera un outil informatique transparent.

A à F

AAA

Authentication, Authorization and Accounting

ADSL

Asymmetric Digital Subscriber Line

AES

Advanced Encryption Standard

AFNIC

Association française pour le nommage Internet en coopération

AH

Authentication Header

AID

Association IDentifier

AIFS

Arbitration Inter Frame Space

AM

Active Mode

AM

Amplitude Modulation

ANFR

Agence nationale des fréquences

AP

Access Point

APSD

Automatic Power Save Delivery

ARCEP

Autorité de régulation des communications électroniques et des postes

ARPA

Advanced Research Project Agency

ART

Autorité de régulation des télécommunications

ASCII

American Standard Code for Information Interchange

ASFI

Accès sans fil à Internet

ASK

Amplitude Shift Keying

ASN.1

Abstract Syntax Notation number One

ATIM

Announcement Traffic Indication Message

BLR

Boucle locale radio

BPL

Broadband Power Line

BRAN

Broadband Radio Access Networks

BSA

Basic Service Area

BSS

Basic Service Set

BSSID

Basic Service Set IDentification

CAP

Controlled Access Phase

CBC

Cipher Block Chaining

CBC-MAC

Cipher Bloc Chaining-with Message Authentication Code

CCK

Complementary Code Keying

CCMP

CTR with CBC-MAC Protocol

CDMA

Code Division Multiple Access

CEPT

Conférence européenne des administrations des postes et télécommunications

CF

Contention Free

CFB

Cipher Feed Back

CFP

Contention Free Period

Clusif

Club de la sécurité des systèmes d'information français

CP

Contention Period

CPL

Courant porteur en ligne

CRC

Cyclic Redundancy Code ou code de redondance cyclique

CSMA/CA

Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD

Carrier Sense Multiple Access /Collision Detection

CTR

Counter Mode

CTS

Clear To Send

CW

Contention Window

DA

Destination Address

DBPSK

Differential Binary Phase Shift Keying

DCS

Digital Cellular System

DCF

Distributed Coordination Function

DDoS

Distributed Denial of Service

DECT

Digital European Cordless Telephone

DES

Data Encryption Standard

DFS

Dynamic Frequency Selection

DHCP

Dynamic Host Configuration Protocol

DIFS

Distributed Inter Frame Space

DoD

Department of Defense

DoS

Denial of Service

DPSK

Differential Phase Shift Keying

DQPSK

Differential Quadrature Phase Shift Keying

DS

Distribution System

DSLAM

Digital Subscriber Line Access Multiplexor

DSSS

Direct Sequence Spread Spectrum

DTIM

Delivery Traffic Indication Message

EAP

Extensible Authentication Protocol

EAPol

EAP over LAN

ECB

Electronic Code Book

EDCA

Enhanced Distributed Channel Access

EDCF

Enhanced Distributed Coordination Function

EDGE

Enhanced Data for GSM Evolution

EIRP

Equivalent Isotropic Radiated Power

EPCF

Enhanced Point Coordination Function

ESA

Extended Service Area

ESP

Encapsulating Security Payload

ESS

Extended Service Set

ESSID

Extended Service Set IDentifier

ETSI

European Telecommunications Standards Institute

FAI

Fournisseur d’accès à Internet

FC

Frame Control

FCC

Federal Communications Commission

FCS

Frame Sequence Check

FDMA

Frequency Division Multiple Access

FFT

Fast Fourrier Transform

FHSS

Frequency Hopping Spread Spectrum

FM

Frequency Modulation

FSK

Frequency Shift Keying

FTP

File Transfer Protocol

G à P

GEK

Group Encryption Key

GFSK

Gaussian Frequency Shift Keying

GIK

Group Integrity Key

GMK

Group Master Key

GPRS

General Packet Radio Service

GRE

Generic Routing Encapsulation

GSM

Global System for Mobile

GTK

Group Temporal Key

HCCA

HCF Controlled Channel Access

HCF

Hybrid Coordination Function

HiperLAN

High Performance LAN

HomePlug CC

Command & Control

HomeRF

Home Radio Frequency

HPAV

HomePlug AV

HSDPA

High Speed Downlink Packet Access

HTTP

HyperText Transfer Protocol

HTTPS

HyperText Transfer Protocol over TLS

IAPP

Inter-Access Point Protocol

IBSS

Independent Basic Service Set

ICV

Integrity Check Value

IE

Information Element

IEEE

Institute of Electrical and Electronics Engineers

IETF

Internet Engineering Task Force

Internet

Inter Networking

IP

Internet Protocol

IPSec

IP Security

IrDA

Infrared Data Association

ISM

Industrial, Scientific and Medical

ITS

Intelligent Transportation Systems

IV

Initialisation Vector

KCK

Key Confirmation Key

KEK

Key Encryption Key

L2TP

Layer 2 Transport Protocol

LAN

Local Area Network

LLC

Logical Link Control

LoS

Line of Sight

MAC

Medium Access Control

MAN

Metropolitan Area Network

MD 5

Message Digest 5

MIC

Modulation par impulsion codée

MIC

Message Integrity Code

MiM

Man in the Middle

MIME

Multipurpose Internet Mail Extensions

MIMO

Multiple Input Multiple Output

MMPDU

MAC Management Protocol Data Unit

MPDU

MAC Protocol Data Unit

MSDU

MAC Service Data Unit

MTU

Maximum Transfer Unit

NAV

Network Allocation Vector

NLoS

Non Line of Sight

NTIC

Nouvelles technologies de l’information et de la communication

OFB

Output Feed Back

OFDM

Orthogonal Frequency Division Multiplexing

OSI

Open Systems Interconnection

OUI

Organizationally Unique Identifier

PAE

Port Access Entity

PAN

Personal Area Network

PC

Point Coordinator

PCF

Point Coordination Function

PDA

Personal Digital Assistant

PIFS

PCF Inter Frame Space

PIRE

Puissance isotrope rayonnée équivalente

PKI

Public Key Infrastructure

PLC

Power Line Communications

PLCP

Physical Layer Convergence Protocol

PLF

Polarization Loss Factor

PM

Phase modulation

PMD

Physical Medium Dependent

PMK

Pairwise Master Key

PN

Packet Number

POS

Personal Operating Space

PPDU

PHY Protocol Data Unit

PPP

Point to Point Protocol

PPTP

Point to Point Tunneling Protocol

PRNG

Pseudo-Random Number Generator

PS

Power Save

PSDU

PLCP Service Data Unit

PSK

Pre Shared Key

PSK

Phase Shift Keying

PTK

Pairwise Transient Key

Q à W

QAM

Quadrature Amplitude Modulation

QAP

QoS Access Point

QBSS

QoS Basic Service Set

QoS

Quality of Service

QPSK

Quadrature Phase Shift Keying

QSTA

QoS Station

RA

Receiver Address

RADIUS

Remote Authentication Dial In User Service

RC4

Rivest Cipher n4

RFC

Request for Comments

RIFS

Reduced Inter Frame Space

RLAN

Radio Local Area Network

RLE

Réseau local d’entreprise

RLL

Radio Local Loop

RNIS

Réseau numérique à intégration de service

RPC

Remote Procedure Call

RPV

Réseau privé virtuel

RSA

Rivest, Shamir and Adelman

RSN

Robust Security Network

RSNA

Robust Security Network Association

RTC

Réseau téléphonique commuté

RTS

Request to Send

SA

Source Address

SC

Sequence Control

SDM

Spatial Diversity Multiplexing

SHA

Secure Hash Algorithm

SIFS

Short Inter Frame Space

SOHO

Small Office Home Office

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SNR

Signal to Noise Ratio

SSH

Secure Shell

SSID

Service Set IDentifier

SSL

Secure Socket Layer

STBC

Space Time Bloc Code

TA

Transmitter Address

TC

Traffic Class

TCP

Transmission Control Protocol

TDMA

Time Division Multiple Access

TID

Traffic Identifier

TIM

Traffic Indication Map

TK

Temporal Key

TKIP

Temporal Key Integrity Protocol

TLS

Transport Layer Security

TMK

Temporal MIC Key

TPC

Transmit Power Protocol

TSC

TKIP Sequence Counter

TSN

Transition Security Network

TXOP

Transmit opportunity

UDP

User Datagram Protocol

UIT

Union internationale des télécommunications

UMA

Unlicensed Mobile Access

UMTS

Universal Mobile Telecommunications System

UNII

Unlicensed National Information Infrastructure

USB

Universal Serial Bus

UWB

Ultra Wide Band

VLAN

Virtual Local Area Network

VoWi-Fi

Voice over Wireless Fidelity

VPN

Virtual Private Network

WAN

Wide Area Network

WAP

Wireless Application Protocol

WAVE

Wireless Access in Vehicular Environment

WDS

Wireless Distribution System

WECA

Wireless Ethernet Compatibility Alliance

WEP

Wired Equivalent Privacy

Wi-Fi

Wireless Fidelity

WiMax

Worldwide Interoperability for Microwave Access

WISP

Wireless Internet Service Providers

WLAN

Wireless Local Area Network

WLL

Wireless Local Loop

WMM

Wireless Multi-Media

WPA

Wi-Fi Protected Access

WPA2

Wi-Fi Protected Access 2