Le WIFI : Standard 802.11

WIreless **FI**delity **ou Wlan**

Réalisé par Xavier CABANAT et
Nicolas DUGNACH
TSMSI Montpellier promotion 2003-2005
Version du document : 1.0
Date : 11/05/05

Sommaire

1. Historique et futur du WIFI.

Après des débuts modestes en 1997 en tant que standard du sans fil à 1 et 2 Mbits/s dans la bande des 2,4 Ghz, WIFI a vu ses débits passer à 11 Mbits/s en 1999 et plus récemment à 54 Mbits/s dans les deux bandes de fréquences des 2,4 Ghz et 5 Ghz.
Il a rapidement gagné en popularité au sein des entreprises, avec la possibilité pour les employés de se connecter au réseau, même loin du bureau.
Une multitude de fabricants ont élaboré des solutions conformément à un standard commun, et un programme de certification d'interopérabilité a été mis en place par la WI-FI Alliance, par conséquent les performances du matériel WIFI ont augmenté tandis que les coûts chutaient rapidement.
Parvenue au rang de technologie de grande consommation, WIFI est désormais livré en tant que fonctionnalité standard sur de nombreux ordinateurs portables et appareils portatifs.
De simples cartes pour PC peuvent opérer à des débits de 1 à 54 Mbits/s dans les deux bandes.

Le standard 802.11 de l'IEEE, ou WIFI, était au départ une application essentiellement destinée aux entrepôts, à la gestion d'inventaire et à la liaison des caisses enregistreuses. Cette application s'est développée pour être utilisé par le plus grand nombre, au domicile comme au travail, aujourd'hui, WIFI est principalement employé en tant qu'extension sans fil à haut débit de l'omniprésent réseau Ethernet, nous reliant sans effort à Internet et à nos applications de bureau.

WIFI continuera à proliférer dans des applications que ses inventeurs n'ont sûrement pas imaginées.
De nouvelles extensions au standard sont en cours de développement, qui renforceront la sécurité, offriront un support pour la qualité de service (QOS), faciliteront la gestion de l'environnement sans fil et porteront les débits bien au-delà des 100 Mbits/s.
Ces nouvelles extensions ne se limiterons pas à améliorer les performances de WIFI dans les applications existantes mais donneront lieu à de nouvelles applications, telles que la téléphonie de qualité avec la voix sur IP sans fil ou le streaming vidéo à destination d'un grand écran mural.

2. Introduction.

2.1. Définition :

Le WI-FI répond à la norme *IEEE* 802.11. La norme *IEEE 802.11* (*ISO/IEC 8802-11*) est un standard international décrivant les caractéristiques d'un réseau local sans fil (*WLAN*).

■ Le nom Wi-Fi (contraction de *Wireless Fidelity*) correspond initialement au nom donné à la certification délivrée par la WECA (http://www.weca.org/) Etats-Unis (*Wireless Ethernet Compatibility Alliance*), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11.

■ C'est la Wi-Fi Alliance qui pose le label " Wi-Fi " et certifie les produits des constructeurs en France. Ce groupe réunit plus de deux cents sociétés différentes.

■ Par abus de langage (et pour des raisons de marketing) le nom de la norme se confond aujourd'hui avec le nom de la certification. Ainsi un réseau Wifi est en réalité un réseau répondant à la norme 802.11.

2.2. L'IEEE : Institute of Electricaland Electronics Engineer :

Normes	Définition concise
802.1	Modèle architectural séparant les deux couches OSI Physique et Liaison en 3 couches : PLS,MAC, LLC
802.2	Norme IEE couche LIAISON
802.3	Norme IEE ETHERNET / CSMA/CD
802.4	Norme IEEE TOKEN BUS (industriel IBM) – Anneau à jetons
802.5	Norme IEEE TOKEN BUS (non propriétaire inspiré d'IBM)
802.6	Norme IEEE de réseau métropolitain à double bus.
802.7	Norme IEEE FDDI (Fiber Distributed Data Interface) – Fibre Optique
802.8	Projet IEEE sur les Fibres Optiques / Résilié le 11/09/2002
802.9	Norme IEEE Integrated Service LAN (ISLAN)
802.10	Norme IEEE de sécurité réseau 802 (SILS : Standard for Interoperable Lan Security)
802.11	Série de normes IEEE pour réseau local sans fil

2.3. Concernant les débits :

■ **802.11 :** L'ancêtre du réseau sans fil, sur 2,4 GHz modulation DSSS ou saut de fréquence (aucune norme imposée), d'un débit de 2 Mb/s et pratiquement pas interopérable de constructeur à constructeur.

■ **802.11a :** (baptisé *WiFi 5*) historiquement c'est le second projet de réseau Ethernet sans fil sur 5 GHz, elle permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). Pas de compatibilité avec 802.11, 802.11b(+) et g(+). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.

■ **802.11b :** premier réseau Ethernet sans fil rétrocompatible avec 802.11, sur 2,4 GHz, offrant un débit physique de 11 Mb/s, 6 Mb/s réels (modulation DSSS, accès par CSMA/CA et détection de porteuse)

ν 802.11b+ : (Rétrocompatible avec 802.11) amélioration de la norme 802.11b, offrant un débit physique de 22 Mb/s, il s'agit d'une mode **non-standard** utilisant une puce propriétaire Texas Instrument. La majorité des cartes ne l'utilisent pas (afin de réduire les coûts) et sont passées directement au 802.11g (54 Mbits/s) qui est de toute façon plus rapide et un standard officiel.

■ **802.11g :** (Rétrocompatible avec 802.11) est la norme la plus répandue actuellement. Adaptation d'OFDM aux réseaux 802.11b (compatibilité) (passage à 54 Mb/s, 30 Mb/s en réel). La norme 802.11g a une compatibilité ascendante avec la norme 802.11b.

■ **802.11g+ :** (Rétrocompatible avec 802.11) augmentation du débit max. théorique en le portant à 108Mbit/s sur la bande de fréquence 2.4Ghz. Rétrocompatible avec le 802.11 et 802.11b.
Le dépassement du débit théorique de 54Mbps se fait par compression de données ou par concaténation de canaux. Du fait de cette **absence de standard**, il convient d'être très prudent avec cette déclinaison du 802.11g qui est, lui, entièrement standardisé. La plupart du temps un réseau WiFi voulu en g+ ne fonctionnera qu'en g quand on ne prend pas un maximum de précautions.
Dans la pratique on obtiendra un débit théorique de 70Mbps.

2.4. Concernant la sécurité :

■ **802.1x : Sous-section du groupe de travail 802.11i** visant à l'intégration du protocole EAP (authentification) dans les trames Ethernet (indépendamment de tout protocole PPP, contrairement aux accès RAS conventionnels). 1x permet l'usage d'un serveur d'authentification de type Radius.

■ **802.11i :** Amélioration au niveau MAC destinée à renforcer la sécurité des transmissions, et se substituant au protocole de cryptage WEP. La norme *802.11i* a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'*AES* (*Advanced Encryption Standard*) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.

2.5. Concernant les constructeurs :

■ 802.11c : Complément de la couche MAC améliorant les fonctions « pont », reversé au Groupe de Travail 802.11d

■ 802.11d : Adaptation des couches physiques pour conformité aux exigences de certains pays particulièrement strictes (essentiellement la France et le Japon)

■ 802.11e : Complément de la couche MAC apportant une qualité de service aux réseaux 802.11a, b et g. Norme en voie d'achèvement

■ 802.11f : Document normatif décrivant l'interopérabilité inter constructeurs au niveau de l'enregistrement d'un point d'accès (AP) au sein d'un réseau, ainsi que les échanges d'information entre AP lors d'un saut de cellule (roaming). Norme en voie d'achèvement

■ 802.11h : Amélioration de la couche MAC visant à rendre compatible les équipements 802.11a avec les infrastructures Hiperlan2.

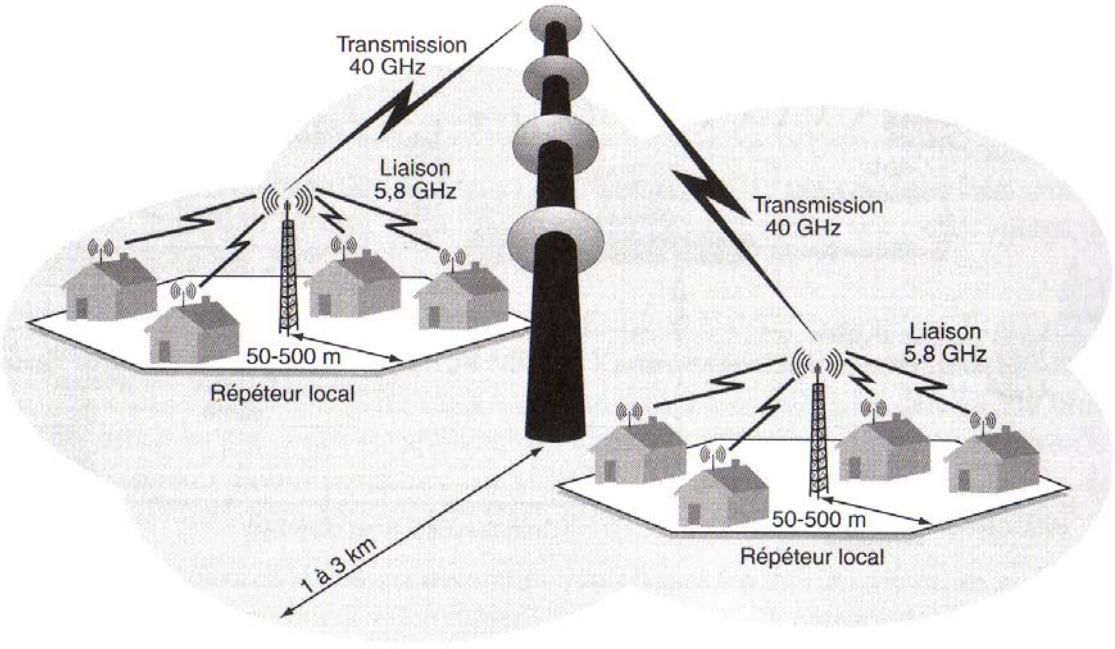
802.11h s'occupe notamment de l'assignation automatique de fréquences de l'AP et du contrôle automatique de la puissance d'émission, visant à éliminer les interférences entre points d'accès. En cours d'élaboration, travail commun entre l'IEEE et l'ETSI .

2.6. Capacité des points d'accès.

	Exemple de type d'application	**Nombre utilisateurs**
802.11b	– Consultation messagerie – Navigation Internet	50
	– Téléchargement de fichier peu volumineux	25
	– Téléchargement de fichier volumineux – VoIP, vidéoconférence…	10
802.11a **802.11g**	– Téléchargement de fichier volumineux – VoIP, visé	50

3. Le 802.16 (WiMax)

L'initiative WiMax est née du désir de développer des liaisons hertziennes concurrentes des techniques xDSL terrestres. Après de longues années d'hésitation, son vrai démarrage a été favorisé par l'arrivée de la norme IEEE 802.16. voici son utilisation.



À partir d'une antenne d'opérateur, plusieurs répéteurs propagent les signaux vers des maisons individuelles pour leur donner accès à la téléphonie et à l'équivalent d'une connexion xDSL. Sur la figure, la connexion avec l'utilisateur s'effectue en deux temps en passent par un répéteur. Il est toutefois possible d'avoir une liaison directe entre l'utilisateur et l'antenne.

4. HyperLan

- Concurrent « déchu » du 802.11.
- Essentiellement supporté par INTEL
- Plus commercialisé depuis plusieurs mois.

5. HyperLan II

- Successeur d'HyperLan, utilisant la bande des 5 Ghz
- Concurrent du 802.11a
- Faible potentiel face au WIFI

6. Type d'usage.

Les Réseaux ouverts au public dans le cadre de projet de développement local

■ Les implantations sont possibles partout depuis 25 juillet 2003 - Déclaration à ART uniquement demandée

■ Toute installation extérieure n 'est plus soumise à une autorisation préalable fournie par l'ART (Autorité des Réseaux et Télécommunications). Toutefois, la déclaration est obligatoire.

offres gratuites qui propose des réseau WIFI libre haut débit leur philosophie le plus souvent s'inspire des logiciels libres la volonté de gratuité, de partage pour tous.
Exemple : fédération France wireless, paris sans fil.

http://www.paris-sansfil.info/Accueil
http://www.wireless-fr.org/spip/

Bornes d'accès WI-FI dans les lieux dits de passage : "Hot Spots"

■ lieux de passage à forte influence, tels que les aéroports, les gares, les complexes touristiques, bars, hôtels … (le CNIT, l'Aéroport de Roissy-Charles-de-Gaulle…)

■ Pas d'autorisation lorsqu 'elles sont raccordées directement à un réseau ouvert au public existant (en général un opérateur de télécommunications).

■ offres payantes :
Les opérateurs télécoms et autres FAI proposent des abonnements, à durée limitée (5€ pour 20 minutes, 10 à 20 € pour 2 heures selon l'opérateur) ou illimitée pendant une période donnée (30€ pour 24 heures).
Exemple : orange, SFR

7. Comment ça marche ?

7.1. Le principe de fonctionnement.

Le WIFI fonctionne sous le principe de la transmission radio, un émetteur et un récepteur s'envoie des données binaire modulé en fréquence sous une porteuse pouvant varié suivant la norme employé par le matériel et le pays résident.

Pour la France la porteuse de modulation va de 2.457 Ghz à 2.472 Ghz.
Si les réseaux locaux sans fil, ou WLAN issus du standard 802.11 deviennent si omniprésents dans les déploiements de réseaux c'est principalement en raison de leur facilité d'implémentation et d'utilisation. Pourtant, l'architecture 802.11 est tout sauf simple, les défis que pose un support de transmission non guidé sont plus complexes que ceux du support Ethernet guidé.
La sous-couche MAC doit fournir un mécanisme d'accès équitable au support, tandis que les stations Ethernet câblées emploient la méthode d'accès CSMA/CD (Carrier Sense Multiple Access/Collision Detection), qui leurs permet de détecter les collisions, les stations 802.11 ne sont pas en mesure d'effectuer cette détection, c'est pourquoi la sous-couche MAC 802.11 doit fournir davantage de fonctions et être évolutive, tout en limitant la surcharge du service.

Les réseaux 802.11 offrent intrinsèquement une très grande souplesse. Trois types de topologies peuvent être déployées pour concevoir un WLAN :

- IBSS (Independent Service Set)
- BSS (Basic Service Set)
- ESS (Extented Service Set)

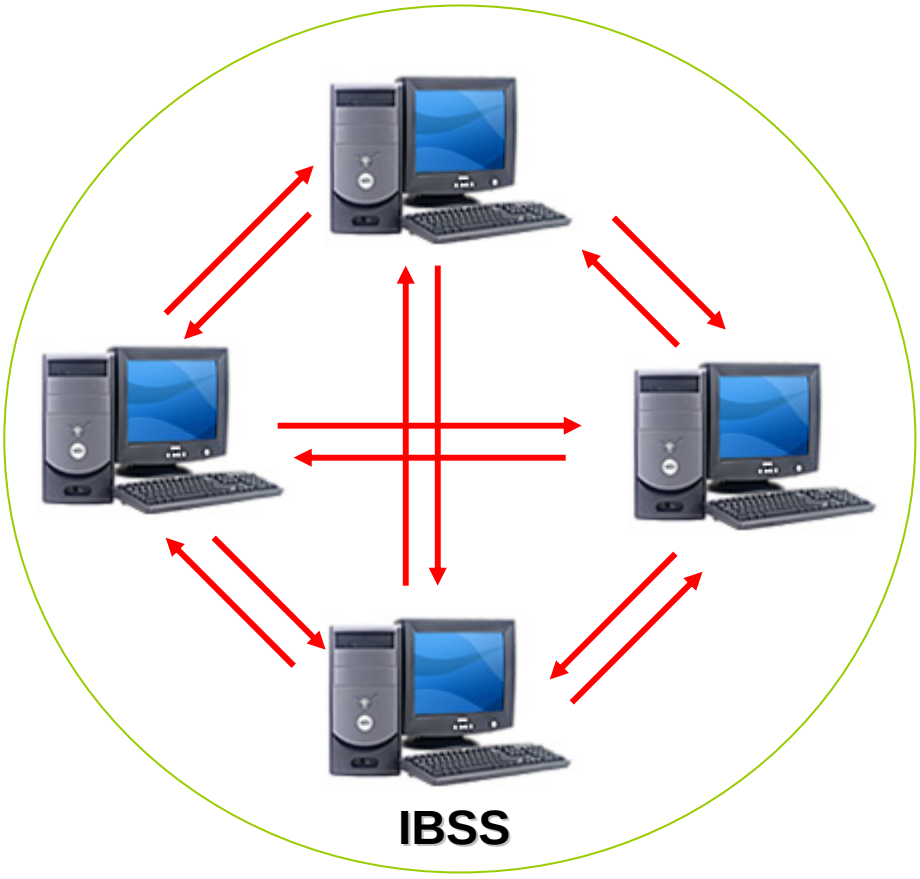
Un service set, ou ensemble de services, consiste en un groupement logique d'équipement, dans un WLAN, les transmissions se font sur une porteuse radio, c'est-à-dire un signal émis dans les fréquences hertziennes. Une station réceptrice peut se trouver dans la plage de fréquences de plusieurs stations émettrices appartenant à des groupes différents, pour permettre au récepteur de trier les signaux reçus afin de ne retenir que ceux qui l'intéressent, l'émetteur préfixe un identifiant de service set, ou SSID (Service Set Identifier), aux données qu'il transmet.

IBSS (ou WLAN ad-hoc) : Un IBSS est un groupe de stations qui communiquent directement entre elles, il s'agit donc d'un WLAN peer-to-peer, elles n'ont donc pas besoin de AP (Access Point) point d'accès, il ne demande pas d'étude préalable et sa mise en place est simple, car il est généralement petit et dure seulement le temps d'échanger les données nécessaires. Il n'existe aucune limite standard concernant le nombre d'équipements pouvant faire partie d'un IBSS, comme chacun d'eux est un client, il arrive que certains membres ne puissent communiquer en raison du problème du nœud caché, malgré cela, aucun mécanisme n'est prévu pour assurer une fonction de relais dans un IBSS.
En l'absence d'AP, la synchronisation est gérée par les clients eux-mêmes, le client qui initie l'IBSS définit l'intervalle de transmission des trames balises ou « Beacon » pour créer un ensemble de valeurs TBTT (Target Beacon Transmission Time), chacune d'elles marquant le début d'une nouvelle période de transmission beacon, à chaque TBTT, chaque client accomplit les actions suivantes :

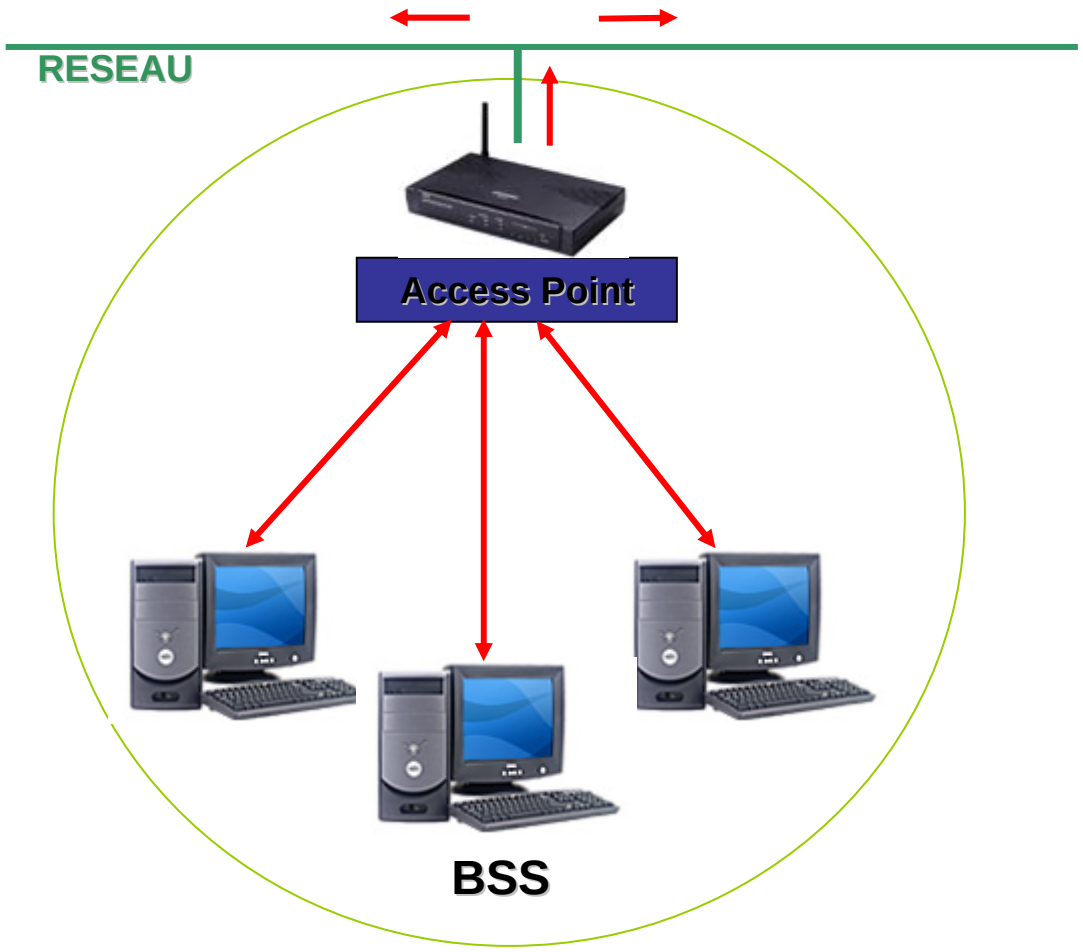
- Il suspend le temporisateur de backoff en cours datant de la dernière TBTT, ce temporisateur détermine le délai d'attente avant la prochaine transmission de données.
- Il détermine un nouveau délai aléatoire.
- S'il reçoit une trame beacon avant l'expiration de ce délai, il reprend son temporisateur de backoff. Si le délai expire sans qu'il n'y ait reçu une trame beacon, il envoie lui-même une trame beacon et reprend son temporisateur de backoff.

En raison du problème du nœud caché, qui est évoqué plus loin, il peut arriver que plusieurs trames beacon soient envoyées par différents clients pendant la période de transmission beacon, auquel cas, certains clients en recevront plusieurs. Cette possibilité prévue par le standard ne doit pas poser de problème puisque les clients attendent en fait la réception de la première trame beacon correspondant à leur délai aléatoire.

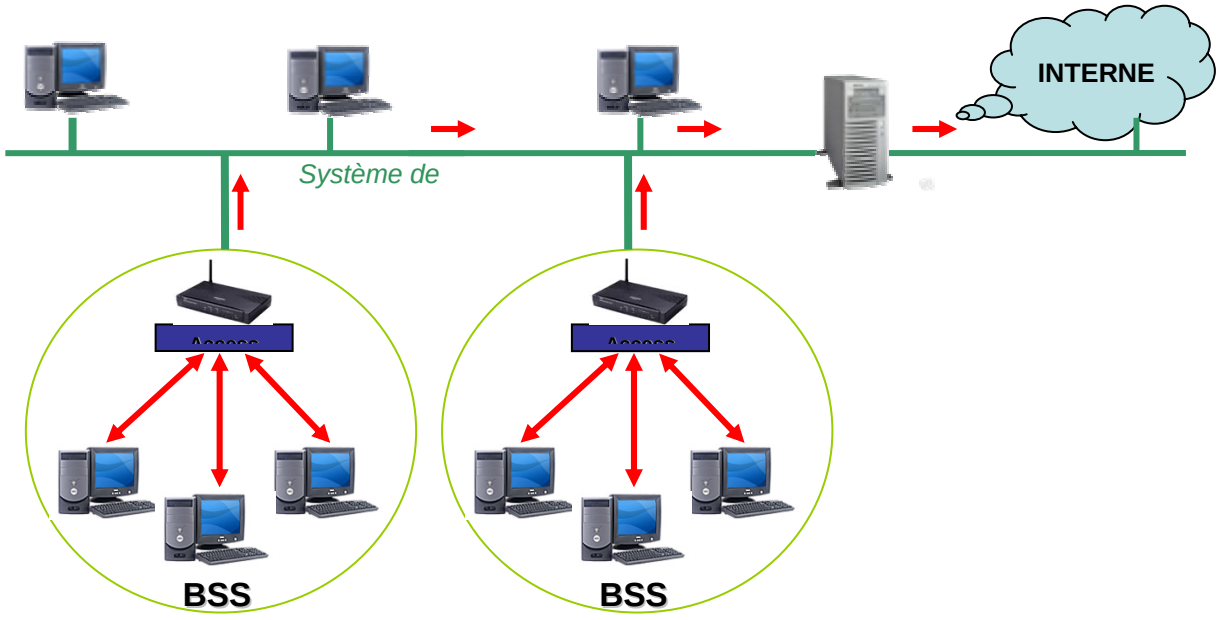
Chaque trame beacon contient une valeur TSF (Time Synchronization Function) de synchronisation d'horloge. Lorsqu'un client reçoit une trame beacon, il examine la TSF qu'elle contient et met à jour sa propre valeur si celle est reçue est supérieure, signifiant que l'horloge de l'émetteur est plus rapide. Ce processus a pour effet de régler progressivement la vitesse d'horloge de tous les équipements sur celle du client le plus rapide. Dans un grand réseau ad-hoc, où les clients ne peuvent pas tous communiquer directement, la synchronisation peut être assez longue.



BSS : Un BSS est un groupe de station 802.11 qui communiquent entre elles par l'intermédiaire d'une station spéciale, appelée Point d'Accès, ou AP (Access Point). Les clients ne peuvent communiquer directement et sont obligés de passer par l'AP, qui achemine les rames vers la destination appropriée. L'AP peut disposer d'un port de liaison montante (uplink) vers le réseau câblé, par exemple une liaison Ethernet, auquel cas on parle de BSS d'infrastructure.



ESS : Plusieurs BSS d'infrastructure peuvent être reliés entre eux via leur interface uplink. Dans l'univers 802.11, cette interface relie le BSS au système de distribution, ou DS (Distribution System). Un ensemble de BSS interconnectés via le DS s'appelle un ESS (Extented Service Set), même si les spécifications 802.11 permettent que la liaison montante vers le DS soit sans fil, elle consiste la plupart du temps en un câble Ethernet.



7.2. Présentation du CSMA/CA :

Le processus CSMA/CD peut être comparé à une audioconférence, un participant qui souhaite parler doit attendre que tous les autres se taisent. Lorsque la ligne est libre, il peut tenter de parler. Si un autre participant prend la parole au même moment, les deux interlocuteurs doivent s'arrêter et essayer de nouveau une fois le silence revenu.
CSMA/CA est plus contraignant que CSMA/CD, voici comment se déroulerait une audioconférence selon cette méthode :

- Avant de prendre la parole, un participant indique pendant combien de temps il compte occuper le canal, donnant une idée aux autres participants de leur durée d'attente avant de pouvoir s'exprimer à leur tour.
- Aucun participant ne peut intervenir avant que le temps de parole du participant en cours soit écoulé.
- Un participant ne peut savoir que sa voix a été entendue par les autres participants que s'il en reçoit la confirmation.
- Si les deux participants parlent en même temps, ils ignorent. Le fait de ne pas recevoir de confirmation leur indique toutefois qu'ils n'ont pas été entendus.
- Lorsqu'un participant ne reçoit pas de confirmation, il patiente pendant une durée aléatoire puis tente de parler de nouveau.

Les règles plus strictes de CSMA/CA contribuent à éviter les collisions. Cette prévention est essentielle dans les réseaux sans fil puisqu'il n'existe aucun mécanisme explicite de détection des collisions. Une collision est détectée implicitement lorsque l'émetteur ne reçoit pas d'acquittement.

L'implémentation 802.11 de CSMA/CA est principalement incarnée par la fonction DCF (Distributed coordination Function). Voici les principales composantes de cette implémentation dans un réseau 802.11 :

- Écoute de la porteuse
- Fonction de coordination distribuée, ou DCF
- Trames d'acquittement
- Réservation du support au moyen de trames RTS (Request To Send) et CTS (Clear To Send).

Les deux autres asspects importants suivants de l'accès au support 802.11 sont indépendants de CSMA/CA :

- Fragmentation des trames
- Fonction de coordination par AP, ou PCF (Point Coordination Function)

L'écoute de la porteuse

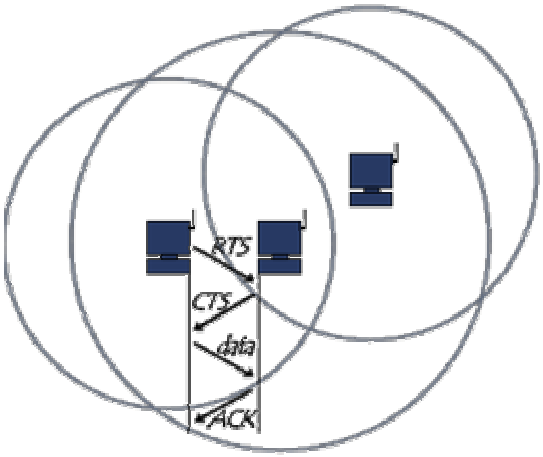
Une station qui souhaite émettre doit d'abord écouter le support sans fil pour déterminer s'il est occupé ou non. S'il l'est, elle doit différer sa transmission jusqu'à ce qu'il soit libre. Pour savoir si le support est disponible, elle peut procéder de deux manières :

- Examiner la couche physique (couche 1, ou PHY) afin de détecter la présence d'un signal porteur

- Utiliser un mécanisme d'écoute virtuelle de la porteuse, appelé NAV (Network Allocation Vector).

Je ne vais pas passer en détail tous ce qui se passe lors de l'émission et de la réception de trame, je vais simplifier en expliquant le schéma ci-dessous :

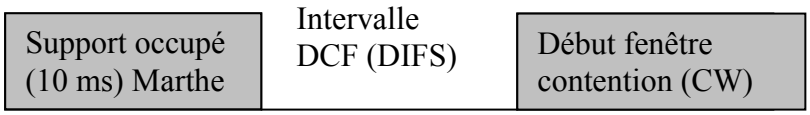
Voici l'émission d'une trame :



- La station voulant émettre écoute le réseau. Si le réseau est encombré, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé *DIFS* pour *Distributed Inter Frame Space*), alors la station peut émettre. La station transmet un message appelé *Ready To Send* (noté *RTS* signifiant *prêt à émettre*) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur (généralement un point d'accès) répond un *Clear To Send* (*CTS*, signifiant *Le champ est libre pour émettre*), puis la station commence l'émission des données.
- A réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (*ACK*). Toutes les stations avoisinantes patientent alors pendant un temps qu'elle considère être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.

7.3. La fonction DCF :

Représentation temporelle de l'accès au support avec DCF

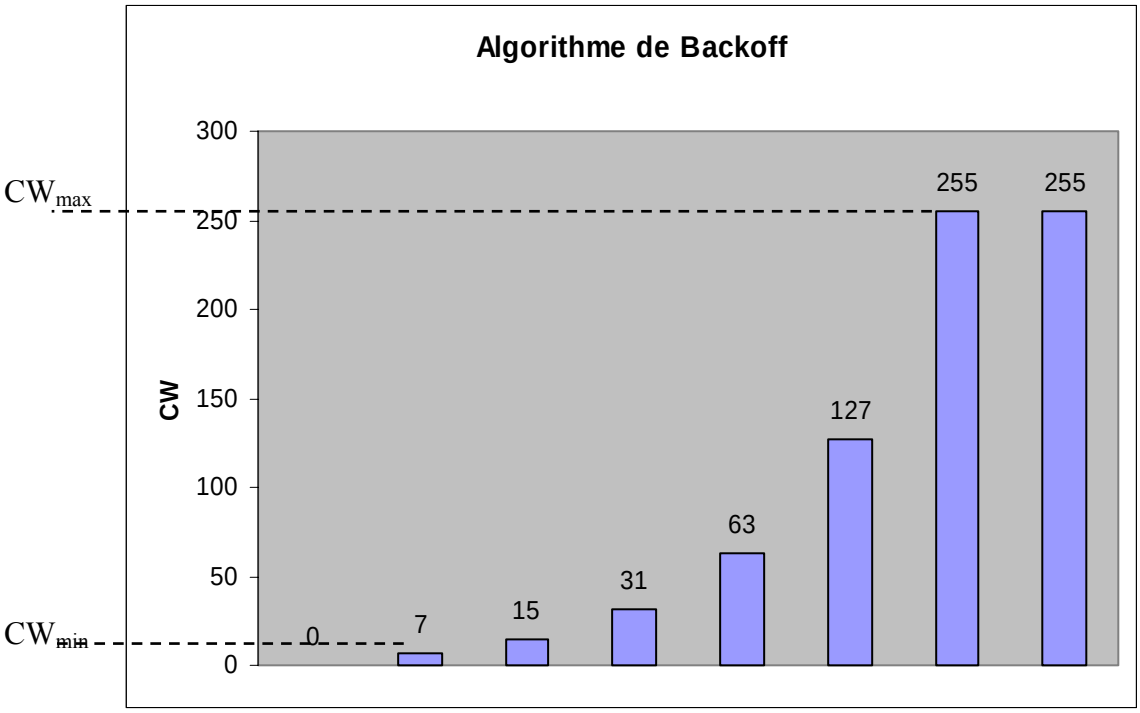


Avec DCF, une station qui veut émettre doit patienter pendant un intervalle se temps déterminé après que le support est devenu libre. Cet intervalle se nomme DIFS

(Distributed Inter-Frame Space). Lorsqu'il expire, le support redevient utilisable par les autres stations.

Pour exemple, prenons des stations que nous appellerons Viviane, Georges et Marthe, supposons que Viviane et Georges veuillent envoyer des trames lorsque Marthe termine de transmettre. Les deux stations doivent pour cela avoir le même NAV et détecter que le support est libre. Il est fort probable qu'elles tentent d'émettre en même temps, provoquant une collision. Pour éviter cette situation, DCF utilise un temporisateur de backoff aléatoire.

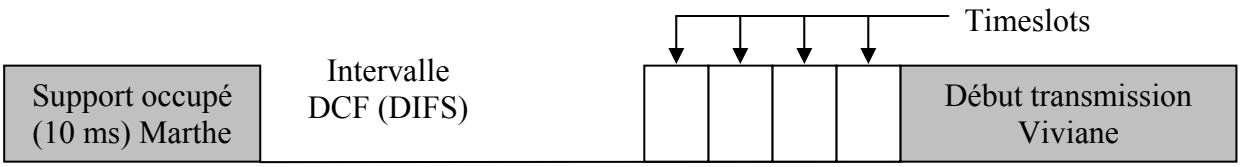
L'algorithme de backoff sous-jacent sélectionne aléatoirement une valeur comprise entre 0 et la valeur courante de la fenêtre de contention, ou CW (Contention Windows). Les valeurs minimale et maximale par défaut de cette fenêtre varient selon les fabriquants et sont stockées sur la carte réseau de la station. La limite inférieure de la plage des valeurs de backoff est de 0 timeslot. Sa limite supérieure peut aller de CW_{min} à CW_{max} . Imaginons ici que CW_{min} = 7 et CW_{max} = 255.



La valeur aléatoire choisie par l'algorithme de backoff correspond au nombre de timeslots d'inactivité du support durant lesquels la station doit attendre avant de transmettre. Le timeslot est une valeur dérivée de la couche PHY et se fonde sur les caractéristiques radio du BSS.

Revenons maintenant à notre exemple avec Viviane qui est prête à transmettre. Son temporisateur NAV a atteint 0, et sa couche PHY indique que le support est libre. Viviane, ou plutôt sa station sélectionne, une valeur de backoff situé entre 0 et la CW courante, qui est ici de 7, puis patiente pendant le nombre de timeslots choisi avant d'émettre.

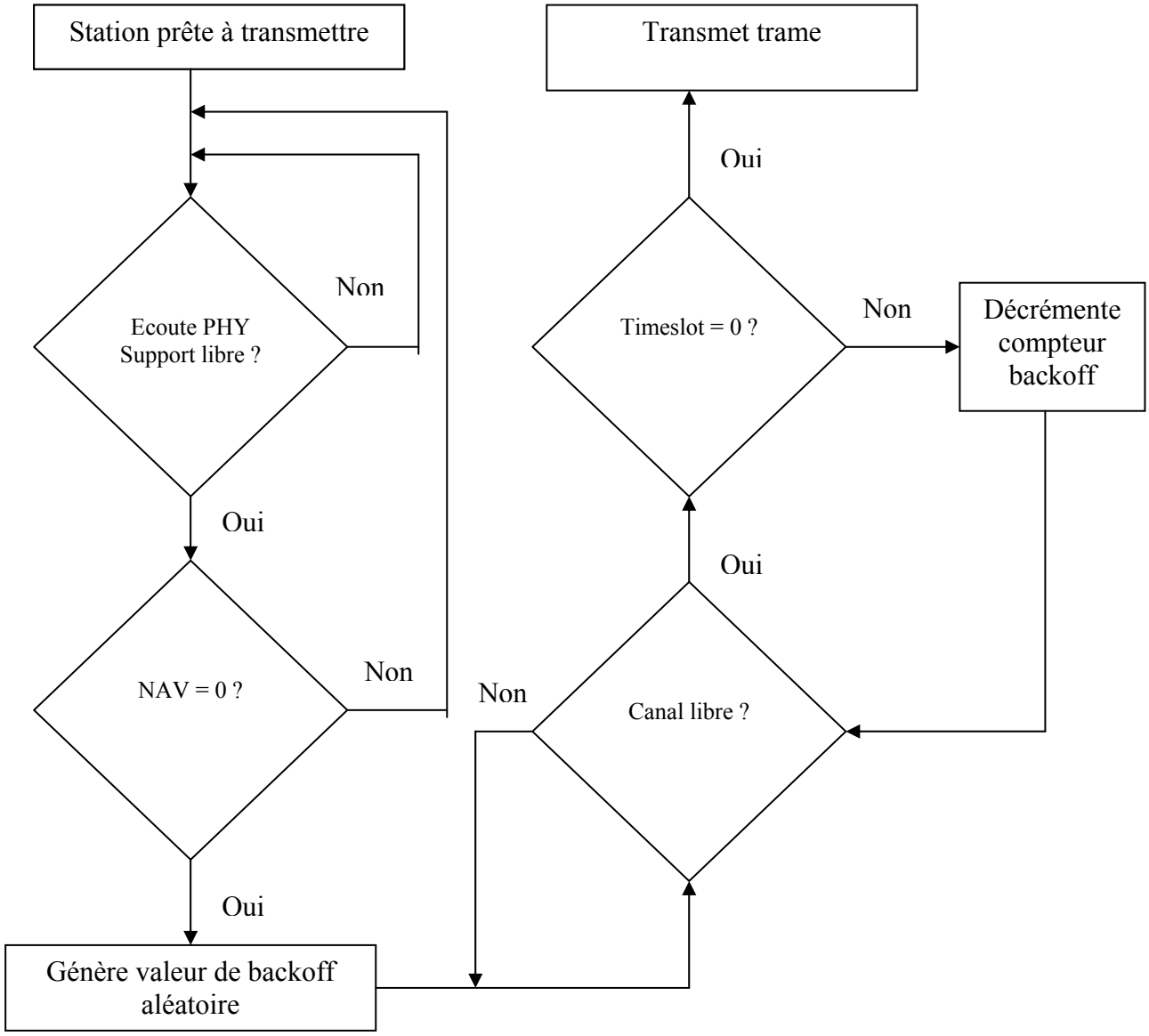
Ci-dessous, voici un exemple avec un temporisateur de backoff de 4 timeslots.



Une fois que les quatre timeslots se sont écoulés, Viviane peut envoyer ses données. Mais que se passe t-il si Georges possède un temporisateur de backoff de deux timeslots au moment où Viviane a encore ses quatre timeslots ? Viviane détecte en ce cas une nouvelle durée dans la trame émise par Georges et met à jour son NAV en conséquence. Elle doit alors attendre que son NAV atteigne 0 et que sa couche PHY signale un support libre d'accès avant de reprendre la décrémentation de son temporisateur de backoff là où elle l'a laissé. Cela revient à dire qu'elle patiente pendant encore deux timeslots.

Comment Viviane peut-elle savoir si sa trame est arrivée à destination ? Conformément aux spécifications 802.11, la station réceptrice envoie une trame d'acquittement à l'émetteur. Si ce dernier ne reçoit pas de trame d'acquittement, il en déduit qu'une collision s'est produite sur le support. Il réinitialise alors son compteur de retransmission, double la CW et entame à nouveau le processus d'accès.

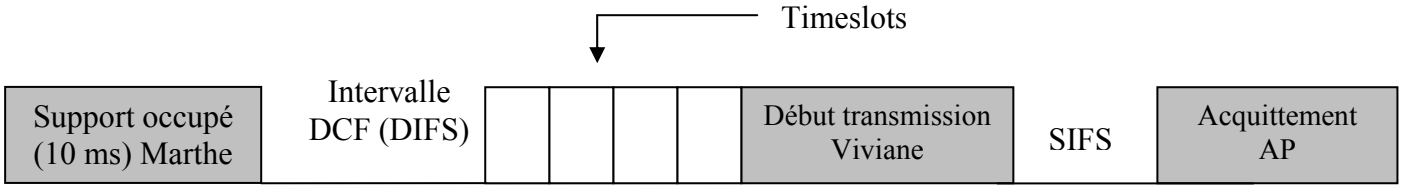
Voici le processus d'accès au support avec DCF.



7.4. Les Trames d'acquittement :

Une station qui reçoit une trame, exempte d'erreur en accuse réception en renvoyant une trame d'acquittement à l'émetteur. Puisqu'elle doit accéder au support pour cela, on peut imaginer que l'acquittement ait du retard en raison de contention avec les autres stations. La transmission des trames d'acquittement est un cas particulier. Ces trames peuvent passer outre le processus de backoff et n'attendre qu'un bref intervalle, appelé SIFS (Short Inter-Frame Space), avant d'être envoyées. Plus court que l'intervalle DIFS de deux timelots, cet intervalle offre à la station réceptrice toutes les chances de pouvoir accuser réception d'une trame reçue avant qu'une autre station n'occupe le support.

Si nous revenons à notre cas, au moment ou Viviane dispose d'un temporisateur de backoff de quatre timeslots. A expiration de son temporisateur, et si le support est libre, elle envoie une trame à Geoges. L'AP reçoit la trame et patiente le temps d'un intervalle SIFS avant d'envoyer une trame d'acquitement à Viviane.



Si Viviane ne reçoit pas l'acquittement, elle double la CW, l'amenant à 15, et recommence le processus de backoff. Pour chaque tentative d'accès qui échoue, elle incrémente un compteur de retransmission. La CW continue à doubler jusqu'à atteindre CW_{max}. La sous-couche MAC peut continuer à essayer de transmettre la trame, mais une fois que le compteur de retransmission a atteint un seuil défini par l'administrateur, Viviane tente de réserver le support.

7.5. Le Problème de nœud caché et les trames RTS/CTS :

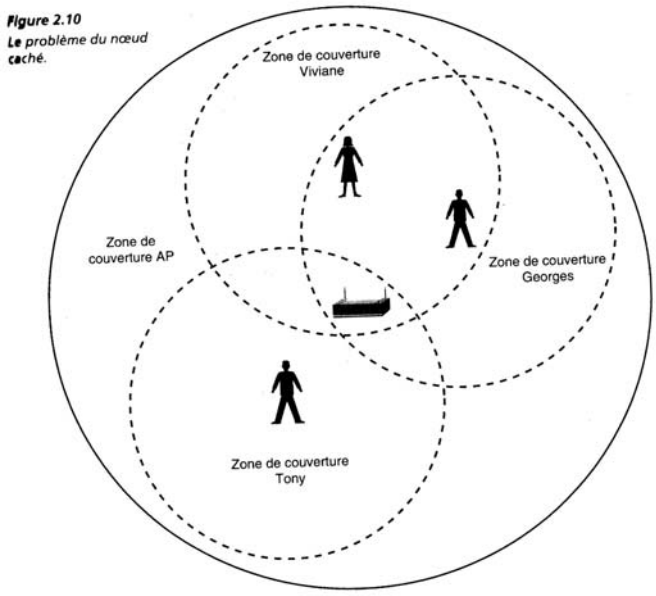
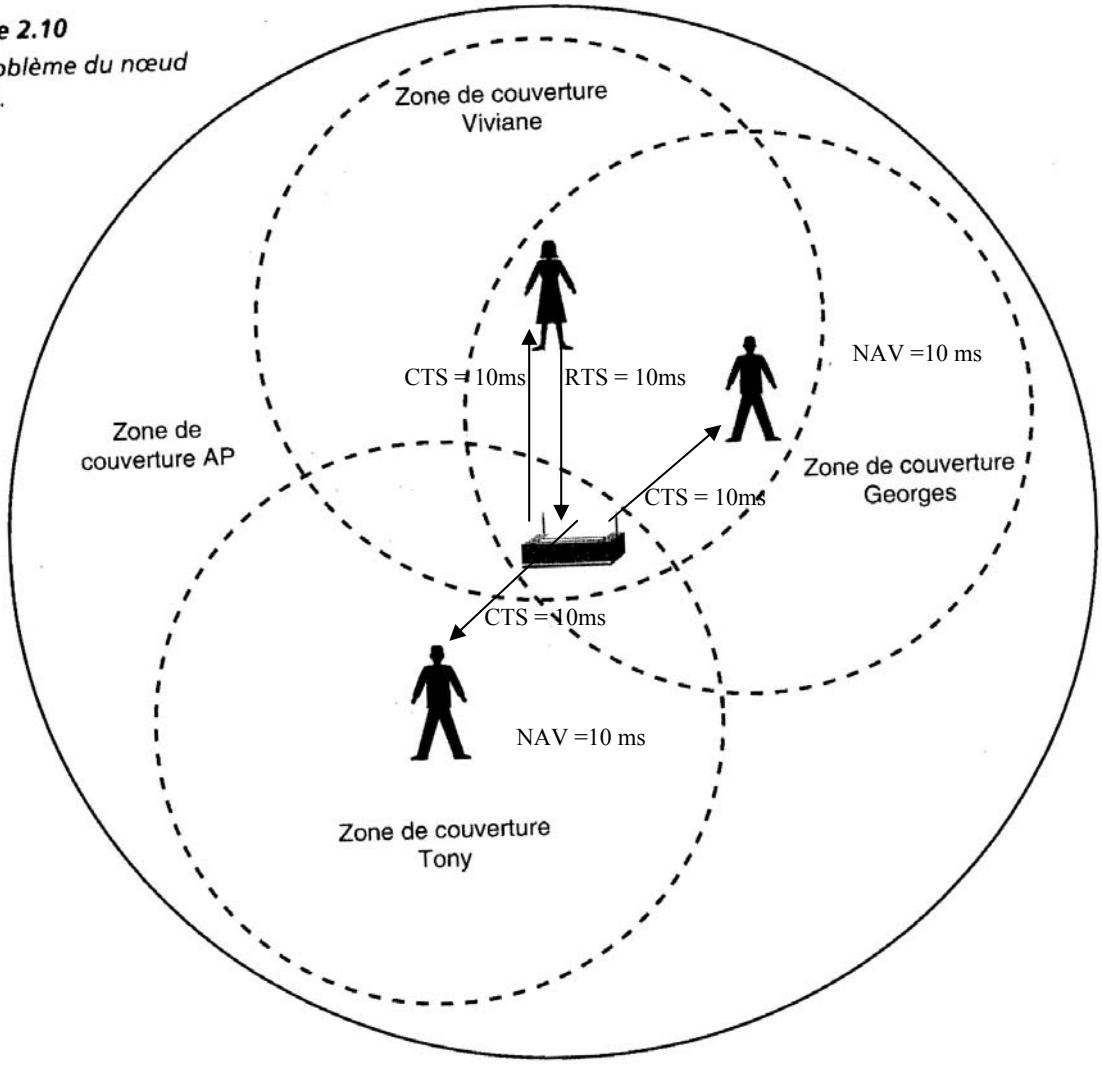


Figure 2.10
Le problème du nœud caché.

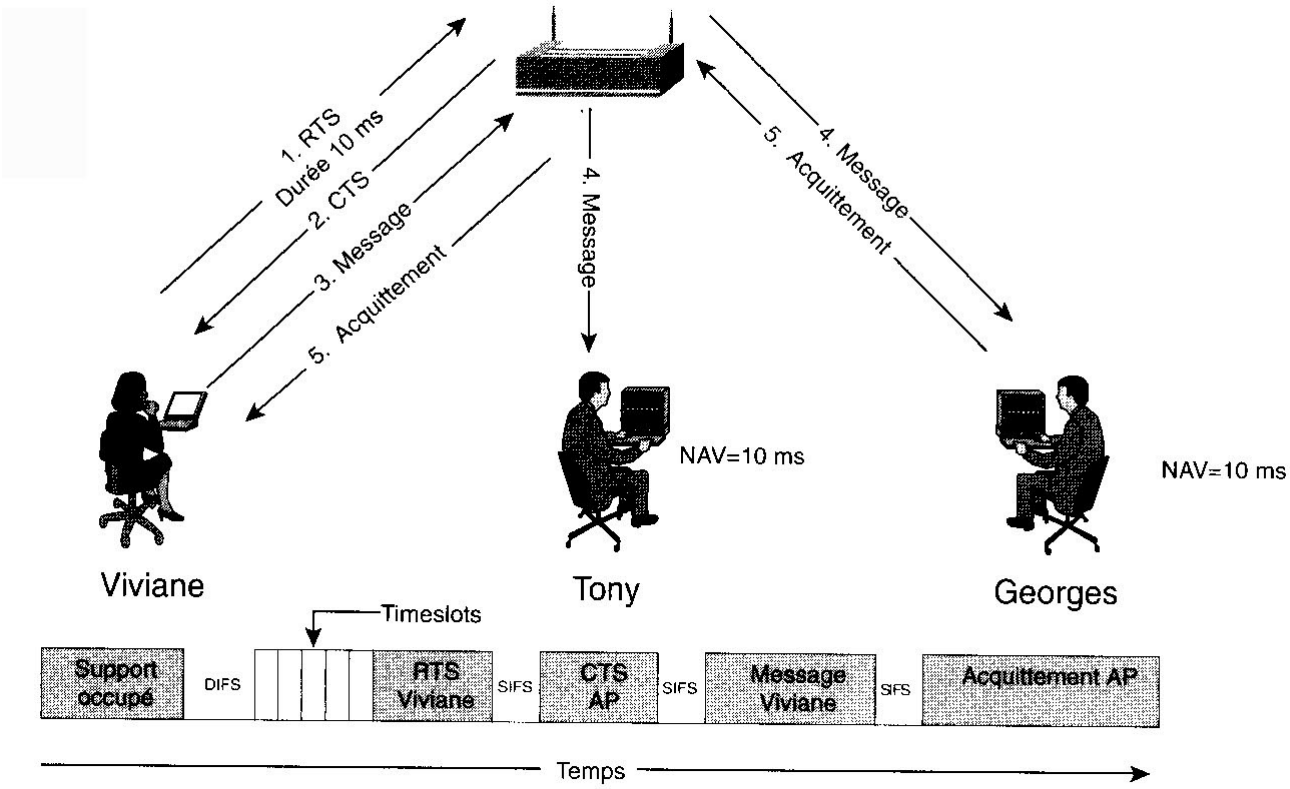
Il se peut que Viviane ne parvienne pas à transmettre en raison d'une autre station qui se trouve dans la zone de couverture de l'AP mais pas dans la sienne propre, comme illustré à la figure 2.10.Viviane et Georges se trouvent chacun dans la zone de couverture de l'autre ainsi que dans celle de l'AP, mais pas dans celle de Tony. Ce dernier se trouve lui aussi dans la zone de couverture de l'AP et tente de transmettre. On se trouve ici dans la situation dite du nœud caché (hidden node) car Tony n'est visible ni de Viviane ni de Georges.

Pour réserver le support, Viviane utilise une trame de contrôle spéciale, appelée RTS (Request To Send), qui correspond en fait à une demande d'émission. Cette trame est envoyée à l'AP pour lui indiquer, ainsi qu'à toutes les stations qui se trouvent dans sa zone de couverture, la durée escomptée de l'échange de trames de Viviane, ce qui inclut la trame initiale et celle d'acquittement.
Lorsqu'il reçoit la trame RTS de Viviane, l'AP répond par une trame de contrôle nommée CTS (Clear To Send), c'est-à-dire une autorisation à émettre. Cette trame contient une valeur de durée suffisamment longue pour permettre l'échange de Viviane. Toutes les stations qui se trouvent dans la zone de couverture de l'AP, ici Tony et Georges, reçoivent également la trame CTS et mettent à jour leur NAV, comme illustré à la figure ci-dessous.

Figure 2.10
Le problème du nœud caché.



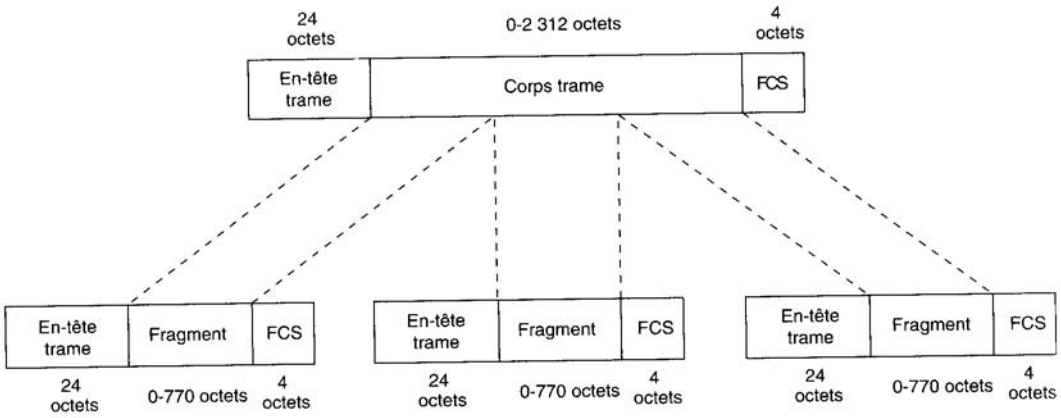
La trame RTS de Viviane doit passer par le processus DCF, comme n'importe quelle autre trame. En revanche, à l'instar d'une trame d'acquitement, la trame CTS correspondante de l'AP échappe à ce processus et doit seulement attendre un intervalle SIFS pour être transmise.



Lorsque Georges reçoit la trame de Viviane via l'AP, il envoie immédiatement un acquittement. Bien que son NAV soit différent de zéro, puisqu'il l'a précédemment mis à jour à réception de la trame CTS, il faut seulement attendre un intervalle SIFS.

7.6. Fragmentation des trames :

La fragmentation des trames est une fonction de la sous-couche MAC qui vise à augmenter la fiabilité des transmissions sur le support sans fil. Elle consiste à décomposer chaque trame en fragments de taille plus petite, qui sont envoyés individuellement (voir figure ci-dessous). Le principe étant qu'un petit fragment a davantage de chances d'être transmis correctement dans ce milieu hostile. Chaque fragment donne lieu à un acquittement. En conséquence, si l'un deux subit une altération ou une collision, seul ce fragment doit être retransmis, et non la trame entière, ce qui permet d'accroître le début utile du support.



Sur certains AP professionnels comme CISCO Systems, la taille des fragments peut être définie par l'administrateur réseau. La fragmentation s'applique uniquement aux trames unicast, épargnant de ce fait les trames broadcast et multicast. En outre les fragments d'une trame sont envoyés en rafale lors d'une même itération du processus d'accès DCF.
Si elle améliore la fiabilité, la fragmentation contribue en contrepartie à augmenter la surcharge du service (overhead) du protocole MAC 802.11. En effet, chaque fragment inclut les informations d'en-tête 802.11 et requiert une trame d'acquittement, faisant chuter le débit effectif de la station sans fil. La fragmentation est donc une fonction à double tranchant.

7.7. La fonction PCF

La fonction de coordination par AP, ou PCF (Point Coordination Function), est un mécanisme d'accès optionnel utilisé en plus de DCF, qui vise à assurer une livraison sans contention des trames via l'AP. La plupart des fabricants d'équipements ne l'implémentent pas car elle augmente la surcharge de service du protocole sur le BSS. Les améliorations qui sont prévues pour la qualité de service (QOS) de 802.11 s'appuient sur PCF.

Nous allons décrire le mode opératoire de cette fonction, qui implique un coordinateur, ou PC (Point Coordinateur), et des stations PCF, appelées stations CF-Pollable dans les spécifications 802.11.

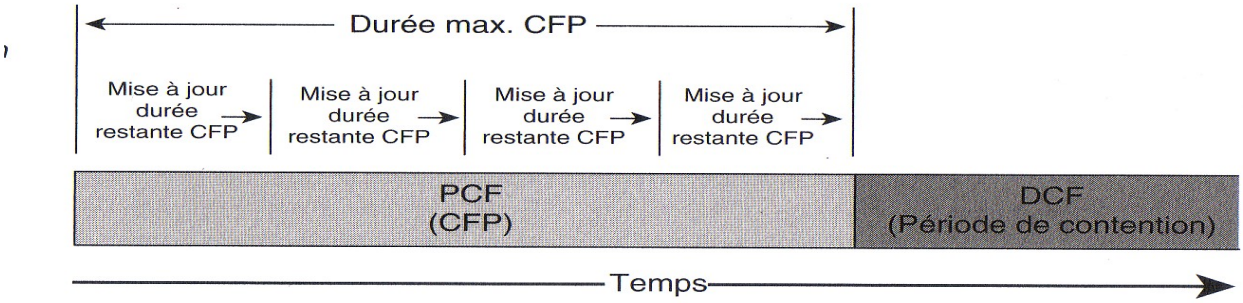
7.7.1. La fenêtre CFP

La période sans contention, ou CFP (Contention Free Period), est la fenêtre pendant laquelle opère PCF. Elle débute à intervalles réguliers, faisant suite à une trame beacon contenant un élément d'information, ou IE (Information Element), appelé DTIM (Delivery Traffic Indication Map). Sa fréquence est déterminée par l'administrateur réseau.

Au début d'une période CFP, l'AP prend le rôle de coordinateur (PC). PCF ne peut donc être utilisé que dans un BSS d'infracstructure. Chaque client 802.11 définit son NAV avec la valeur Durée maximale CFP (CFP MaxDuration), laquelle est incluse dans l'IE Jeu de paramètres CF (CF Parameter Set), décrit plus loin. Cette valeur indique la durée maximale de la fenêtre CFP, mais le PC peut y mettre fin avant. L'AP transmet des rames beacon à intervalles réguliers. Les trames beacon envoyées pendant la période CFP contiennent un

champ Mise à jour durée restante CFP (CFP DurationRemaining), qui sert à mettre à jour le NAV des stations avec la durée restante de la période.

Voici ce processus :

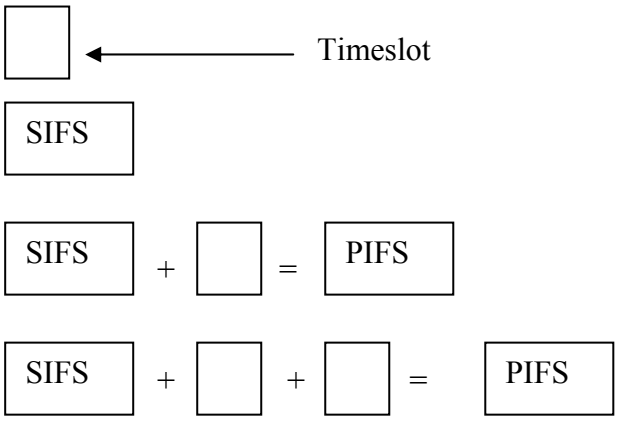


Contrairement à DCF, PCF n'autorise pas les stations à accéder librement au support et à envoyer des données. Les stations peuvent transmettre (une trame à la fois) uniquement lorsqu'elles y sont invitées par le PC au moyen d'une trame de polling. Ce dernier peut envoyer des trames de données aux stations, les inviter à transmettre, accuser réception de trames nécessitant un acquittement de niveau MAC et terminer la période CFP.

Fonctionnement du PC

Lorsque la CFP débute, le PC doit accéder au support de la même manière qu'une station DCF, à cette différence près qu'il doit seulement patienter le temps d'un intervalle appelé PIFS (PCF Inter-Frame Space). Cet intervalle est supérieur d'un timeslot au SIFS et inférieur d'un timeslot au DIFS, permettant aux stations PCF d'accéder au support avant les stations DCF, tout en autorisant les trames de contrôle, comme celles d'acquittement, à avoir la plus grande chance d'être transmise.

Illustration entre tous ces intervalles et un timeslot.



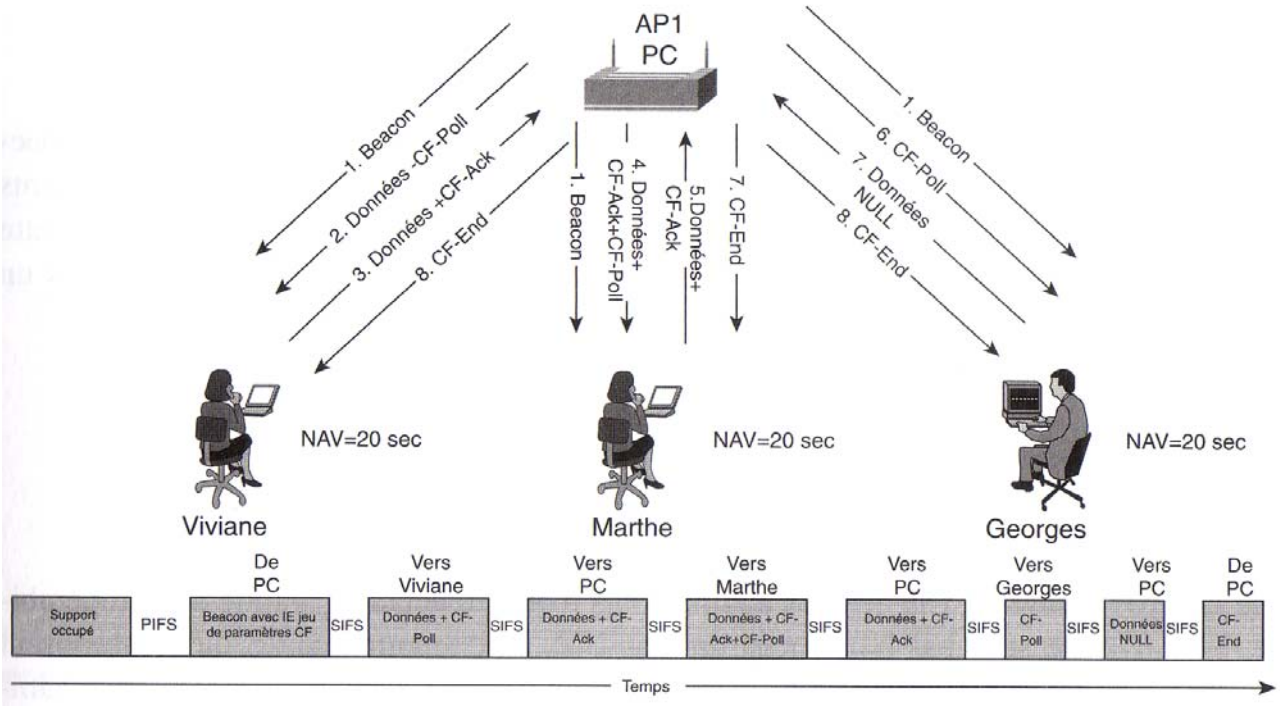
A l'issue d'un intervalle PIFS, le PC envoie la trame beacon initiale contenant l'IE Jeu de paramètre CF. Il attend un autre intervalle PIFS puis envoie une des trames suivantes à une station CF-Pollable :

- Trame de données ;

- Trame de polling (CF-Poll) ;
- Trame combinant données et polling (Data+CF-Poll) ;
- Trame de fin de CFP (CF-End).

Si le PC n'a pas de trame à envoyer et qu'il n'y ait pas de station CF-Pollable, la CFP est considérée comme étant nulle. Immédiatement après la trame beacon, le PC envoie une trame CF-End pour fermer la fenêtre CFP.

Exemple de fonctionnement de PCF :



AP1 envoie une trame beacon indiquant le début d'une CFP. Cette fenêtre est configurée pour durée vingt secondes. Viviane, Marthe et Georges mettent à jour leur NAV pour refléter cette durée. A l'issue d'un intervalle SIFS, AP1 transmet à Viviane une trame qu'il conservait en tampon à son attention ainsi qu'une trame Data+CF-Poll pour lui permettre d'envoyer des données. A réception de cette dernière, Viviane émet une trame de données et une trame d'acquittement sans contention combinées (Data+CF-Ack) après un intervalle SIFS. Notez que Viviane ignore alors son NAV.

AP1 examine sa liste de polling et en arrive à Marthe. Il utilise une trame combinée (Data+CF-Ack+CF-Poll) pour lui envoyer des données, accuser réception de la trame de Viviane et inviter Marthe à transmettre. Bien que destinée à Marthe, cette trame combinée permet d'accuser réception de la dernière trame de Viviane du fait de la nature partagée de l'accès au support 802.11. Marthe attend un intervalle SIFS et envoie une trame Data+CF-Ack.

Ap1 passe ensuite à Georges. Il n'a pas de trame de données pour lui en tampon et lui envoie donc seulement une trame CF-Poll. Georges n'a pas non plus de trame à envoyer et répond par une trame sans données. Bien que la période CFP ne touche pas encore à sa fin, AP1 émet une trame CF-End pour la terminer et repasser dans le mode normal d'accès au support. C'est-

à-dire DCF. Lorsqu'il reçoivent la trame CF-End, Viviane, Marthe et Georges mettent à jour leur NAV.

8. Les technologies de la couche physique 802.11

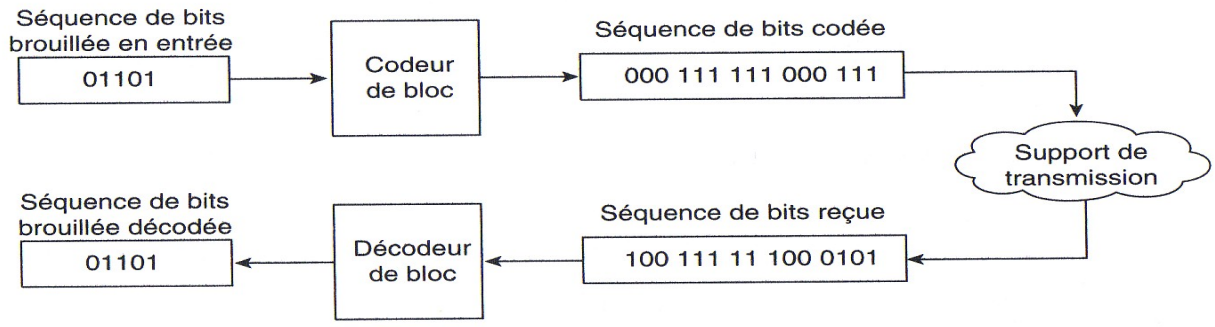
8.1. Principes de base de la transmission du signal :

Le brouillage :

Si les émetteurs modernes sont capables de transmettre des données à haut débit c'est parce que leur conception se fonde en grande partie sur l'hypothèse que les données qui leur sont fournies sont aléatoires. Toutefois il est concevable et même fréquent que les données à transmettre ne soient pas du tout aléatoires, pouvant même contenir des motifs récurrents ou de longues séries de 0 ou de 1. Le brouillage (scrambling) désigne la technique utilisée pour transformer des séquences de bits structurées à émettre en séquences paraissant aléatoires. On parle aussi de blanchiment (whitening) du flux de données. Le récepteur accomplit le processus inverse pour rétablir la structure originale des séquences. La plupart des techniques de blanchiment permettent au processus de débrouillage (descrambling) de se synchroniser sur celui de brouillage.

Le codage :

Si le brouillage a permis aux ingénieurs de développer des systèmes de communication dotés d'une plus grande efficacité spectrale, c'est la technique du codage (coding) qui a rendu possible la transmission de données à haut débit sur des canaux bruités. Tous les canaux comportent du bruit, ce qui introduit des erreurs sous la forme de bits corrompus ou modifiés. Le codage permet de maximiser la quantité de données envoyées sur un support bruité. Dans son principe, il consiste à remplacer des séquences de bits altérés. Prenons l'exemple illustré ci-dessous :

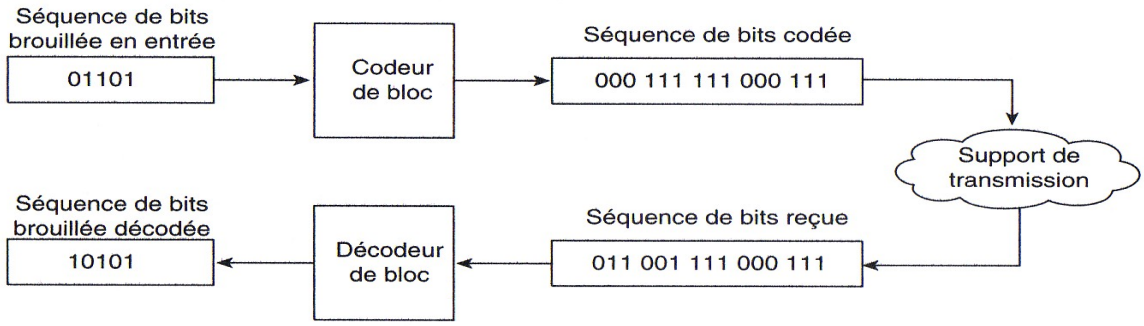


Supposons que vous vouliez communiquer la séquence 01101 par téléphone à un ami. Vous pouvez vous mettre d'accord pour répéter chaque bit trois fois, ce qui donne la séquence 000111111000111. Même si votre ami n'entend pas bien la séquence originale 01101 d'après

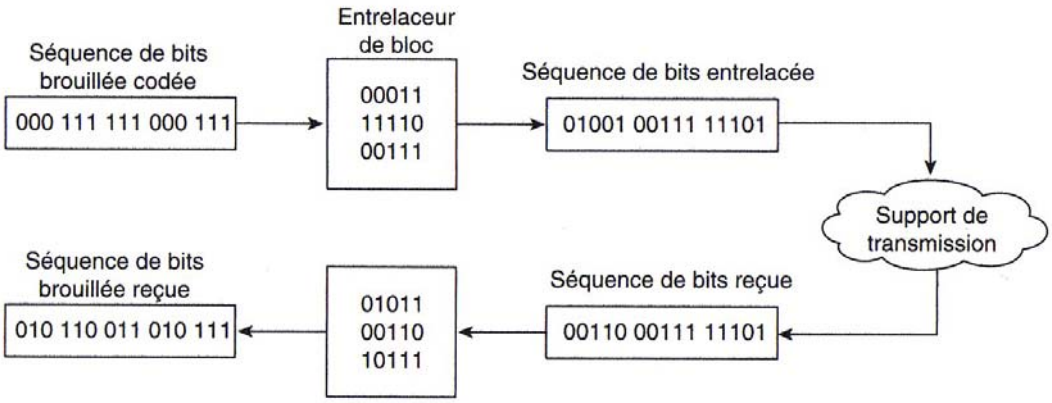
les bits majoritaires. Ce codeur a beau être très simple et manquer d'efficacité, il permet néanmoins de saisir le principe du codage.
Le type de codage le plus courant aujourd'hui dans les systèmes de communication est le codage convolutif. Il peut être implémenté assez facilement sur le plan matériel au moyen de registres à décalage et additionneurs. Contrairement à l'exemple précédent, qui illustre un codage en blocs sans mémoire (memory-less block code), le codage convolutif opère avec mémoire (finite memory code). Cela signifie que le résultat n'est pas seulement une fonction de la dernière entré mais aussi de plusieurs entrées précédentes. La longueur de contrainte (contraint length) désigne la « longueur » du codeur, c'est-à-dire le nombre d'états disponibles en entrés pour alimenter sa logique combinatoire, qui produit les symboles en sortie. Les codeurs sont souvent décrits par leur taux, ou rendement. Par exemple, dans un codeur convolutif de taux ½, à chaque bit en entrée sont produits deux bits en sortie. Lorsque vous comparez des codeurs, sachez qu'un taux supérieur signifie un débit de donnée supérieur mais également une sensibilité accrue au bruit.

L'entrelacement :

Une des hypothèses élémentaires du codage est que les erreurs introduites lors de la transmission sont des événements indépendants. C'est le cas dans l'exemple précédent, où les bits 1 et 14 de la séquence communiquée sont corrompus. Les erreurs de bits sont rarement indépendantes et se produisent en série. Toujours dans l'exemple précédent, imaginez qu'un camion passe à proximité pendant la première partie de la conversation, empêchant votre ami de vous entendre distinctement. En supposant qu'il reçoive la séquence 011001111000111, comme illustré à la figure ci-dessous, il en conclut que la séquence d'origine est 10101, ce qui est erroné.



Pour cette raison, les entrelaceurs (interleaver) ont été introduits afin de disperser les bits d'erreur de blocs de sorte qu'ils aient l'air plus indépendants. Un entrelaceur peut être implémenté de façon logicielle ou matérielle. Dans les deux cas, sa fonction principale est de dispenser les bits adjacents en plaçant entre eux des bits non adjacents. Dans notre exemple, au lieu de lire simplement la séquence de 15 bits à votre ami, vous pourriez placer les bits dans une matrice, cinq par ligne, puis les lire par colonne, donc trois à la fois, comme illustré à la figure ci-dessous. Votre ami les écrirait dans une matrice par colonne trois à la fois puis les lirait par ligne cinq à la fois et appliquerait ensuite la règle de codage pour extraire la séquence d'origine.



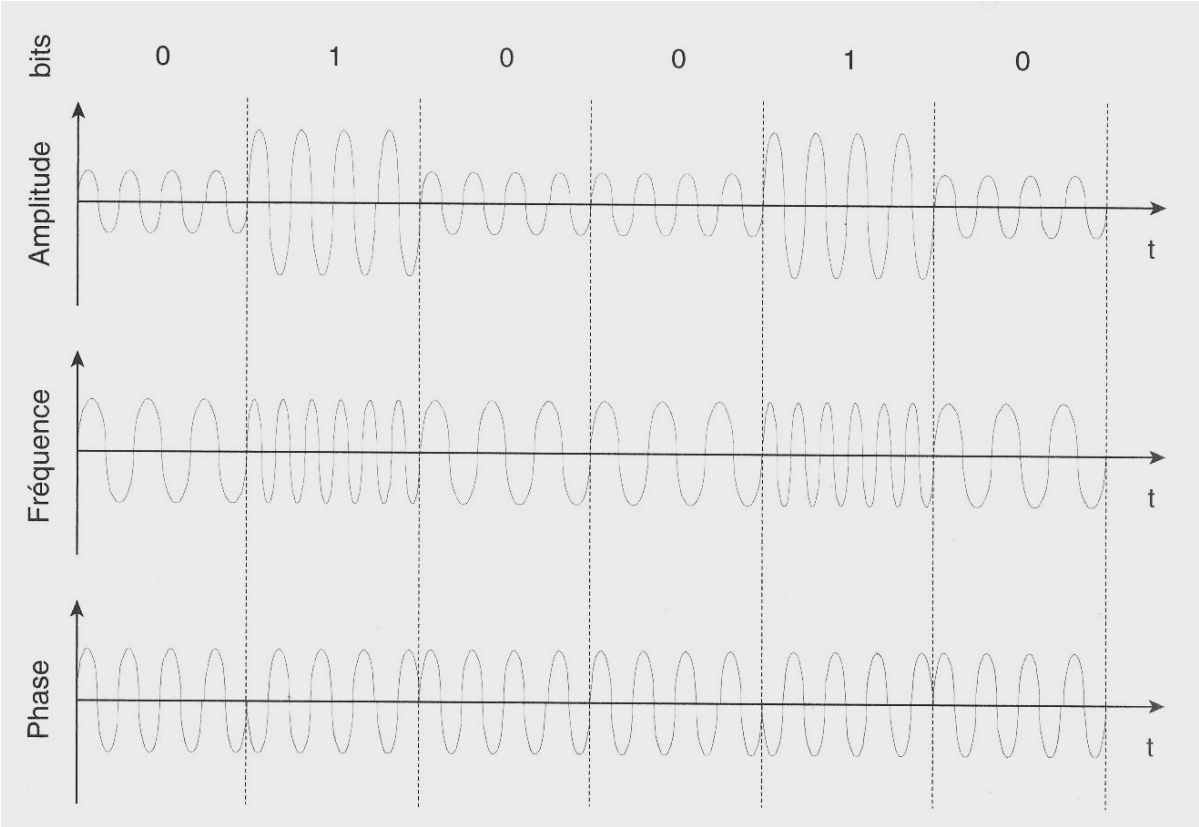
Le mapping bits/symboles et la modulation :

Le processus de modulation applique le flux de bits à une porteuse dans la bande de fréquences utilisée. Si vous vous représentez la porteuse (carrier) comme une onde sinusoïdale, le processus de modulation peut porter sur l'amplitude, la fréquence ou la phase, comme le montre la figure ci-dessous.

8.2. L'émission radio FM :

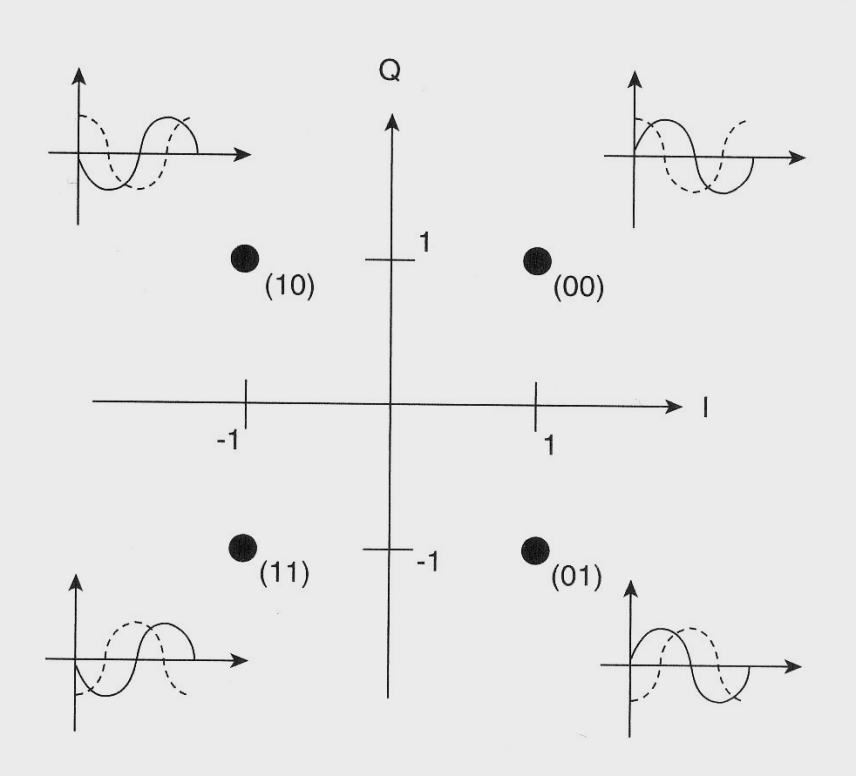
Nous avons vu précédemment que les données sont modulées en fréquence sur une porteuse qui peut avoir une fréquence différente suivant la norme utilisée, le canal utilisé et le pays.

Pour transmettre des bits en modulation sur une porteuse on peut utilisé trois façons différentes, en utilisant la modulation d'amplitude (AM), la modulation de fréquence (FM) ou une modulation de phase.



Comme le WIFI utilise la modulation de fréquence, pour transmettre les bits, il va utiliser deux signaux qu'il va déphasé pour créer un codage de deux bits, c'est le regroupement en symbole qui se nomme également mapping bits/symboles (symbol mapping).
Cette technique de modulation est appelée QPSK (Quadrature Phase Shift Keying), qui consiste à combiner deux bits en un symbole.

Sur le schéma ci-dessous, le signal en phase apparaît en trait plein et celui en quadrature en pointillés.



Mais aujourd'hui avec l'augmentation des débits, il existe d'autre forme de codage qui sont également basé sur le principe de la modulation QPSK mais beaucoup plus compliqué du fait que l'on envoi plus de bits, je ne traiterai pas ces genres de modulation qui font appels à des connaissances poussé en mathématique et physique.

8.3. Les problèmes des ondes radios :

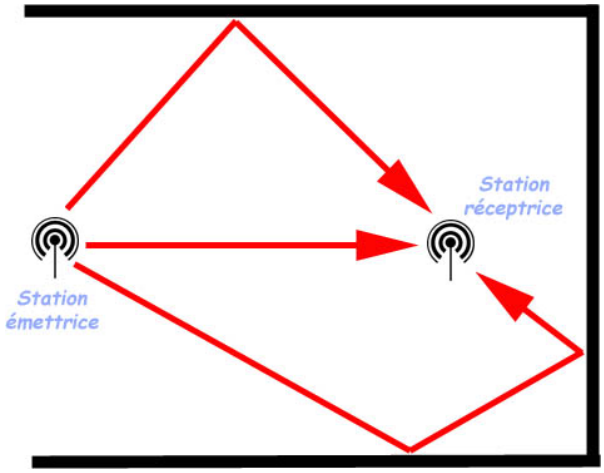
Dans notre quotidien nous sommes entourés d'ondes radios, par exemple dans nos maison, l'antenne TV, les téléphones cellulaires, les radios musicales (AM et FM), …….
Or cela peut provoqué différents problèmes techniques comme des parasites pouvant perturbés le signal WIFI, mais aussi les rebonds du signal l'émission d'ondes radio est omnidirectionnelle, les ondes partent dans tous les sens, et rebondissent en parties sur tous les obstacles qu'elles rencontrent, en particuliers, à nos domiciles, murs, cloison et ameublement, ce qui, suivant le type d'obstacle rencontré affaiblie ou stoppé le signal, ainsi que les fréquences utilisées sont si importantes que le signal s'affaiblit très vite en fonction de la distance entre 2 appareils.

Voici le comportement des ondes radios.

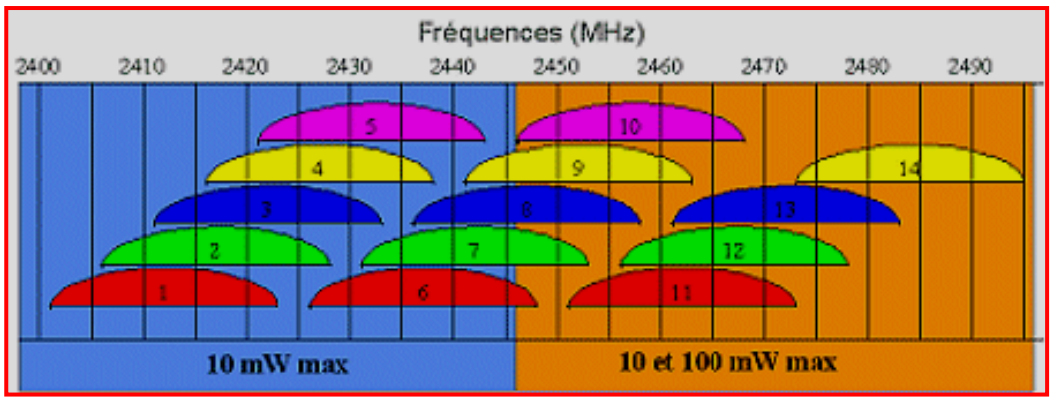
Nous remarquerons que les ondes peuvent empruntées différents chemins pour arriver au récepteur, les ondes sont totalement instables.

Les contraintes techniques :

- Les parasites pouvant perturbés le signal.
- Les rebonds, L'émission d'ondes radio est omnidirectionnelle : les ondes partent dans tous les sens, et rebondissent en parties sur tous les obstacles qu'elles rencontrent, en particuliers, à nos domiciles, murs, cloison et ameublement.
- La distance : les fréquences utilisées sont si importantes que le signal s'affaiblit très vite en fonction de la distance entre 2 appareils.



Canaux et fréquences :



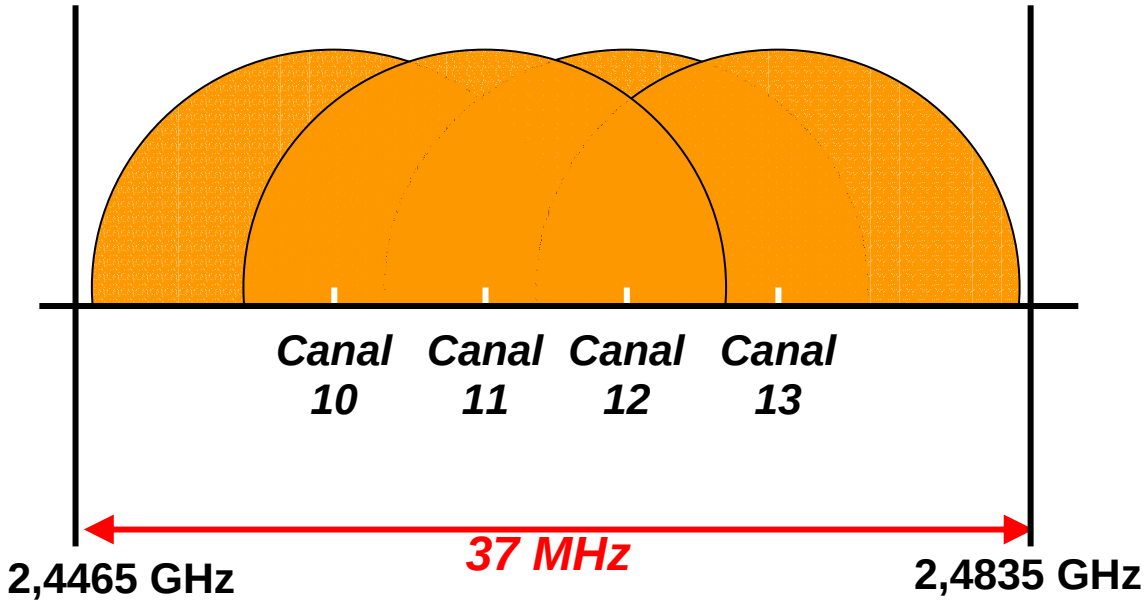
Canal	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Fréquence (GHz)	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462	2.467	2.472	2.484

Le standard 802.11b à une bande de fréquence qui s'étend de *2.400-2.4835 GHz* (d'une largeur de 83.5 MHz) a été découpé en 14 canaux séparés de 5MHz.

- Les 11 premiers sont utilisables aux Etats-Unis.

- **Seuls les canaux 10 à 13 sont utilisables en France.**

Pays	Etats-Unis	Europe	Japon	France
Nombres de sous canaux utilisés	1 à 11	1 à 13	14	10 à 13



Pays	Bandes de fréquences
Etats-Unis *FCC*	2,400 – 2,485 GHz
Europe *ETSI*	2,400 – 2,4835 GHz
Japon *MKK*	2,471 – 2,497 GHz
France *ART*	2,4465 – 2,4835 GHz

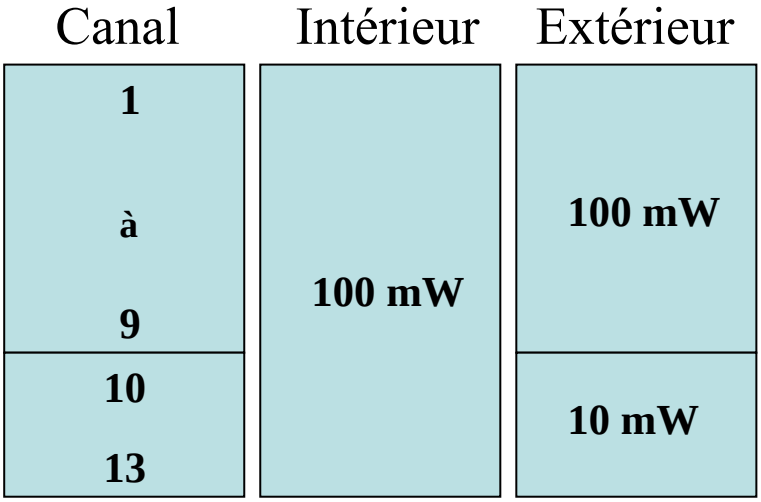
Les normes :

Norme	Débit max (en Mbits/s)	Fréquence utilisée
802,11a	54	5,15/5,35 GHz et 5,725/5,825GHz
802,11b	11	2,400/2,4835 GHz
802,11b+	22	2,400/2,4835 GHz
802,11g	54	2,400/2,4835 GHz
802,11g+	108	2,400/2,4835 GHz

La France ne peut utilisé que les normes b, b+, g et g+

Puissances autorisées (PIRE)

PIRE = (Puissance Isotrope Rayonnée Effective), mesure indiquant la puissance réelle rayonnée par une antenne.



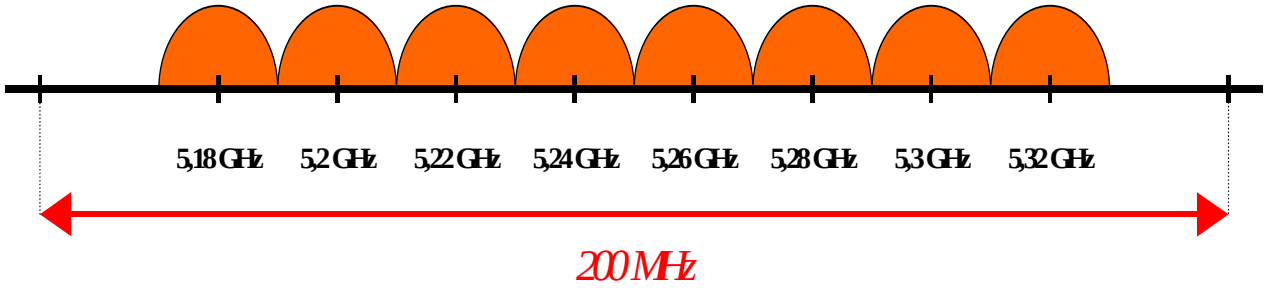
Norme b et g

Débit théorique	Portée (en intérieur)	Portée (à l'extérieur)
54 Mbits/s	27 m	75 m
48 Mbits/s	29 m	100 m
36 Mbits/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m
6 Mbit/s	90 m	400 m

La norme 802.11a (ou WIFI 5)vient d'apparaître, c'est une norme qui prévoit 54 Mbits/s théorique donc 30 Mbits/s réel, cette nouvelle norme fonctionne avec des fréquences tournants autour des 5 Ghz, ce qui pose de gros problème car cette norme n'est absolument pas compatible avec le matériel actuel (fonctionnant sur des fréquences tournant autour des 2,4 Ghz), de plus les matériels compatibles avec cette norme sont beaucoup plus chers, du fait du prix élevé des nouvelles « puces » utilisées.

Voici une petite explication de cette nouvelle norme :

- **Bande UN-II (5 GHZ)**
- **Bande divisée en 8 canaux de 20 MHz**
- **Pas de problème de recouvrement (atténuation du bruit)**
- **Co-localisation de 8 réseaux au sein d'un même espace**
- **Largeur de bande 200 MHZ**



Canal	36	40	44	48	52	56	60	64
Fréquence (GHz)	5,18	5,20	5,22	5,24	5,26	5,28	5,30	5,32

Cette norme sera adaptée à la France, car toutes les fréquences et toutes les puissances engendrées ne pourront pas êtres utilisés.

FREQUENCE en MHZ	Intérieur	Extérieur
5150 5250	200 mW	impossible
5350	200 mW avec DFS/TPC ou equivalent ou 100 mW avec DFS uniquement	impossible
5470 5725	impossible	impossible

9. Qu'elles performances ?

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physiques) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité.

(IEEE : Institut des Ingénieurs Eletriciens & Electroniciens: Institut chargée entre autre de ratifier les différentes normes de transmission de données (ex: IEEE 1394 pour le firewire.. etc.)).

Les différentes normes du wi-fi et leurs débits.

Nom de la norme	nom	description
802.11n	NEW!	Le 802.11n se voudra au minimum deux fois plus rapide que son petit frère, le 802.11g (54 Mbit/s), en plein essor, et dix fois plus que l'historique 802.11b (11 Mbit/s). Les premières spécifications du 802.11n devraient être publiées dans le courant de l'année 2005, pour une mise au point définitive vers 2006 ou 2007. NEW!
802.11a	Wifi5	La norme 802.11a (baptisé *WiFi 5*) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.
802.11b	Wifi	La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11 Mbps (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles.
802.11c	Pontage 802.11 vers 802.1d	La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau *liaison de données*).
802.11d	Internationalisation	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11e	Amélioration de la qualité de service	La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche *liaison de données*. Ainsi cette norme a pour but de définir les besoins des différents paquets en terme de bande passante et de délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la vidéo.

802.11f	Itinérance (roaming)	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole *Inter-Access point roaming protocol* permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée *itinérance* (ou *roaming en anglais*)
802.11g		La norme 802.11g offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. La norme 802.11g à une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b
802.11h		La norme *802.11h* vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, où le *h* de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.
802.11i		La norme *802.11i* a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'*AES* (*Advanced Encryption Standard*) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11Ir		La norme *802.11r* a été élaborée de telle manière à utiliser des signaux infrarouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme *802.11j* est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

10. La sécurité

Pour prendre la mesure de la menace que fait peser sur un réseau d'entreprise le fait d'y relier des WLAN non sécurisés, il suffit d'imaginer un long câble Ethernet tiré depuis ce même réseau jusque sur le parking extérieur. Quiconque dispose d'un moyen de se raccorder au câble peut accéder au réseau.
Les équipements 802.11 communiquent entre eux en utilisant les ondes radio, ou hertziennes, comme support de données. Ces dernières sont transmises en broadcast par l'émetteur dans l'espoir que le récepteur opère dans la même plage de fréquences. L'inconvénient de cette technique de transport est que n'importe qu'elle autre station opérant dans cette plage reçoit aussi les données.
En l'absence d'un mécanisme de sécurité, toutes les stations d'un WLAN sans exception sont en mesure de traiter les données qui y sont transmises. Pour assurer une sécurité minimale, deux composants sont requis :

- Un moyen de déterminer quel utilisateur ou équipement peut exploiter le WLAN.

Cette exigence est satisfaite par des mécanismes d'authentification permettant de contrôler l'accès au réseau local.

- Un moyen de garantir la confidentialité des données.

Cette exigence est satisfaite par des algorithmes de chiffrement.

Chiffrement + Authentification = Sécurité du sans-fil

Les spécifications 802.11 définissent un algorithme de chiffrement appelé WEP (Wired Equivalent Privacy) pour assurer la confidentialité des données, ainsi que deux méthodes d'authentification, Open System Authentification et Shared Key Authentification, qui s'appuient sur cet algorithme et sur la présence de clés WEP côté point d'accès (AP) et côté client pour contrôler l'accès. Etant donnée l'importance de WEP pour la sécurité 802.11, la section suivante rappelle les principes fondamentaux du chiffrement en se concentrant sur les algorithmes utilisés dans ce contexte.

10.1. Le SSID

L'identifiant réseau, où SSID (Service Set ID), est le premier mécanisme de sécurité offert par le WEP pour le contrôle d'accès au réseau. Le SSID est le nom que l'on donne à un réseau ou à un domaine. L'expression « nom de réseau » est surtout utilisée au moment de la configuration du réseau.
Toutes les stations et tous les points d'accès appartenant à un même réseau doivent posséder ce SSID, que les stations soient en mode ad-hoc ou infracstructure. Si une ou plusieurs stations veulent entrer dans un réseau sous le contrôle d'un point d'accès, elles doivent fournir le SSID au point d'accès. La ou les stations n'accèdent au réseau que si ce SSID est correct.
Le SSID est le seul mécanisme de « sécurité » obligatoire de WI-FI.
Ceci étant dit avec le célèbre logiciel de scan de réseau WIFI « NetStumbler », le SSID est trouvé immédiatement même avec un cryptage WEP 64 ou 128 bits.
Suivant, l'infrastructure réseau sans-fil que nous possédons, le SSID se nomme :

- SSID pour une infrastructure IBSS
- **B**SSID pour une infrastructure BSS (**B** = Basic)
- **E**SSID pour une infrastructure ESS (**E** = Extented)

10.2. Rappel sur le chiffrement

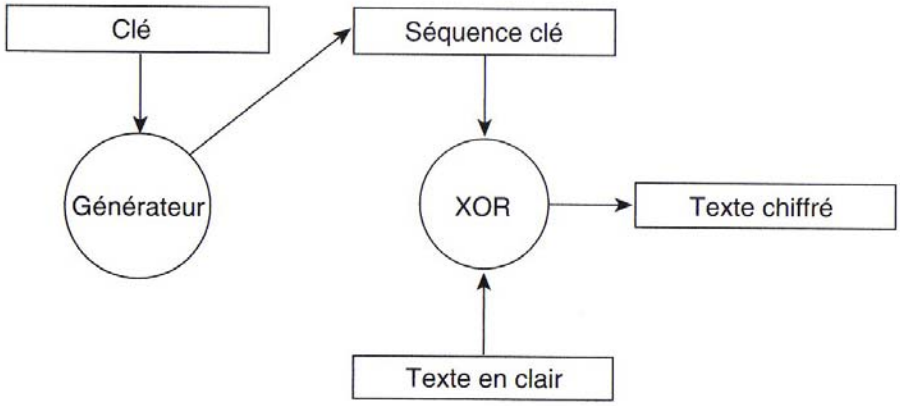
Le chiffrement repose sur l'emploi d'algorithmes pour donner une apparence aléatoire (random) aux données. On distingue deux catégories d'algorithmes de chiffrement :

- Algorithme de chiffrement par flot
- Algorithmes de chiffrement par bloc

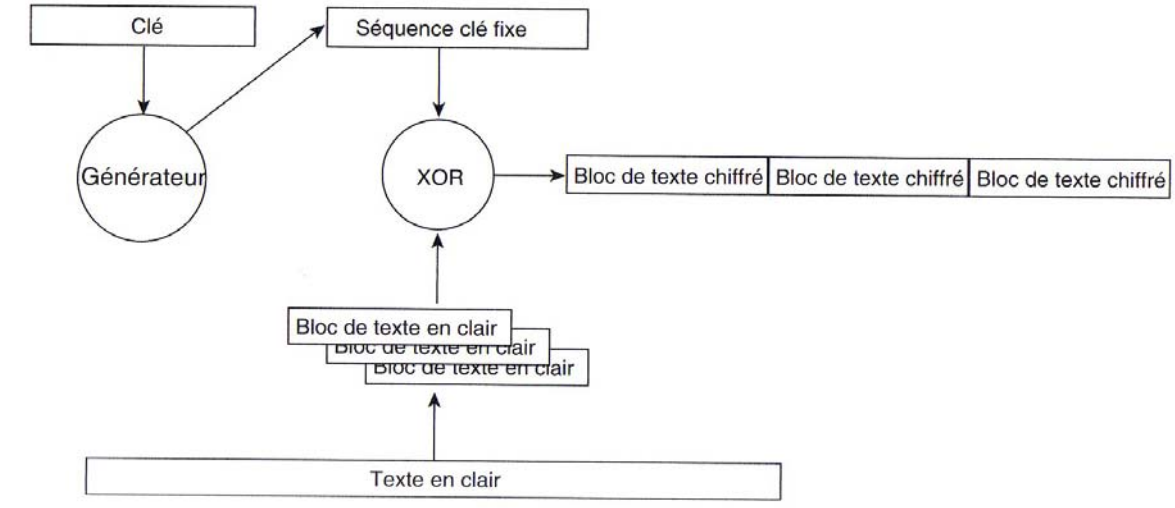
Ces deux types d'algorithmes opèrent en générant une séquence clé (key stream) à partir d'une valeur de clé secrète. Cette séquence clé est ensuite appliquée aux données, ou texte en clair (plaintext), pour produire un résultat chiffré, ou texte chiffré (ciphertext).

La principale différence entre les deux types d'algorithmes réside dans la longueur des données qu'ils traitent. Un algorithme de chiffrement par flot (stream cipher) génère une séquence clé pseudo-aléatoire continue à partir d'une clé initiale. Par exemple, il peut produire une séquence clé de 15 octets pour crypter une trame et une séquence clé de 200

octets pour en crypter une autre. La figure ci-dessous illustre la logique du chiffrement par flot. Les algorithmes appartenant à cette catégorie sont courts et efficaces et consomment en conséquence peu de ressources processeur. WEP se fonde sur RC4, un algorithme par flot connus.



Un algorithme de chiffrement par bloc (block cipher) génère une seule séquence clé de taille fixe. Le texte en clair est fragmenté en blocs, puis la séquence clé est appliquée à chaque bloc indépendamment. Si un bloc de texte en clair est plus petit que la séquence clé, il est complété par une chaine de remplissage. La figure ci-dessous illustre la logique du chiffrement par bloc. Cette catégorie d'algorithmes sollicite davantage le processeur en raison du processus de fragmentation et d'autres aspects propres au chiffrement par bloc, réduisant le dévit effectif des équipements.



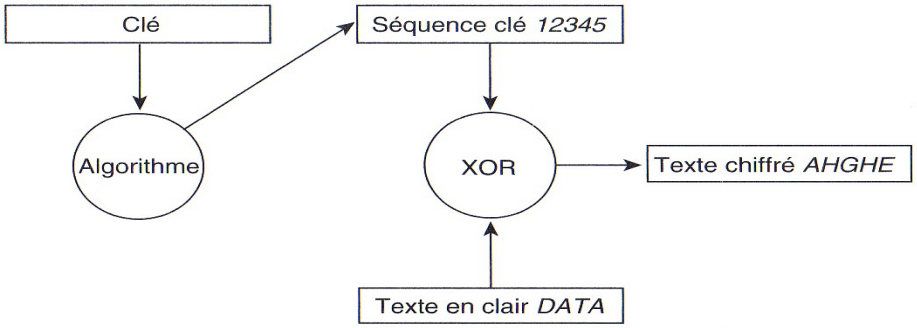
Le mode de chiffrement décrit ici pour les algorithmes par flot et par bloc est connu sous le nom d'ECB (Electronic Code Book). Il se caractérise par le fait qu'un même texte en clair en entrée donne toujours un même résultat chiffré. Cela constitue un risque potentiel pour la sécurité car une personne non autorisée pratiquant l'écoute clandestine peut identifier des séquences récurrentes dans le texte crypté et commencer à deviner le contenu d'origine.

Les techniques de chiffrement suivantes permettent d'éliminer cette vulnérabilité :

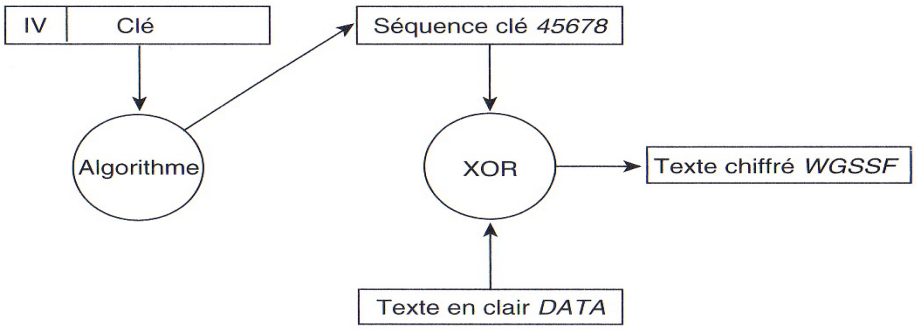
- Vecteurs d'initialisation
- Modes avec feedback

10.3. Vecteur d'initialisation

Un vecteur d'initialisation, ou IV (Initialisation Vector), est un nombre ajouté à la clé, qui vise à modifier la séquence clé obtenue. L'IV est concaténé à la clé avant de générer la séquence clé. Chaque fois que l'IV change, la séquence change également. La figure ci-dessous montre deux scénarios de chiffrement par flot, l'un sans IV et l'autre avec. Dans le premier texte en clair XXX combiné à la séquence clé 12345 donne toujours le texte chiffré AHGHE. Dans le second, le même texte en clair, combiné cette fois à une séquence clé produite à partir de la clé et d'un IV concaténé, donne un résultat chiffré différent. Le standard 802.11 recommande de changer l'IV pour chaque trame. De la sorte, si une même trame est transmise à deux reprises, sa version cryptée est chaque fois différente.



1. Chiffrement sans vecteur d'initialisation



2. Chiffrement avec un vecteur d'initialisation IV

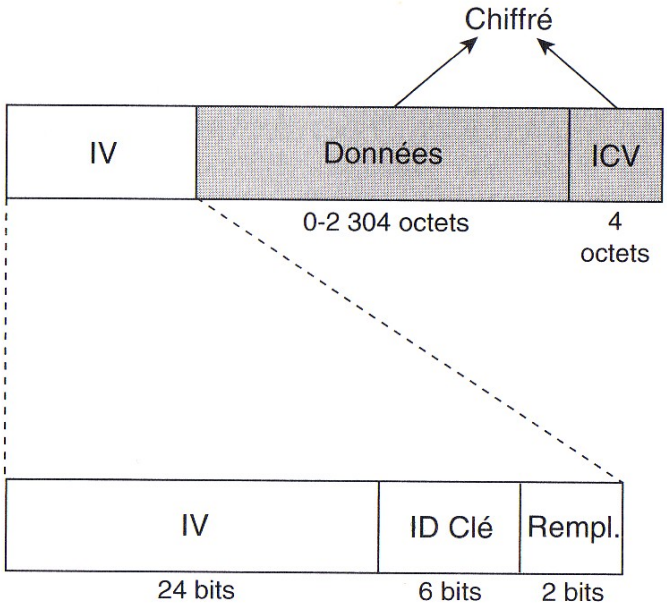
10.4. Mode avec feedback

Les modes avec feedback, parfois appelés modes de rétroaction, introduisent des changements dans le processus de chiffrement de façon à éviter d'obtenir un même texte chiffré pour un même texte en entrée. Généralement employés en conjonction avec les algorithmes de chiffrement par bloc.

10.5. Le chiffrement dans le standard 802.11

Les spécifications 802.11 prévoient l'algorithme WEP (Wired Equivalent Privacy) pour garantir la confidentialité des données échangées. Cet algorithme utilise de son côté l'algorithme de chiffrement par flot RC4. La nature symétrique de RC4 demande l'emploi de clés WEP identiques, de 40 ou 104 bits, sur les clients et les AP, ces clés devant être configurées de façons statique. Le principal atout de WEP est qu'il n'impose qu'une faible surcharge de calcul. Même si aujourd'hui les PC compatibles 802.11 sont courants, ce n'était pas le cas en 1997. La plupart des équipements de WLAN étaient alors de type ASD (Application-Spécific Device), c'est-à-dire dédiés à une application spécifique, à l'exemple des lecteurs de code barres, des tablets PC et des téléphones 802.11. Ces équipements possèdent généralement un processeur peu puissant car les applications qui s'exécutent dessus ne sont pas très gourmandes. WEP est simple à implanter et ne totalise pas plus d'une trentaine de lignes de code dans certains cas. Sa légèreté le rend idéal pour le chiffrement des communications des ASD.

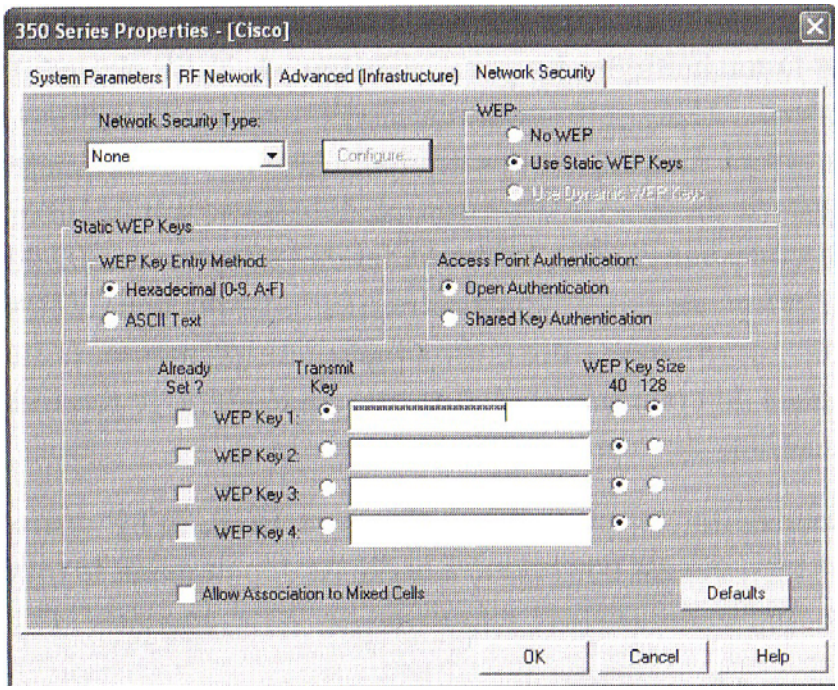
Pour éviter le mode de chiffrement ECB, WEP utilise un vecteur d'initialisation (IV) de 24 bits, qui est concaténé à la clé de départ avant le traitement par RC4. la figure ci-dessous illustre une trame cryptée au moyen de WEP, incluant l'IV.



L'IV doit être différent pour chaque trame de façon à prévenir les collisions d'IV. Une collision d'IV survient lorsqu'une même paire IV/clé WEP est réutilisée, produisant la même séquence clé. Ces collisions donnent à un attaquant éventuel l'opportunité de deviner le texte en clair à partir des séquences récurrentes rencontrées dans le texte chiffré. Le rôle des IV étant précisément d'empêcher cela, la majorité des fabricants implémentent un renouvellement des IV par trame sur leurs équipements.

Le standard 802.11 requiert la configuration statique de clés WEP identiques sur les équipements client et d'infrastructure. Il est possible de définir un maximum de quatre clés sur chaque nœud, mais une seule peut être utilisée à la fois pour un même flux de trafic.

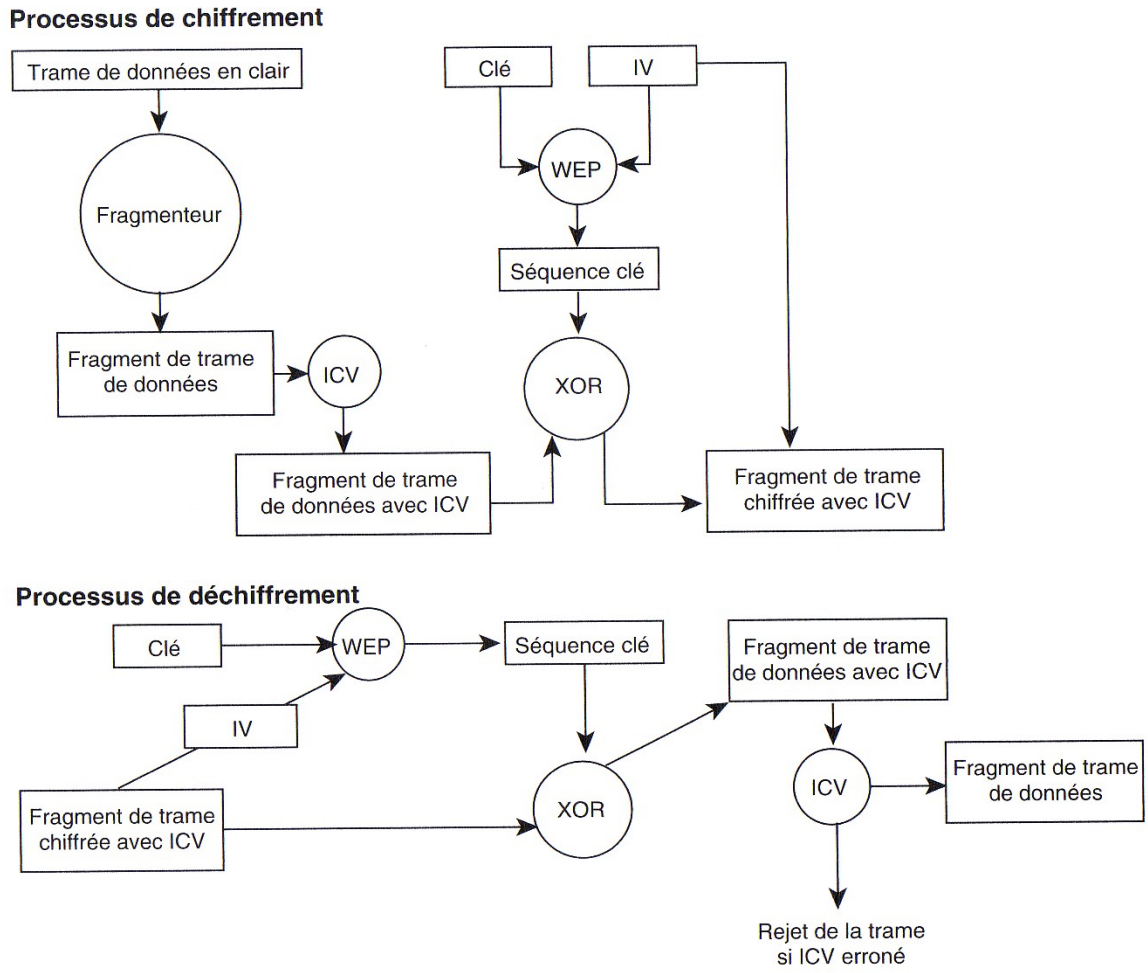
La figure ci-dessous présente la fenêtre de configuration de WEP pour un client CISCO Aironet.



Le chiffrement WEP s'applique uniquement aux trames de données et lors de l'authentification Shared Key. Il permet de crypter les champs suivants d'une trame de données 802.11 :

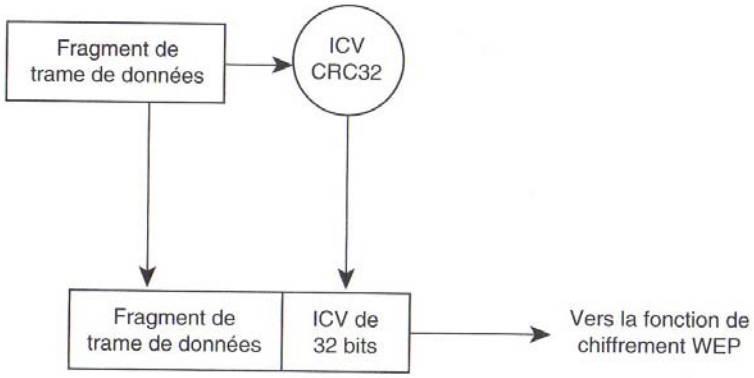
- Champ de données ou de charge utile
- Champ ICV (Integrity Check Value)

Tous les autres champs sont transmis sans être cryptées. L'IV doit être envoyé en clair dans la trame de sorte que la station réceptrice puisse s'en servir pour déchiffrer les données et l'ICV. La figure suivante illustre les étapes de chiffrement, de transmission, de réception et de déchiffrement avec WEP.



Outre le chiffrement des données, le standard 802.11 définit une valeur de 32 bits, l'ICV, qui sert à contrôler l'intégrité de la trame. Le récepteur peut ainsi déterminer si la trame reçue est ou non corrompue. Cette valeur vient compléter le champ FCS (Frame Check Sequence) des couches 1 et 2, qui permet de détecter les erreurs de transmission.

L'ICV est calculée à partir de tous les champs de la trame à l'aide de la fonction polynominale CRC32 (Cyclic Redundancy Check 32-bits). L'émetteur calcule l'ICV et place le résultat dans le champ ICV. Ce dernier étant inclus dans la portion cryptée de la trame, son contenu est incompréhensible. Le récepteur décrypte la trame, calcule une ICV et la compare au champ ICV de la trame reçue. Si les deux valeurs correspondent, la trame est considérée comme étant authentique. Dans le cas contraire, la trame est supprimée. La figure suivante montre la logique de calcul de l'ICV.



10.6. L'authentification dans le standard 802.11

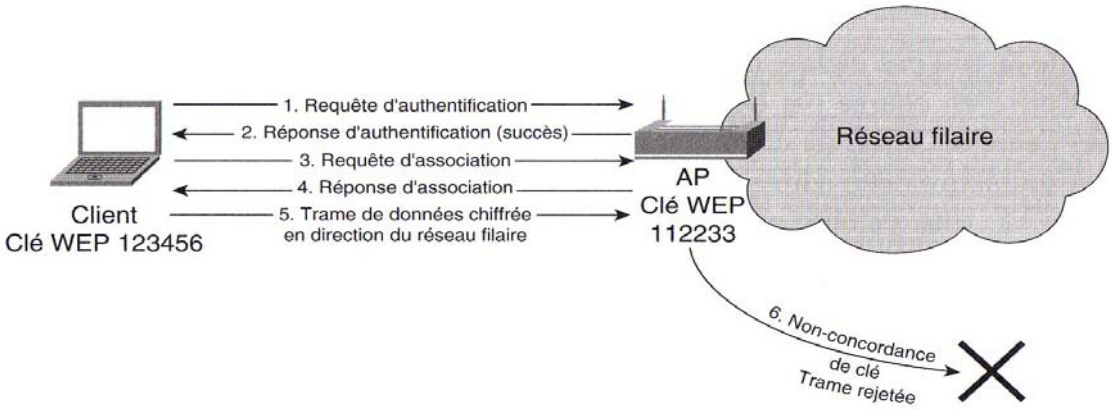
Le standard 802.11 spécifie les deux mécanismes d'authentification suivants pour les clients d'un WLAN :

- Open System
- Shared Key

L'authentification Open System repose sur un algorithme d'authentification dit nul, c'est-à-dire que l'AP accepte toutes les requêtes d'authentification. Même s'il peut sembler inutile à première vue de définir un tel algorithme, l'authentification est nécessaire pour permettre aux équipements d'accéder rapidement au réseau.

LE CONTRÖLE AVEC L'AUTHENTIFICATION Open system s'appuie sur la clé WEP configurée au préalable sur le client et l'AP. Ceux-ci ne peuvent communiquer que s'ils possèdent la même clé. S'ils n'ont pas été configurés pour utiliser WEP, il n'existe aucune sécurité dans le BSS. N'importe quel équipement peut dès lors participer au WLAN, et les trames de données sont transmises sans être cryptées.

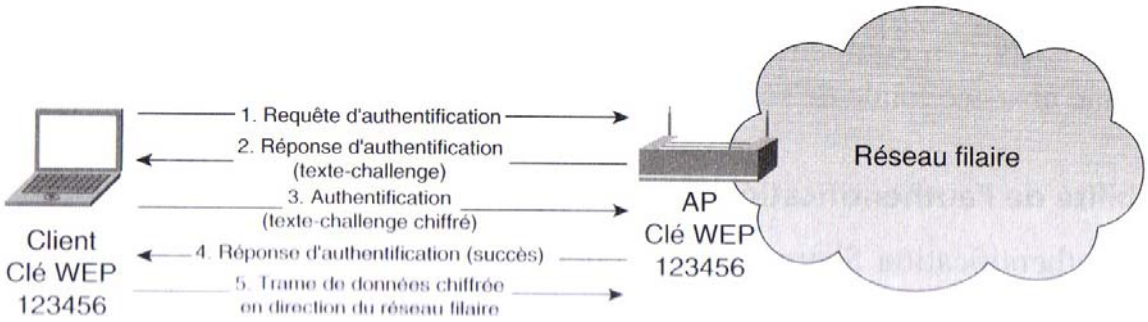
A l'issue de l'authentification et de l'association, le client peut commencer à envoyer et recevoir des données. Si sa clé diffère de celle de l'AP, il est dans l'impossibilité de chiffrer et déchiffrer correctement les trames, lesquelles sont supprimées par le client et par l'AP. Ce processus fournit essentiellement un moyen de contrôler l'accès au BSS, comme illustré ci-dessous.



Contrairement à l'authentification Open System, l'authentification Shared Key exige que WEP soit activé sur le client et l'AP et qu'une même clé soit configurée sur les deux équipements. Voici les étapes du processus :

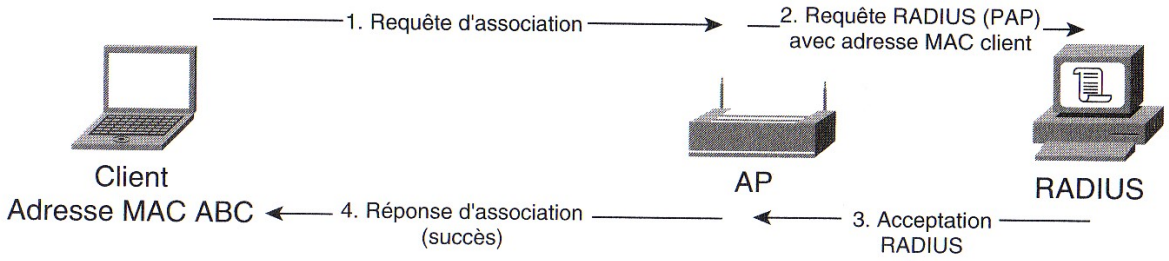
- Le client envoie à l'AP une requête pour l'authentification Shared Key.
- L'AP répond avec un texte-challenge en clair.
- Le client chiffre le texte-challenge et place le résultat dans une trame de réponse.
- Si l'AP peut déchiffrer la trame et extraire le texte-challenge initial, le client reçoit un message de réussite.
- Le client peut accéder au WLAN.

Si ces deux mécanismes d'authentification ont en commun d'utiliser des clés WEP pour le contrôle d'accès, seule l'authentification Shared Key requiert qu'elles soient identiques côté client et côté AP pour permettre au client de s'associer. La figure ci-dessous illustre ce processus.



10.7. L'authentification par adresse MAC

Bien qu'elle ne soit pas incluse dans les spécifications 802.11, l'authentification par adresse MAC est prise en charge par de nombreux fabricants. Elle consiste dans son principe à comparer l'adresse MAC du client à une liste d'adresses autorisées configurée localement ou bien à soumettre cette adresse à un serveur d'authentification externe, comme illustré ci-dessous. Elle s'ajoute aux mécanismes d'authentification 802.11 Open System et Shared Key, réduisant le risque que des équipements non autorisés accèdent au réseau. Imaginez un WLAN avec de nombreuses stations. Pour faire en sorte qu'un AP particulier ne puisse communiquer qu'avec trois équipements spécifiques, l'authentification 802.11 ne suffirait pas puisque toutes les stations et l'AP possèdent la même clé WEP. Il faudrait donc configurer en plus l'authentification par adresse MAC.



10.8. Les failles de sécurisé du standard 802.11

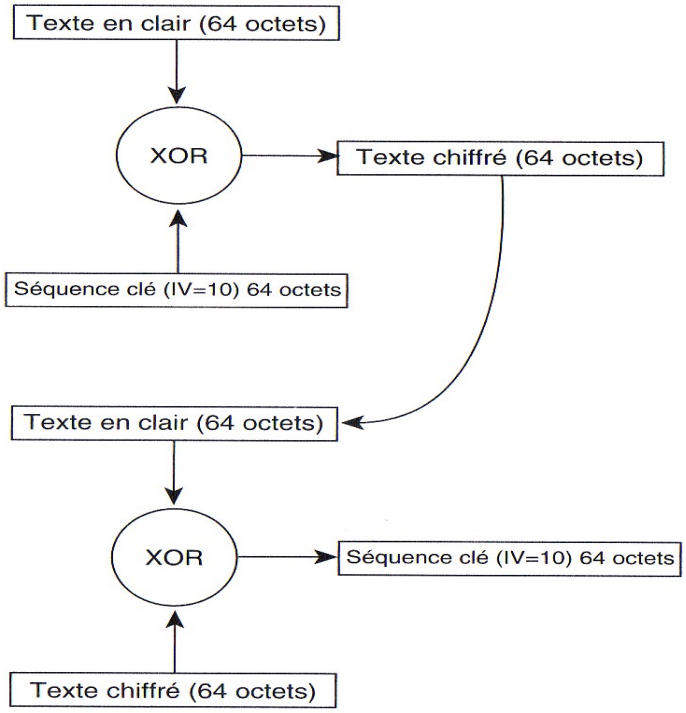
La section précédente a présenté les mécanismes d'authentification et de chiffrement mis en œuvre dans les réseaux 802.11. Ce n'est un secret pour personne que la sécurité de ces mécanismes est déficiente. A peine le standard était-il ratifié que plusieurs documents mettaient en évidance ses vulnérabilités.

10.8.1. Vulnérabilité de l'authentification Open System

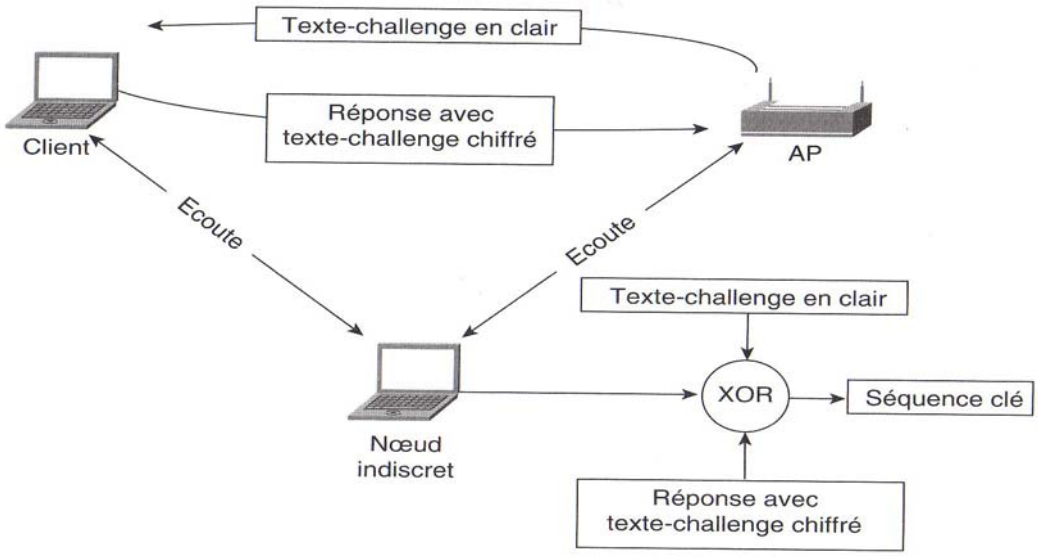
L'authentification Open System n'offre aucun moyen permettant à l'AP de déterminer si un client est ou non valide. Cette caractéristique devient une vulnérabilité lorsque le chiffrement WEP n'est pas implémenté dans le WLAN. Même si WEP est configuré de façon statique sur le client et l'AP, cette authentification ne renseigne pas sur l'identité de l'utilisateur du WLAN. Un équipement autorisé entre les mains d'un utilisateur non autorisé revient à une absence totale de sécurité.

10.8.2. Vulnérabilité de l'authentification Shared Key

Lors de l'authentification Shared Key, le client doit utiliser une clé WEP préalablement partagée pour déchiffrer le texte-challenge reçu de l'AP. Pour authentifier le client, l'AP doit déchiffrer la réponse et s'assurer que le texte-challenge obtenu est le même que celui envoyé initialement au client.
Le texte-challenge étant transmis en clair sur la liaison hertzienne, cette authentification est vulnérable à une attaque dite par texte en clair connus (known plaintext). Cette attaque exploite la logique mathématique sous-jacente au chiffrement. Nous avons décrit précédemment le processus de chiffrement comme étant l'application d'une séquence clé à un texte en clair pour produire un texte chiffré. La séquence clé et le texte en clair sont en fait combinés au moyen de l'opérateur XOR, également appelé « OU Exclusif ». Si l'attaquant opère un XOR sur le texte-challenge en clair et le texte chiffré correspondant, il il obtient la séquence clé dérivée de la paire IV/clé WEP. Voici l'illustration de la dérivation de la séquence clé.



Il suffit donc à un attaquant de capturer le texte-challenge et le texte chiffré pour être en mesure de découvrir la séquence clé par un opérateur XOR. Il peut ensuite déchiffrer les trames ayant la même longueur que la séquence, à condition que l'IV utilisé pour produire cette dernière soit le même que celui ayant servi à chiffrer la trame. La figure ci-dessous montre comment un attaquant peut écouter clandestinement le processus d'authentification Shared Key et déterminer la séquence clé.



10.8.3. Vulnérabilité de l'authentification par adresse MAC

Selon le standard, les adresses MAC sont transmises en clair dans toutes les trames 802.11. En conséquence, un WLAN qui emploie l'authentification par adresse MAC est exposé à un risque d'usurpation, ou spoofing, de l'adresse MAC d'un client valide.
Le spoofing d'adresse MAC est possible avec les cartes réseau 802.11 sur lesquelles l'adresse UAA (Universally Administered Address) peut être remplacée par une adresse LAA (Locally Administered Address). L'UAA est l'adresse MAC qui est gravée sur la carte par le fabricant. Un attaquant pourrait utiliser un analyseur de protocole pour obtenir une adresse MAC valide dans le BSS et localiser une carte compatible LAA pour usurper cette adresse.

10.8.4. Vulnérabilité du chiffrement WEP

La faiblesse la plus critique du standard 802.11 a été révélée par trois cryptanalystes, Fluhrer, Mantin et Shamir. Dans leur publication, ils révèlent qu'il est possible de dériver une clé WEP en collectant passivement toutes les trames d'un WLAN.
Cette faille a trait à la façon dont WEP implémente l'algorithme KSA (Key Scheduling Algorithm) de RC4. Un certain nombre d'IV dits faibles (weak) peuvent permettre d'obtenir des octets de la clé WEP par analyse statistique. Des chercheurs de AT&T et de la Rice University aux Etats-Unis ainsi que les développeurs de l'utilitaire **AirSnort** ont tenté d'exploiter cette vulnérabilité et vérifié qu'il était effectivement possible de dériver des clés WEP de 40 ou 104 bits après seulement **quatre millions de trames**. Sur un WLAN 802.11b à fort trafic, cela peut se traduire par la découverte d'une clé WEP toutes les heures environ, rendant WEP inefficace pour assurer la confidentialité des données.

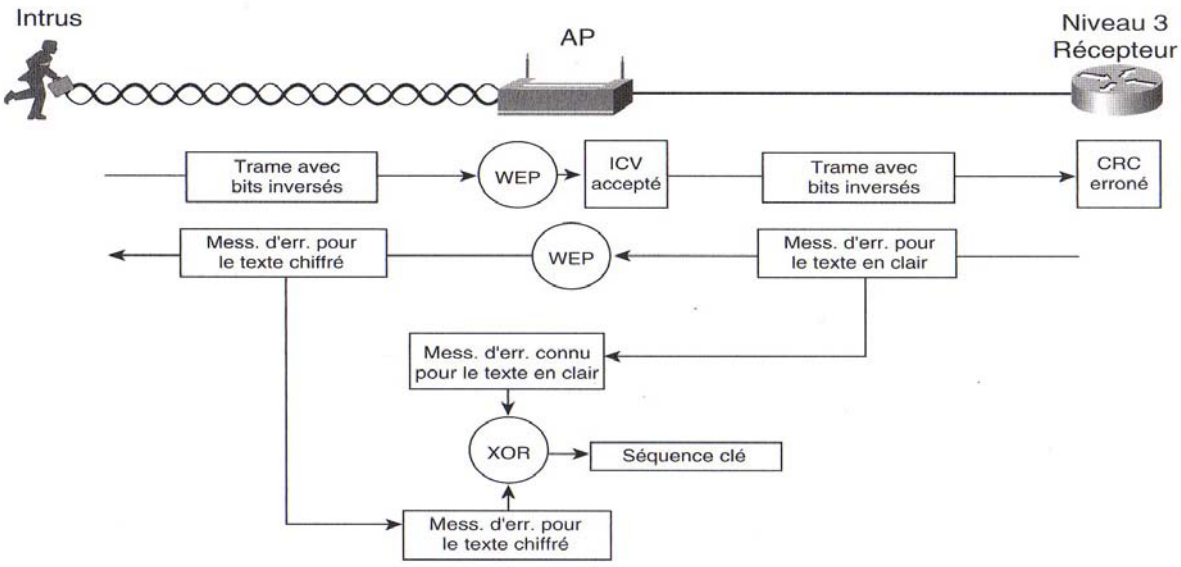
Il s'agit là d'une attaque passive, puisque l'attaquant écoute clandestinement le BSS et collecte simplement les trames transmises. Contrairement à l'attaque par texte-challenge connu liée à l'authentification Shared Key, cette attaque par analyse statique permet de récupérer directement la clé WEP et non plus seulement la séquence clé. Muni de cette information, l'intrus peut ensuite accéder au BSS grâce à un équipement authentifié, à l'insu des administrateurs réseau.

Comme si cette vulnérabilité ne suffisait pas, une seconde catégorie d'attaques à été théorisée mais jamais encore implémentée. Ces attaques, dites par induction, procèdent selon le même principe que l'attaque sur Shared Key : un texte en clair connu et un résultat chiffré correspondant sont utilisés pour dériver une séquence clé.
Comme expliqué précédemment, une séquence clé permet le déchiffrement de trames pour une paire IV/clé WEP et une longueur spécifiques. Un attaquant s'efforce normalement de collecter autant de séquences clés que possible pour élaborer une base de données qui lui servira à s'introduire sur le réseau et à décrypter le trafic. Dans un WLAN qui n'emploie pas l'authentification Shared Key, les attaques par inversion de bits (bits flipping) permettent de dériver un grand nombre de séquences clés en un court laps de temps.

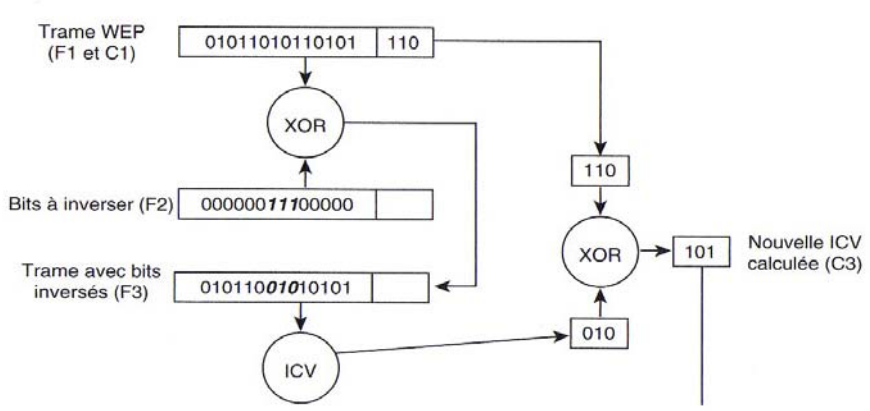
Une attaque par inversion de bits exploite la vulnérabilité de l'ICV. En effet, l'ICV est calculée au moyen de la fonction polynomiale CRC32, laquelle s'avère inefficace pour garantir l'intégrité des messages. Les propriétés mathématiques de cette fonction permettent de falsifier une trame et de modifier l'ICV sans même avoir besoin de connaître le contenu original de la trame.
Bien que la charge utile puisse varier d'une trame 802.11 à une autre, bon nombre d'éléments restent inchangés et occupent toujours la même position. Un attaquant peut profiter de cela pour altérer le champ de données de la trame afin de modifier le paquet de niveau supérieur.

Voici comment se déroule une attaque par inversion de bits (Voir figure ci-dessous) :

1. L'attaquant capture une trame sur le WLAN.
2. Il inverse des bits aléatoires dans la charge utile de la trame.
3. Il modifie l'ICV (ce processus est décrit plus loin).
4. Il transmet la trame modifiée.
5. Le récepteur, qu'il soit client ou AP, calcule l'ICV en se fondant sur le contenu de la trame reçue.
6. Il compare l'ICV obtenue au champ ICV de la trame.
7. Il accepte la trame modifiée.
8. Il la transmet à un équipement de niveau supérieur (routeur ou PC hôte).
9. Comme des bits ont été inversés dans le paquet de niveau 3, la vérification par total de copntrôle échoue à ce niveau.
10. La pile IP du récepteur produit une erreur prévisible.
11. L'attaquant écoute le WLAN pour capturer le message d'erreur chiffré.
12. lorsqu'il le récupère, il dérive la séquence clé, comme dans l'attaque par capture et reproduction d'IV, parfois aussi appelée rejeu d'IV.



Cette attaque se fonde sur la vulnérabilité de l'ICV. Une question se pose cependant : cette valeur étant placée dans la portion chiffrés de la trame, comment un attaquant s'y prend-il pour la modifier de façon à tenir compte de l'inversion des bits ? Il procède en fait selon la logique suivante, illustrée ci-dessous :



1. La trame F1 possède l'ICV C1.
2. Une nouvelle trame, F2, de même longueur de F1, avec des bits à 1 dans les positions concernées par l'inversion, est générée.
3. La trame F3 est créée par XOR de F1 et F2.
4. L'ICV de F3 est calculée (C2).
5. L'ICV C3 est générée par XOR de C1 et C2.

10.8.5. Le problème de la gestion des clés WEP statiques

Le standard 802.11 ne définit aucune méthode spécifique pour la gestion des clés WEP. Le fait que WEP supporte uniquement l'emploi de clés configurées de façon statique ne constitue pas une vulnérabilité en soi. Toutefois, étant donnée que l'authentification 802.11 identifie un équipement et non un utilisateur, le vol ou la perte d'une carte réseau sans fil pose un problème pour la sécurité du réseau. Les administrateurs se voient alors obligés de configurer manuellement une nouvelle clé sur tous les équipements 802.11.

Ce risque reste acceptable pour les déploiements 802.11 de petite envergure, pour lesquels la gestion des équipements utilisateur est simple. Lorsque les utilisateurs sans fil se comptent en milliers, un mécanisme de génération et de distribution des clés est nécessaire.

10.9. Sécurité des WLAN 802.11

L'industrie du WLAN à pris conscience des vulnérabilités que présentent les fonctions dans 802.11, pour tenter d'apporter des solutions à la fois acceptables pour les installations existantes et évolutives, l'IEEE a développé des extensions améliorant ces fonctionnalités. Des changements ont été apportés sous la forme du projet de standard 802.11i, lequel n'a pas encore été ratifié. Pour cette raison, la WIFI Alliance a rassemblé un sous-ensemble de composantes de 802.11i sous l'appellation WPA (**W**IFI **P**rotected **A**ccess).

La sécurité des réseaux sans fil repose sur les quatre aspects suivants :

- **Le contexte (framework) d'authentification.** Il forme le cadre sous-jacent à l'algorithme d'authentification et permet l'échange sécurisé de messages entre le client, l'AP et le serveur d'authentification.
- **L'algorithme d'authentification.** C'est la logique qui contrôle l'identité d'un utilisateur.
- **L'algorithme de confidentialité des données.** C'est le mécanisme qui permet de protéger les données contre toute utilisation frauduleuse, même en cas d'interception.
- **L'algorithme d'intégrité des données.** C'est le mécanisme qui permet à un récepteur de détecter si le contenu d'une trame a été ou non altéré depuis son émission.

10.9.1. Le contexte d'authentification

Le contexte d'authentification de 802.11 se présente sous la forme d'une trame de gestion d'authentification. Elle sous-tend les algorithmes d'authentification Open Shared et Shared Key mais ne contient aucun mécanisme propre lui permettant d'authentifier elle-même un client. Nous avons vu les défauts de l'authentification de 802.11, il convient de comprendre ce qui doit être apporté pour pouvoir offrir une authentification sécurisée sur un WLAN.

Voici les caractéristiques essentielles qui manques au standard 802.11 :

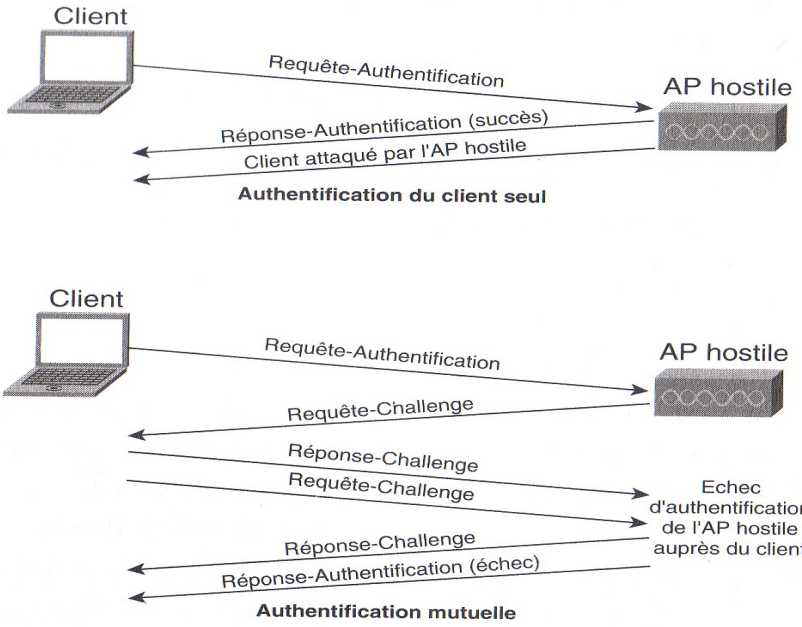
- Authentification de l'utilisateur au moyen d'un mécanisme central
- Clés de chiffrement générées dynamiquement
- Gestion des clés de chiffrement
- Authentification mutuelle

Il est primordial pour la sécurité d'un réseau de pouvoir authentifier un utilisateur. Les méthodes Open System ou Shared Key permettent de vérifier la légitimité d'un «équipement, mais elles n'empêchent pas un intrus de s'emparer d'une station autorisée pour se connecter au réseau. Certaines situations, telles que la perte ou le vol d'un équipement ou même le départ d'un employé, obligent l'administrateur à reconfigurer une nouvelle clé sur tous les AP et clients. Par contre, un contrôle centralisé des utilisateurs au moyen d'un serveur AAA (**A**uthentification, **A**uthorization, **A**ccounting), tel que le permet **RADIUS**, donne la possibilité d'autoriser ou d'interdire l'accès à des utilisateurs indépendamment de l'équipement à partir duquel ils se connectent.

Un autre aspect positif indirect de l'authentification des utilisateurs est qu'elle réclame l'emploi de clés de chiffrement spécifiques pour chaque utilisateur. Les méthodes qui offrent la faculté de générer des clés de façon dynamique s'intègrent bien au modèle de sécurité et l'administration des WLAN. De plus, elles exonèrent l'administrateur du besoin de saisir et gérer manuellement des clés pour chaque équipement devant accéder au réseau. Une clé est générée dynamiquement lorsque l'utilisateur émet une demande d'accès au réseau puis supprimée lorsqu'il termine sa session. Si vous devez interdire l'accès à un utilisateur, il suffit de désactiver son compte.

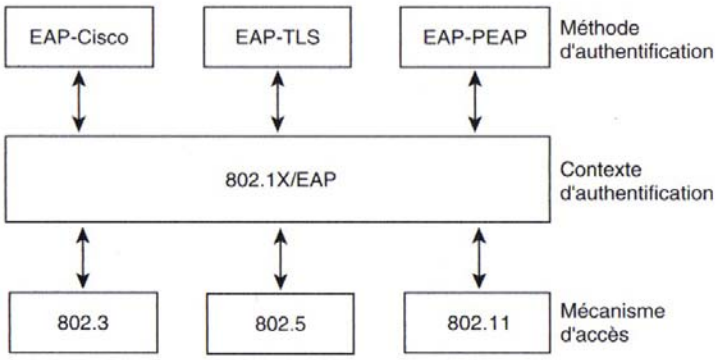
L'authentification mutuelle est un processus bidirectionnel. Cela revient à dire que l'identité de l'utilisateur est vérifiée mais que le réseau aussi doit être authentifié par le client. Avec Open System et Shared Key, l'AP ou le réseau authentifie le client, mais celui-ci n'a aucun moyen de s'assurer que l'AP ou le réseau auquel il se connecte est valide, le standard 802.11 n'ayant pas prévu de méthode pour cela. Par conséquent, un AP ou une station hostile peut se

faire passer pour un point d'accès légitime et détourner les données émanant d'un client. La figure ci-dessous, illustre ce point en présentant une séquence d'authentification unidirectionnelle et un dialogue d'authentification mutuelle, qui présente à l'évidence une meilleure protection.



Les fabricants d'équipements pour WLAN 802.11 et l'IEEE ont compris la nécessité de remplacer les mécanismes existants, à la fois pour l'authentification et le chiffrement. Comme évoqué plus haut, des travaux réalisés par le groupe de travail « i » du comité 802.11 sont en cours et seront publiés une fois terminés sous la désignation 802.11i.

L'IEEE a comblé les insuffisances de l'authentification 802.11 en apportant un nouveau contexte d'authentification sous la forme du standard 802.11x. Ce dernier fournit une authentification étendue à toutes les topologies de la couche liaison de la famille 802.xx une fonction que l'on rencontre normalement dans les couches supérieures et s'appuie sur le contexte d'authentification de PPP (**P**oint-to-**P**oint **P**rotocol), appelé EAP (**E**xtensible **A**uthentification **P**rotocol). En un mot, 802.1x encapsule les messages EAP pour qu'ils puissent être utilisés au niveau 2. Les spécifications de 802.11i incorporent ce nouveau contexte en réclamant son emploi pour authentifier un utilisateur. La figure ci-dessous illustre son positionnement vis-à-vis des différents protocoles d'authentification compatibles avec EAP et de ces topologies.



EAP (RFC 2284) et 802.1x ne prévoient pas l'emploi d'un algorithme d'authentification spécifique. L'administrateur d'un réseau a donc la possibilité d'employer toute méthode compatible avec EAP pour assurer l'authentification 802.1x. La seule exigence est que le demandeur d'accès (supplicant), en l'occurrence le client 802.11, et le serveur responsable de l'authentification supporte l'algorithme d'authentification EAP.

Voici quelques exemples de mécanismes admis :

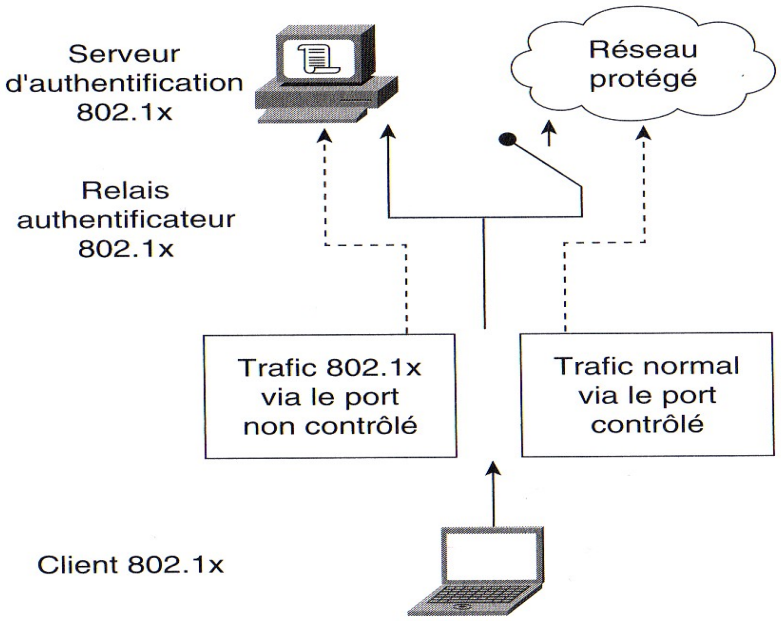
- **EAP-TLS (Transport Layer Security).** Ce mécanisme similaire à SSL (secure Sockets Layer) fonctionne au niveau de la couche liaison. Il utilise des certificats numériques afin de créer un tunnel SSL et assure l'authentification mutuelle.
- **PEAP (Protected EAP).** Cette technique se fonde sur la sécurité apportée par TLS pour créer un tunnel afin de permettre le transfert des éléments d'identité des clients. Il n'impose pas l'usage de certificats aux clients.
- **EAP-MD5 (Message Digest 5).** Semblable au protocole CHAP (Challenge Handshake Authentification Protocol), EAP-MD5 implémente l'authentification au moyen d'un algorithme unidirectionnel utilisant un mot de passe.
- **EAP-Cisco, aussi appelé LEAP (Lightweight EAP).** C'est le premier type d'authentification EAP conçu spécifiquement pour la sécurité des WLAN. LEAP s'appuie sur un algorithme d'authentification mutuelle fondé sur un mot de passe.

L'authentification 802.11x requiert la mise en place de trois processus, ou entités, qui interopèrent :

- **Un processus d'authentification demandeur,** situé sur le client du WLAN.
- **Un processus d'authentification relais (authentificateur),** destiné à faciliter l'exécution de l'ensemble de la procédure et situé sur un point d'accès au réseau.
- **Un processus d'authentification côté serveur,** qui s'exécute sur un serveur RADIUS.

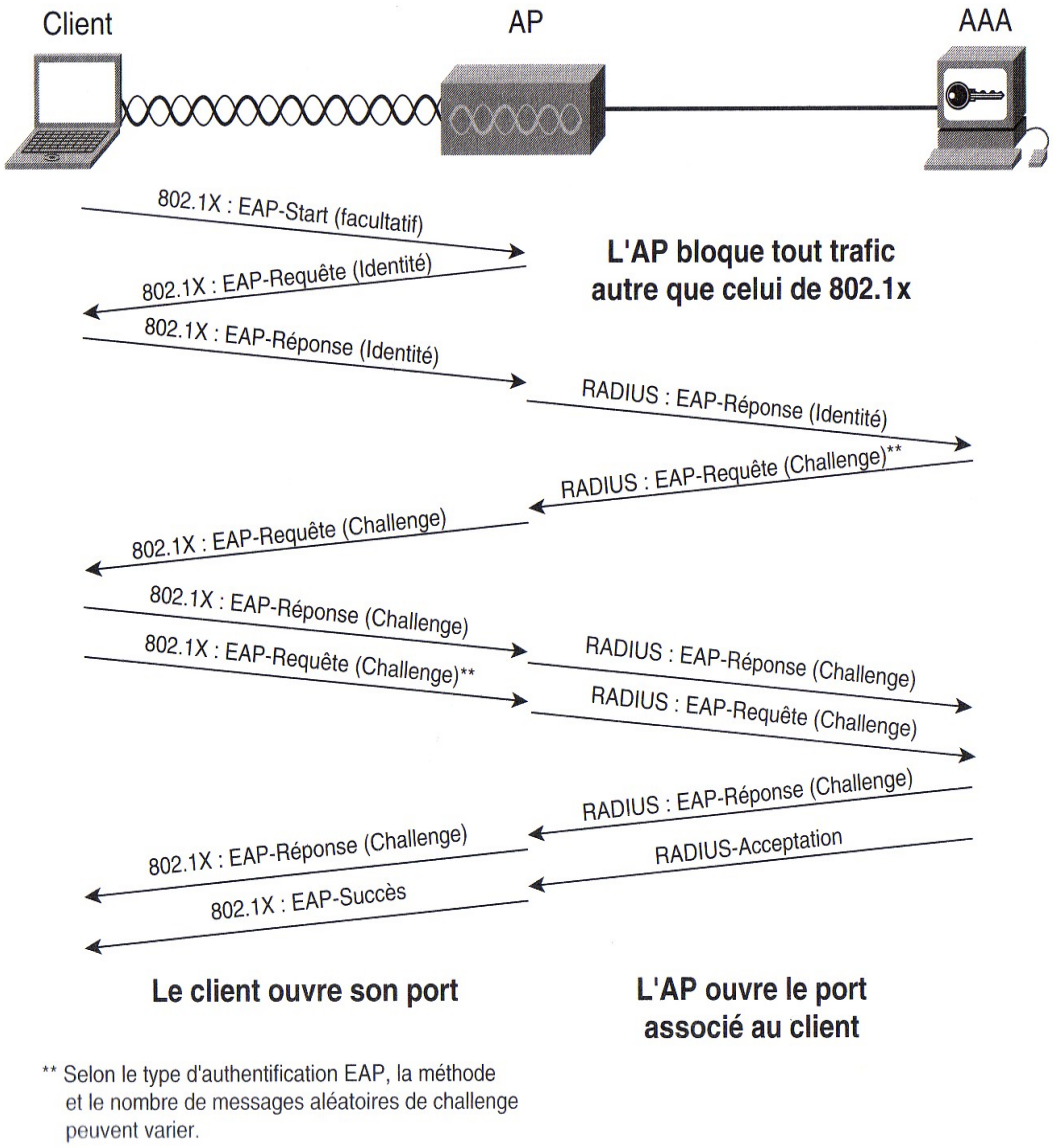
Ce sont donc trois composants logiciels hébergés sur des équipements du réseau. En ce qui concerne 802.11, l'AP authentificateur ouvre un port logique pour chaque client demandeur en se fondant sur l'identifiant d'association du client. Ce port se présente sous la forme de deux chemins de données, l'un incontrôlé et l'autre contrôlé. Le chemin incontrôlé permet l'envoi du trafic d'authentification 802.1x sur le réseau tandis que le chemin contrôlé bloque

le trafic normal jusqu'à ce que l'authentification réussisse. La figure ci-dessous montre ce concept sur un point d'accès authentificateur.



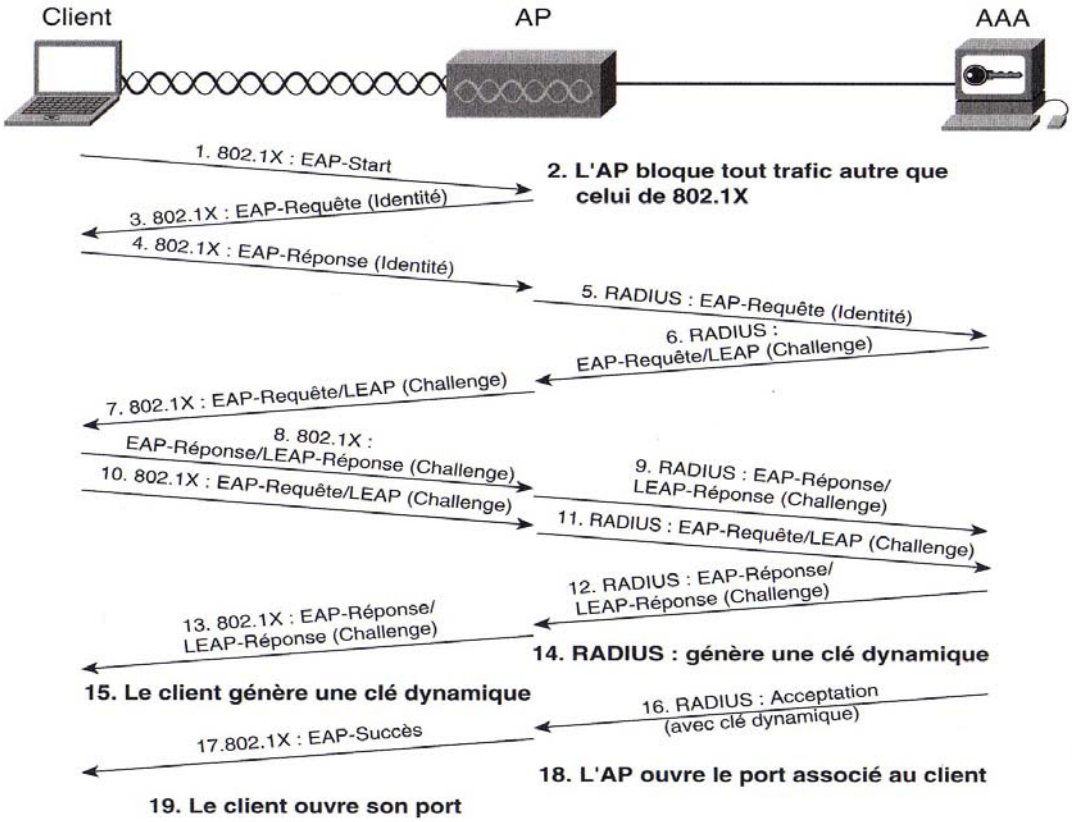
Les échanges de messages 802.1x peuvent varier selon l'algorithme d'authentification utilisé. La procédure générale se déroule de la façon suivante (voir figure suivante).

1. Un client devient actif sur le support et s'associe à l'AP authentificateur.
2. L'authentificateur détecte l'association du client et ouvre un port logique à son intention, mais dans un état non autorisé, de façon que seul le trafic 802.1x puissent passer.
3. Le client peut initier un dialogue avec un message EAP-Start, mais cela n'est pas requis.
4. L'authentificateur envoie au demandeur un message de requête pour obtenir des informations d'identité.
5. Le paquet de réponse du client contenant l'information d'identité est transmis au serveur d'authentification. Le type de cette information varie selon le protocole d'authentification EAP utilisé, mais il s'agit généralement d'un identifiant utilisateur ou d'un équivalent et non d'une chaîne secrète, telle qu'un mot de passe.
6. Le serveur d'authentification est configuré pour authentifier les clients avec un algorithme spécifique. Actuellement, les spécifications 802.1x pour les LAN 802.11 ne stipulent pas d'algorithme particulier à utiliser.
7. Selon l'issue de l'échange d'identité, laquelle est propre à l'algorithme EAP employé, le dernier message spécifique de 802.1x est le paquet RADIUS d'acceptation (Access-Accept) ou de rejet (Access-Reject) que le serveur envoie à l'AP.
8. A réception, l'AP place le port du client dans un état autorisé, et le trafic peut être transmis normalement.



10.9.2. L'algorithme d'authentification

Comme indiqué précédemment, ni 802.11i ni WPA ne demandent l'emploi d'algorithmes spécifiques. Ils recommandent en revanche tous l'usage d'un algorithme implémentant l'authentification mutuelle, la génération dynamique de clés de chiffrement et l'authentification de l'utilisateur. La figure ci-dessous, montre les messages échangés entre un client, un AP et un serveur AAA. Pour mieux exemplifier la procédure, nous nous appuierons plus précisément sur le protocole LEAP ou EAP-Cisco. C'est un algorithme simple et efficace, qui a été conçu spécifiquement pour les WLAN.



Voici le détail de la procédure :

1. Le client devient actif sur le support et envoie un message EAP-Start encapsulé dans une trame 802.1x.
2. L'AP bloque le port du client, n'autorisant que le trafic d'authentification 802.1x à atteindre le réseau.
3. L'AP envoie un message EAP de requête d'identité au client dans une trame 802.1x.
4. Le client lui envoie un message 802.1x de réponse avec son identifiant utilisateur.
5. L'AP transmet l'identifiant au serveur d'authentification dans un paquet RADIUS de requête d'accès (Access-Request).
6. Le serveur d'authentification génère un message de challenge LEAP et l'envoie au client par l'intermédiaire de l'AP dans un paquet RADIUS de réponse (Access-Reponse).
7. l4AP transmet le message de challenge au client dans une trame 802.1x.
8. Le client traite le challenge au moyen de l'algorithme propre à LEAP et envoie une réponse au serveur RADIUS via l'AP.
9. L'AP encapsule la réponse au challenge reçue du client dans un paquet de requête d'accès RADIUS (Access-Request) et transmet ce dernier au serveur.
10. Pour authentifier le réseau, le client envoie à son tour au serveur, toujours par l'intermédiaire de l'AP, une requête de challenge LEAP encapsulée dans une trame 802.1x.
11. L'AP transmet le challenge au serveur dans un paquet de requête d'accès RADIUS.
12. Le serveur envoie via l'AP une réponse au challenge LEAP dans un paquet de réponse.
13. L'AP replace la réponse au challenge dans une trame 802.1x et l'envoie au client.
14. Le serveur génère une clé de chiffrement dynamique à partir du mot de passe de l'utilisateur et de certaines informations de session.

15. Le client génère la même clé. Cette faculté de générer localement la même clé dynamique vient de ce que le client dispose des mêmes informations.
16. Le serveur envoie à l'AP la clé encapsulée dans un paquet RADIUS d'acceptation d'accès (Access-Accept), gage pour l'AP que l'authentification a réussi.
17. L'AP installe la clé dynamique relative au client puis lui envoie un message EAP-Succès encapsulé dans une trame 802.1x.
18. L'AP place le port du client dans un état de transmission autorisée.
19. Le client ouvre son port, en supposant que l'authentification mutuelle a réussi.

LEAP est un algorithme propriétaire de Cisco, qui s'exécute au-dessus d'un contexte d'authentification ouvert. Pour cette raison, les détails de son implémentation, tels que la génération du message et les informations de la réponse, ne sont pas accessibles publiquement. LEAP couvre les exigences définies pour l'authentification sécurisée des utilisateurs dans un WLAN en incluant les fonctionnalités suivantes :

- Authentification de l'utilisateur
- Authentification mutuelle
- Génération dynamique de clés de chiffrement

Pour empêcher un utilisateur d'accéder au réseau, il suffit de désactiver son compte sur le serveur d'authentification centralisé. Dès lors, il ne peut plus s'authentifier avec succès ni générer de clé de chiffrement valide.

10.9.3. Confidentialité des données

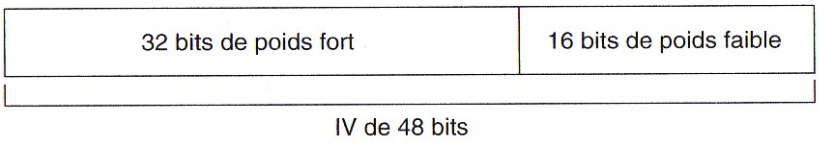
Les faiblesses de WEP ont posé le dilemme suivant aux fabricants et à l'IEEE : comment corriger les failles du chiffrement 802.11 sans nécessiter le remplacement complet du matériel de l'AP ou les cartes d'interfaces des clients ?
L'IEEE y a répondu en introduisant TKIP (Temporal Key Integrity Protocol) comme partie intégrante de 802.11i et WPA. TKIP emploie de nombreuses fonctions essentielles de WEP de manière à conserver l'équipement des clients et l'infrastructure 802.11 en place tout en corrigeant plusieurs vulnérabilités pour fournir un mécanisme efficace de chiffrement des trames. Les améliorations essentielles apportées par TKIP sont les suivantes :

- **Génération d'une clé par trame.** La clé WEP est rapidement changée à chaque trame.
- **Mécanisme de contrôle d'intégrité MIC (Message Integrity Check).** Cette fonction de contrôle efficace empêche l'altération insidieuse d'une trame ainsi qu'une attaque par reproduction, ou rejeu de trame.

Le document élaboré par Fluhrer, Mantin et Shamir décrit la faille de sécurité de l'algorithme RC4 tel qu'il est implémenté dans WEP. Les attaques qui exploitent la faille de l'IV faible, telle celle par Airsnort, visent à collecter plusieurs trames de donnée chiffrées au moyen d'un tel IV. La méthode la plus simple pour y répondre est de changer la clé WEP utilisée pour les communications entre le client et l'AP avant qu'un utilisateur malveillant puisse capturer suffisamment de trames pour en dériver les octets de clé.
L'IEEE a adopté une stratégie mettant en œuvre une clé par trame, appelée Per-Frame Keying, Per-Packet Keying ou encore Fast Packet Keying. Dans ce mécanisme, l'IV, l'adresse MAC de l'émetteur et la clé WEP subissent un traitement au moyen d'une fonction

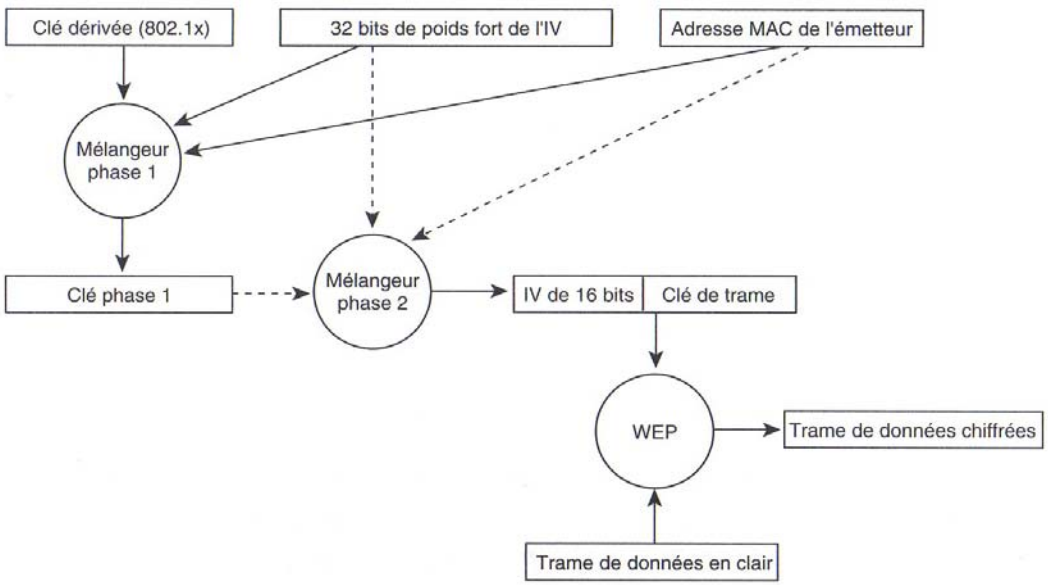
combinatoire en deux phases. Le résultat produit respecte les valeurs standard de 104 bits pour la clé WEP et de 24 bits pour l'IV.

L'IEEE propose également d'augmenter la taille de l'IV de 24 à 48 bits. Les sections suivantes expliquent l'importance d'une extension de l'IV. La figure suivante illustre un exemple d'IV de 48 bits et la façon dont l'IV est divisé pour être utilisé par l'algorithme de génération de clé de trame.



Les étapes suivantes décrivent le processus de génération d'une clé par trame :

1. La clé de base WEP, qui dérive de l'authentification 802.1x, est mélangée avec les 32 bits de poids fort, un nombre de 32 bits peut prendre une valeur entre 0 et 4 294 967 295 de l'IV de 48 bits et l'adresse MAC de l'émetteur. Le résultat produit est une clé intermédiaire, appelée clé de phase 1. Ce processus permet de la placer en cache et de lui donner une direction.
2. La clé de phase 1 est à nouveau mélangée avec l'IV et l'adresse MAC de l'émetteur pour produire la clé de phase 2, soit la clé de trame.
3. L'IV utilisé pour la transmission de la trame a une taille de 16 bits seulement. Il peut prendre une valeur entre 0 et 65535. Les 8 bits restants représentent une valeur fixe de remplissage.
4. La clé de trame est ensuite employée pour chiffrer, via WEP, la charge utile.
5. Lorsque l'espace d'IV de 16 bits est épuisé, la clé de phase 1 est supprimée, et la valeur de 32 bits est augmentée de 1. Par exemple, si elle valait 12, elle passe à 13.
6. La clé de trame est ensuite recalculée à partir de l'étape 2.

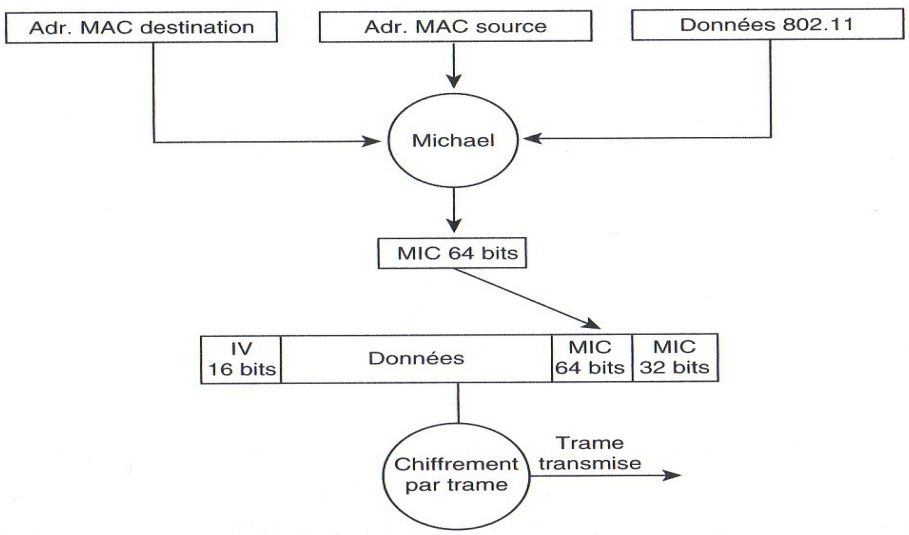


Une clé de trame n'est valide que si la valeur de l'IV de 16 bits n'a pas déjà été utilisée. Sinon, on se trouve dans une situation de collision, qui peut fournir les bases d'une attaque en permettant une dérivation possible de la séquence clé. Pour éviter les collisions d'IV, la clé de phase 1 est recalculée après avoir augmenté de 1 la valeur en cours des 32 bits de poids fort de l'IV. Une nouvelle clé de trame est ensuite créée.

10.9.4. Intégrité des données « MIC »

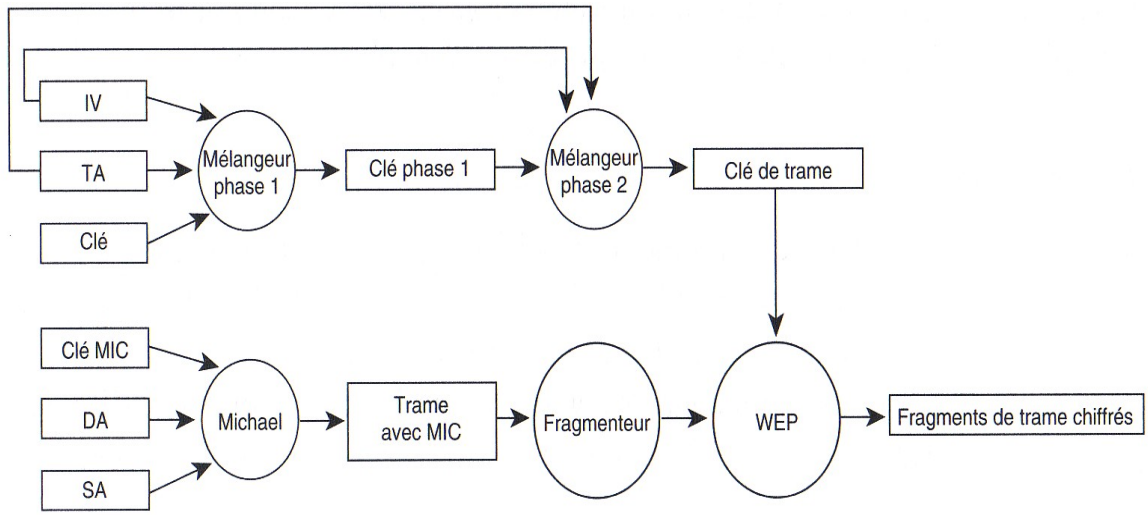
La fonction de contrôle d'intégrité des messages MIC (Message Integrity Check) a été introduite pour améliorer le mécanisme inefficace de l'ICV du standard 802.11. Elle permet de se protéger des attaques visant la modification de la charge utile, telle l'inversion de bit. Elle est utilisée par un algorithme spécifique proposé par l'IEEE sous le nom de « Michael », qui apporte une amélioration au contrôle des trames chiffrées par l'ICV.

Le mécanisme MIC fait usage d'une clé unique différente de celle qui sert au chiffrement des trames de données. Cette clé est combinée avec les adresses MAC destination et source de la trame et la portion charge utile/données (playload) non chiffrée de cette même trame.



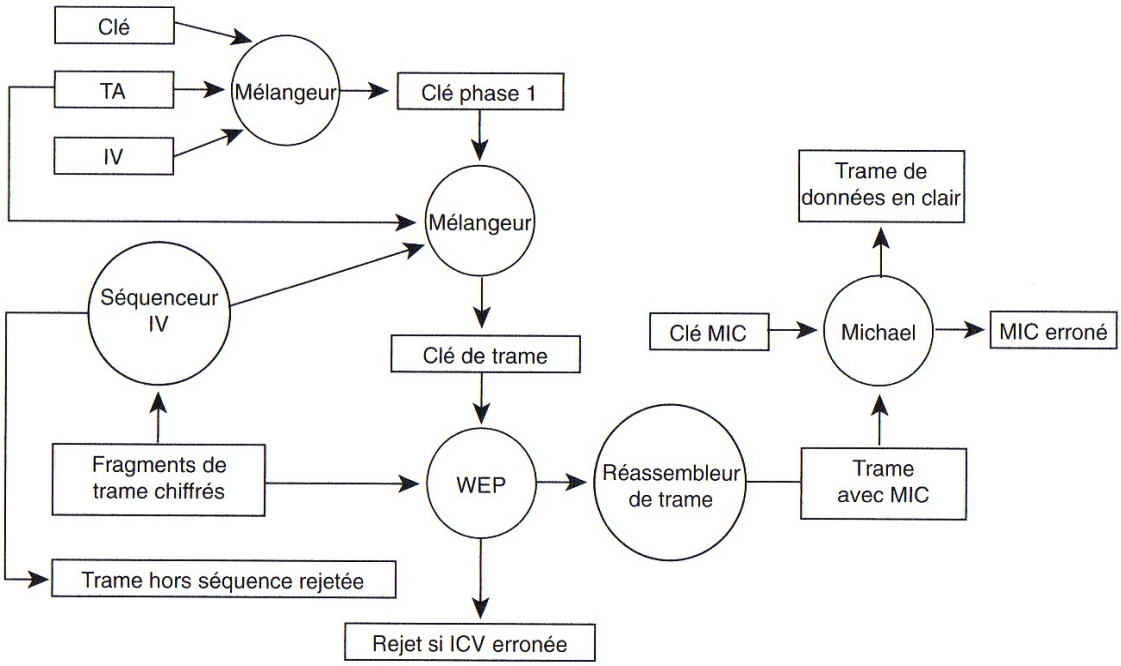
La procédure globale de chiffrement TKIP se déroule de la manière suivante :

1. L'algorithme de création de clé de trame calcule une clé.
2. L'algorithme MIC génère une valeur MIC pour la totalité de la trame.
3. La trame est fragmentée selon les caractéristiques MAC définies pour le processus de fragmentation.
4. La clé de trame chiffre les fragments.
5. les fragments chiffrés sont transmis.



Le processus de déchiffrement de TKIP se déroule de manière semblable mais inversé :

1. La clé de phase 1 est précalculée.
2. La clé de phase 2, ou clé de trame, est calculée à partir de l'IV contenu dans le fragment de trame WEP entrant.
3. Si l'IV appartient à une trame arrivée hors séquence, celle-ci est rejetée.
4. Le fragment de trame est déchiffré, et le contrôle de l'ICV réalisé.
5. Si l'ICV est erronée, la trame est rejetée.
6. Le réassembleur reconstitue la trame originale à partir des fragments déchiffrés.
7. Le récepteur calcule la valeur MIC et la compare à celle du champ MIC de la trame.
8. Si les deux valeurs correspondent, la trame est traitée par le récepteur.
9. Si les valeurs ne correspondent pas, la fonction MIC échoue, et le récepteur initie la phase de contre-mesures MIC.



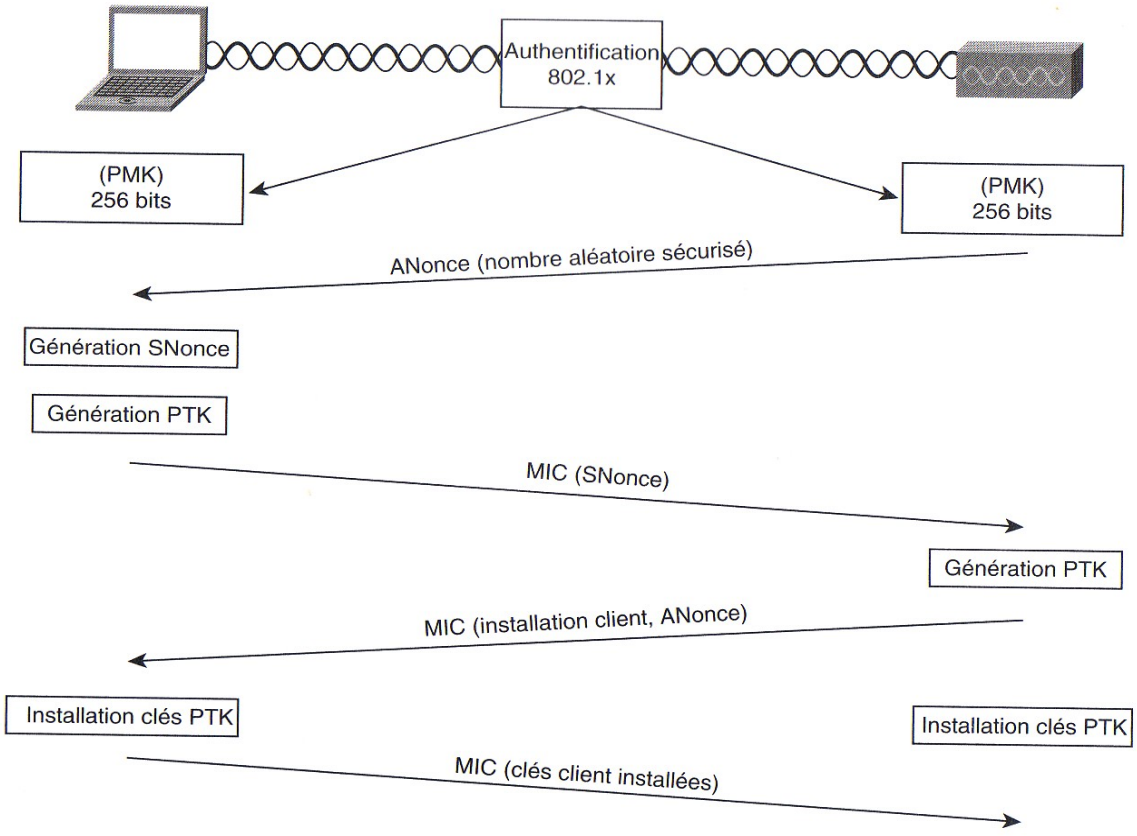
Les contre-mesures MIC consistent en l'exécution des actions suivantes par le récepteur :

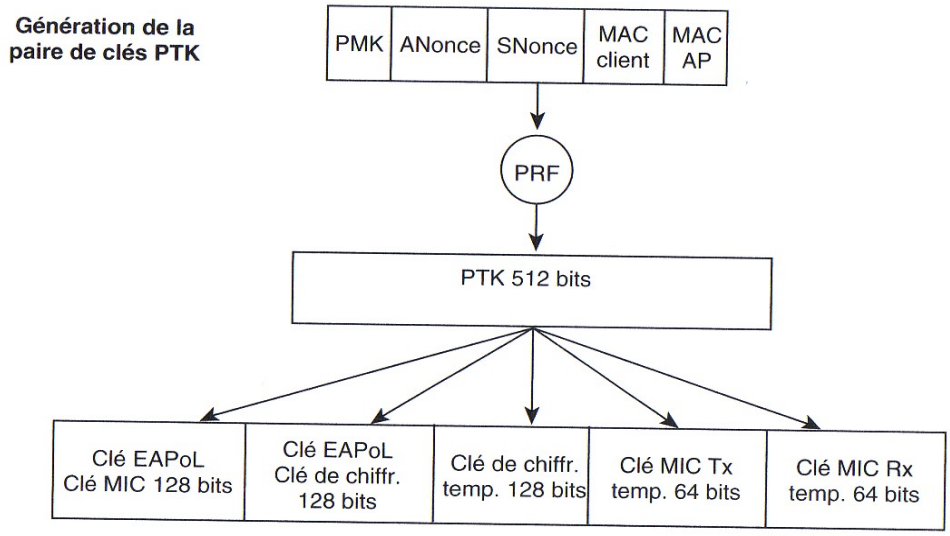
1. Suppression des clés existantes pour l'association.
2. L'évènement est consigné dans un journal en tant qu'évènement lié à la sécurité.
3. Pour ralentir l'attaque, le client à l'origine de la trame fautive ne peut se réassocier et s'authentifier pendant in intervalle de 60 s.
4. Si le client a reçu la trame, il supprime toute autre trame ne faisant pas partie des échanges 802.1x.
5. Le client demande une nouvelle clé.

Les deux mécanismes TKIP présentés ci-dessus mentionnent l'emploi de deux clés : celle de chiffrement de trame et celle de la fonction MIC.

10.9.5. Gestion avancée des clés

Les algorithmes impliqués dans la procédure d'authentification de 802.1x et EAP permettent au serveur RADIUS et au client de générer dynamiquement une clé par l'utilisateur. La clé dérivée pendant l'authentification n'est pas la même que celle qui sert au chiffrement des trames ni à la protection de leur intégrité. Dans 802.1i et WPA, elle s'appelle *clé maître*. C'est elle qui permet de générer les autres clés. La figure ci-dessous montre la hiérarchie des clés unicast 802.11.



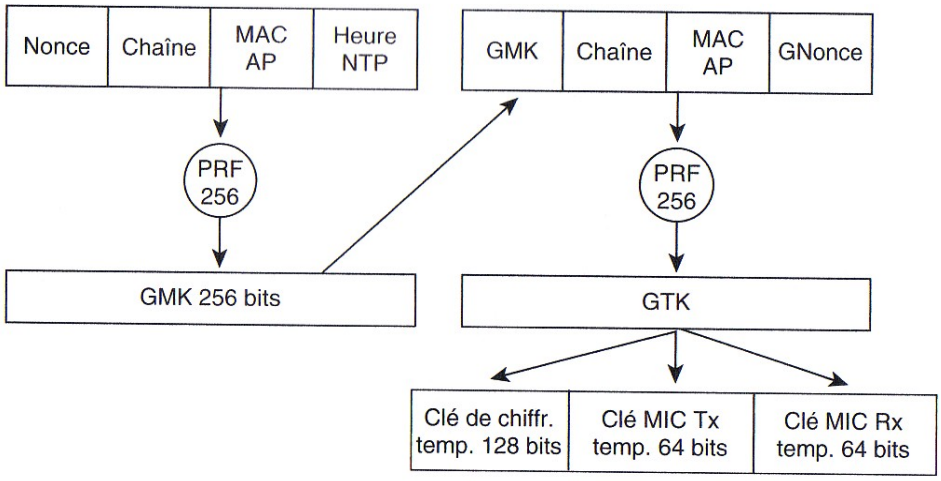


Le mécanisme de génération des clés de chiffrement est un dialogue protocolaire en quatre temps, appelé *four-way handshake*, qui se déroule comme suit :

1. Le client et l'AP installent chacun leur exemplaire de la clé dynamique issue du mécanisme d'authentification 802.1x, la PMK (Pairwise Master Key).
2. L'AP envoie au client un nombre aléatoire sécurisé, appelé « nonce authentificator », ou ANonce, dans une trame 802.1x EAPoL-Key.
3. Le client génère en local un nombre aléatoire sécurisé, appelé « nonce supplicant », ou SNonce.

4. Le client génère la clé éphémère PTK (Pairwise Transien Key), également créée en deux exemplaires, en combinant la PMK, le SNonce, l'ANonce, l'adresse MAC du client, l'adresse MAC de l'AP et une chaîne d'initialisation. Les adresses MAC respectent un ordre, l'adresse de plus faible valeur précédant l'autre. Ce processus s'assure que le client et l'AP traitent les adresses MAC de la même manière.
5. La valeur combinée est traitée par une fonction de génération pseudo-aléatoire, ou PRF (Pseudo-Random Function), pour générer une PTK de 512 bits.
6. Le client envoie à l'AP le SNonce qu'il a généré à l'étape 3 dans un message 802.1x EAPoL-Key protégé par la clé MIC EAPoL-Key.
7. L'AP utilise le SNonce pour calculer la PTK de la même manière que le client.
8. L'AP emploie la clé MIC EAPoL-Key pour valider l'intégrité du message émanant du client.
9. L'AP envoie un message EAPoL-Key indiquant que le client doit installer la PTK et son ANonce, protégé par la clé MIC EAPoL-Key. Cette étape permet au client de vérifier que l'ANonce qu'il a reçu à l'atape 2 est valide.
10. Le client envoie un message EAPoL-Key protégé par la clé MIC EAPoL-Key, indiquant que les clés sont installées.

Le PMK et PTK dérivées sont par essence unicast. Elles sont assignées à un seul utilisateur et ne chiffrent et déchiffrent que les trames unicast. Les trames broadcast requièrent une hiérarchie de clés séparée car l'emploi des clés unicast pour ces trames provoquerait un accroissement considérable du trafic sur le réseau. En effet, l'AP la seule entité dans un BSS susceptible d'envoyer du trafic broadcast ou multicast serait dans l'obligation d'envoyer la même trame, broadcast ou multicast, à chaque utilisateur après l'avoir chiffrée avec la clé de trame appropriée.
L'envoi de trames broadcast et multicast s'appuie sur une hiérarchie de clés de groupe. La clé dite GMK (Group Master Key) se trouve au sommet et est dérivée par l'AP. Le processus de dérivation repose sur une fonction PRF qui produit une GMK de 256 bits. Les valeurs en entré de la fonction PRF-256 sont un nombre aléatoire chiffré, ou encore, une chaîne de texte, l'adresse MAC de l'AP et l'heure au format du protocole NTP (Network Time Protocol). Le schéma ci-dessous montre cette hiérarchie des clés de groupe.



Les valeurs de la GMK, de la chaîne de texte, de l'adresse MAC de l'AP et du GNonce (une valeur émanant du compteur de clé sur l'AP) sont concaténées et traitées par la fonction PRF, qui produit en sortie une clé de groupe éphémère d'une taille de 256 bits, la GTK (Group

Transient Key). Sa structure se décompose en une clé de 128 bits pour le chiffrement broadcast ou multicast, une clé MIC de transmission de 64 bits et une clé MIC de réception de 64 bits. Les clés de chiffrement suivent le même type de fonctionnement que les clés unicast dérivées d'une PMK.

Le client intègre les clés de chiffrement de groupe au moyen d'un message EAPoL-Key. L'AP envoie au client ce message chiffré avec la clé de chiffrement unicast du client. Les clés de groupe sont purgées et régénérées chaque fois qu'une station se désassocie ou se désauthentifie du BSS. En cas de valeur MIC erronée, l'une des contre-mesures à appliquer consiste à purger toutes les clés relatives au récepteur touché, les clés de groupe incluses.

10.9.6. Le chiffrement AES

Les opérations de chiffrement WEP et d'authentification 802.11 sont connues pour leurs faiblesses. Les solutions apportées par l'IEEE et WPA apportent un remède en introduisant TKIP et en offrant des options d'authentification robustes par l'entremise de 802.1x. Ces perfectionnements permettent de sécuriser les WLAN 802.11 tout en préservant l'équipement existant. L'IEEE travaille aussi sur des mécanismes de chiffrement plus robustes et a déjà adopté AES pour ce qui est de la section confidentialité des données du standard 802.11i. WPA n'offre pas de support pour le chiffrement AES. Des versions futures de WPA seront vraisemblablement publiées pour s'aligner sur les spécifications de 802.11i pour le support de solutions de chiffrement AES interopérables.

AES incarne la fonction de chiffrement de prochaine génération approuvée par le NIST (National Institute for Standards and Technology). Cet organisme a invité les acteurs du monde de la cryptographie à produire de nouveaux algorithmes de chiffrement en posant comme condition qu'ils soient totalement publiés et libres de droits. Les critères de jugement des solutions étaient la robustesse du chiffrement et l'ergonomie de l'implémentation.

11. Les serveurs RADIUS

- Windows 2000 Serveur
- Windows 2003 Serveur
- FreeRADIUS (Linux) ⟶ gratuit (le plus utilisé)
- GNU-Radius (Linux) ⟶ gratuit
- OpenRADIUS (Linux) ⟶ gratuit

freeRADIUS Microsoft Windows 2000 Advanced Server Microsoft Windows Server 2003

Nous verrons plus loin la configuration.

11.1. Le wi-fi est t-il sécuriser ?

Les ondes radioélectriques ont intrinsèquement une grande capacité à se propager dans toutes les directions avec une portée relativement grande. Il est ainsi très difficile d'arriver à confiner les émissions d'ondes radio dans un périmètre restreint. La propagation des ondes radio doit également être pensée en trois dimensions. Ainsi les ondes se propagent également d'un étage à un autre (avec de plus grandes atténuations.

La principale conséquence de cette "propagation sauvage" des ondes radio est la facilité que peut avoir une personne non autorisée d'écouter le réseau, éventuellement en dehors de l'enceinte du bâtiment où le réseau sans fil est déployé.

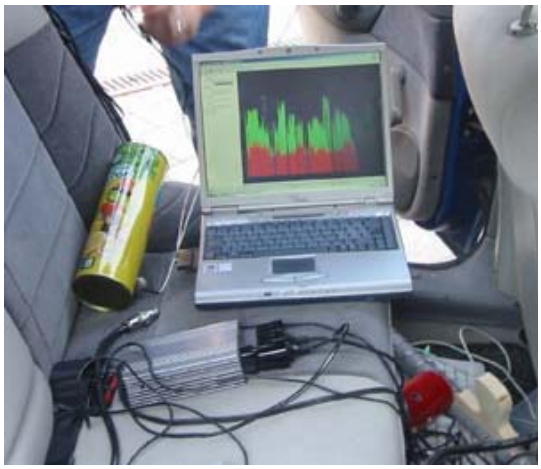
Là où le bât blesse c'est qu'un réseau sans fil peut très bien être installé dans une entreprise sans que le service informatique ne soit au courant ! Il suffit en effet à un employé de brancher un point d'accès sur une prise réseau pour que toutes les communications du réseau soient rendues "publiques" dans le rayon de couverture du point d'accès !

De plus comme nous l'avons vu précédemment, le cryptage WEP présente de très gros problèmes au niveau de la sécurité.

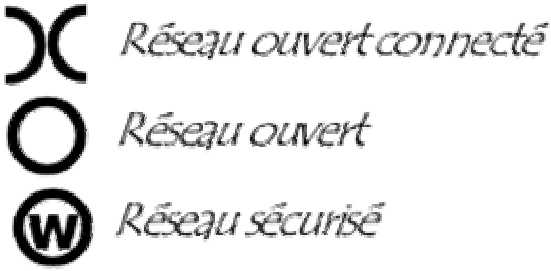
11.2. Les risques en matière de sécurité

11.2.1. Le War-driving (craie-fiti)

Etant donné qu'il est très facile d'"écouter" des réseaux sans fil, une pratique venue tout droit des Etats-Unis consiste à circuler dans la ville avec un ordinateur portable (voire un assistant personnel) équipé d'une carte réseau sans fil à la recherche de réseaux sans fil, il s'agit du war driving (parfois noté wardriving ou war-Xing pour "war crossing"). Des logiciels spécialisés dans ce type d'activité permettent même d'établir une cartographie très précise en exploitant un matériel de géo localisation (GPS, Global Positionning System).



Les cartes établies permettent ainsi de mettre en évidence les réseaux sans fil déployés non sécurisés, offrant même parfois un accès à internet ! De nombreux sites capitalisant ces informations ont vu le jour sur internet, si bien que des étudiants londoniens ont eu l'idée d'inventer un "langage des signes" dont le but est de rendre visible les réseaux sans fil en dessinant à même le trottoir des symboles à la craie indiquant la présence d'un réseau wireless, il s'agit du « war-chalking » (francisé en craieFiti ou craie-fiti). Deux demi-cercles opposés désignent ainsi un réseau ouvert offrant un accès à Internet, un rond signale la présence d'un réseau sans fil ouvert sans accès à un réseau filaire et enfin un W encerclé met en évidence la présence d'un réseau sans fil correctement sécurisé.



Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :

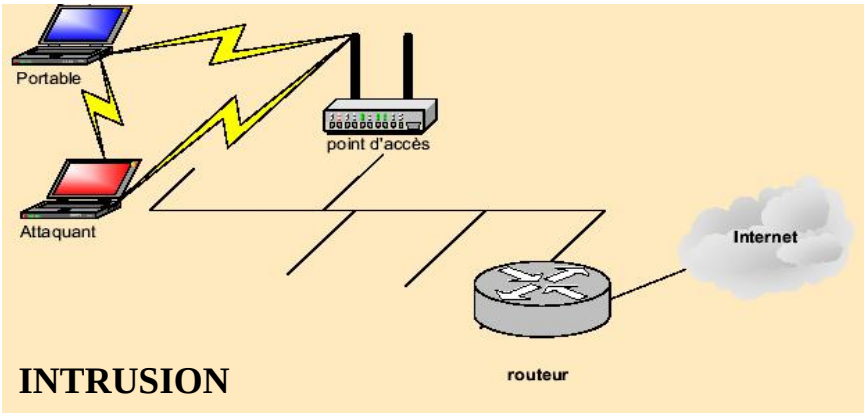
- ✓ L'interception de données consistant à écouter les transmissions des différents utilisateurs du réseau sans fil
- ✓ Le détournement de connexion dont le but est d'obtenir l'accès à un réseau local ou à Internet
- ✓ Le brouillage des transmissions consistant à émettre des signaux radio de telle manière à produire des interférences
- ✓ Les dénis de service rendant le réseau inutilisable en envoyant des commandes factices

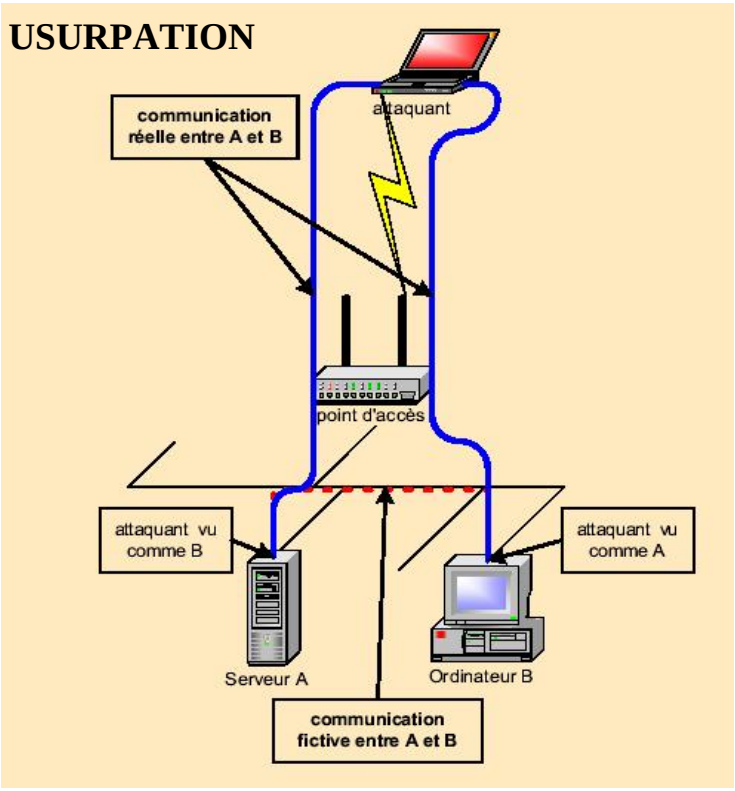
11.2.2. L'interception de données

Par défaut un réseau sans fil est non sécurisé, c'est-à-dire qu'il est ouvert à tous et que toute personne se trouvant dans le rayon de portée d'un point d'accès peut potentiellement écouter toutes les communications circulant sur le réseau. Pour un particulier la menace est faible car les données sont rarement confidentielles, si ce n'est les données à caractère personnel. Pour une entreprise en revanche l'enjeu stratégique peut être très important.

11.2.3. L'intrusion réseau (intrusion, usurpation)

Lorsqu'un point d'accès est installé sur le réseau local, il permet aux stations d'accéder au réseau filaire et éventuellement à Internet si le réseau local y est relié. Un réseau sans fil non sécurisé représente de cette façon un point d'entrée royal pour le pirate au réseau interne d'une entreprise ou une organisation.





Outre le vol ou la destruction d'informations présentes sur le réseau et l'accès à Internet gratuit pour le pirate, le réseau sans fil peut également représenter une aubaine pour ce dernier dans le but de mener des attaques sur Internet. En effet étant donné qu'il n'y a aucun moyen d'identifier le pirate sur le réseau, l'entreprise ayant installé le réseau sans fil risque d'être tenue responsable de l'attaque.

11.2.4. Le brouillage radio

Les ondes radio sont très sensibles aux interférences, c'est la raison pour laquelle un signal peut facilement être brouillé par une émission radio ayant une fréquence proche de celle utilisée dans le réseau sans fil. Un simple four à micro-ondes peut ainsi rendre totalement inopérable un réseau sans fil lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.

11.2.5. Les dénis de service

La méthode d'accès au réseau de la norme 802.11 est basée sur le protocole CSMA/CA, consistant à attendre que le réseau soit libre avant d'émettre. Une fois la connexion établie, une station doit s'associer à un point d'accès afin de pouvoir lui envoyer des paquets. Ainsi, les méthodes d'accès au réseau et d'association étant connues, il est simple pour un pirate d'envoyer des paquets demandant les dés association de la station. Il s'agit d'un déni de service, c'est-à-dire d'envoyer des informations de telle manière à perturber volontairement le fonctionnement du réseau sans fil.

D'autre part, la connexion à des réseaux sans fil est consommatrice d'énergie. Même si les périphériques sans fil sont dotés de fonctionnalités leur permettant d'économiser le maximum d'énergie, un pirate peut éventuellement envoyer un grand nombre de données (chiffrées) à une machine de telle manière à la surcharger. En effet, un grand nombre de périphériques portables (assistant digital personnel, ordinateur portable, ...) possèdent une autonomie limitée, c'est pourquoi un pirate peut vouloir provoquer une surconsommation d'énergie de telle manière à rendre l'appareil temporairement inutilisable, c'est ce que l'on appelle un déni de service sur batterie.

11.3. Les logiciels de piratage

11.3.1. Faiblesse du RC4 et vulnérabilité du WEP

- Le WEP comporte une faille profonde liée à l'algorithme RC4 lui-même.
- Un certain nombre d'IV dits « faibles » (contenant des informations sur la clé) peuvent permettre d'obtenir des octets de la clé WEP par analyse statistique.
- Estimation de crackage WEP :
    - Clé de 40 bits : 518 400 trames
    - Clé de 104 bits : 1 347 840 trames
    - Sur un réseau à fort trafic une clé peut se découvrir en 30 minutes

11.3.2. Les logiciels WIFI

Nom du logiciel	Type	OS	Licence	Divers
NetStumbler / MiniStumbler	Logiciel	Windows / Pocket PC	Gratuit	• Scanner et détecteur par l'intermédiaire d'un GPS • Informe sur le type de cryptage, …
Aircrack	Logiciel	Linux et Windows	Gratuit	• Sniff réseau et décryptage clé WEP 64 et 128 bits

AiroPeek NX et VX	Logiciel	Windows	Payant ($1495)	• Sniff réseau • Gestion d'audit professionnel
Airsnort	Logiciel	Linux et Windows	Gratuit	• Sniff de réseau
Airscanner	Logiciel	Pocket PC	Payant	• Scanner et détecteur par l'intermédiaire d'un GPS
WPA cracker	Logiciel	Linux	Gratuit	• Décryptage de clé WPA-PSK
CoWPatty	Logiciel	Linux	Gratuit	• Décryptage de clé WPA-PSK
WepCrack et WepWedgie	Logiciel	Linux	Gratuit	• Décryptage de clé WEP 64 et 128 bits
Kismet / Kismac	logiciel	Linux / Pocket PC	Gratuit	• Données en temps réel • Signal de réception pour géolocalisation
Auditor Security Collection	OS	Linux	Gratuit	Live CD basé sur Knoppix contenant tous les utilitaires de scan, spoofing et décryptage WEP, WPA, ainsi que pour l'Ethernet.

11.3.3. Logiciel pour le spoofing d'adresse Mac

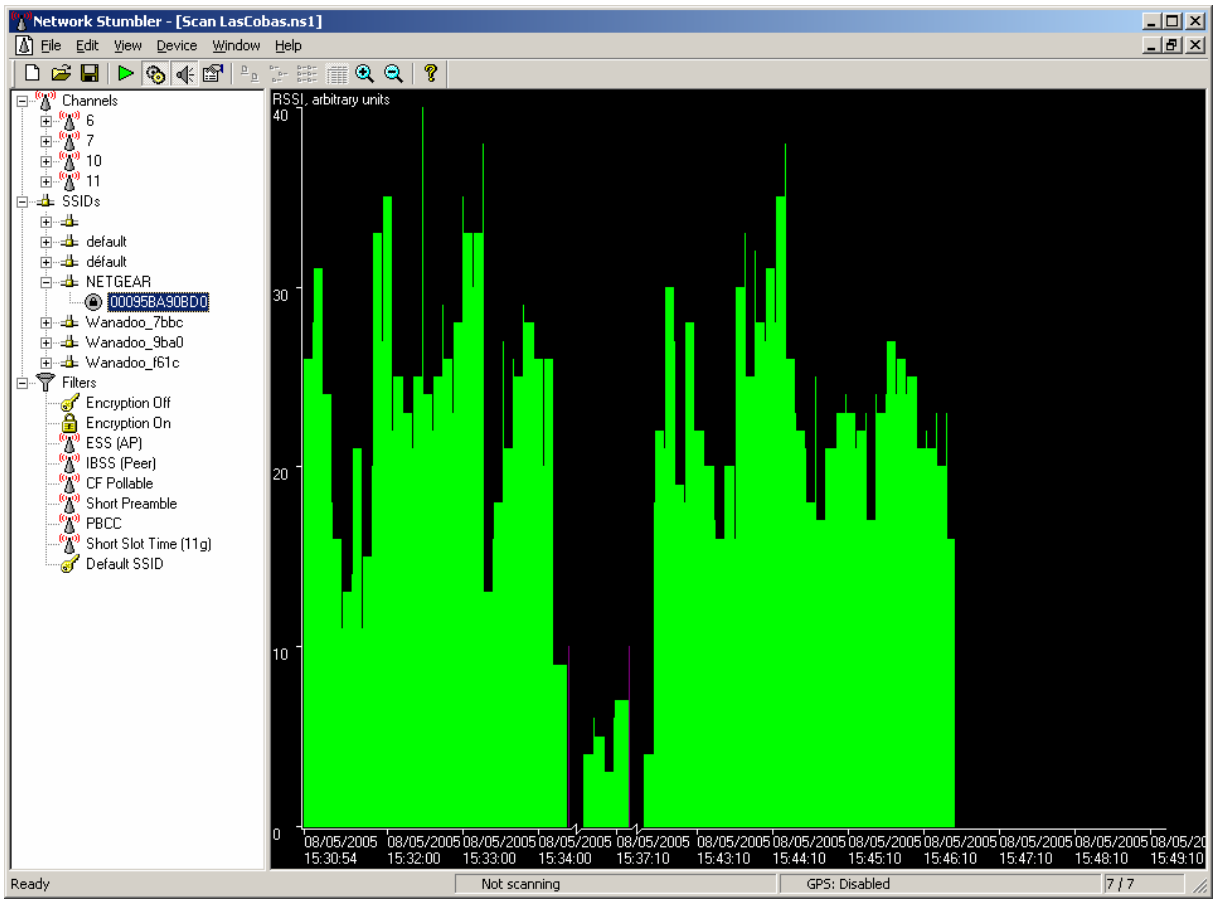
- A-Mac Address Change (Windows) Payant
- SMAC (Windows) Payant
- GNU MAC Changer (Linux)

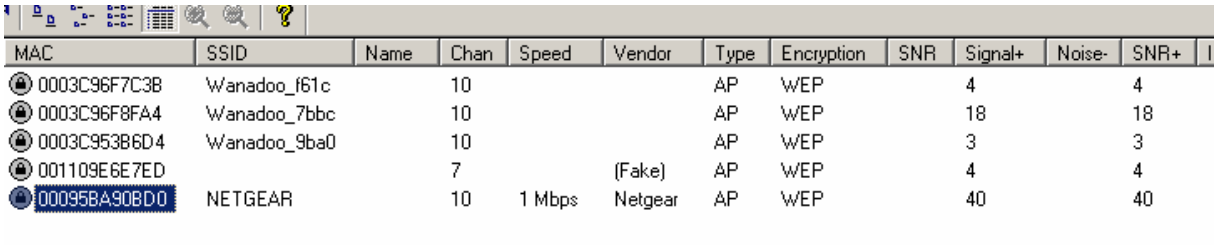
11.3.4. NetStumbler :

NetStumbler permet d'identifier et de qualifier les réseaux Wifi environnants. Chaque réseau est détaillé avec un numéro du canal, un SSID, un débit, le type de périphérique Wifi (point d'accès, routeur...), le SNR, l'adresse IP (si elle est disponible), la force du signal et le bruit. Un graphe mesure en temps réel la force du signal.

Un système de filtrage permet d'identifier les points d'accès avec ou sans Encryption.

NetStumbler peut être relié à un système GPS pour localiser le/les point(s) d'accès



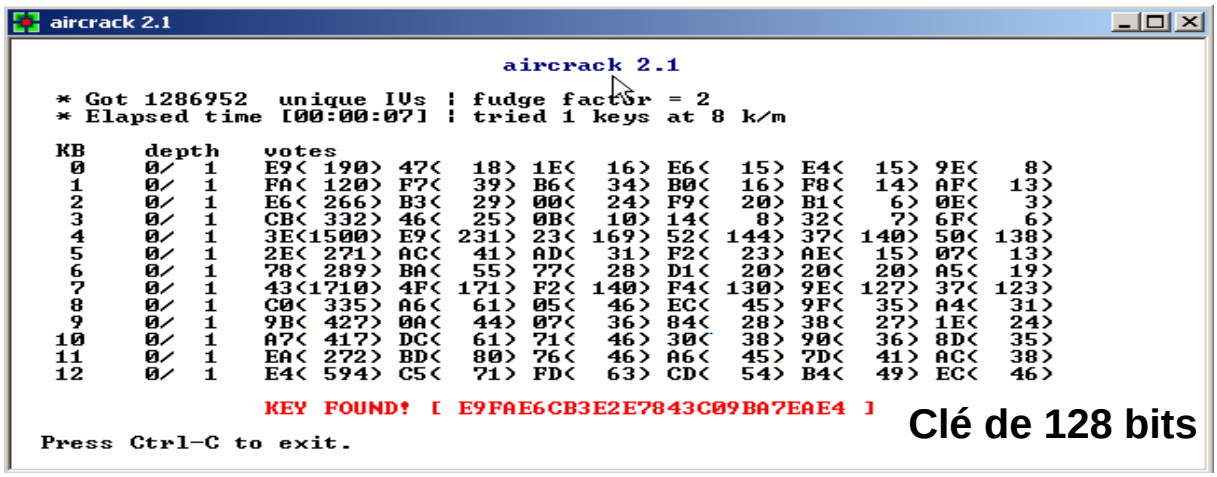


MAC	SSID	Name	Chan	Speed	Vendor	Type	Encryption	SNR	Signal+	Noise-	SNR+
0003C96F7C3B	Wanadoo_f61c		10			AP	WEP		4		4
0003C96F8FA4	Wanadoo_7bbc		10			AP	WEP		18		18
0003C953B6D4	Wanadoo_9ba0		10			AP	WEP		3		3
001109E6E7ED			7		(Fake)	AP	WEP		4		4
00095BA90BD0	NETGEAR		10	1 Mbps	Netgear	AP	WEP		40		40

11.3.5. Aircrack

Aircrack est un briseur de clef WEP 802.11. Il implémente l'attaque dénommée Fluhrer-Mantin-Shamir (FMS), ainsi que d'autres nouvelles attaques du talentueux développeur nommé KoreK. Quand suffisamment de paquets ont-été récoltés, Aircrack peut presque instantanément récupérer la clef WEP.

Fonctionne uniquement avec les drivers « WildPacket »



11.3.5.1. Explication sur AirCrack ?

11.3.5.1.1. Qu'est ce que Aircrack ?

Aircrack est un briseur de clé WEP 802.11. Il implémente l'attaque dénommée Fluhrer-Mantin-Shamir (FMS), ainsi que d'autres nouvelles attaques du développeur nommé KoreK. Quand suffisamment de paquets ont-été récoltés, Aircrack peut presque instantanément récupérer la clé WEP.

11.3.5.1.2. Comment AirCrack fonctionne ?

Chaque paquet chiffré avec une clé WEP est associé à un vecteur d'initialisation (IV) de 24 bits. Certains IVs laissent passer des informations sur certains octets de la clé, ainsi, statistiquement, la clé correcte émerge quand suffisamment d'IVs ont été récoltés.

11.3.5.1.3. Combien de paquets faut-il pour récupérer une clé WEP ?

Cela dépend de la chance et de la taille de la clé. Pour une clé de 64 bits, environs 150 000 IVs unique sont généralement suffisant. Pour des clés de 128 bits, entre 500 000 et 1 million de paquet seront nécessaires.

11.3.5.1.4. Questions sur AirCrack :

J'ai X millions d'IVs mais Aircrack ne trouve pas la clé.

La découverte des clés WEP n'est pas une science exacte, parfois cela peut ne pas fonctionner du premier coup. Pour augmenté les chances de réussir, collecter le maximum de paquet crypter possible, on peut également augmenté les chances en augmentant le facteur Fudge (bêtise en anglais) particulièrement lors des clés de 64 bits.

```
4 : bruteforce fudge factor (current: 2)
```

Sinon, si la clé WEP à changer pendant le sniffage, alors AirCrack ne réussira pas à trouvé la clé.

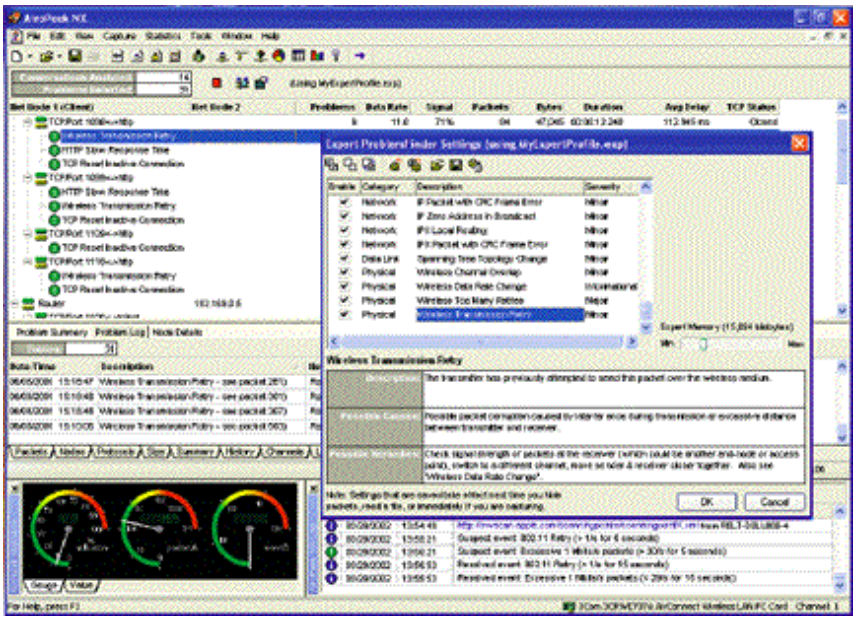
Le renifleur que j'utilise a l'air incapable de capturer la moindre IV !

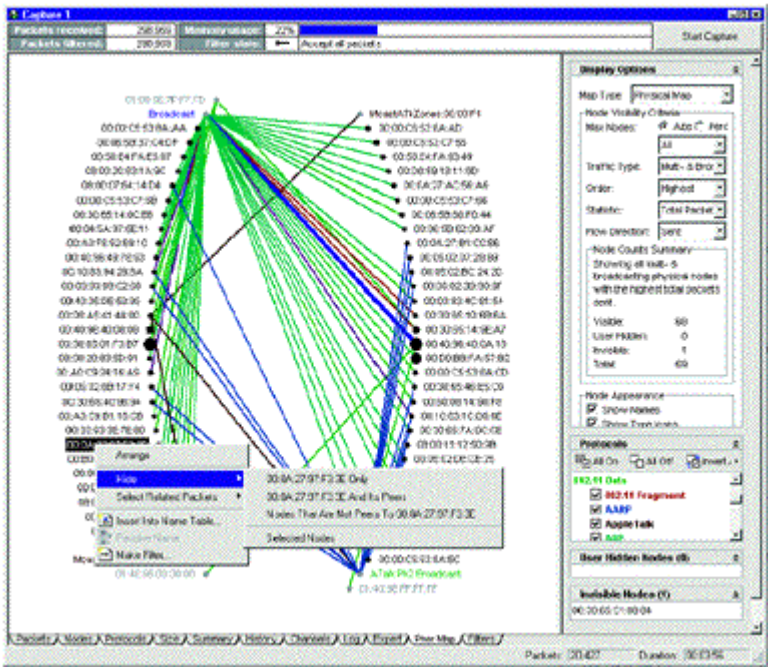
Evidement, il est impossible de capturer des paquets cryptés s'il n'y a pas de trafic, …
Assurez vous que la carte sans fil avec le Vlan (n'essayez pas de craquer des réseaux 802.11g avec une carte 802.11b).
Assurez vous également que le drivers WildPacket utilisé est bien adapté à votre carte (Chipset, …), sinon, même si celui-ci est bien reconnu par Windows et Windows vous indique qu'il est bien installé (dans Propriété système → Gestionnaire de périphérique, aucun point d'exclamation jaune ou de croix rouge sur la carte sans fil), lors du sniffage, il ne pourra pas récupéré les IV malgrès tous les paquets reçu.
Sinon, si vous êtes trop loin du point d'accès, vous allez seulement voir les trames « beacon » non crypter (trame de synchronisation AP/Client ou Client/Client suivant l'infrastructure réseau utilisé) qui sont à la vitesse la plus lente : 1 Mb/s mais vous ne pourrez pas capturer le traffic qui va plus vite, dans ce cas, il peut être utile d'utiliser une antenne directionnelle à gain fort.

J'ai un énorme fichier pcap mais AirCrack ne trouve aucun IV dedans ?

Les IV's capturés de réseau protégées par WPA sont inutiles pour craquer les clés WEP et AirCrack va automatiquement les éliminer.

11.3.6. AiroPeek





- **Une interface utilisateur qui permet de localiser et résoudre les problèmes facilement.**
- **Décryptage des clés WEP**
- **Décode le protocole 802.11**
- **L'analyse et le contrôle du respect de la politique de sécurité.**
- **Des audits du site (format HTML, XML, texte, …).**
- **L'analyse des réseaux WIFI locaux et distant.**
- **Des captures simultanés**
- **Gère des filtres de scan, peut envoyé des alarmes**
- **…**

Fonctionne uniquement avec les drivers « WildPacket »

En bref, un excellent logiciel d'audit et sécurité réseau WIFI.
PS : Il existe la même version de ce logiciel pour les réseaux Ethernet (EtherPeek).

11.3.7. Est-ce que tout le monde peut piraté le WIFI ?

- Non.
- Cela nécessite quelques connaissances sur le fonctionnement des logiciels ainsi que sur le WIFI.
- Les **logiciels de craquage de clé** nécessitent des drivers très spéciaux (WildPacket issu du logiciel AiroPeek), qui ne sont pas accepté par toutes les cartes WIFI (suivant le chipset de la carte).
    - Pourquoi ? : Car en Wifi les données sont envoyé en Broadcast, donc si la carte réseau voit que les paquets ne lui sont pas attribué elle les rejettes.
    - Ce drivers permettent de modifier le mode de fonctionnement de la carte réseau, en lui faisant renvoyé tous les paquets dans le pc.
    - http://www.wildpackets.com/support/drivers (c'est driver sont inclus dans le répertoire d'installation de AiroPeek).

 **Si la référence d'une carte réseau portant la marque Y fonctionne avec un pilote « Wildpacket », cela ne veut absolument pas dire que toutes les cartes réseaux de cette même marque fonctionneront également. (Dépendance avec le Chipset) ainsi que les révisions de la carte (Rev.X) (Modèle récent ou antérieur), les chipsets qui fonctionnent le plus souvent sous Windows ou Linux sont : Atheros, CISCO Aironet, Prismll, …**

11.4. Les méthodes pour sécuriser son réseau au maximum

Les cryptages WEP :

Les normes 802.11b, g et a utilisent plusieurs mécanismes de sécurité dont le plus connu est le cryptage WEP (voir 1.). Le WEP utilise un codage sur 40bits facilement cassable. C'est pourquoi les constructeurs l'ont porté à 64 voir 128bits. L'utilisation de clé plus longues peut se faire au détriment de la compatibilité.. Étant donne que ce n'est pas prévu par le standard. Même s'il reste des lacunes avec le WEP une clé de 128bits possède n niveau de sécurité suffisant pour peu qu'on la change régulièrement.

Le filtrage d'adresse MAC

Celui-ci peut filtrer les adresses MAC. L'adresse MAC est une adresse unique que chaque périphérique réseau possède. Elle est indissociable de celui-ci et a la forme suivante: AA-BB-CC-DD-EE-FF. Les 6 premiers éléments indiquent le constructeurs, par ex: 00-30-AB pour un produit NEATGEAR. Les 6 derniers identifient le produit. En renseignant une table de filtrage MAC au

niveau du PA, on autorise que les adresses connues à utiliser le réseau. Cette méthode n'est pas infaillible mais est relativement efficace dans 90% des cas.

Mise en place d'un VPN

http://www.universtelecoms.com/wifi/indexwifi.htm

Quelques méthodes simples pour sécuriser son réseau wi-fi

- ✓ Utiliser un SSID personnel et non pas par défaut.
- ✓ Désactivez sur votre AP le broadcast SSID (Emission en clair du SSID sur le réseau). C'est utile dans le cas où le réseau contient plusieurs AP qui n'ont pas le même SSID; cela permet au station qui changent de BSSS de pouvoir se reconnecter. Mais c'est une très mauvaise façon de faire, en général, il vaut mieux utiliser un SSID unique pour tout le réseau. (Copyright UniversalTonton)
- ✓ Eviter d'utiliser un serveur DHCP (IP dynamiques) sur le WLAN.
- ✓ Eviter d'utiliser le sous réseau 192.168.0.x avec le groupe de travail WORKGROUP
- ✓ Le cryptage WEP 128 bits (Moyennement sécurisé)
- ✓ Le cryptage WPA-PSK (Un peu plus sécurisé)
- ✓ Le cryptage WPA avec serveur d'authentification + protocole EAP-TLS (Hautement sécurisé)
- ✓ Utilisez une passphrase compliquée pour générer vos clefs (genre pas de 'maman' ou 'papa'), et, si vous etes vraiment parano, n'utilisez pas la fonction d'échange de clef automatique.(Copyright UniversalTonton)

- ✓ Utiliser le filtrage d'adresses MAC en cas d'utilisation d'un AP.

- ✓ N'utiliser les partages de fichiers que si nécessaire et de façon plus sécurisé et utilisant des comptes utilisateurs plutôt que le compte invité de Windows

- ✓ Si on possède des fichiers sensibles et que l'on utilise une partition NTFS (win2k/XP): utiliser le cryptage de données. sans le certificat (à sauvegarder précieusement) le fichier est illisible même si partagé sur le réseau.

- ✓ Mise en place d'un VPN

En attendant la mise en place de la norme 802.11i destinée à sécuriser fortement les réseaux sans-fil, les constructeurs ont développé la norme WPA (Wi-Fi Protected Access). WPA vient combler les trous de sécurité du WEP utilisé jusqu'a présent. WPA s'adresse surtout aux entreprises qui ont un grand besoin de sécurisation avancé du réseau.

Ainsi une mise à jour Windows (uniquement disponible pour Windows2000 et windowsXP) permet de mettre l'outil de configuration à jour du WPA: Mise à jour WPA microsoft.
Les constructeurs proposent en général une mise à jour de firmware/driver pour que leurs équipements gèrent cette norme. Norme qui est parfaitement interoperable il faut dire.

Pour combler les trous du WEP le WPA remplace le protocole d'encryptage (RC4) par le TKIP:

Protocole TKIP (Temporal Key Integrity Protocol)
Pour 802.11, le cryptage WEP (Wired Equivalent Privacy) est facultatif. Pour WPA, le cryptage avec le protocole TKIP est exigé. Le protocole TKIP remplace WEP par un nouvel algorithme de cryptage plus puissant que l'algorithme WEP, mais qui utilise les fonctionnalités de calcul présentes sur les périphériques sans fil existants afin d'effectuer les opérations de cryptage. Le protocole TKIP offre également les fonctionnalités suivantes :
*la vérification de la configuration de sécurité une fois les clés de cryptage déterminées ;
*la modification synchronisée de la clé de cryptage mono diffusion pour chaque trame ;
*la détermination d'une clé de cryptage mono diffusion de départ unique pour chaque authentification de clé pré partagée

A cela s'ajoute l'authentification 802.1x (Radius et EAP). L'authentification 802.1x nécessite la mise en place d'un serveur (RADIUS), cela s'adresse donc plus aux entreprises qu'aux particuliers. En cas d'absence de serveur d'authentification un system de clé pre-partagé est utilisé.

Elément le plus important du WPA: prise en charge de l'algorithme AES. Facultatif pour l'instant, car nécessitant une modification importante des équipements, l'AES est une référence en tant qu'algorithme de cryptage. Il est destiné à remplacer le RC4 utilisé dans le WEP. AES sera complètement implémenté avec la norme 802.11i. En attendant grâce au

WPA et à condition de posséder du matériel compatible, on peut protéger son réseau en utilisant le cryptage AES.

12. La création du réseau

12.1. Le matériel utilisé

- Pour créer un réseau sans fil, il faudra au minimum, un AP et une carte réseau ou uniquement deux cartes réseaux (suivant l'infrastructure réseau que vous désirez crée (IBSS, BSS, ESS)).
- Actuellement la plupart du matériel vendu est compatible avec les normes 802.11b et 802.11g ainsi que parfois avec la norme 802.11g+.
- Attention, les liaisons WIFI se font en « broadcast », le débit et par conséquent partagé entre tous les postes WIFI connecté au réseau.

12.1.1. Les routeurs/Points d'accès

Linksys-Cisco WRT54G : WRT54G Linksys Routeur AP WiFi 54 Mbs ADSL haut débit switch 4 p Firewall (Port Wan RJ 45), SANS MODEM INTEGRE

- Standards IEEE : 802.3, IEEE 802.3u, IEEE 802.11b,IEEE 802.11g
- Canaux : 13 Canaux (Europe)
- Ports :
- Un port Internet 10/100 RJ-45 pour les Modem/CableDSL
- Quatre ports LAN 10/100 RJ-45 Commutés
- Un port d'alimentation électrique
- Système de câblage : Type Categorie 5, 5e ou 6
- Débits : Jusqu'à 54Mbps (Wireless), 10/100Mbps (Ethernet)
- LEDs :Power, DMZ, Diag
- WLAN : Act, Link
- LAN : Link/Act, Full/Col, 100
- Internet : Link/Act, Full/Col, 100
- Puissance d'émission : 15 dBm

- Modulation : 802.11b CCK, DQPSK, DBPSK, 802.11g OFDM
- Protocoles réseau : TCP/IP, IPX/SPX, NetBEUI

DG834GFS 5 en 1 : Modem routeur ADSL, switch, point d'accès 802.11g (54 Mbit/s) et véritable firewall intégré

- Nouveau Design, plus compact
- Connexion à 54 Mbit/s (norme 802.11g) compatible 11 Mbit/s (norme 802.11b)
- Antenne 2dBi détachable
- Génération de clé WEP 40(56), 64 et 128 bits, saisies manuellement ou par mot clé
- ACL : authentification par adresse MAC des cartes autorisées à la connexion
- Disable SSID broadcast
- Support WPA et WPA-PSK
- Modem ADSL intégré
- Interface WEB en français
- Avec le nouveau Firmware (2.10.09) prise en charge de 5 canneaux VPN

12.1.2. Les points d'accès

WG302 point d'accès 802.11b, g et g+ (11/54/108 Mbit/s)

- Connexion à 108 Mbit/s (Super g)
- Compatible 54 Mbit/s (norme 802.11g) et 11 Mbit/s (norme 802.11b)
- Fonction POE (norme 802.3af)
- 2 antennes détachables 5 dBi
- Disable SSID broadcast
- Génération de clés WEP 40(56), 64 et 128 bits, saisies manuellement ou par mot clé
- ACL : authentification par adresse MAC des cartes autorisées à la connexion
- Support WPA et WPA – PSK (Contrôle d'accès Radius)
- Support de la fonction Bridge : Point à point - Point à multipoint - répéteur avec équipement compatible norme WDS (Wireless Distribution Signal)
- Configuration via agent web
- Serveur DHCP
- Manageable SNMP et SSH

12.1.3. Les cartes réseau PCI, PCMCIA et USB

DWL-G520 Carte PCI Super G 108Mbps 802.11g

- Taux de transfert :
- 802.11b : 1, 2, 5.5, 11 Mbit/s
- 802.11g : 6, 9, 12, 18, 24, 36, 48 et 54 Mbit/s
- 802.11g+ : 108 Mbit/s
- Fréquence : 2.457 - 2.472 GHz (France)
- Cryptage : 40-bit (également appelé 64-bit), 128 bit WEP
- Idéale pour le Video Streaming
- Sécurité sans fil renforcée avec 802.1X et WPA

Fonctionne parfaitement avec le logiciel d'audit AiroPeek, Aircrack, Kissmet, … grâce à son chipset « Atheros »

DWL-G650 Carte PC Cardbus Super G 108Mbps 802.11g

- Taux de transfert :
- 802.11b : 1, 2, 5.5, 11 Mbit/s
- 802.11g : 6, 9, 12, 18, 24, 36, 48 et 54 Mbit/s
- 802.11g+ : 108 Mbit/s
- Fréquence : 2.457 - 2.472 GHz (France)
- Cryptage : 40-bit (également appelé 64-bit), 128 bit WEP
- Idéale pour le Video Streaming
- Sécurité sans fil renforcée avec 802.1X et WPA

Fonctionne parfaitement avec le logiciel d'audit AiroPeek, Aircrack, Kissmet, … grâce à son chipset « Atheros »

Netgear WG111 : Netgear WG111 Adaptateur / Clef USB 2.0 vers Wifi 54 Mbs Ultra-Compact

- Adaptateur Wifi 54 Mbs / USB
- Boitier au format Dongle
- USB 2.0 - 40 fois plus rapide
- Câble USB pour déporter la clef
- Configuration ultra-rapide
- Cryptage WEP 40/64 et 128 bits hardware
- Mode 11 et 54 Mbs
- Antennes interne

Linksys-Cisco WMP54G : Linksys Cisco WMP54G Carte adapatateur PCI WiFi 54 Mbs 802.11g antenne 5dB

- Standard : 802.11b, Draft 802.11g
- Modulations : 802.11b: CCK (11 Mbps), DQPSK (2 Mbps),
- DBPSK (1 Mbps); 802.11g: OFDM
- Canaux : 802.11b, 11 canaux (US, Canada), draft 802.11g
- 13 Canaux (Europe), 14 Canaux (Japon)
- Interface : PCI 32 bits
- Vitesse : Jusqu'à 54Mbps
- Diodes d'affichage : Activité : Fixe avec le lien établi,
- clignote en fonction du trafic
- Securité : WEP et WPA
- Clefs WEP : 64 Bit and 128 Bit

Linksys-Cisco WPC54G

- Standard : 802.11b, Draft 802.11g
- Modulations : 802.11b: CCK (11 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps);
- 802.11g: OFDM
- Canaux : 802.11b, 11 canaux (US, Canada), draft 802.11g 13 Canaux (Europe),

- 14 Canaux (Japon)
- Interface : CardBus 32 bits
- Vitesse : Jusqu'à 54Mbps
- Diodes d'affichage : Alimentation, lien
- Securité : WEP; sous Windows XP seulement : AES, TKIP, 802.1x
- Clefs WEP : 64 Bit and 128 Bit

12.1.4. Les Caméras IP WIFI

D-Link DCS-5300G

- Caméra Internet indépendante dotée de CPU et de RAM, qui n'a pas besoin d'être reliée à un PC
- Moteur rotatif intégré permettant d'orienter la caméra automatiquement, avec support d'angles de mouvement extrêmement larges
- Accès local grâce à Ethernet ou à un réseau local sans fil 802.11g
- Accès à distance à partir d'un navigateur Web
- Prise en charge de DDNS et de UPnP pour une configuration aisée en environnement réseau
- Mise en œuvre pour la détection des intrus avec saisie d'images fixes et avertissement par e-mail
- Puissant logiciel de saisie d'images et d'enregistrement vidéo
- Configuration Web, utilitaire distant fourni

Linksys WVC54G

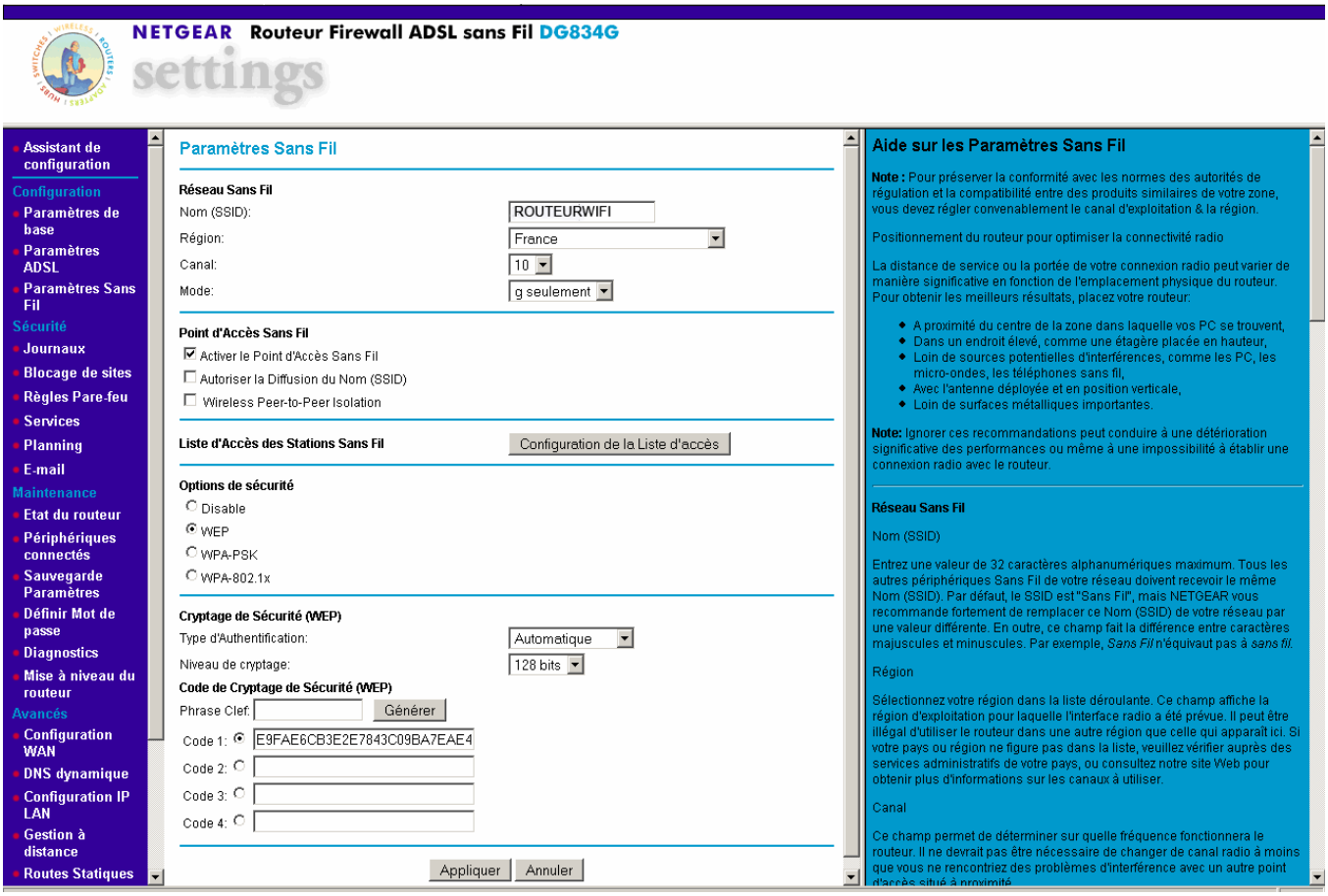
- Model Number : WVC54G
- Standards : IEEE 802.11b, IEEE 802.11g, IEEE 802.3, IEEE 802.3u
- Ports : One 10/100 Auto Crossover (MDI/MDI-X) port,Power port, 2.5mm MIC IN
- Protocols : TCP/IP, HTTP, DHCP, NTP, SMTP, UPnP (Discovery only)
- Buttons : One Reset Button
- Cabling : Type RJ-45
- Indicators : LEDS: Ready, Act/Link, Ethernet, Wireless;LCD Display of IP Address
- Security features : User Authentication, WEP Encryption,Motion Detection
- WEP key bits : 64/128 Bit
- Field of View : 57 degrees

- Brightness : Auto/Manual Adjustment

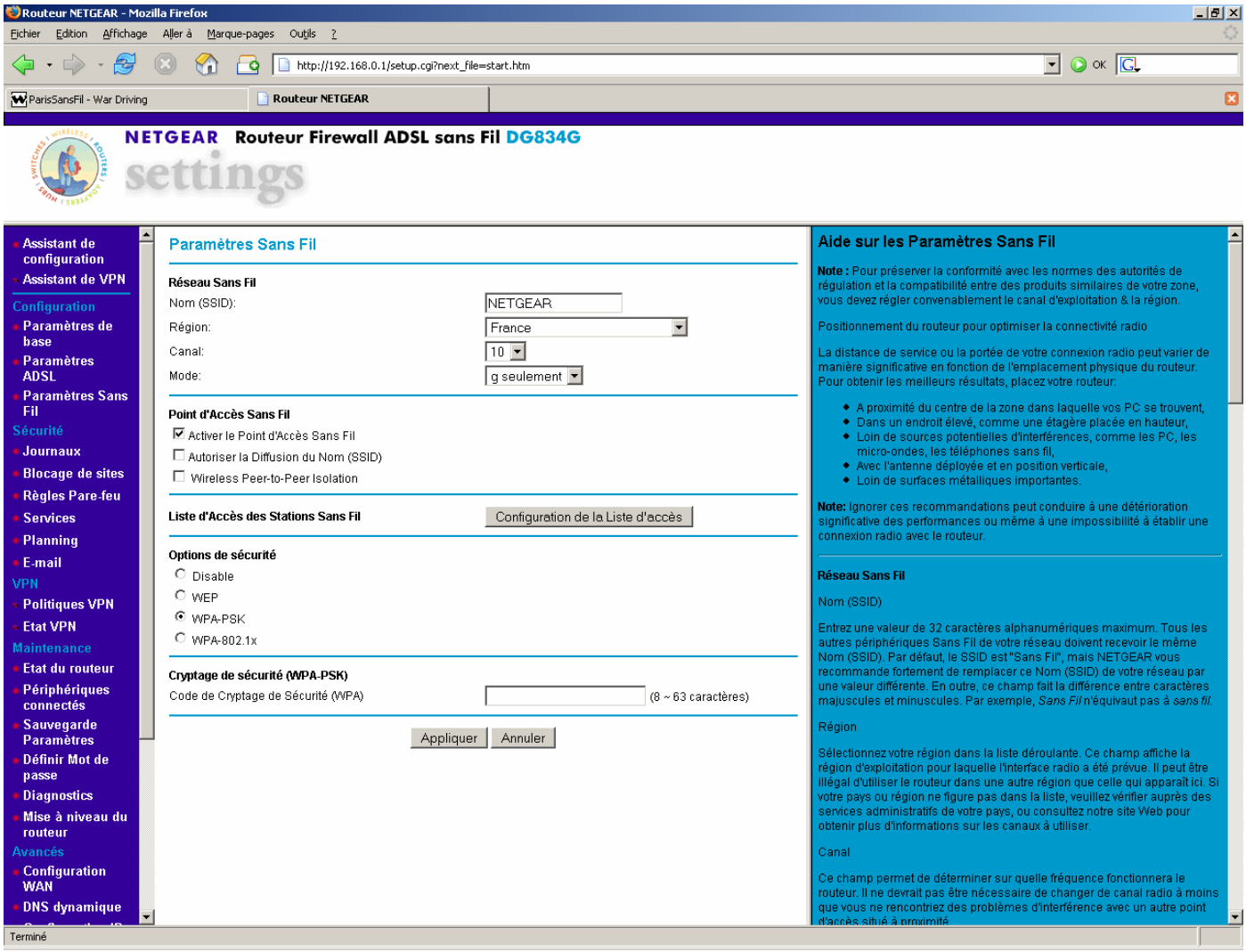
13. Configuration matériel

13.1. Exemple de configuration d'un routeur/modem avec point d'accès WIFI (NETGEAR DG834G) :

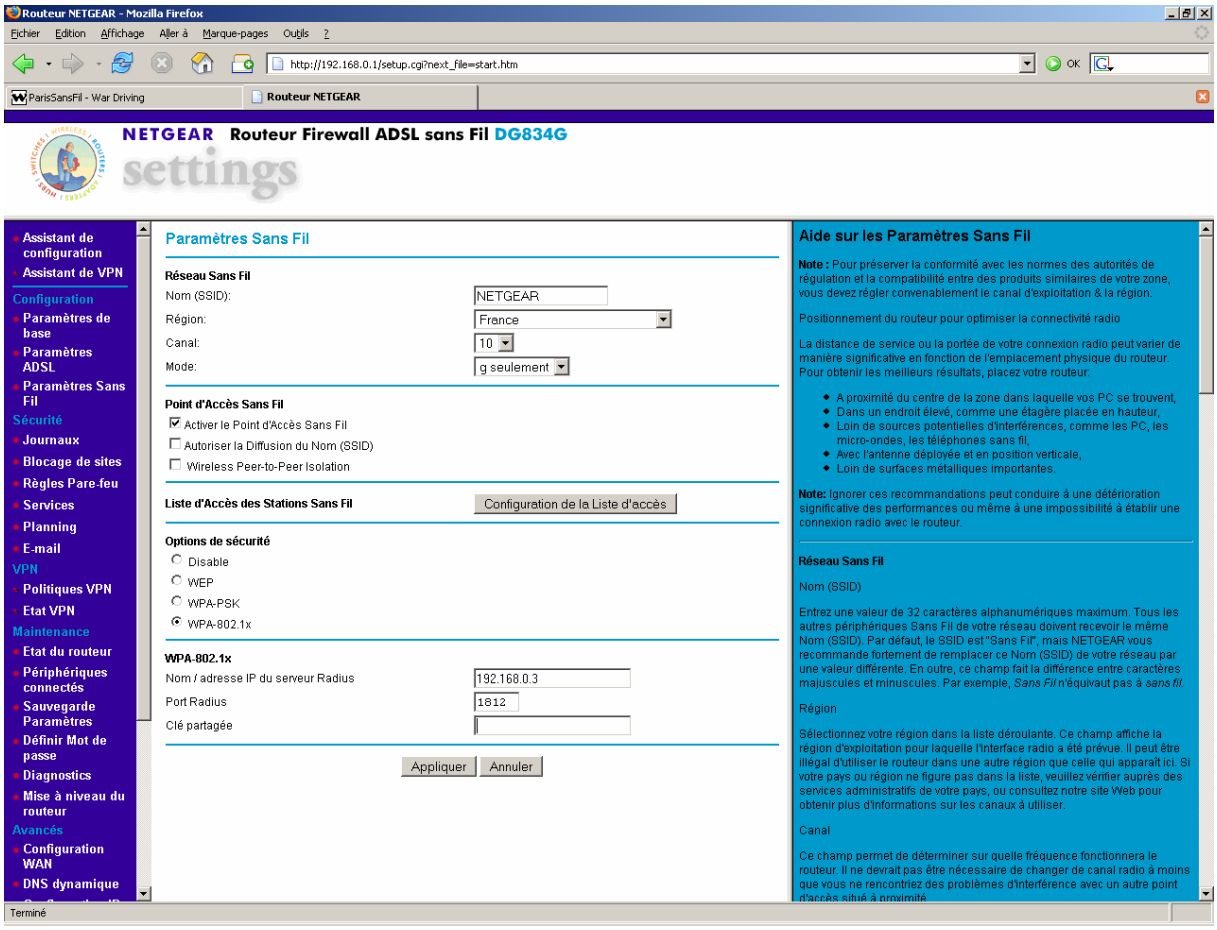
Ce routeur prend en charge plusieurs canaux, bien entendu il est conseiller d'utiliser uniquement les canaux autorisés par le pays où nous nous trouvons.



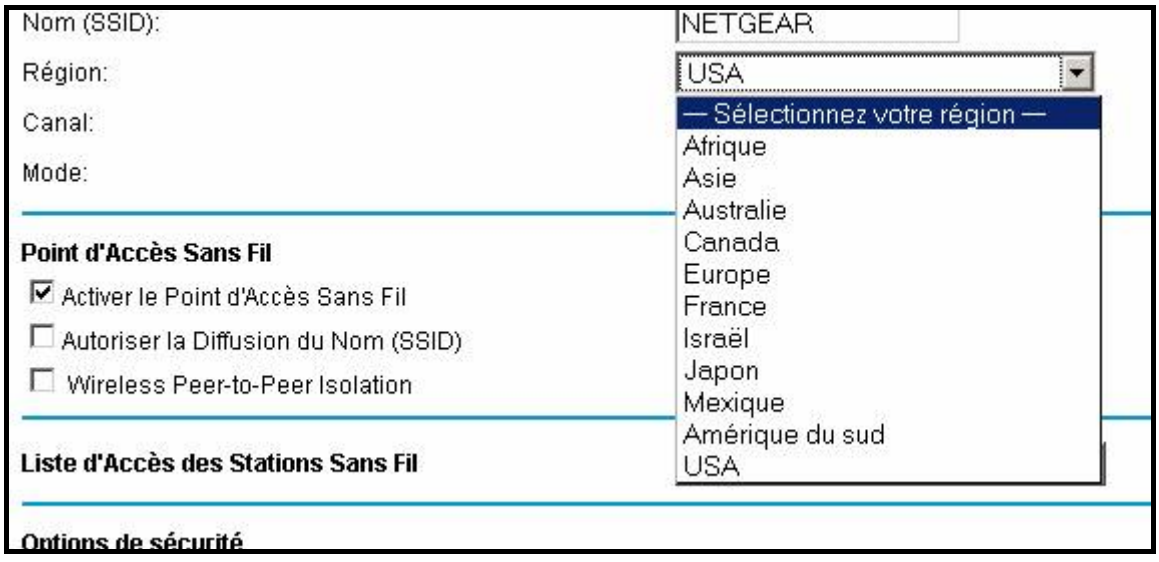
Cas d'une configuration WEP

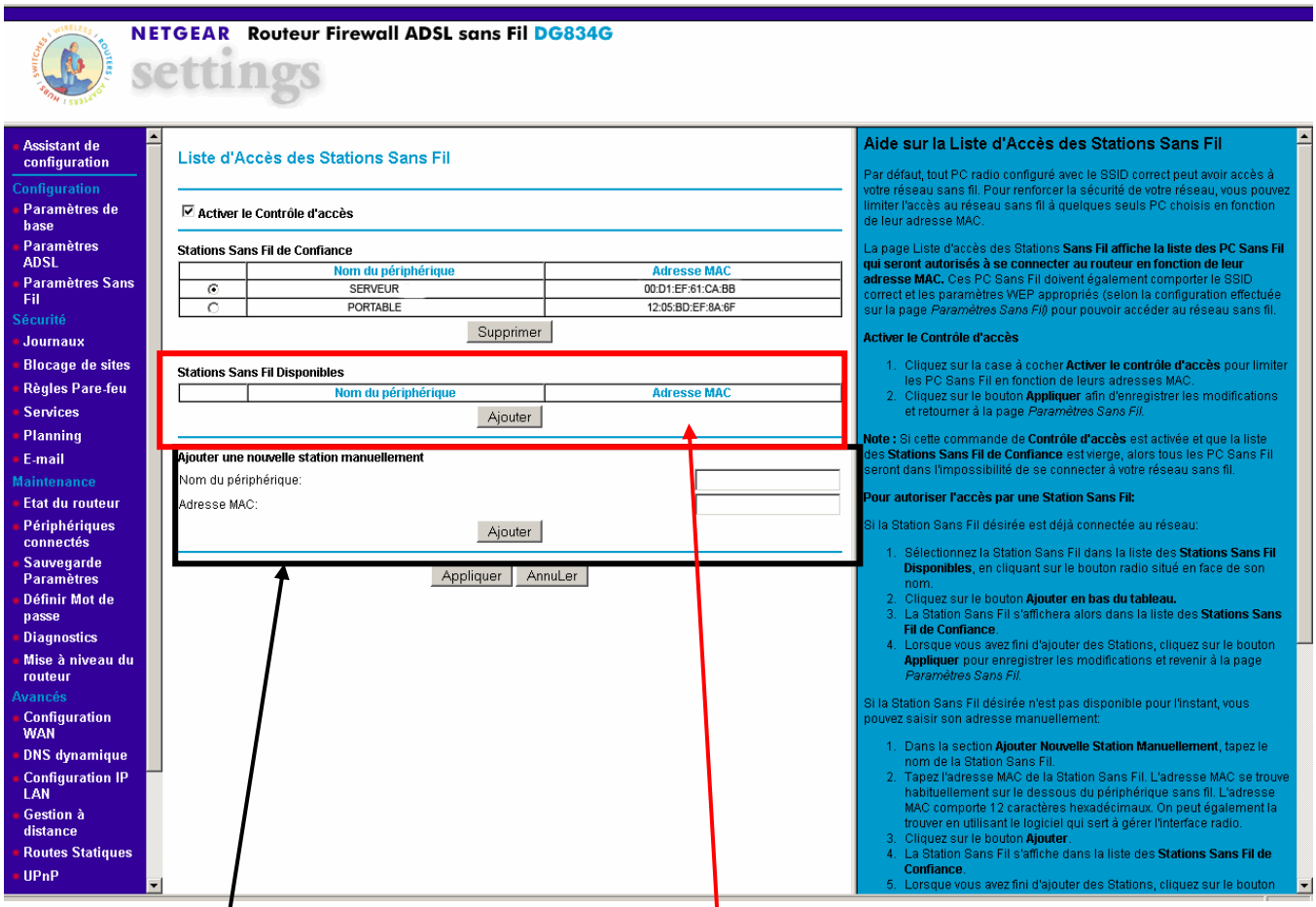


Cas d'une configuration WPA-PSK



Cas d'une configuration WPA

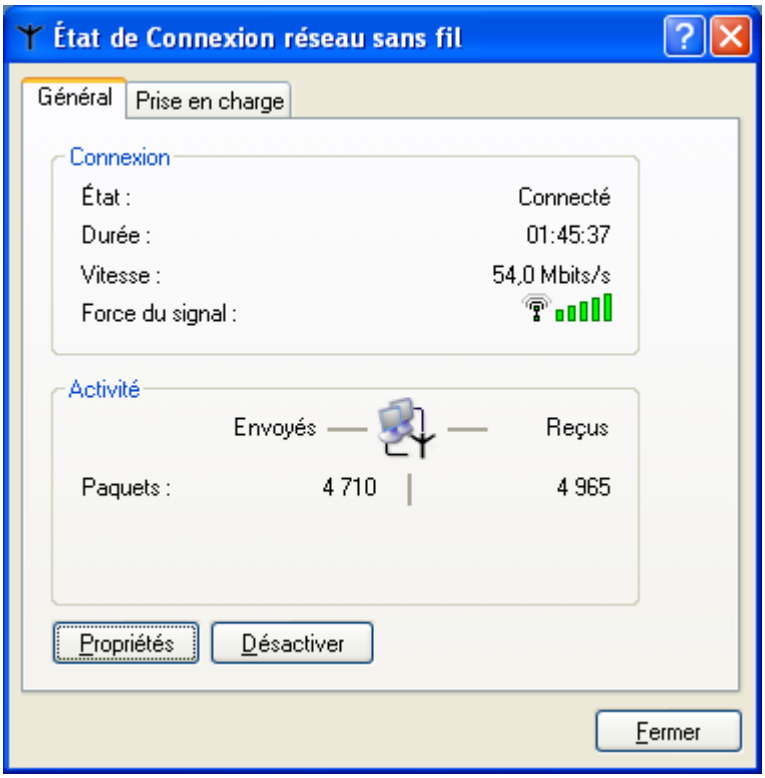




On peut rentré les stations sans fils de confiance à la main

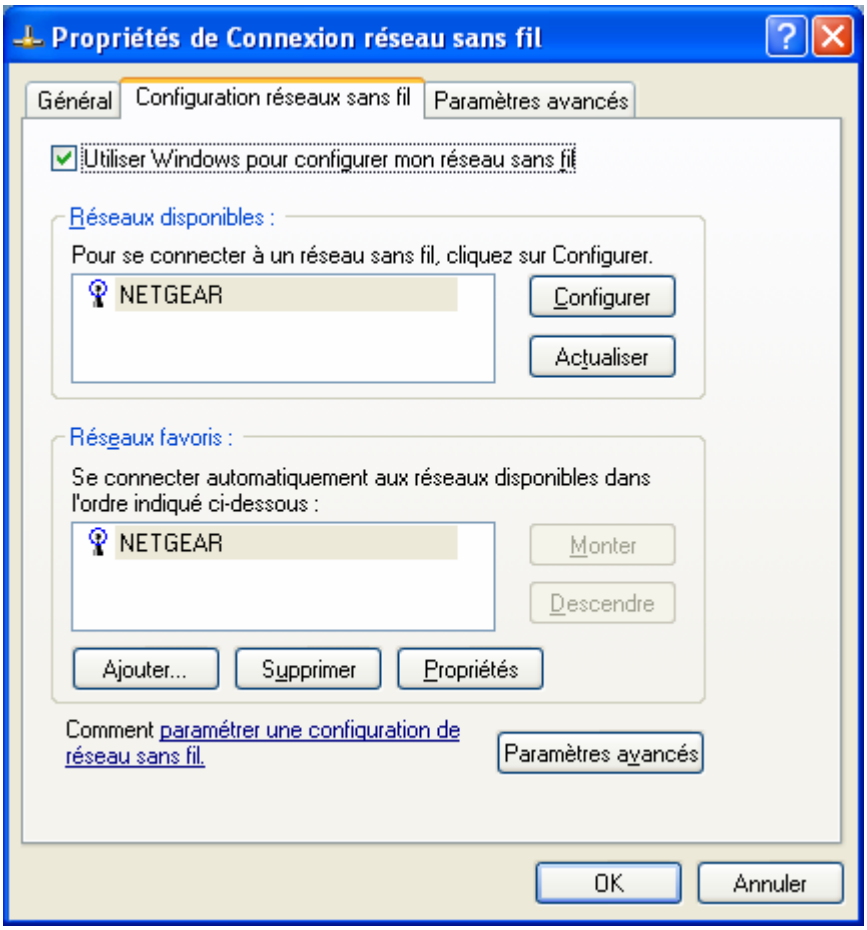
Ou si celles-ci sont déjà configurer pour ce réseau, elles apparaissent directement dans ce tableau et il suffit de cliquer sur « Ajouter » pour quelles soit dans les stations de confiance.

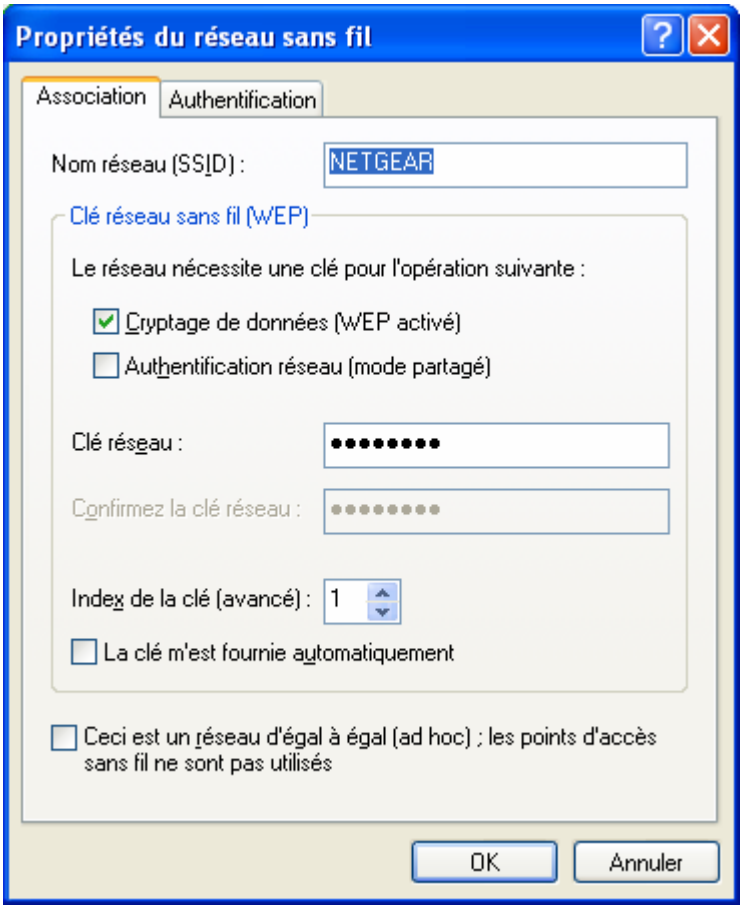
13.2. Exemple de configuration d'une carte WIFI LINKSYS-CISCO WMP54G :



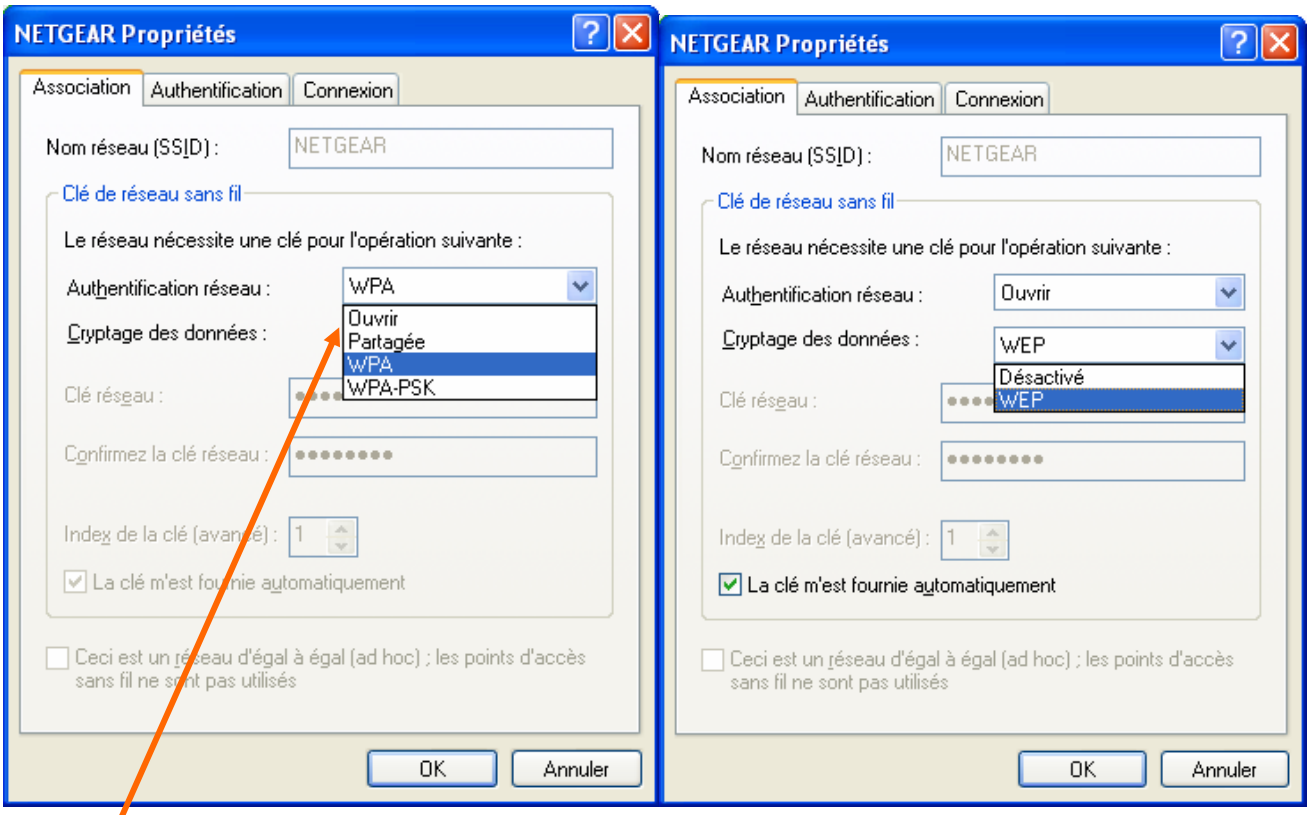
13.2.1. Configuration WEP

Lorsque nous utilisons une clé WEP ainsi que un SSID non diffusé, il faudra configurer totalement la carte réseau, en respectant la casse, les espaces, …
Nous remarquerons également, que la longueur de la clé montrée ci-dessous, ne correspond absolument pas à la longueur de la clé rentrée.


Propriétés de Connexion réseau sans fil
Général
Configuration réseaux sans fil
Paramètres avancés
Utiliser Windows pour configurer mon réseau sans fil
Réseaux disponibles :
Pour se connecter à un réseau sans fil, cliquez sur Configurer.
NETGEAR
Configurer
Actualiser
Réseaux favoris :
Se connecter automatiquement aux réseaux disponibles dans l'ordre indiqué ci-dessous :
NETGEAR
Monter
Descendre
Ajouter...
Supprimer
Propriétés
Comment paramétrer une configuration de réseau sans fil.
Paramètres avancés
OK
Annuler

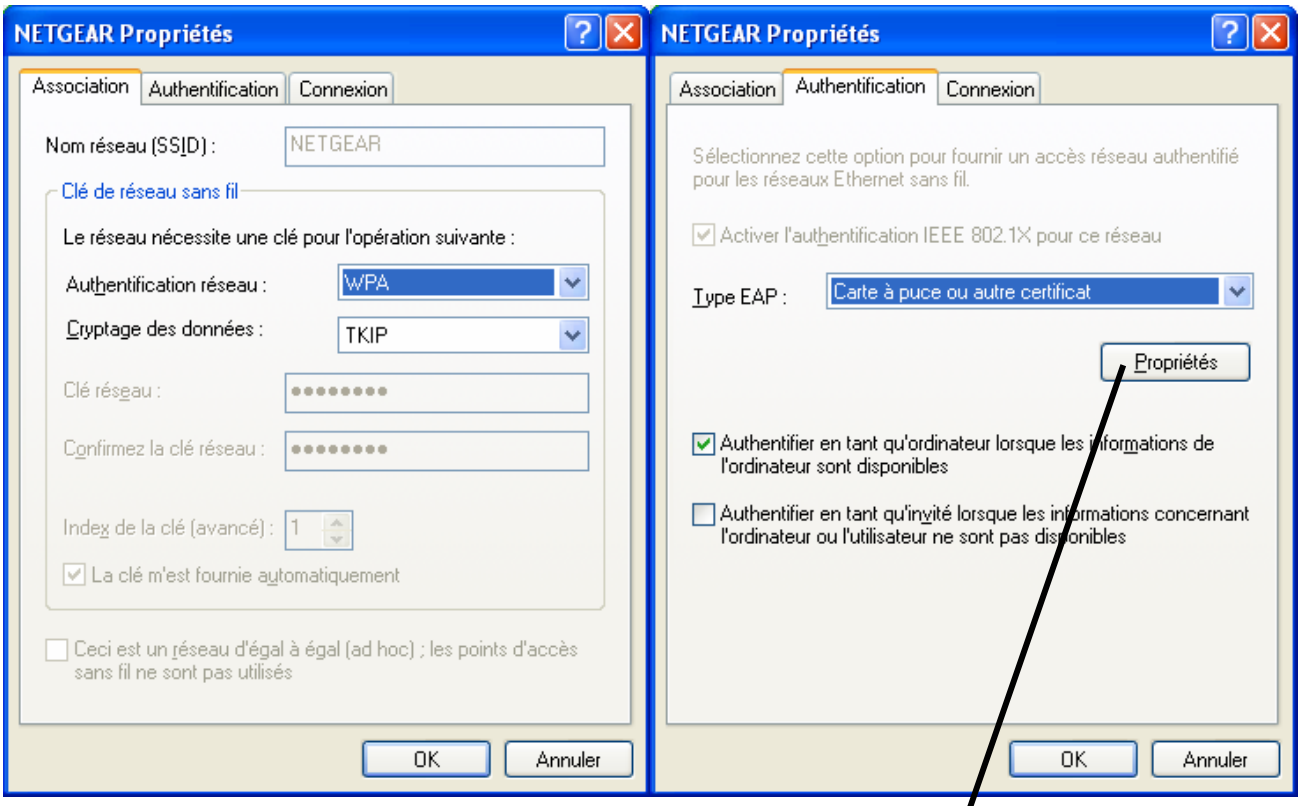

Propriétés du réseau sans fil
Association
Authentification
Nom réseau (SSID) :
NETGEAR
Clé réseau sans fil (WEP)
Le réseau nécessite une clé pour l'opération suivante :
Cryptage de données (WEP activé)
Authentification réseau (mode partagé)
Clé réseau :
Confirmez la clé réseau :
Index de la clé (avancé) :
1
La clé m'est fournie automatiquement
Ceci est un réseau d'égal à égal (ad hoc) ; les points d'accès sans fil ne sont pas utilisés
OK
Annuler

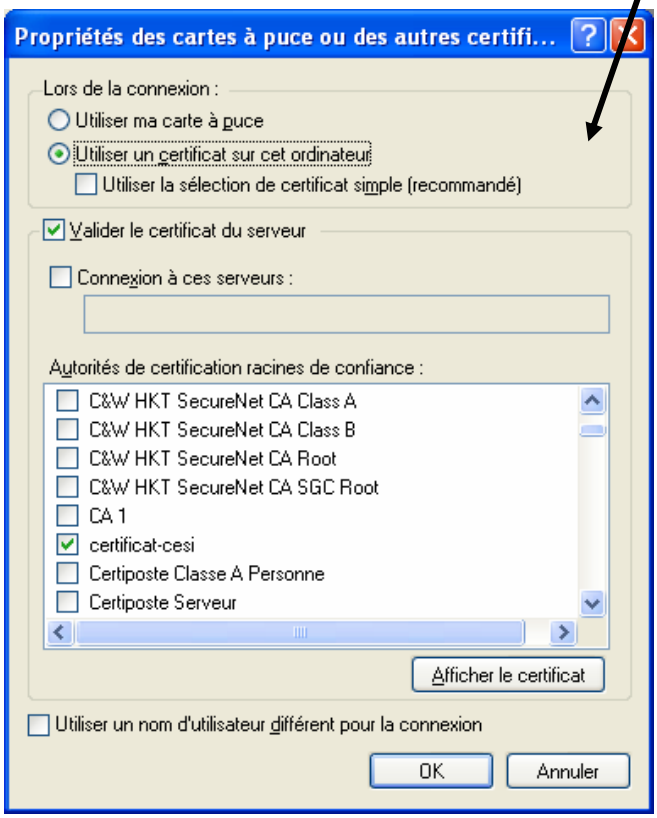
Avec les dernières mise à jours Windows XP (SP2), vous verrais apparaître une nouvelle fenêtre ressemblant à celle-ci, car la prise en charge du WPA et WPA-PSK a était rajouté.



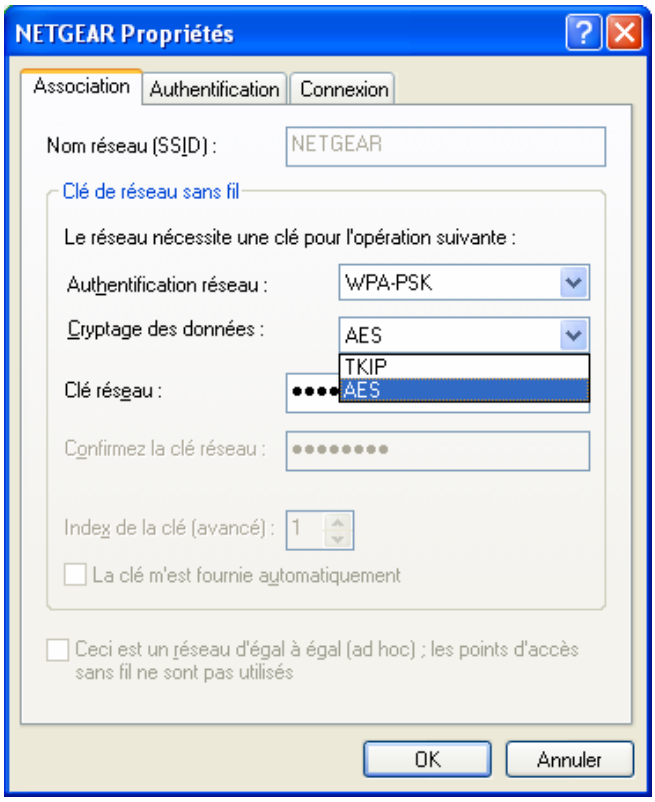
Ouvrir = mécanisme d'authentification WEP Open System (p.41)
Partagé = mécanisme d'authentification WEP Shared Key (p.41)

13.2.2. Configuration WPA


NETGEAR Propriétés
Association
Authentification
Connexion
Nom réseau (SSID) :
NETGEAR
Clé de réseau sans fil
Le réseau nécessite une clé pour l'opération suivante :
Authentification réseau :
WPA
Cryptage des données :
TKIP
Clé réseau :
Confirmez la clé réseau :
Index de la clé (avancé) :
1
La clé m'est fournie automatiquement
Ceci est un réseau d'égal à égal (ad hoc) ; les points d'accès sans fil ne sont pas utilisés
OK
Annuler
NETGEAR Propriétés
Association
Authentification
Connexion
Sélectionnez cette option pour fournir un accès réseau authentifié pour les réseaux Ethernet sans fil.
Activer l'authentification IEEE 802.1X pour ce réseau
Type EAP :
Carte à puce ou autre certificat
Propriétés
Authentifier en tant qu'ordinateur lorsque les informations de l'ordinateur sont disponibles
Authentifier en tant qu'invité lorsque les informations concernant l'ordinateur ou l'utilisateur ne sont pas disponibles
OK
Annuler


Propriétés des cartes à puce ou des autres certifi...
Lors de la connexion :
Utiliser ma carte à puce
Utiliser un certificat sur cet ordinateur
Utiliser la sélection de certificat simple (recommandé)
Valider le certificat du serveur
Connexion à ces serveurs :
Autorités de certification racines de confiance :
C&W HKT SecureNet CA Class A
C&W HKT SecureNet CA Class B
C&W HKT SecureNet CA Root
C&W HKT SecureNet CA SGC Root
CA 1
certificat-cesi
Certiposte Classe A Personne
Certiposte Serveur
Afficher le certificat
Utiliser un nom d'utilisateur différent pour la connexion
OK
Annuler

13.2.3. WPA-PSK



14. À quoi ça sert et à qui ?

- Le WIFI peut servir à plusieurs niveaux et à plusieurs personnes, par exemple:
- Un commercial délocalisé de son poste de travail et désirant continuer à travailler à distance ou consulté ses mails.
- Une société ou un particulier se trouvant dans un vieil immeuble et ne désirant pas percé les murs pour implanter un réseau informatique filaire.
- Qui n'a jamais rêvé d'être en plein été dans un parc avec son portable et pouvoir se connecter sur le net ou travailler or de son bureau.
- Certain type d'entreprise l'utilisant déjà, en voici une courte description :

Magasin :

Ce type de commerce s'appuie sur des applications client-serveur pour la gestion des stocks et de la chaîne logistique. Les WLAN apportent aux employés la mobilité dont ils ont besoin pour accéder rapidement et efficacement aux informations d'inventaire, avec des mises à jour instantanées vers les systèmes et base de données « back-end ».

Exemple concret : Chocolaterie CANTALOU à Perpignan : Ce groupe dispose dans le local des stocks d'un réseau WIFI permettant aux caristes de pouvoir retrouver facilement les produits, de faire des économies sur les trajets fait avec les transpalettes et de gérer automatiquement le stock grâce à des PDA spéciaux (conçu pour l'application utilisée).

Explications : Lorsqu'un transporteur vient chercher des produits, la personne s'occupant de sa commande rentre sur son PDA tout les produits de la commande, les données sont envoyées à l'AS400, l'AS400 a dans sa mémoire, le placement précis de chaque produit dans chaque allée, … du stock, par conséquent il donne au cariste l'ordre ainsi que le chemin a

emprunté pour chercher les produits le plus rapidement possible et en limitant le trajet, de cette manière, la société fait des économies sur les frais des roues des transpalettes (car elles usent moins), les commandes sont traitées plus rapidement et le stock est automatiquement mis à jour sur la quantité de marchandise entrée/sortie.

Hôpitaux et autres instituts médicalisés :

L'emploi du WIFI peut réaliser un retour sur investissement en tirant parti d'un WLAN pour le suivit des patients, la distribution des médicaments ou le traitement des feuilles de maladie, ainsi que pour fournir une mobilité accrue aux médecins et infirmière, leur permettant d'être lus efficaces et de mieux satisfaire les besoins des patients, ainsi que faire de très grosse économie de papier et augmenté la sécurité des données (secret médical) du fait que le nombre de papier est réduit.
De nombreuses entreprises commencent à développer des applications mobiles pour PDA qui permettent aux médecins et infirmières de traiter les formulaires de sécurité sociale et autres plus rapidement et surtout avec moins d'erreurs, limitant le nombre de demandes rejetées pour cause d'imprécision ainsi que les délais de remboursement.
De plus cela ajoute une mise à jour constante sur les fiches patients, ce qui permet à plusieurs médecins ou autre personnel médical d'avoir l'état des soins constamment mis à jour est disponible et également au personnel s'occupant de l'administratif d'avoir des fichier patients complet et avec un minimum d'erreur.

Universités et autres établissements scolaires :

Grâce au WLAN, les institutions peuvent assurer une couverture totale des locaux pour amener le réseau à l'étudiant, et non l'inverse. Les WLAN peuvent offrir un accès réseau dans des endroits qu'on ne s'imaginait pas pouvoir connecter il y a encore quelques années. Si elle peut sembler coûteuse au départ, l'installation d'une infrastructure sans fil se révèle à long terme plus avantageuse financièrement que la pose de nouveaux câbles ou la modification de l'infrastructure de câblage existante.
Le déploiement du sans fil dans un environnement éducatif présente des défis, puisqu'il est ici question de couvrir de nombreuses salles de classe. Il est aussi souvent nécessaire de couvrir les espaces verts entourant les bâtiments ainsi que les locaux communs et les cafétérias densément peuplés. La principale difficulté est d'offrir une infrastructure capable de supporter des clients de divers fabricants, car les étudiants disposent souvent de leur propre ordinateur et leur propre carte WIFI, ceci étant dit, aujourd'hui la plupart des portables vendus et équipés de carte réseau WIFI, prennent en charge les normes 802.11b et g ainsi que le protocole de cryptage WEP.

Lieux publics :

Les déploiements pour l'accès public visent essentiellement à fournir un accès à Internet via le support sans fil dans les lieux publics, tels que hôtels, cafés, aéroports, gares, restaurants et autres lieux de passage ou de réunion appelés « hotspot ». Etant donné que la plupart de ces secteurs n'ont pas l'intention de proposer un accès gratuit, nombre de développement du sans-fil dans ce domaine vont dans le sens d'une authentification liée d'une manière ou d'une autre aux systèmes de facturation.

Voici une annonce trouvée sur le site http://presencepc.com :

« *Nous vous l'annoncions récemment, le WiMax prenait place à bord des trains Anglais. Aujourd'hui, le Wi-Fi est disponible de façon payante dans beaucoup de gares SNCF. Et bien le Wi-Fi sera utilisable à bord de certains TGV, il fallait s'y attendre. Accessible dans un premier temps à bord du TGV Thalys reliant Bruxelles à Paris, il devrait ensuite s'étendre sur plus de trains.*
Le principe utilisé est hautement technologique: pour réaliser ce petit exploit, la SNCF a posé une antenne sur un wagon capable de maintenir un contact avec un satellite placé en orbite géostationnaire, alors que le train se déplace à une vitesse de 300km/h. Ce projet a été rendu possible grâce au soutien de l'agence spatiale européenne et à la société britannique 21Net qui mis au point la très complexe antenne.
Selon notre source, ce service serait gratuit jusqu'à la fin du mois de mai. Amusez-vous bien... »

Voici une autre annonce trouvée sur http://pcinpact.com

« *Depuis un petit moment, McDonald's France propose l'accès à Internet sans fil grâce au WiFi dans quelques fat food. Aujourd'hui, 30 fat food sont d'ores et déjà équipés. McDo s'est associé avec Intel et l'opérateur WiFi METEOR Networks pour fournir ce service.*

Pour se connecter, il suffit tout simplement d'avoir un PDA ou un ordinateur portble équipé du WiFi, la connection se fait diectement, sans qu'il y ait besoin au préalable de configurer sa machine.

Il faudra avant tout accepter les règles de bon usage du WiFi, McDonald's précise que le téléchargement peer to peer est interdit pour garantir la sécurité et le respect de la réglementation, engagement sur la nature des sites consultés.

McDonald's France et de ses partenaires souhaitent équiper environ 150 restaurants d'ici la fin de l'année. »

Voici un site où vous pourrez trouvé tout les points d'accès payant et/ou gratuit dans les département, il recherche dans les hôtels, aéroports, gares, restaurants, … en vous donnant l'adresse complète ainsi que tous les renseignements pour s'y rendre :**http://www.journaldunet.com/wifi/localisation**

Services de sécurité publique :

Aux Etats-Unis, des projets pilotes testent l'emploi de PDA 802.11 reliés par voie hertzienne à des caméras sans fil pour permettre aux forces de l'ordre d'assister à des délits sans être physiquement présents sur les lieux. Evidemment, un aspect crucial est la sécurité, laquelle peut être implémentée au moyen de mécanismes d'authentification et de chiffrement, protégeant ainsi les informations de sécurité publique.

15. Les antennes

Omnidirectionnelle

Patch

Yagi

Parabole (grille)

Dipôle

Ricoré

15.1. Antenne Omnidirectionnelle

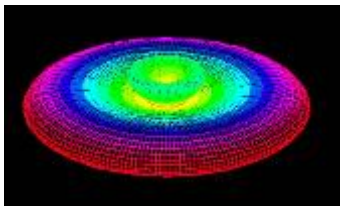
Ces antennes ont un gain variant de 0 à 15 dBi environ, sachant que les antennes les plus abordables financièrement parlant, et d'une taille raisonnable, sont celles situées aux environs de 8 dBi.
Leur rayonnement s'effectue sur 360°.

Elles sont utilisées pour établir une réseau urbain de type client-serveur, permettant de fournir un accès au réseau, dans un parc par exemple.

L'antenne omni s'installe en général sur le point d'accès raccordé au réseau, les clients utilisent eux des antennes directives polarisées verticalement pour se relier à ce point central.

Exemple d'antenne omnidirectionnelle :

Super vue en 3D de la propagation des ondes avec une antenne Omni :

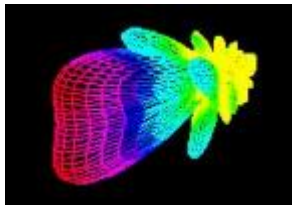


15.2. Antenne Directionnelle

Ces antennes ont habituellement un gain élevé, de 5 dB minimum jusqu'à 24 dB environ, avec un rayonnement directif.
Elles permettent d'établir des liaisons point à point, mais également de couvrir une zone limitée dans le cas d'une antenne à angle d'ouverture important (antenne panneau).

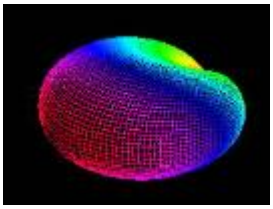
Les clients d'un réseau WiFi utilisent de telles antennes pour se relier aux points d'accès, et par là même au réseau. Attention de bien respecter les polarisations : verticale pour se relier à une antenne omni, verticale ou horizontale pour relier deux directives entre elles.

Vu en 3D de la propagation des ondes :

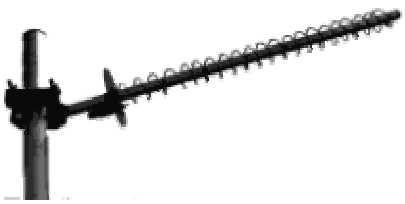


15.3. Antenne Patch

Vu en 3D de la propagation des ondes :



15.4. Antenne Hélicoïdale



Il existe plusieurs modèles d'antennes directives : panneau, paraboles pleines, paraboles grillagées, patch, Yagi (bande étroite, peu conseillée pour le WiFi), en polarisation circulaire (pour les liaisons lointaines en milieu urbain ou perturbé eau, océan, fleuve, etc.).

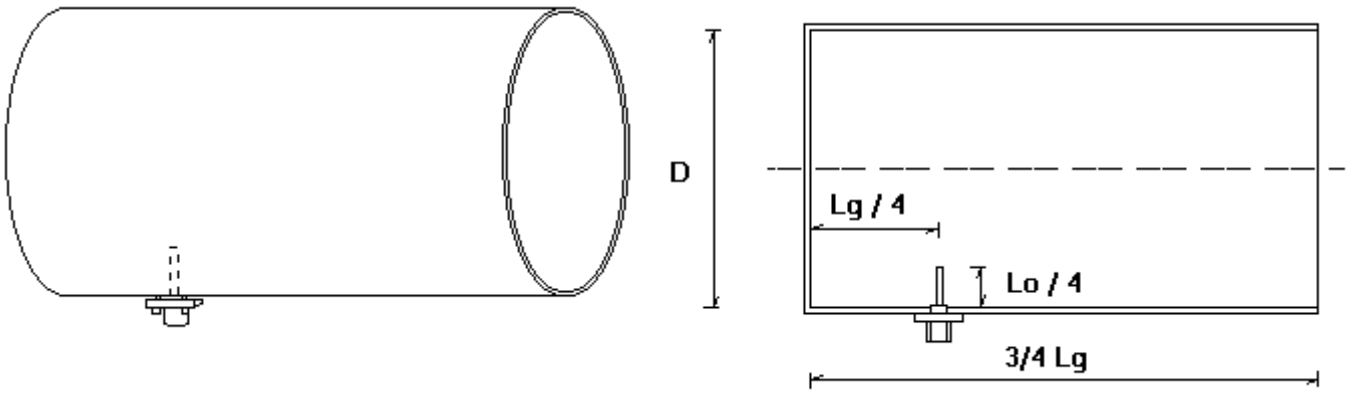
Une antenne directive se caractérise par son gain (cf: ci-dessus), mais également par son angle d'ouverture :

- Une antenne de 10 dB et 60° d'ouverture, pourra tout à fait convenir pour couvrir, par exemple, une place en centre ville, voir un quartier complet.
- Une antenne de 14 dB avec 40° d'ouverture couvrira elle une zone plus longue, mais plus étroite.
- Une antenne parabolique grillagée de 24 dB, ouvrant à 10°, servira à établir une liaison sur plusieurs kilomètres.

15.5. Construction d'une antenne Ricoré

- un connecteur N socle
- une boîte métallique évidemment
- un petit morceau de tige métallique d'environ 2 mm de diamètre
- une perceuse
- un foret à métal (ou à bois ça marche aussi) du diamètre de votre connecteur
- une fer à souder et de l'étain

le dimensionnement:

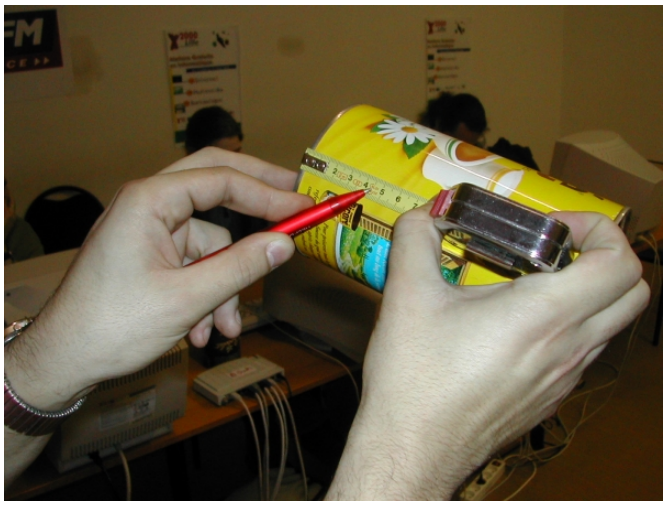


Lg function of tube diameter @ 2.45 GHz		
Diamètre intérieur du tube D/mm	Lg / mm de longueur de vague	Lg / 4
90	202,7	51
95	186,7	47
100	175,7	44
105	167,6	42
110	161,5	40

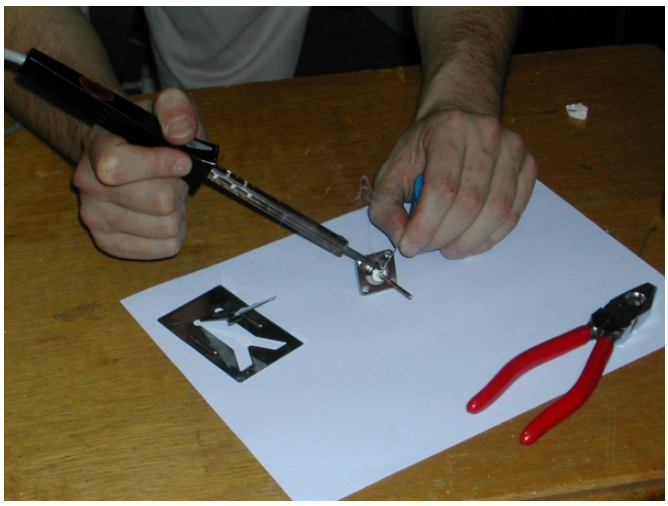
Le moteur de calcul pour trouver les dimensions adaptées à votre boîte.

Méthode pas à pas pour une boîte de 10cm de diamètre :

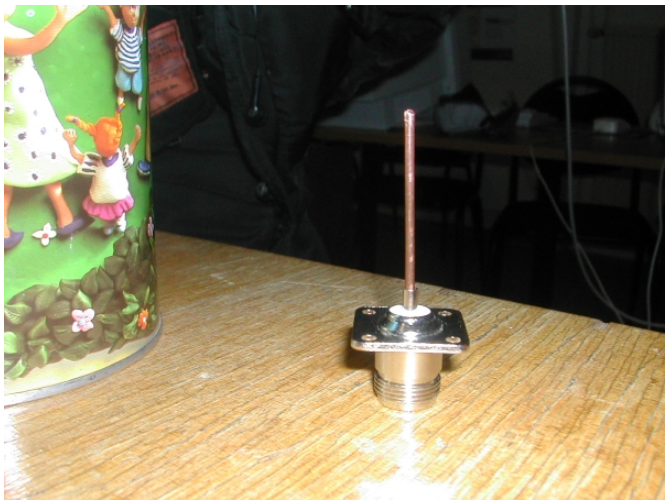
1. Percer un trou à exactement 44 mm du fond de la boîte pour pouvoir passer la tête du connecteur



2. Souder un morceau de tige métallique sur l'âme du connecteur N.



3. Couper la tige métallique de manière à ce qu'avec le connecteur son extrémité soit à 31 mm de la paroi de la boîte.



4. Fixer grâce au jeu d'écrou ou à quelques points de soudure le connecteur N sur la boîte. Et voilà !

16. Réglementation

Fin novembre 2002, l'autorité de régulation des télécoms a autorisé pour la première fois, sous certaines conditions, la mise en place des réseaux locaux sans fil (RLAN) ouverts au public, plus communément appelés hotspots wi-fi. Jusqu'à cette date les RLAN en France était très réglementés, et uniquement autorisés pour les usages privés.

Résumé de la situation légale du WIFI en France datée du 4 février 2003.

Le Wi-Fi, opérant dans la bande de fréquence des 2,4 GHz est soumis en France à certaines règles.

Cas 1 : Dans quel cas dois je déposer un dossier

Seules les demandes d'expérimentation qui concernent la constitution de réseaux (établissement de liens points à points pour mailler des bornes entre elles) sont soumises a une demande de dossier. Si le dossier est accepté, cette expérimentation est menée jusque 18 mois à compter du 12 novembre 2002.

Cas 2 : Je suis un particulier, je veux partager mes données en WIFI et/ou mon accès Internet en WIFI avec mes voisins de pallier, donc EN INTERIEUR, au sein de mon immeuble.

Vous pouvez librement utiliser le matériel Wi-Fi (802.11b) en intérieur et le connecter à ce que vous voulez (L'Internet notamment) et ce jusqu'à 100mW de PIRE.

Néanmoins si vous habitez hors des 58 départements autorisés par l'ART (la liste est fournie par l'ART), il faut rester sur les canaux 10 à 13 sinon la limite est à 10 mW.

Cas 3 : Je suis un particulier et je veux partager mes données en WIFI et/ou mon accès Internet en WIFI, EN EXTERIEUR

J'habite dans l'un des 58 départements soumis à l'autorisation de l'ART :

Pas besoin de poser une demande de dossier. Il vous faut juste savoir si votre Fournisseur d'accès Internet autorise le partage de bande passante. Dans le cas ou une seule borne est reliée à un accès haut débit (xdsl, cable) pour le partager avec d'autres utilisateurs , cette borne est considérée comme équipement terminal et vous êtes seulement tenus de respecter la PIRE maximum (gain d'antenne inclus). Vous n'avez pas besoin d'autorisation. Foncez !

Vous pouvez émettre jusqu'au canal 7 jusqu'à 100mW de PIRE. Au delà c'est 10mW ou il faut quand même une autorisation de la défense (dossier).

J'habite hors des 58 départements : Il vous faut faire une demande de dossier et ça limite aux propriété privées. Aussi, plus il y aura de dossiers plus la dérogation sera rapide.

Cas 4 : Mon Fournisseur d'accès Internet n'autorise pas le partage de bande passante

Changez de FAI. Il y au moins 1 FAI en France qui acceptent le partage de bande passante. Si vous etes curieux de ce qui peux se passer dans ce type de cas, lisez cette présentation.

Cas 5 : Y a-t-il une limite de puissance en intérieur et extérieur?

Depuis le 25 juillet 2003, les démarches pour installer un hot spot Wi-fi sont considérablement allégées. L'ART (Autorité de Régulation des Télécoms)

vient d'élargir le cercle des départements autorisés pour l'utilisation du sans fil en extérieur, tous les départements métropolitains sont autorisés. L'utilisation d'une borne simple reliée au net et rayonnant à l'extérieur est désormais légale SANS dépôt de dossier.

Exemple d'offre :

Offre orange :
- Du temps de connexion se matérialisant sous forme de cartes à gratter contenant un code de connexion temporaire
Identifiant + mot de passe).
Ou la possibilité d'acheter votre temps de connexion directement en ligne avec votre carte bancaire, depuis la page d'accueil du service du hotspot.
- Pas de contraintes ni de formalités à l'achat.

> Du temps de connexion Internet sans contraintes :

- Pas de limitation en nombre de connexions ou en volume de données échangées,
- Le décompte du temps de connexion débute à partir de la 1ère connexion et se décompte à la seconde,
- Le crédit est irrévocablement perdu s'il n'est pas utilisé pendant la durée de validité de la carte.

Pass 2 H - 10 € TTC 2 H de connexion valables 24 H	Pass 24 H - 30 € TTC 24 H de connexion valables 24 H	Pass meeting - 40 €TTC 24 H de connexion valables 24 H pour 5 utilisateurs simultanément	Pass 4 H-1 mois - 30 € TTC 4 H de connexion, utilisable pendant 30 jours

17. ANNEXE

17.1. Installation et configuration de RADIUS sur Windows 2003 Serveur

(Documentation tiré du site http://www.laboratoire-microsoft.org)

Sécuriser un réseau Wi-Fi avec Windows 2003 Server

Lors de la mise en place d'un réseau Wi-Fi (**Wi**reless **Fi**delity), la sécurité est un élément essentiel qu'il ne faut pas négliger.

Effectivement, avec l'émergence de l'espionnage informatique et l'apparition du Wardriving, il est désormais difficile d'avoir une confiance totale dans la sécurité des réseaux Wi-Fi, même en utilisant le protocole sécurisé WEP (*Wired Equivalent Privacy*) et un filtrage au niveau des adresses Mac (*Media Access Control Address*).

Nous vous proposons donc d'étudier au cours de cet article la mise en place d'une infrastructure Wi-Fi sécurisé WPA (Wi-Fi Protected Access) 802.1X utilisant un serveur Radius et une authentification par certificat (EAP-TLS : *Extensible Authentication Protocol-Transport Layer Security*).

17.1.1. 1. Présentation de WPA et 802.1X

En attendant la nouvelle norme 802.11i en cours d'élaboration, la Wi-Fi Alliance et l'IEEE ont décidé de définir le protocole WPA afin de combler les lacunes du protocole WEP.

Précédemment les réseaux Wi-Fi disposaient de clés WEP fixes, décidées sur les points d'accès.

Mais l'utilisation des clés WEP a révélé deux faiblesses importantes:

- L'utilisation d'algorithmes cryptographiques peu développés l'a rendu très vulnérable. Il suffit de quelques heures à un éventuel pirate pour casser les clés utilisées.
- Seconde faiblesse, l'impossibilité d'authentifier un ordinateur ou un utilisateur qui se connecterai au réseau.

Afin de pallier au problème de cryptographie, WPA définit deux nouvelles méthodes de chiffrement et de contrôle d'intégrité:

- TKIP (*Temporal Key Integrity Protocol*) : ce protocole a été conçu afin de s'adapter au mieux au matériel existant. Il utilise RC4 comme algorithme de chiffrement, ajoute un contrôle d'intégrité MIC et introduit un mécanisme de gestion des clés (création de clés dynamiques à un intervalle de temps prédéfini)
- CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) : à priori plus puissant que TKIP, il utilise AES comme algorithme de chiffrement. C'est la solution qui semble se distinguer à long terme. Cependant ce protocole est totalement incompatible avec le matériel actuel.

WPA utilise le protocole 802.1X . Également appelé EAPOL (EAP Over Lan) il est utilisé comme méthode de transport pour l'authentification EAP. C'est est une réponse au besoin d'authentifier les machines ou les utilisateurs connectés sur un réseau local. Il permet donc de transférer les paquets d'authentification vers divers éléments d'un réseau mais offre aussi un mécanisme pour échanger des clés qui vont être utilisées pour chiffrer les communications et en contrôler l'intégrité.

Le protocole 802.1X définit trois catégories d'acteur jouant chacun un rôle différent.

- Le supplicant : il s'agit du poste de travail qui demande à accéder au réseau.
- L'authenticator : c'est le dispositif Wi-Fi (également client Radius, voir chapitre suivant) fournissant la connexion au réseau. Il supporte deux états, non autorisé et autorisé, mais il ne joue que le rôle de relais dans l'authentification.
- Le serveur d'authentification : Il s'agit d'un serveur implémentant une solution Radius

WPA est donc une solution complexe, cependant, un mode spécial de WPA (WPA-PSK : *Pre Shared Key*) existe également afin de permettre aux particuliers de profiter de cette sécurité sans disposer de serveur d'authentification. La configuration du WPA-PSK commence par la détermination d'une clé statique ou d'une "passphrase" comme pour le WEP. Mais, en utilisant TKIP, WPA-PSK change automatiquement les clés à un intervalle de temps prédéfini.

17.1.2. 2. Présentation de l'authentification EAP

Il existe différentes méthodes d'authentification pour EAP (*Extensible Authentication Protocol*).

Voici les différents méthodes classées de la moins sûre à la plus sûre

- EAP-MD5: C'est la plus simple. Le client est authentifié par le serveur en utilisant un mécanisme de défi réponse. Le serveur envoie une valeur aléatoire (le défi), le client concatène à ce défi le mot de passe et en calcule, en utilisant l'algorithme MD5, une empreinte (" hash ") qu'il renvoie au serveur. Le serveur qui connaît le mot de passe calcule sa propre empreinte, compare les deux et en fonction du résultat valide ou non l'authentification. Une écoute du trafic peut dans le cas d'un mot de passe mal choisi, permettre de le retrouver par une attaque par dictionnaire ou par force brute.
- LEAP (*Lightweight EAP*): est un méthode propre à Cisco qui repose sur l'utilisation de secrets partagés pour authentifier mutuellement le serveur et le client. Elle n'utilise aucun certificat et est basé sur l'échange de défi et réponse.
- EAP-TTLS (*tunneled* Transport Secure Layer) : utilise TLS comme un tunnel pour échanger des couples attribut valeur à la manière de RADIUS11 servant à l'authentification. Pratiquement n'importe quelle méthode d'authentification peut être utilisée.
- PEAP (*Protected EAP*): est une méthode très semblable dans ses objectifs et voisine dans la réalisation à EAP-TTLS. Elle est développée par Microsoft. Elle se sert d'un tunnel TLS pour faire circuler de l'EAP. On peut alors utiliser toutes les méthodes d'authentification supportées par EAP.
- EAP-TLS(*Extensible Authentication Protocol-Transport Layer Security*): C'est la plus sûre. Le serveur et le client possèdent chacun leur certificat qui va servir à les authentifier mutuellement. Cela reste relativement contraignant du fait de la nécessité de déployer une infrastructure de gestion de clés. Rappelons que TLS, la version normalisée de SSL (*Secure Socket Layer*), est un transport sécurisé (chiffrement, authentification mutuelle, contrôle d'intégrité). C'est lui qui est utilisé de façon sous-jacente par HTTPS, la version sécurisée de HTTP, pour sécuriser le Web.

Nous utiliserons donc la méthode EAP-TLS qui propose à ce jour le plus de sécurité.

Avec la méthode EAP-TLS l'authentification du client d'accès peut se faire de différentes façons :

- A l'aide d'un certificat personnel associé à la machine, l'authentification a lieu au démarrage de la machine.
- A l'aide d'un certificat personnel associé à l'utilisateur, l'authentification a lieu après l'entrée en session (" logon ") de l'utilisateur.

Il est possible de combiner les deux précédentes méthodes. La valeur de la clé de registre "HKEY_LOCAL_MACHINE\Software\Microsoft\EAPOL\Parameters\General\Global\Auth Mode" permet de modifier ce comportement :

- 0 authentification de la machine au démarrage, en cas d'échec authentification de l'utilisateur au logon

- 1 authentification de la machine au démarrage, puis authentification de l'utilisateur au logon
- 2 uniquement authentification de la machine

Nous utiliserons des certificats du type X509v3 Extended Key Usage délivrés par le site Web de l'autorité de certification.

17.1.3. 3. Présentation de Radius

Le serveur Radius (*Remote Authentication Dial-In User Service*) a été initialement conçu pour authentifier des connexions par modem (PPP).

Désormais Radius peut être utilisé pour centraliser l'authentification, l'autorisation et la gestion des comptes pour les connexions d'accès à distance, VPN, Wi-Fi...

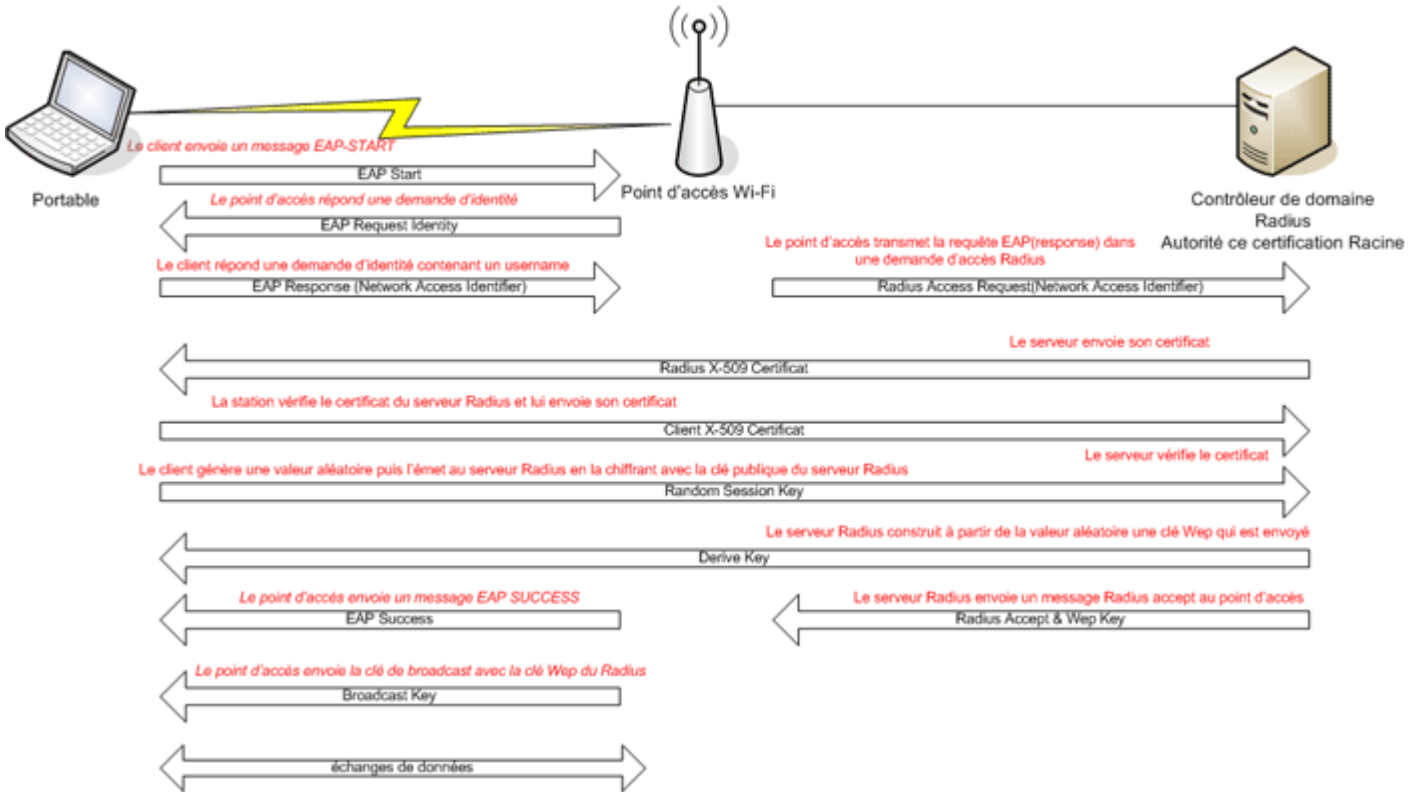
Il est possible par exemple sous Windows 2003 Server de créer des stratégies d'accès pour autoriser des utilisateurs, des groupes d'utilisateurs, des ordinateurs ou tout autre ressource voulant se connecter au réseau.

Le protocole Radius assure les échanges entre un client Radius (borne d'accès Wi-Fi, authenticator) et le serveur d'authentification. Il s'agit d'un protocole UDP utilisant les ports 1812 pour l'authentification et 1813 pour la comptabilité.

Un environnement Radius est composé :

- D'un serveur Radius qui centralise l'authentification, l'autorisation et la gestion des comptes
- D'un client Radius, c'est-à-dire un serveur d'accès distant ou une borne d'accès Wi-Fi (authenticator) qui reçoit les demandes d'authentification RADIUS des clients et les retransmet au serveur Radius.
- D'un client d'accès à distance ou Wi-Fi (supplicant) équipé de Windows XP, 2000 et certains autres systèmes d'exploitation non Microsoft.

Dans notre cas nous utiliserons une authentification de type EAP-TLS, le protocole Radius ne servira donc qu'à transporter du TLS et définir quel utilisateur ou quel groupe aura accès au réseau.



17.1.4. 4. Installation d'une autorité de certificat racine

Dans notre cas l'installation se fera sur un serveur contrôleur de domaine Windows 2003 Server.

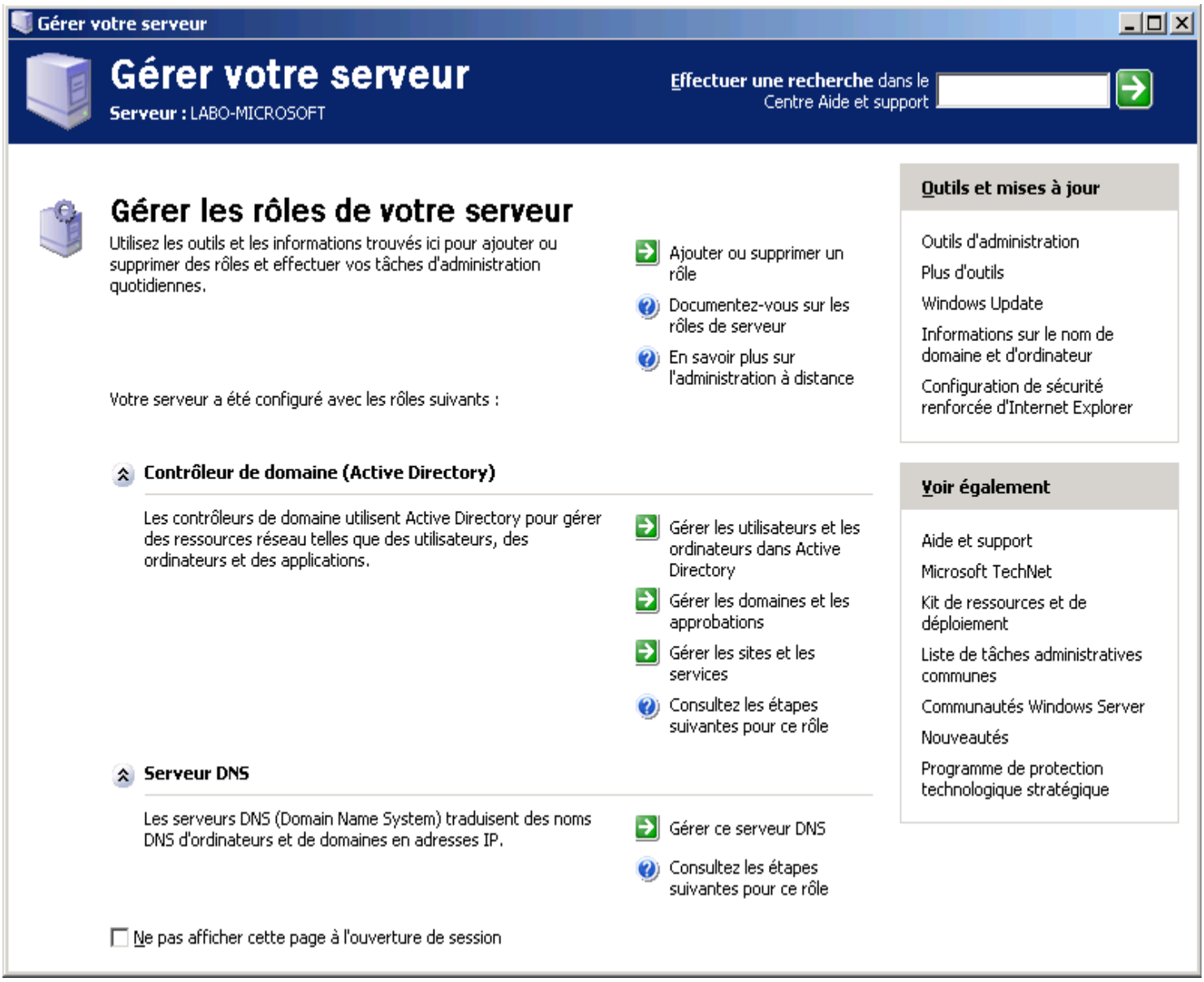
L'installation d'une autorité de certificat racine nécessite tout d'abord l'installation des services IIS (Internet Information Server).

- Installation des Services IIS

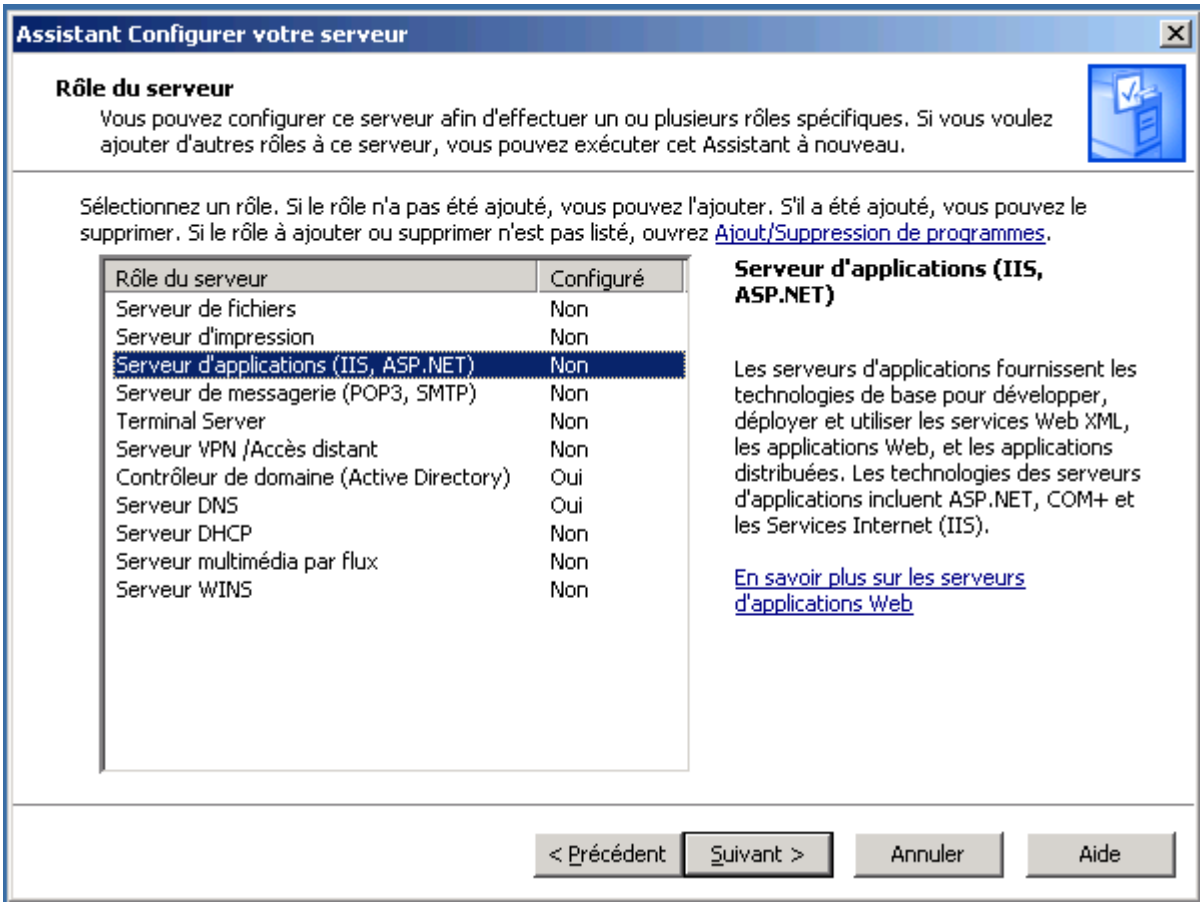
L'installation des Services IIS peut s'effectuer de deux manières :

- 1 ère possibilité : par l'outil " Gérer votre serveur " situer dans les outils d'administrations

Il va donc falloir ajouter un rôle à notre serveur

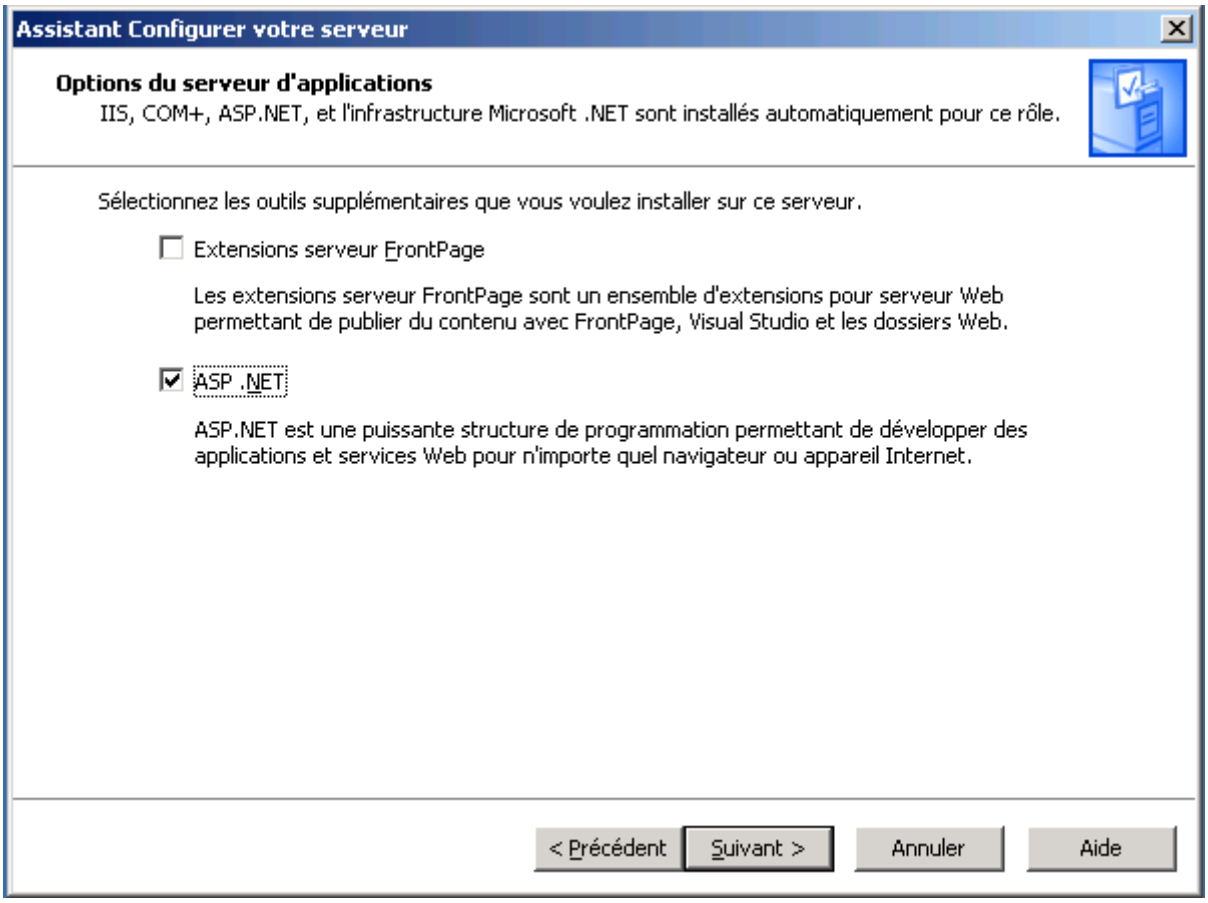


On choisit alors Serveurs d'application (IIS, ASP.NET)

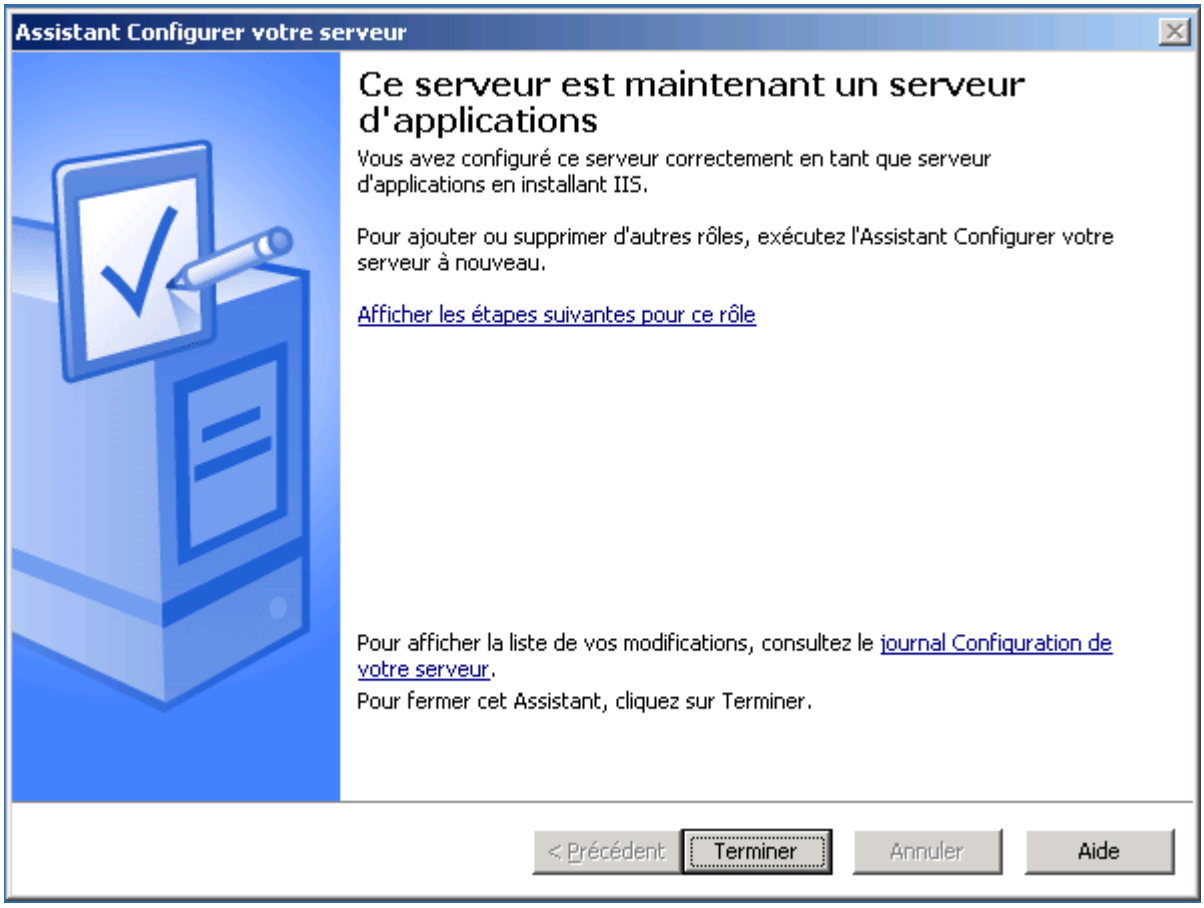


Puis nous avons le choix d'installer les extensions du serveur FrontPage et/ou la structure ASP.NET

Dans notre cas nous utiliserons ASP.NET car l'autorité de certificat nécessite cette technologie

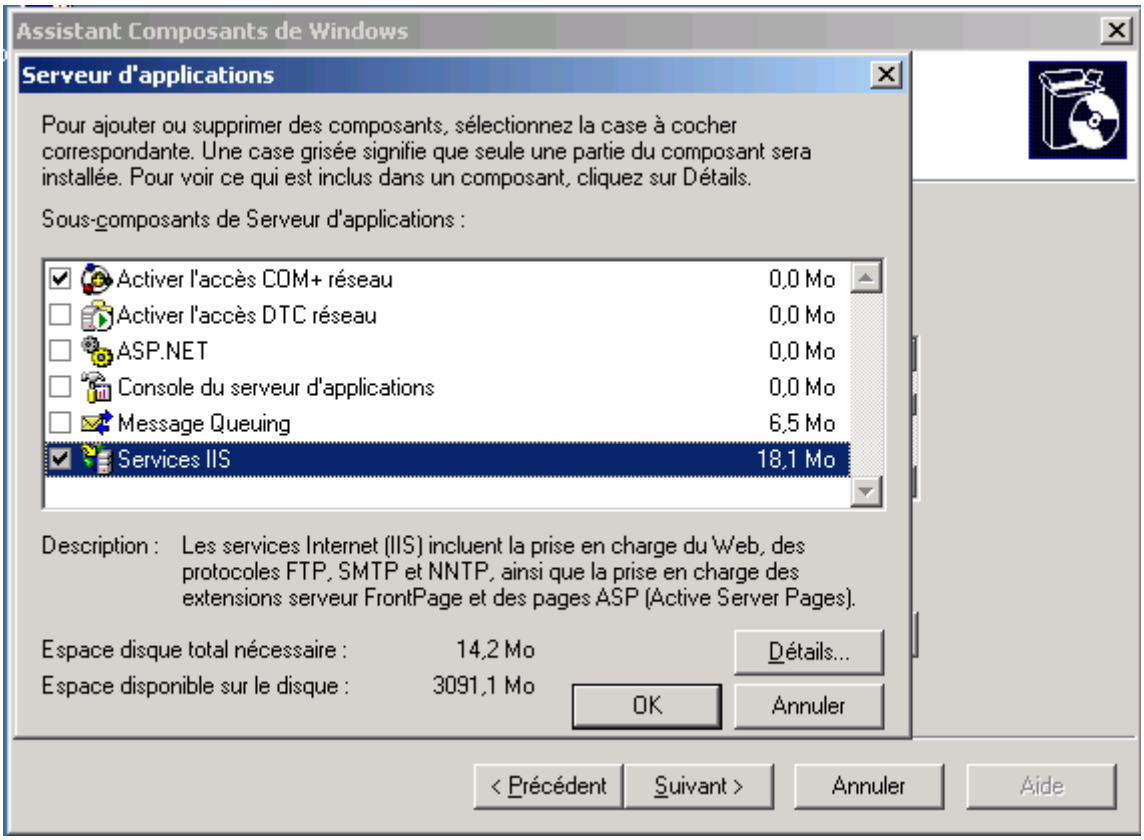


L'installation est alors terminée.



- 2 ème possibilité : par l'outil " Ajout/Suppression de composants Windows " situé dans " Ajout/Suppression de programmes " du Panneau de configuration.

Sélectionner Serveur d'applications puis cocher Services IIS



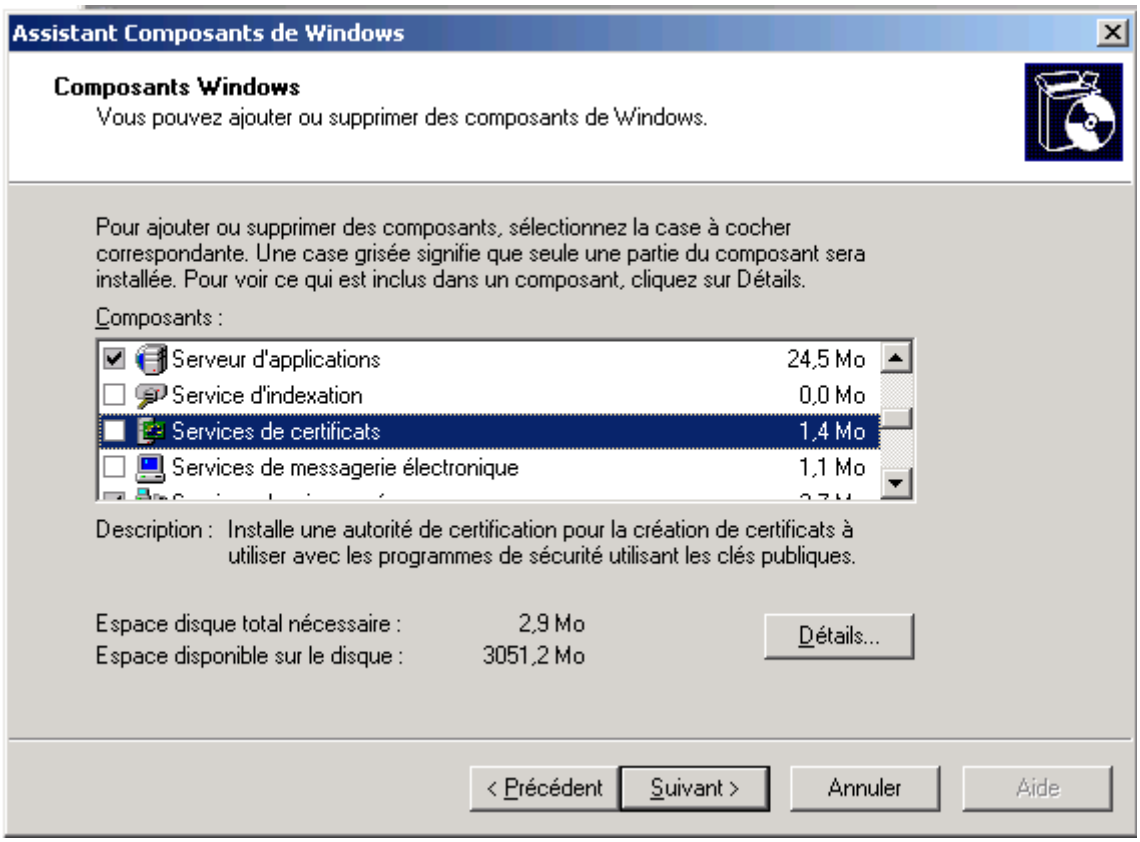
L'installation peut donc commencer après avoir valider notre choix L'installation est maintenant terminée.

Nous allons donc pouvoir installer une Autorité de Certification Racine.

- Installation d'une Autorité de Certification Racine

Nous utilisons l'outil " Ajout/Suppression de composants Windows " situé dans " Ajout/Suppression de programmes " du Panneau de configuration.

Puis on sélectionne Services de certificats

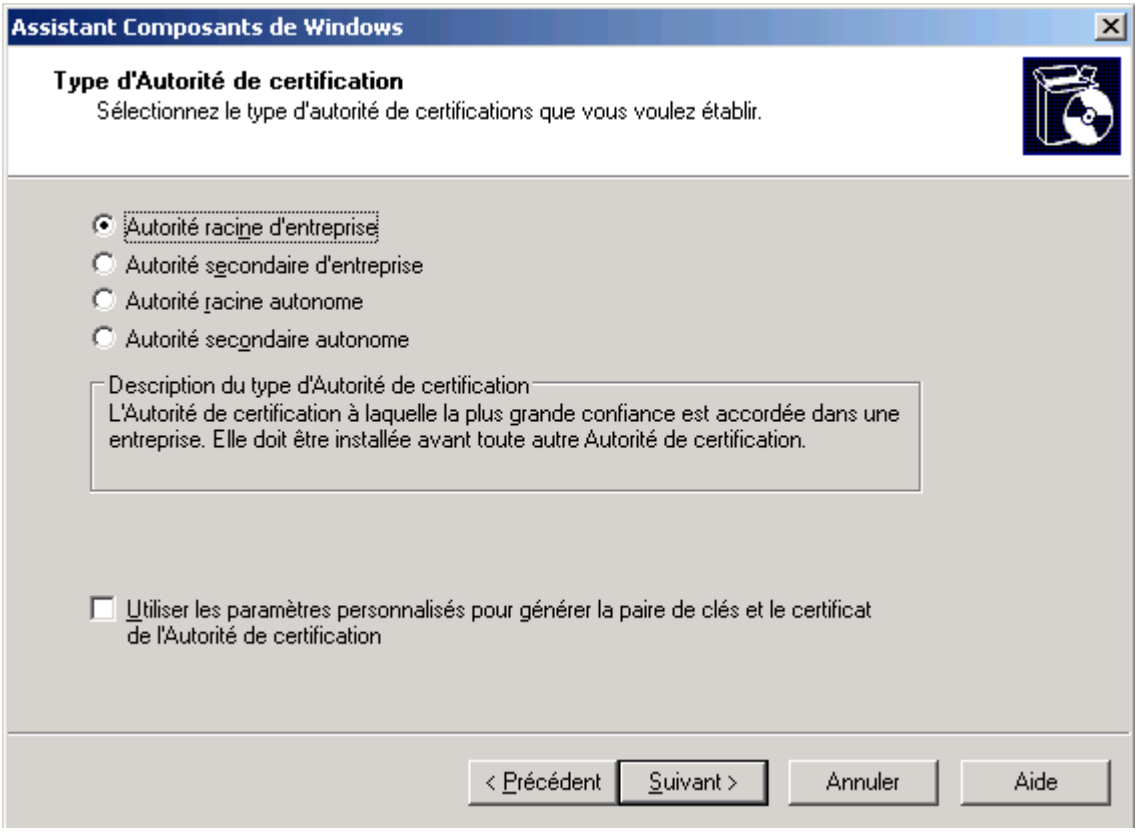


Un message d'erreur apparaît alors

Le message stipule qu'après installation des Services de certificats l'ordinateur ne pourra ni changer de nom ni changer de domaine, les certificats émis par votre autorité risquerait de ne plus être valide.

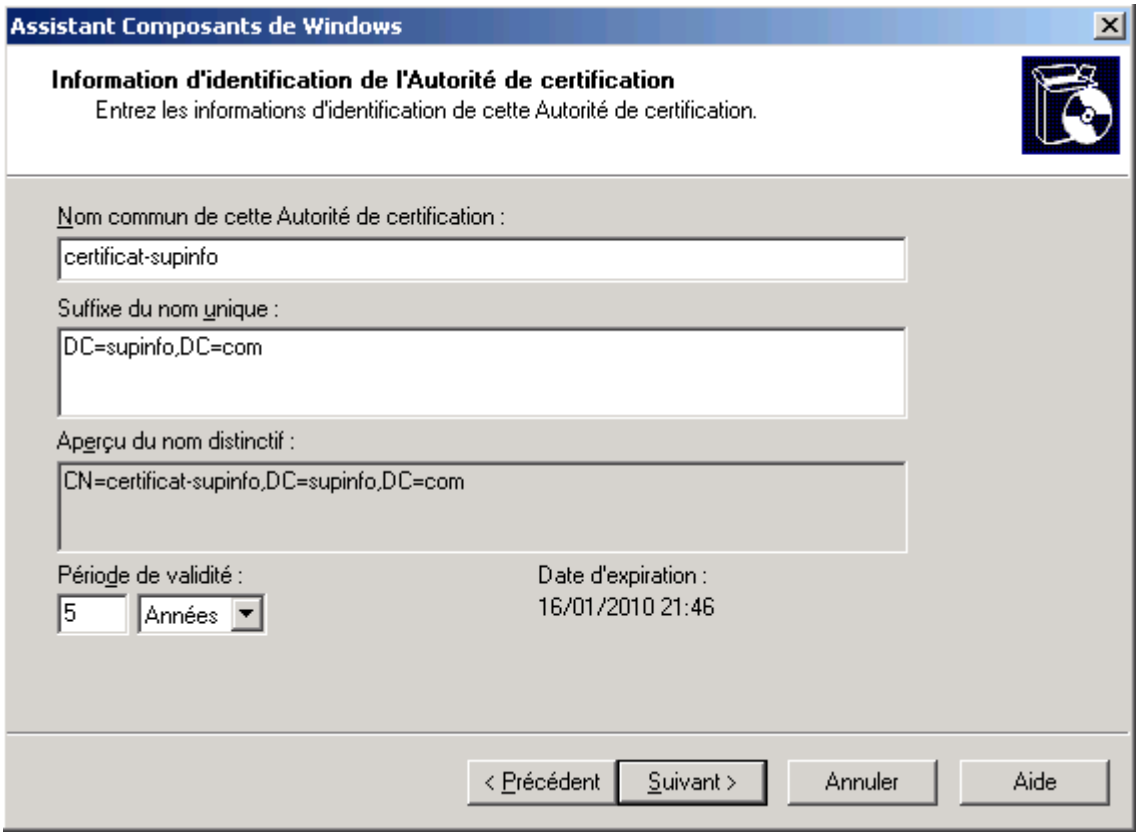
Nous validons par oui puis continuons l'installation.

Il faut désormais sélectionner Autorité racine d'entreprise car il s'agit de la première autorité installée

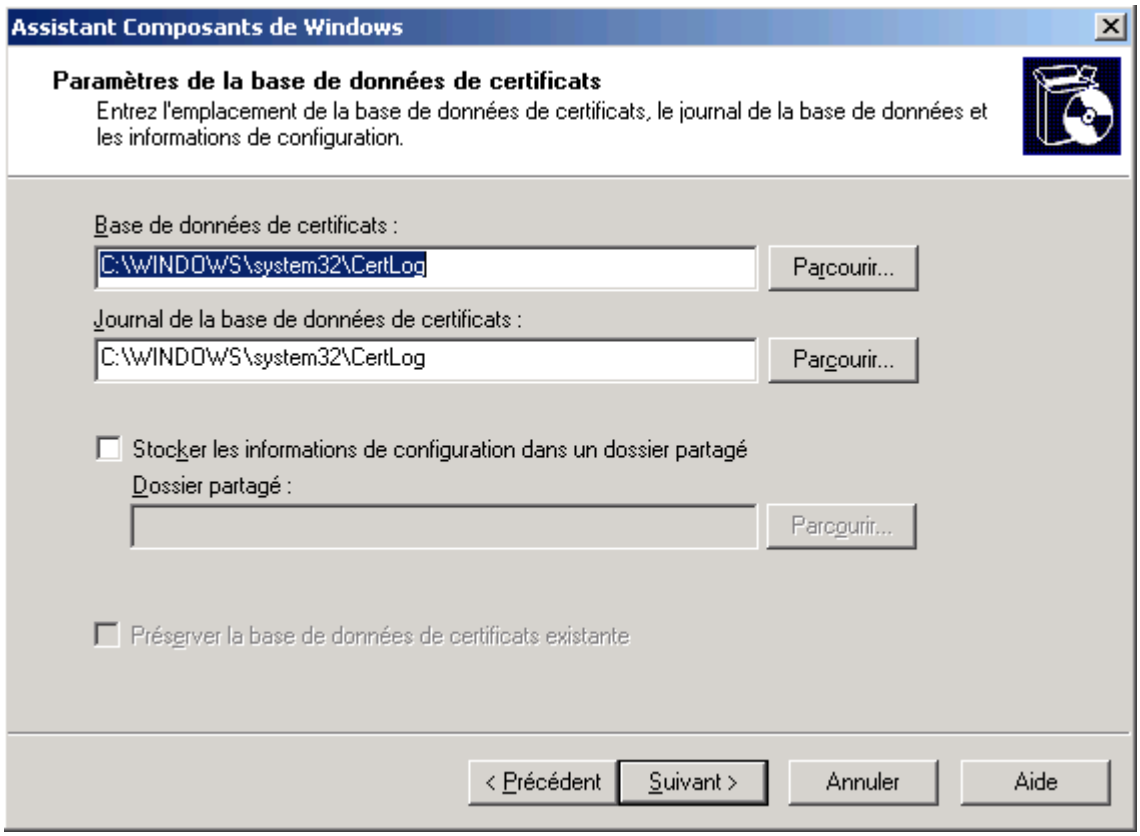


L'installation continue, il faut alors choisir le nom de notre autorité.

Dans notre cas nous choisirons : certificat-supinfo

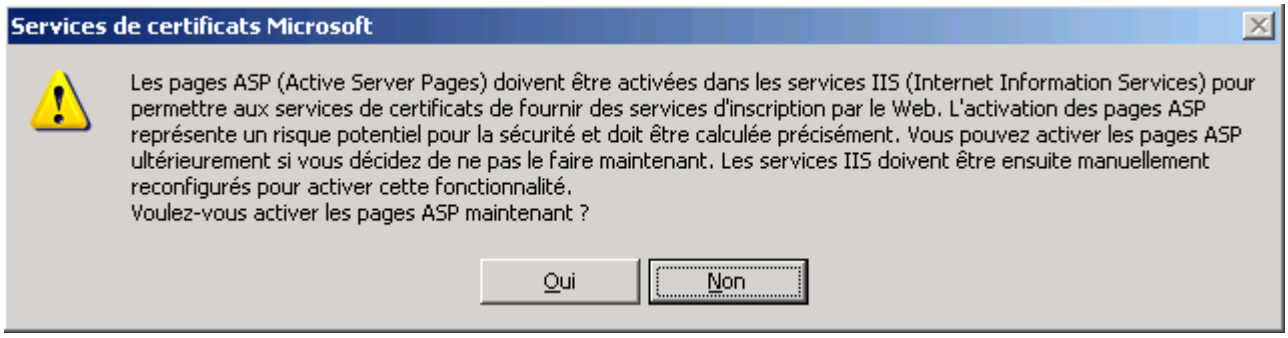


Puis on sélectionne l'emplacement de la base de données et le journal de certificats.



Pour continuer l'installation les Services IIS doivent être redémarrés, on valide donc par oui.

L'installation nous signale qu'ASP doit être activé pour permettre aux services de certificats de fournir un service d'inscription par le Web. On valide donc par oui.



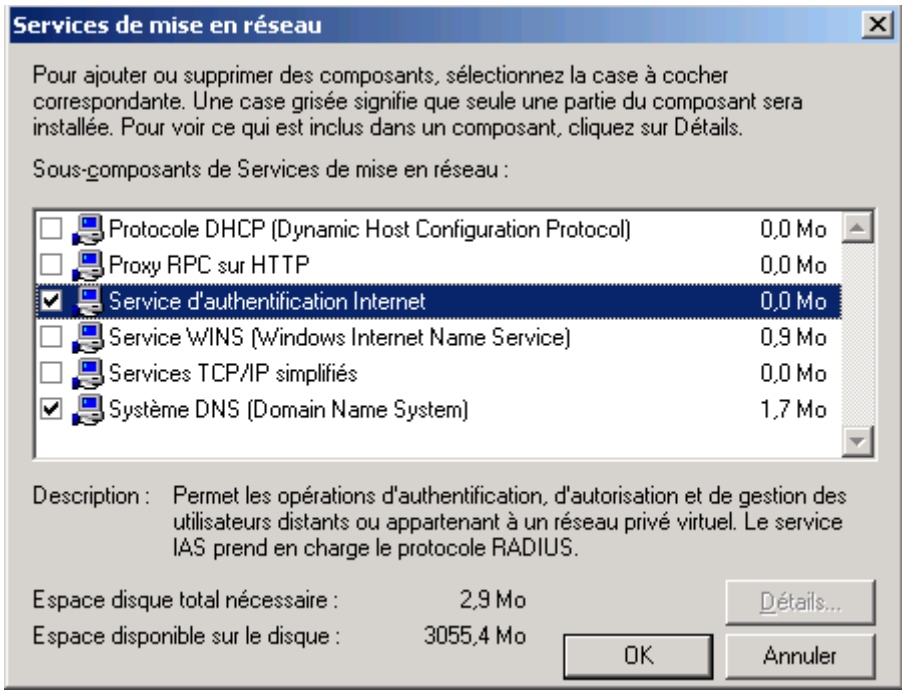
L'installation des Services de certificat est maintenant terminée.

17.1.5. 5. Installation et Configuration du serveur Radius

- Installation

Nous utilisons l'outil " Ajout/Suppression de composants Windows " situé dans " Ajout/Suppression de programmes " du Panneau de configuration.

Nous sélectionnons par la suite Services de mise en réseau, puis dans détails il faut cocher Service d'Authentification Internet.



Puis l'installation continue.

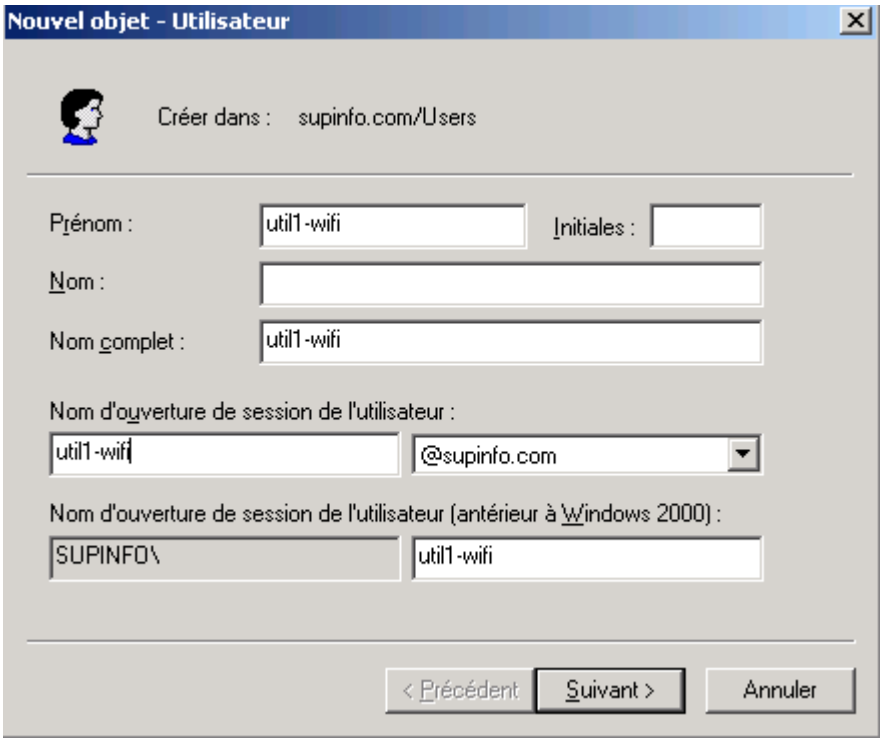
Après l'installation nous allons créer un utilisateur et un groupe dans Active Directory pour les utilisateurs du réseau Wi-fi, avant de passer à la configuration du serveur Radius.

- Création d'un utilisateur et d'un groupe dans Active Directory

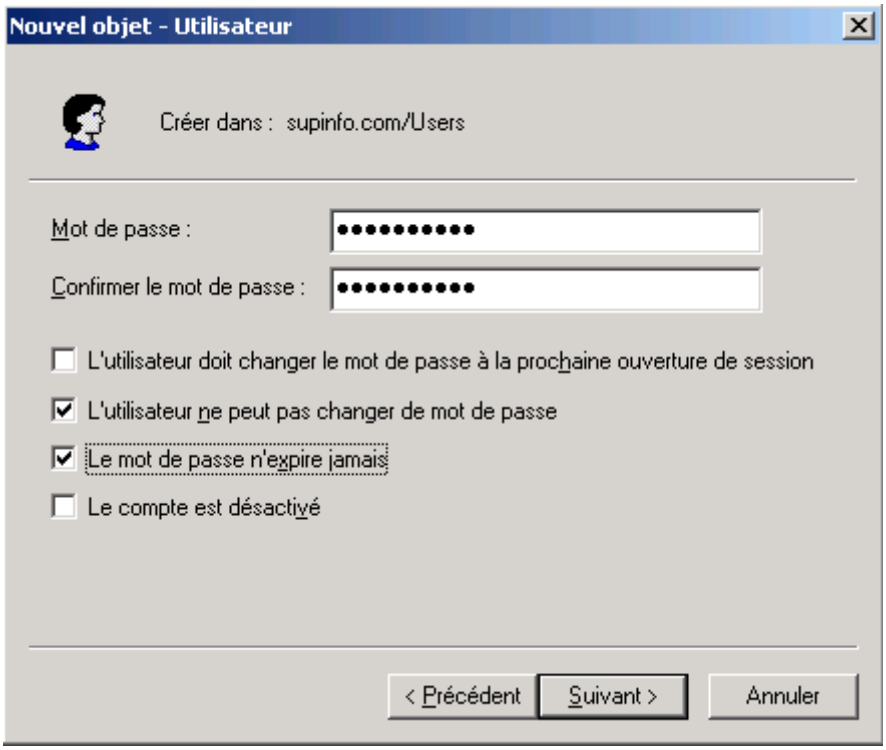
Allez dans le menu Démarrer puis Outils d'administration et enfin sélectionner Utilisateurs et ordinateurs Active Directory.

Dans le dossier Users faites un click droit avec la souris puis nouveau utilisateur.

On créer alors un utilisateur util1-wifi

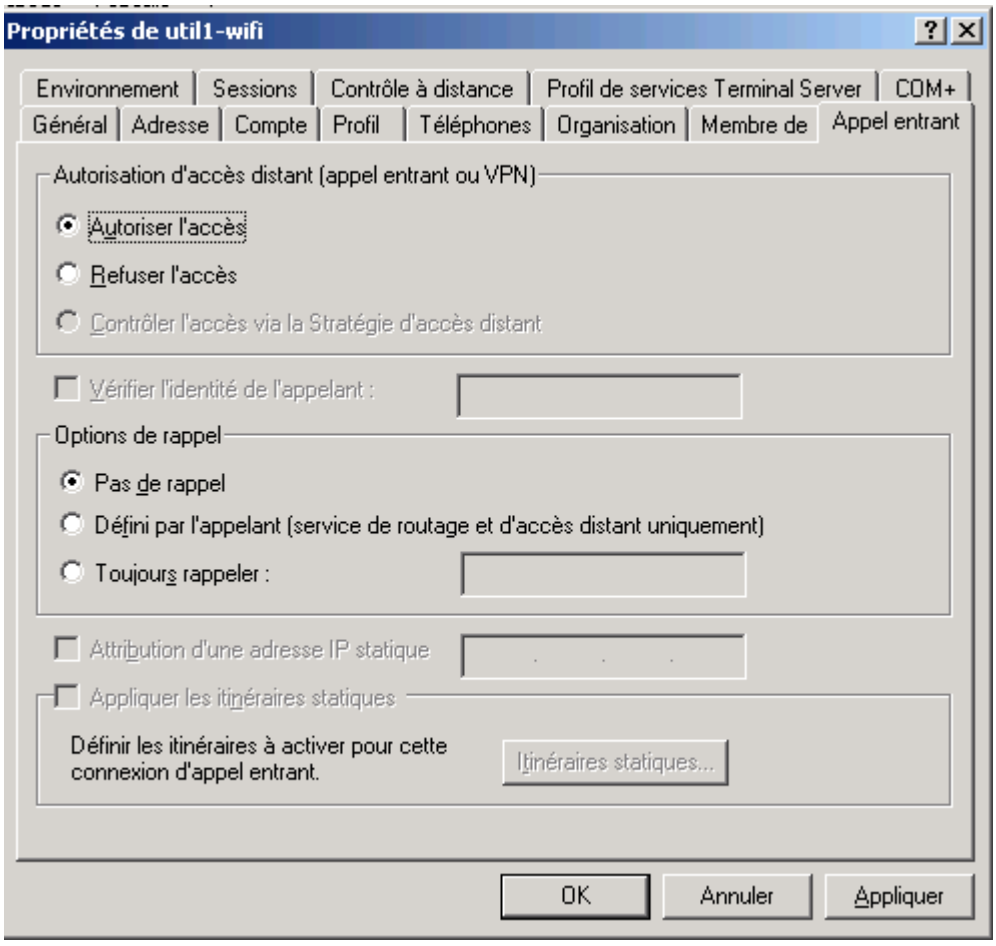


On entre ensuite le mot de passe, ainsi que les options concernant le compte.



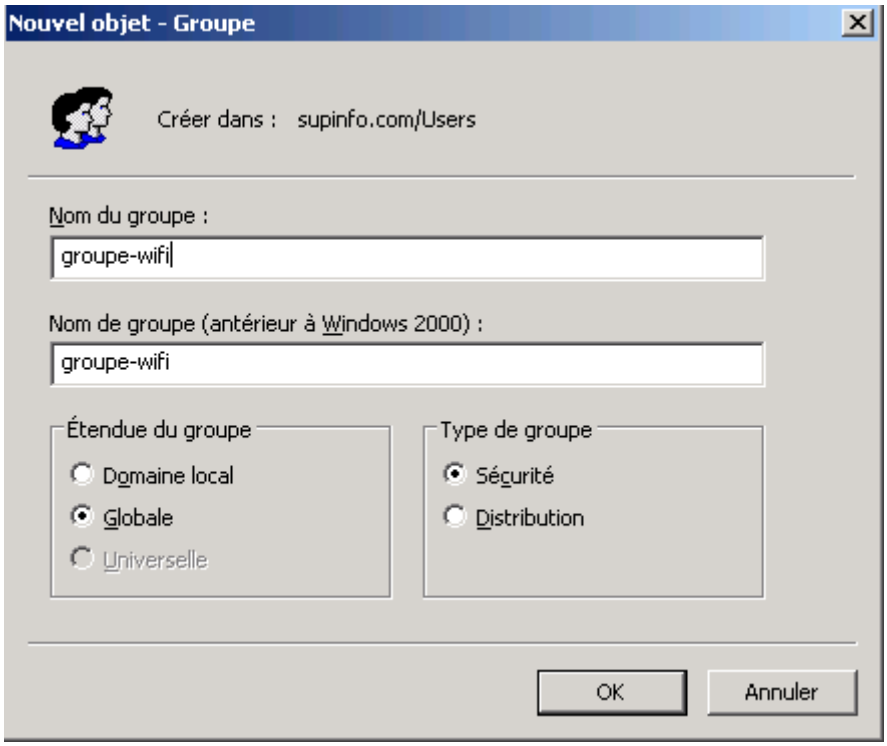
Puis faire un click droit sur l'utilisateur util1-wifi puis aller dans propriétés dans l'onglet Appel entrant.

Puis dans Autorisation d'accès distant (appel entrant ou VPN) cochez Autoriser l'accès.



Nous pouvons maintenant créer un groupe d'utilisateurs qui contiendra les utilisateurs autorisés à accéder au réseau Wi-Fi.

Dans le dossier Users faire un click droit puis nouveau groupe que l'on appellera groupe-wifi.



Faire un click droit sur le groupe groupe-wifi puis aller dans propriétés.

Dans l'onglet Membres sélectionnez ajouter.

On ajoute alors l'utilisateur util1-wifi.

On valide par deux fois par ok, util1-wifi fait donc maintenant partie de groupe-wifi.

On peut donc passer à la configuration du serveur Radius.

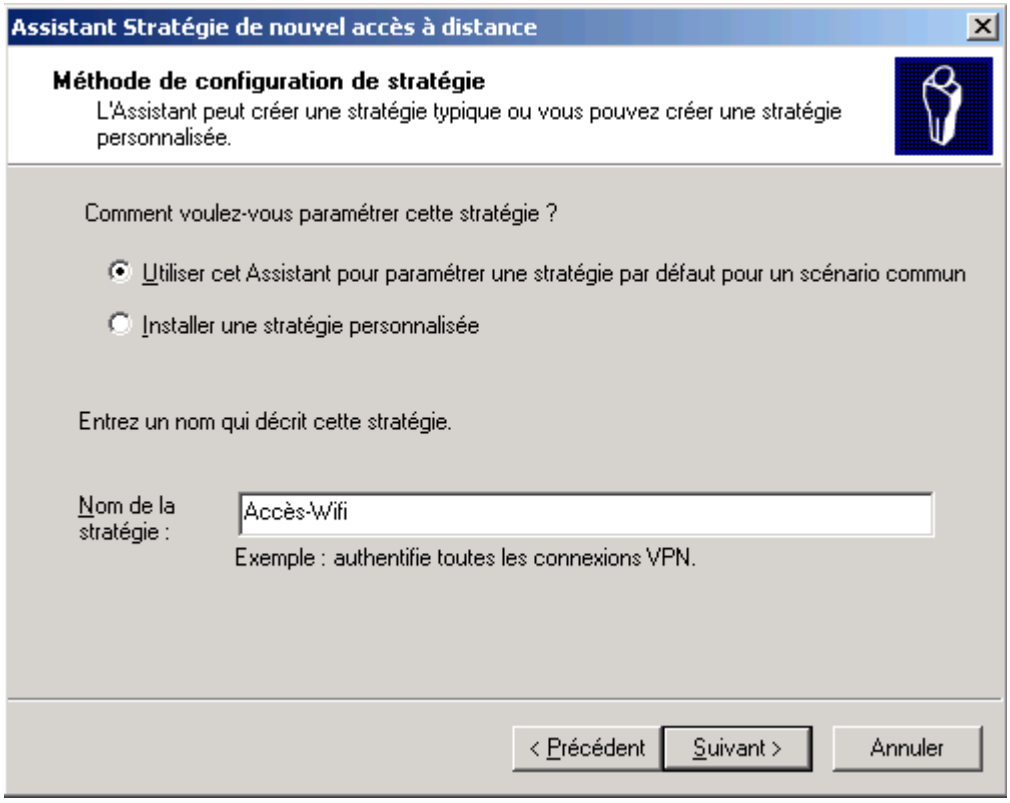
- Configuration du serveur Radius

Tout d'abord allez dans le menu Démarrer puis Outils d'administration et enfin sélectionner Service d'authentification Internet.

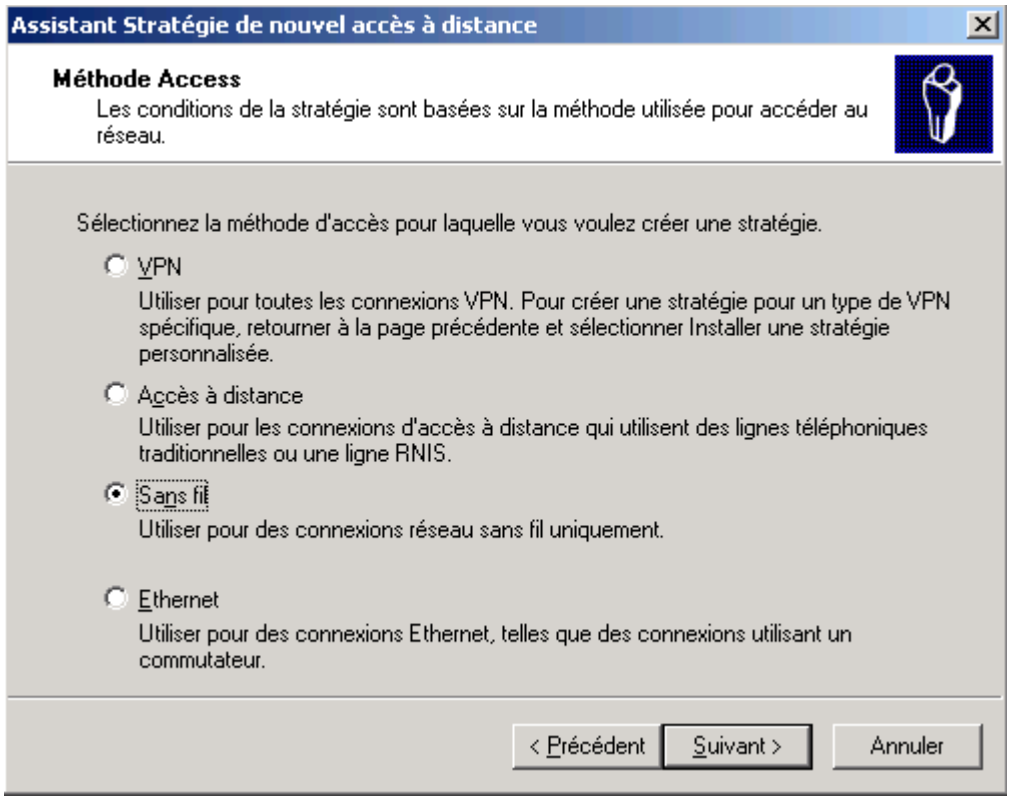
Dans le dossier Stratégie d'accès distant fait un click droit puis nouvelle stratégie d'accès distant.

Cochez utiliser cet assistant pour paramétrer une stratégie par défaut pour un scénario commun.

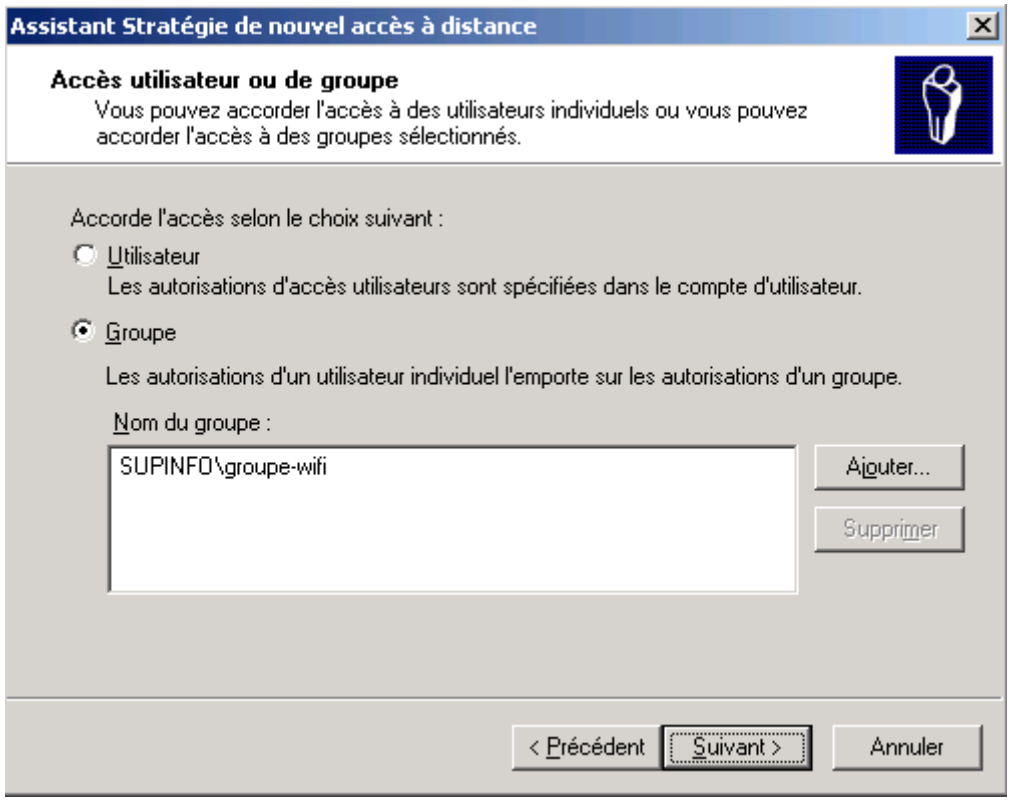
Puis entrez le nom de la nouvelle stratégie.



Validez par suivant puis cocher la méthode d'accès sans fil.



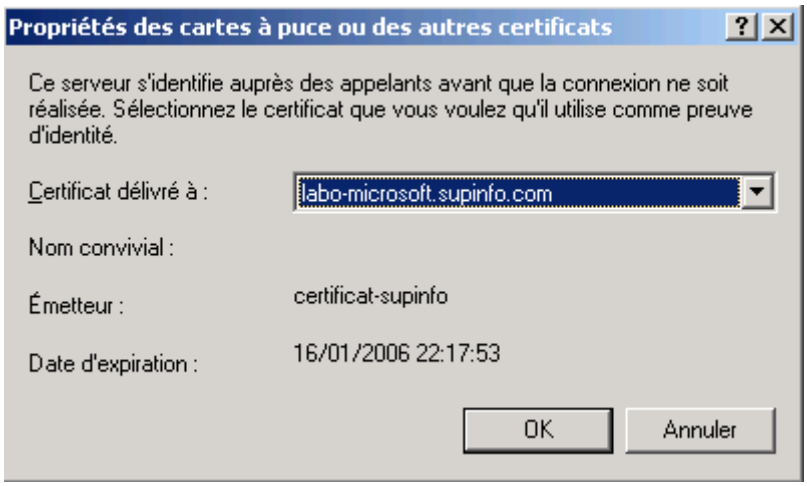
On continue en validant par suivant puis on ajoute le groupe groupe-wifi à la liste d'accès.



Cliquer sur suivant puis sélectionnez Carte à puce ou autre certificat.

Sélectionner configurer pour vérifier qu'il s'agit bien du serveur sur lequel vous venez d'installer l'autorité de certification racine.

Dans notre cas, l'émetteur est certificat-supinfo et le certificat est délivré à labo-microsoft.supinfo.com (nom DNS du serveur).

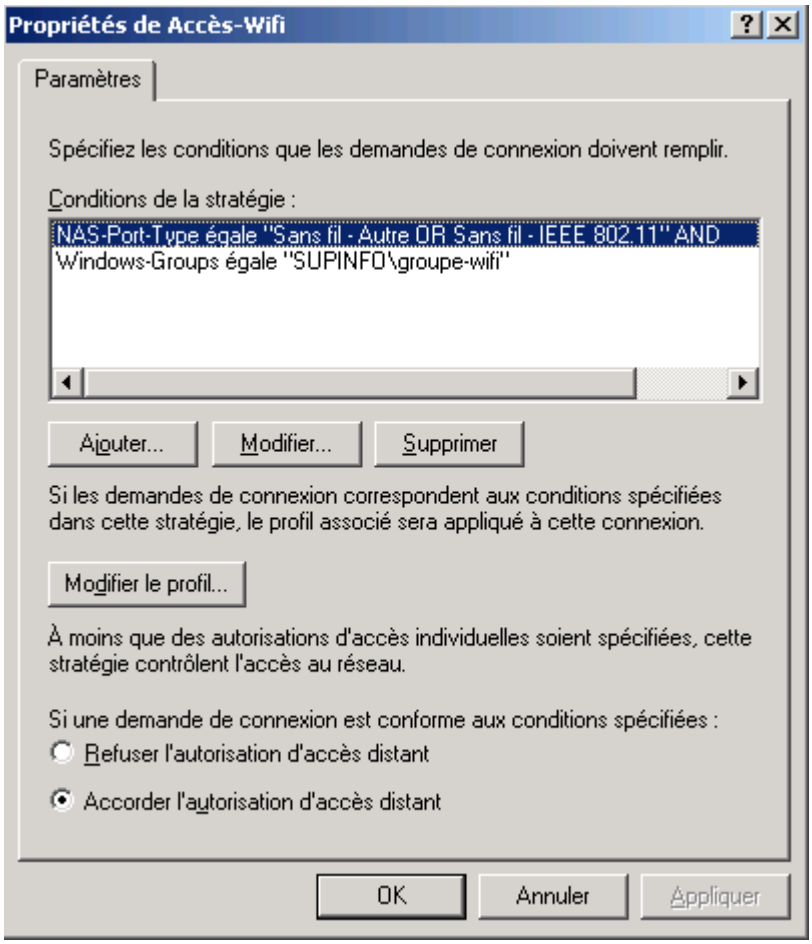


On fini l'installation en cliquant sur suivant et terminer.

Nous allons maintenant vérifier les paramètres de la nouvelle stratégie.

Faites un click droit sur la nouvelle stratégie Accès-Wifi puis propriétés.

Vérifiez que l'option accorder l'autorisation d'accès distant est bien cochée.

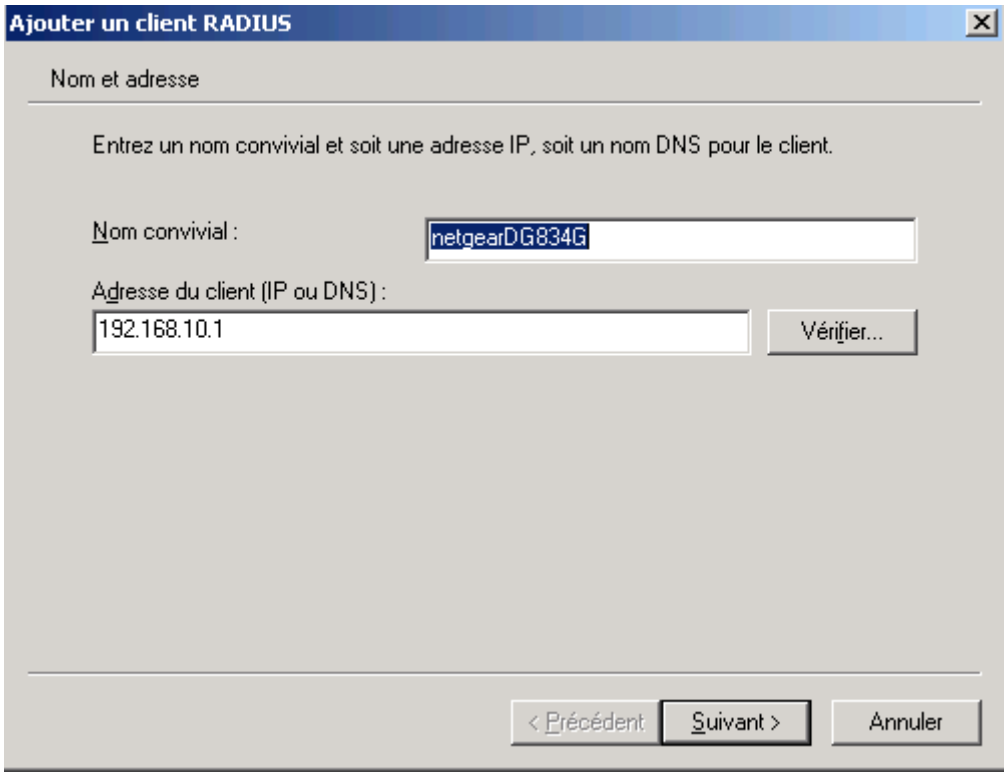


Puis fermez la fenêtre en cliquant sur ok.

Maintenant, dans le dossier Client Radius faites un click droit puis ajouter un client RADIUS.

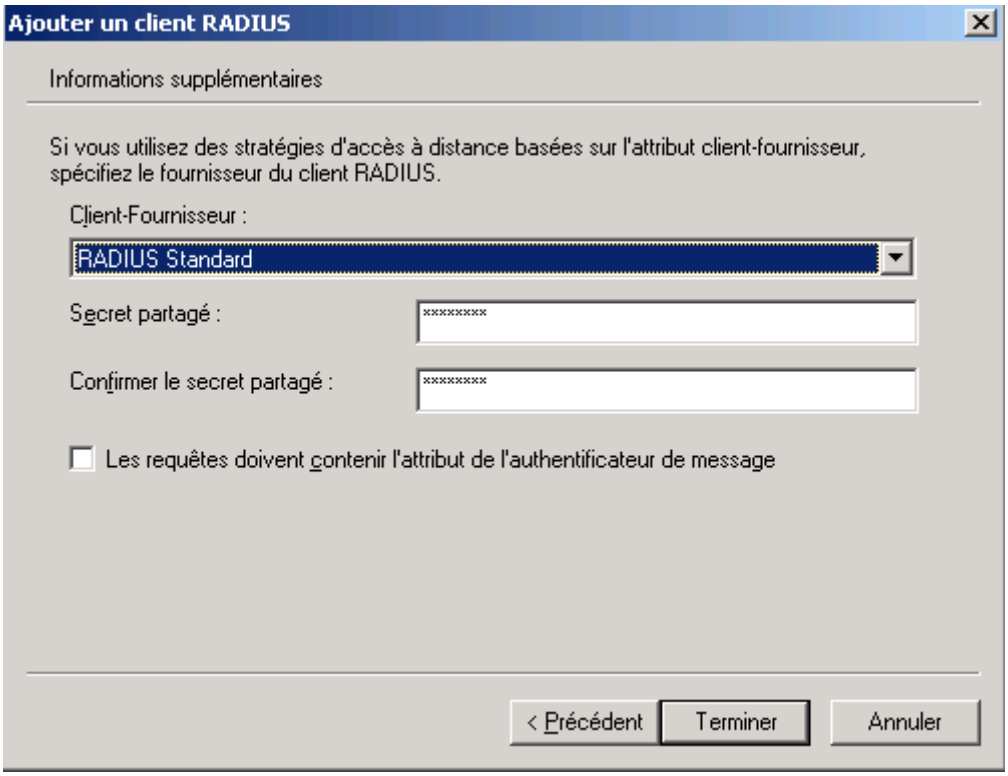
Puis entrez un nom convivial qui sera celui de votre point d'accès Wi-Fi ainsi que son adresse IP.

Dans notre article nous utiliserons un modem routeur ADSL NetgearDG834G faisant office de point d'accès Wi-Fi.



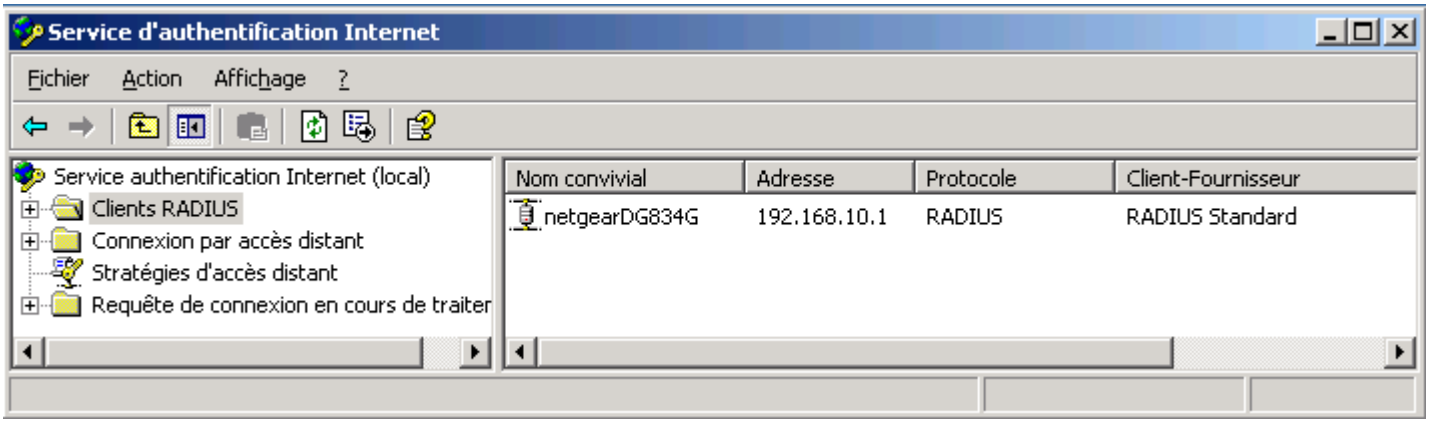
Validez par suivant puis définir le secret partagé entre le point d'accès et le serveur Radius.

Dans notre cas nous utiliserons un attribut du client Radius de type standard, mais si la marque de votre point d'accès est mentionnée il vaut mieux utiliser cet attribut.



Puis cliquez sur terminer.

Le point d'accès apparaît alors dans la liste des clients Radius.



La configuration du serveur Radius est maintenant terminée

17.1.6. 6. Configuration du point d'accès Wi-Fi

Dans notre article nous utiliserons un modem routeur ADSL NetgearDG834G faisant office de point d'accès Wi-Fi, mais la majorité des points d'accès des autres fournisseurs sont aussi compatibles.

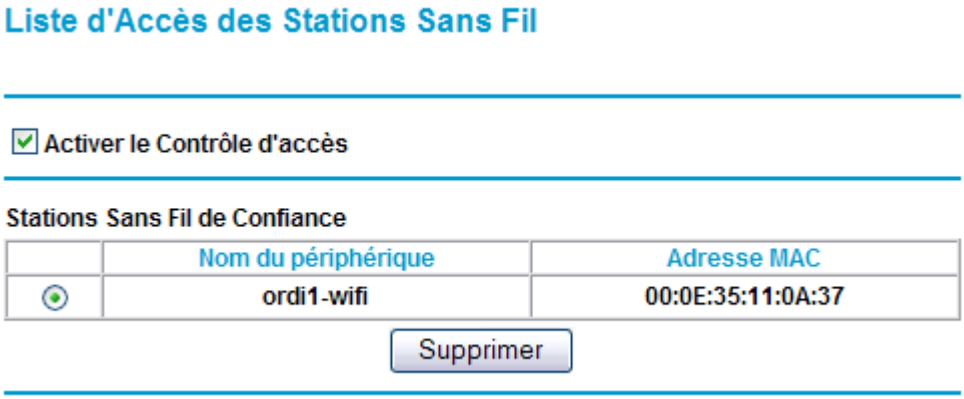
Ouvrez Internet Explorer et saisissez l'adresse votre point d'accès, dans notre article http://192.168.10.1

Entrez votre login et votre mot de passe puis aller dans le menu paramètres sans fil.

Première sécurité désactiver la diffusion du nom SSID (*Service Set Identifier*) ce qui empêchera que le nom de votre réseau ne soit visible aux yeux de tous.

Puis cliquez sur le bouton configuration de la liste d'accès.

Deuxième sécurité entrez la liste des adresses MAC que vous autoriserez à accéder au réseau.

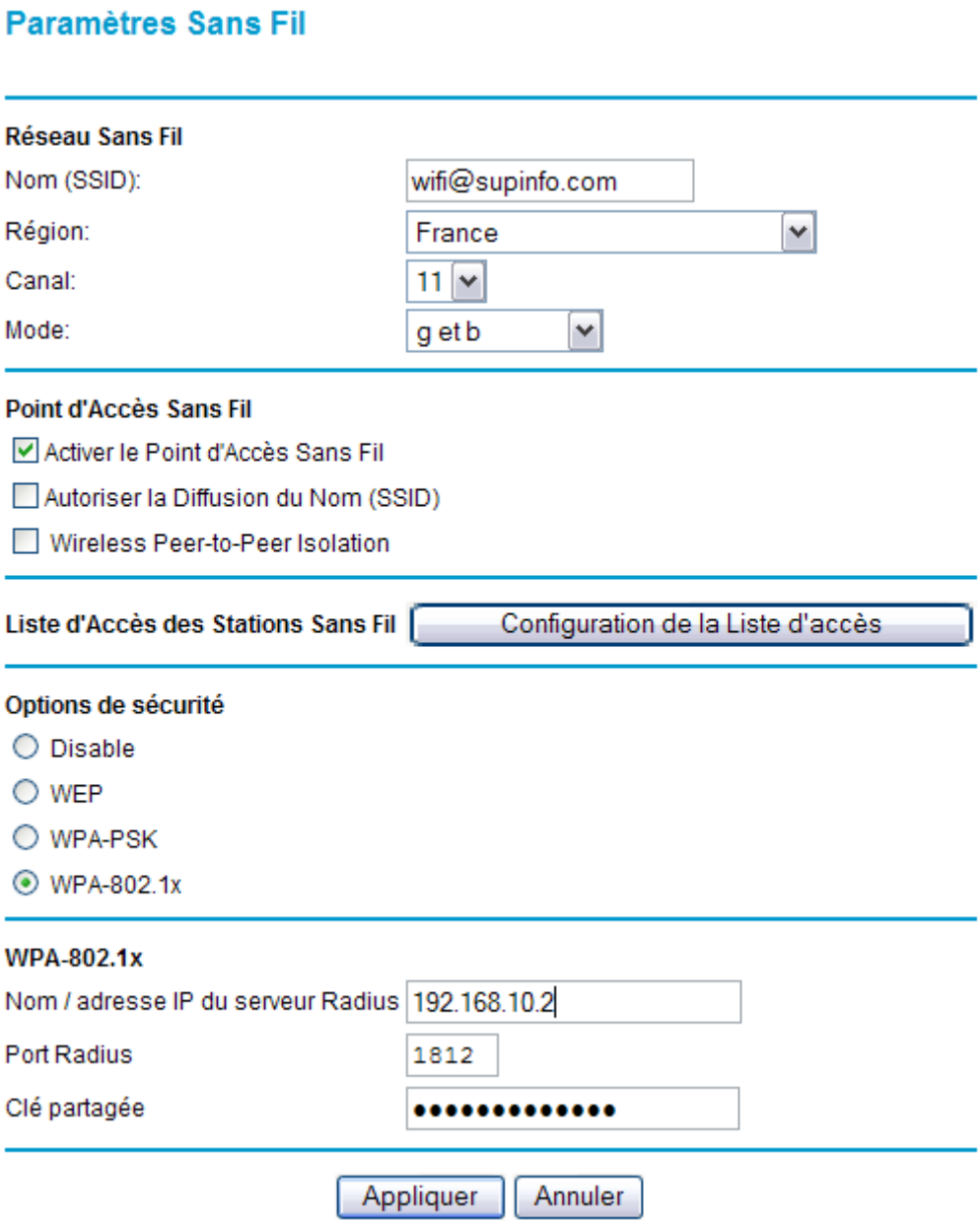


Enfin choisissez l'option de sécurité WPA-802.1X

Entrez l'adresse IP de votre Serveur Radius.

Entrez le port de communication (par défaut 1812).

Puis entrez la même clé partagée que celle que vous avez saisie sur le serveur Radius pour le point d'accès.



Validez en cliquant sur appliquer.

La configuration de la borne d'accès est maintenant terminée.

Nous allons pouvoir passer à la configuration des clients d'accès Wi-Fi.

17.1.7. 7. Configuration des clients d'accès Wi-Fi

Dans notre cas nous utiliserons un Windows XP SP2.

- Installation du certificat

Nous allons devoir récupérer un certificat émis par l'autorité de certification.

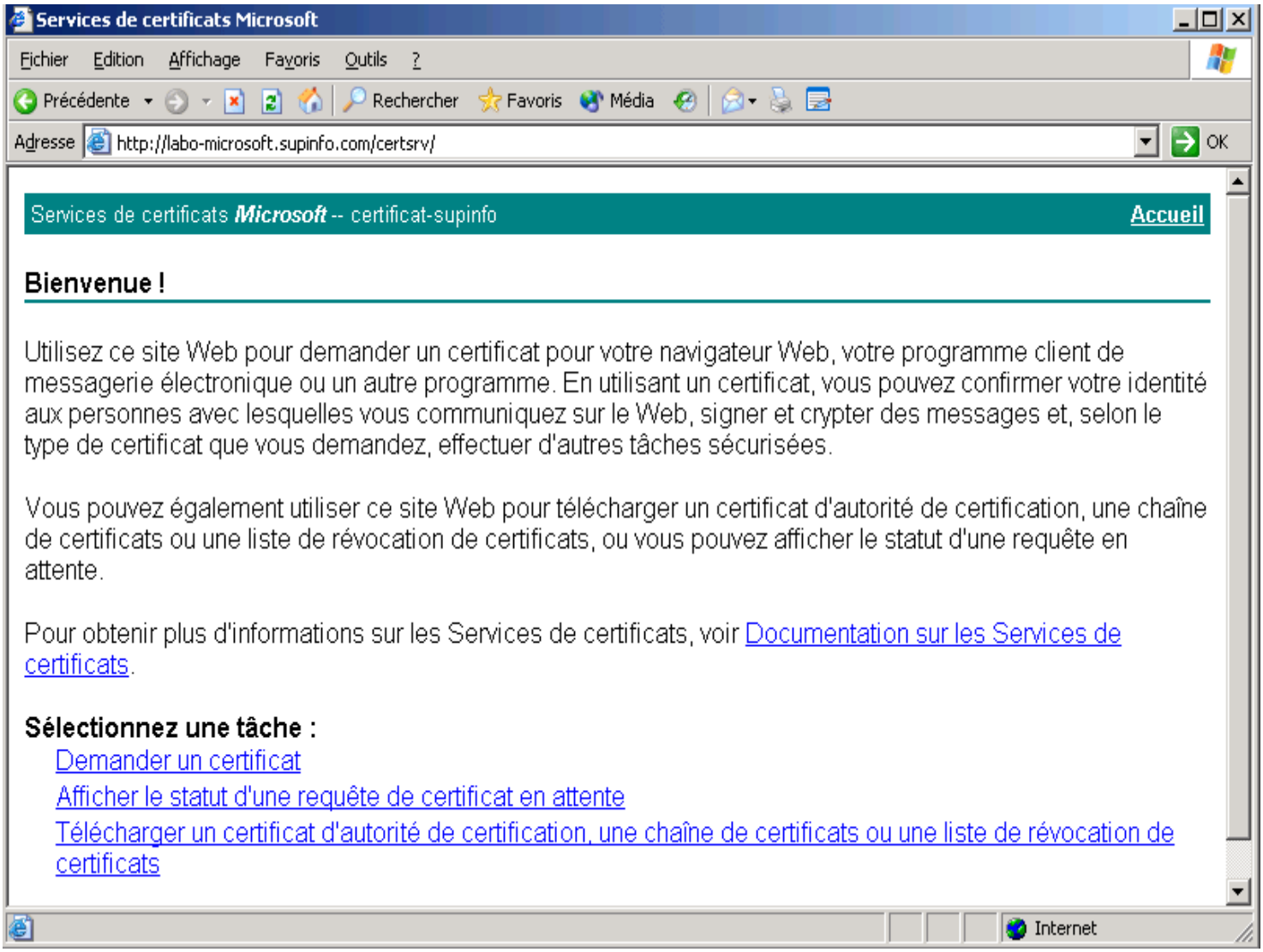
Tout d'abord ouvrez une session sous le nom de l'utilisateur qui recevra le certificat sur cette machine.

Puis ouvrir Internet Explorer et se connecter sur le serveur Web de l'autorité de certification : http:// "nom de votre serveur "/certsrv

Dans notre article http://labo-microsoft.supinfo.com/certsrv

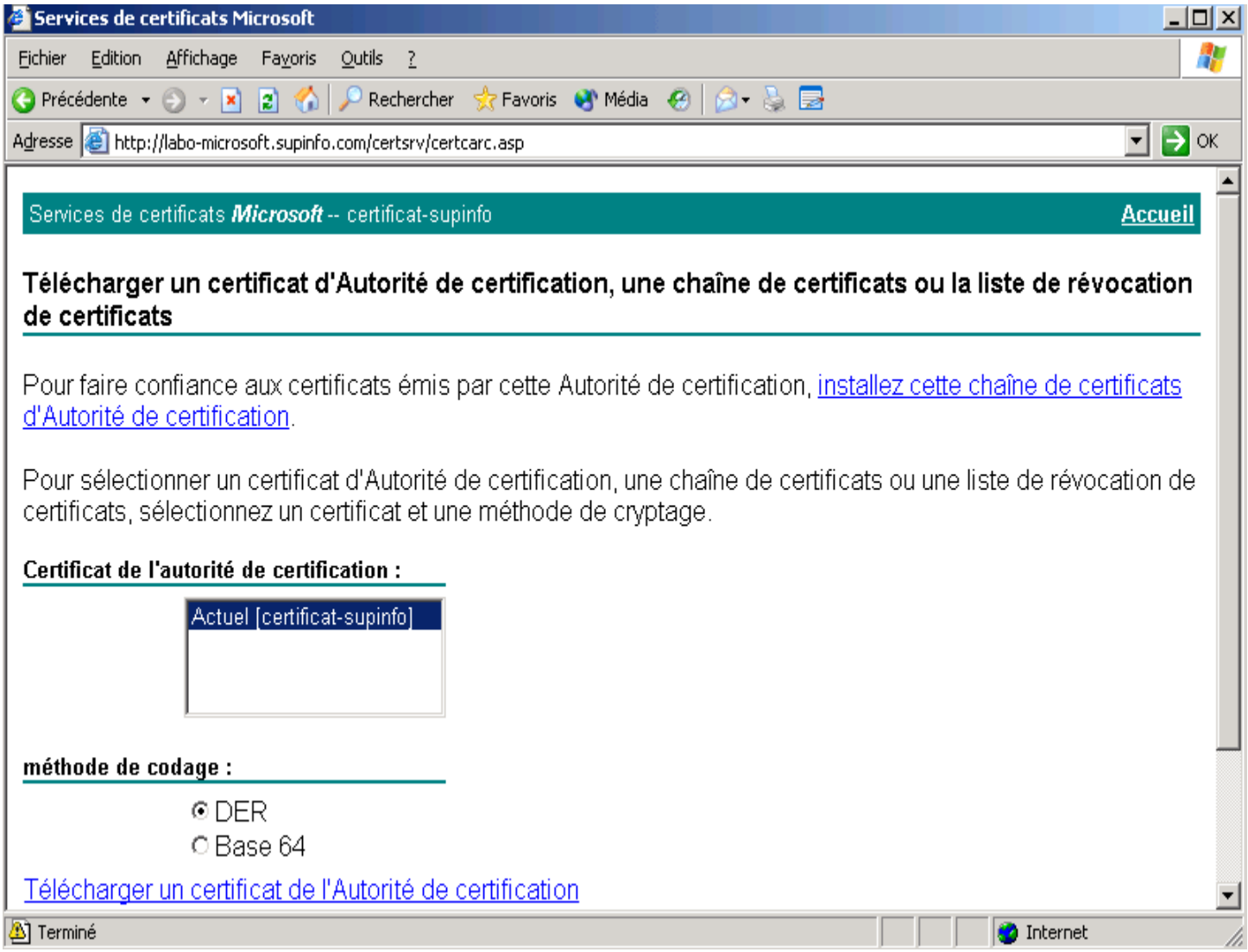
Entrez le login et le mot de passe de l'utilisateur (util1-wifi).

Vous arrivez alors sur la page d'accueil

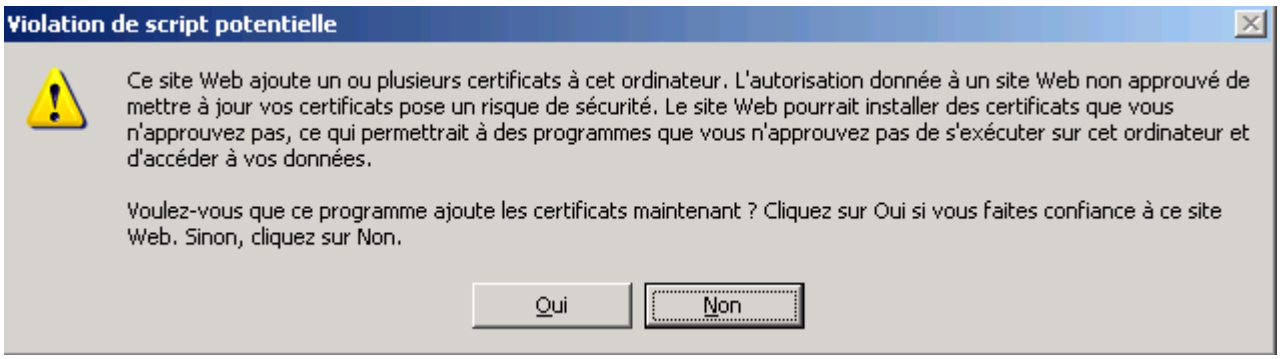


Il faut maintenant installer une chaîne de certificats, pour ce faire cliquer sur le lien correspondant en bas de la fenêtre.

Puis cliquez sur installez cette de chaîne de certificats d'autorité de certification.

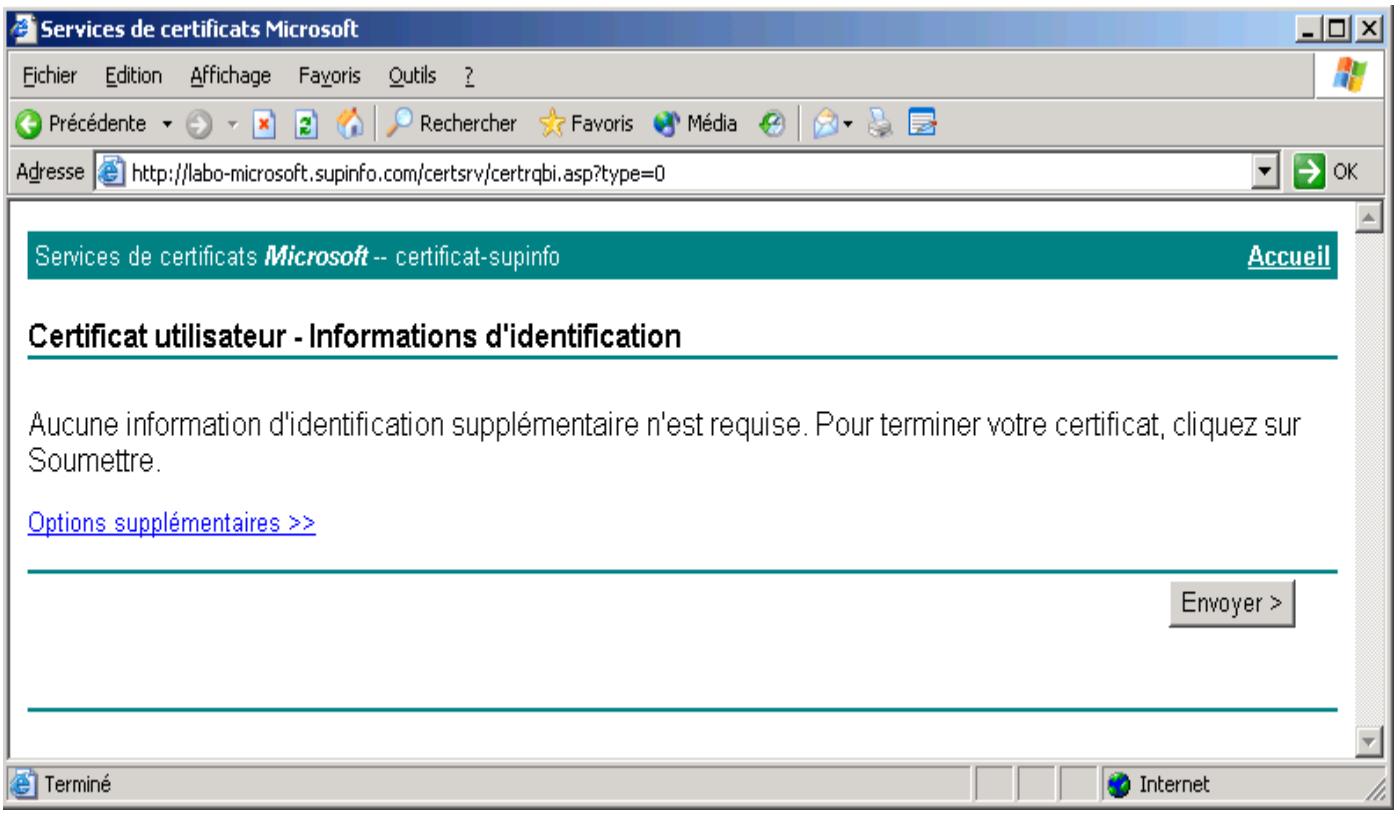


Une fenêtre s'ouvre vous demandant de confirmer l'installation, cliquez sur oui.

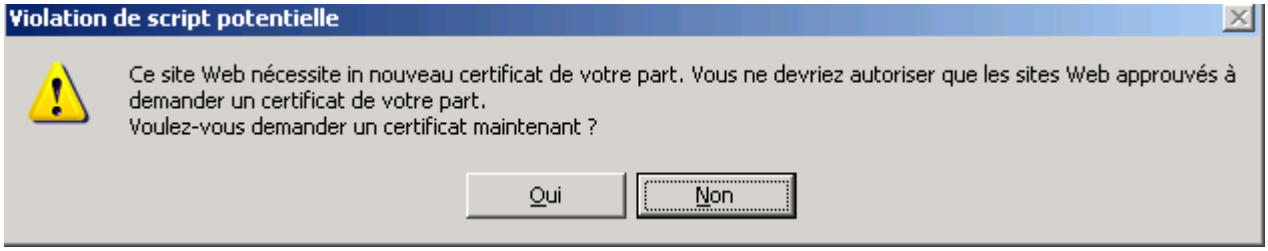


Puis retournez à la page d'accueil.

Suivez le lien demander un certificat, puis le lien certificat utilisateur et enfin cliquer sur le bouton envoyer.

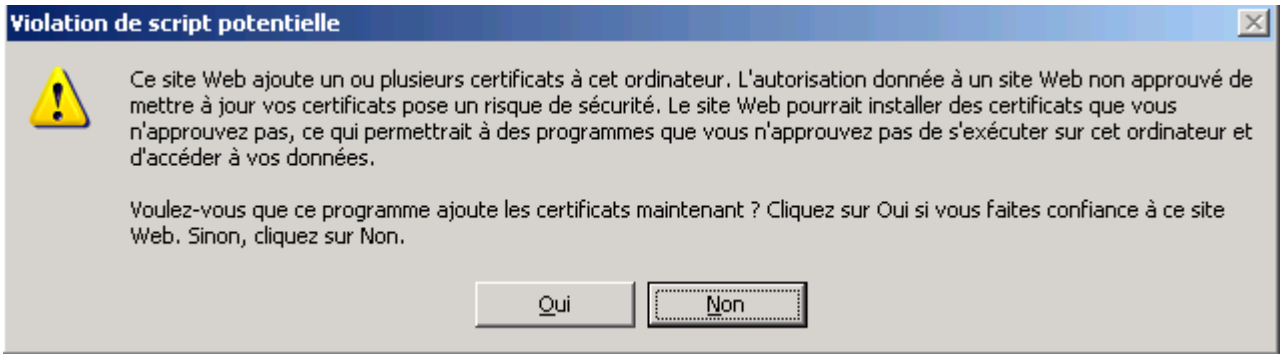


Confirmez la demande de certificat en cliquant sur oui.



Suivez le lien installer ce certificat.

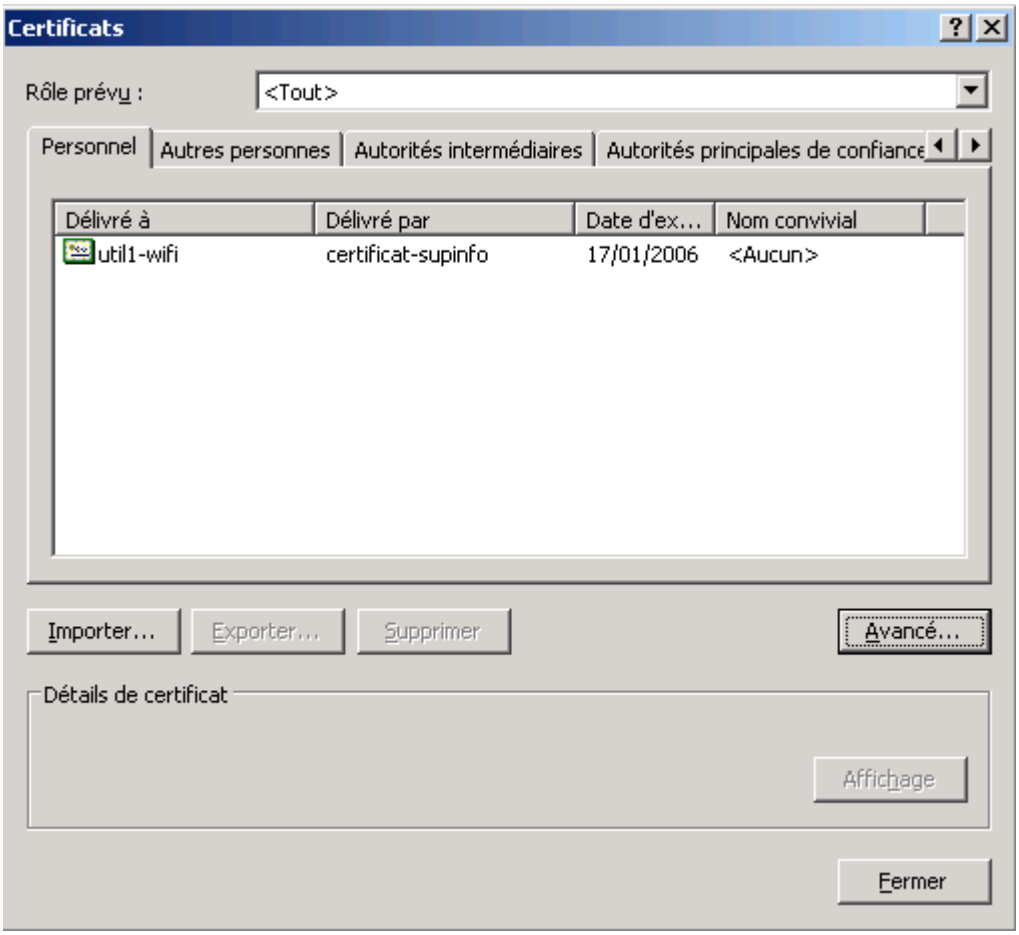
Puis cliquer sur oui pour valider que faites confiance à ce site.



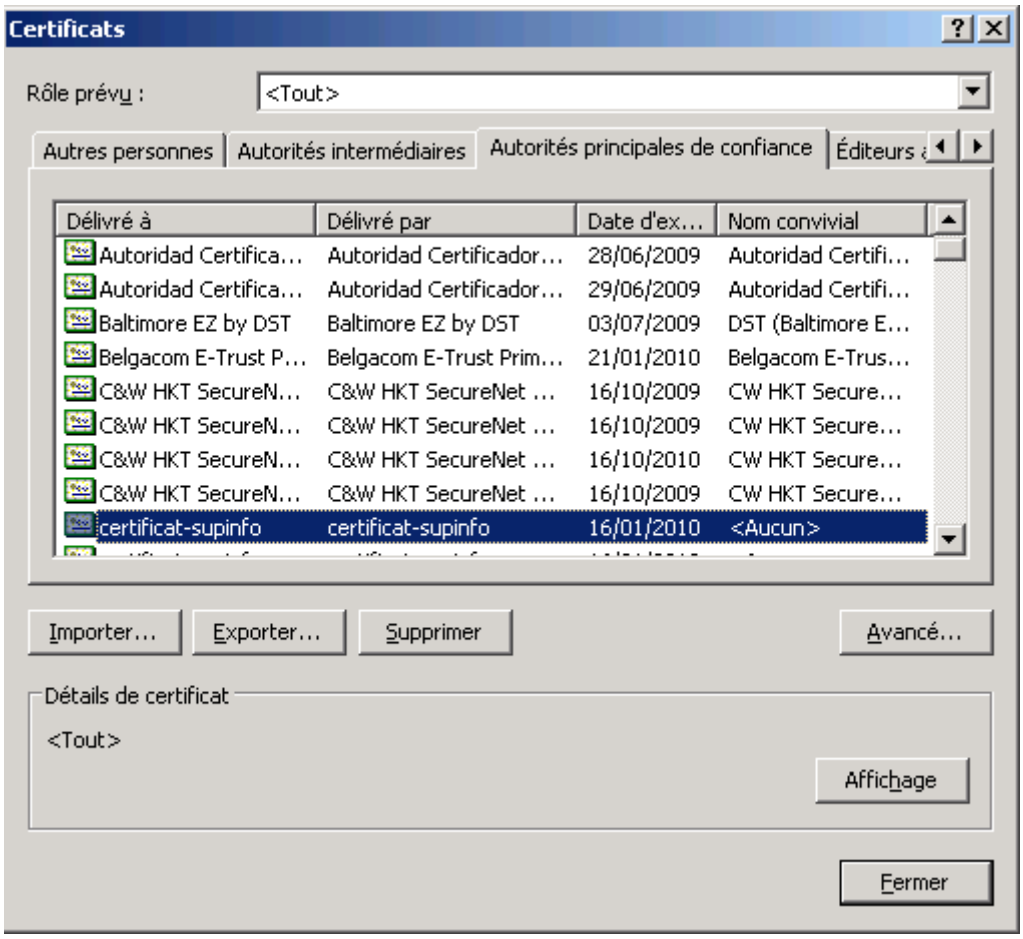
Le certificat est maintenant installé.

Pour vérifier que les paramètres soient corrects, dans Internet Explorer allez dans le menu déroulant outils puis option Internet puis dans l'onglet contenu, enfin cliquez sur certificats.

Vérifiez que le certificat pour l'utilisateur util1-Wifi est bien présent.



Vérifiez également que le serveur de certificat est bien présent dans la liste des autorités principales de confiance.



L'installation du certificat est maintenant terminé nous allons pouvoir passer à la configuration de la connexion réseau sans-fil.

- Configuration de la connexion réseau sans-fil

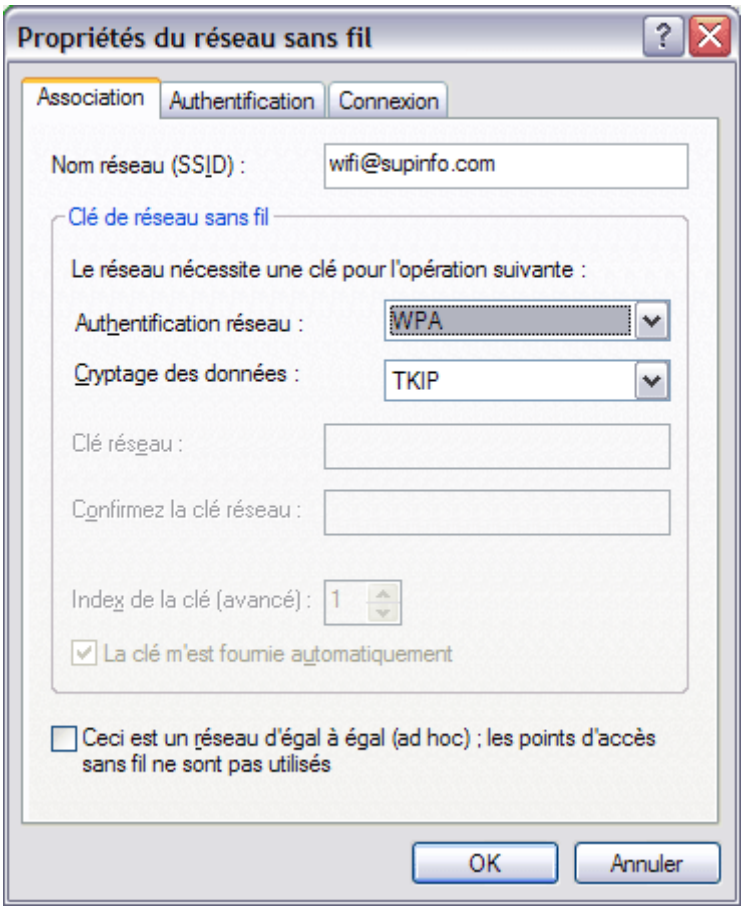
Allez dans Panneau de Configuration puis Connexions réseaux.

Faites un click droit sur la connexion réseaux sans-fil puis entrez dans les propriétés.

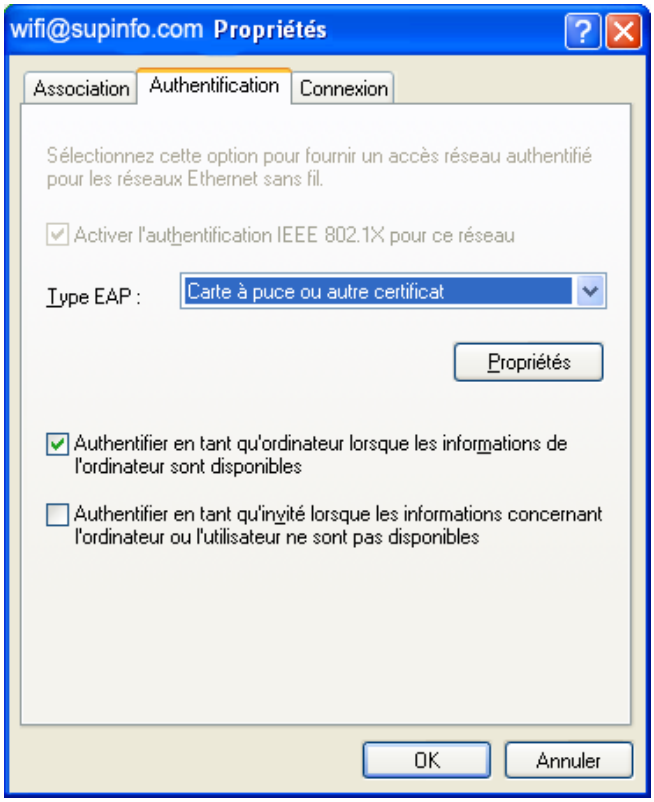
Dans l'onglet Configuration réseaux sans-fil cliquez sur ajouter.

Entrez le nom de votre réseau.

Choisissez une authentification de type WPA et un cryptage de type TKIP.

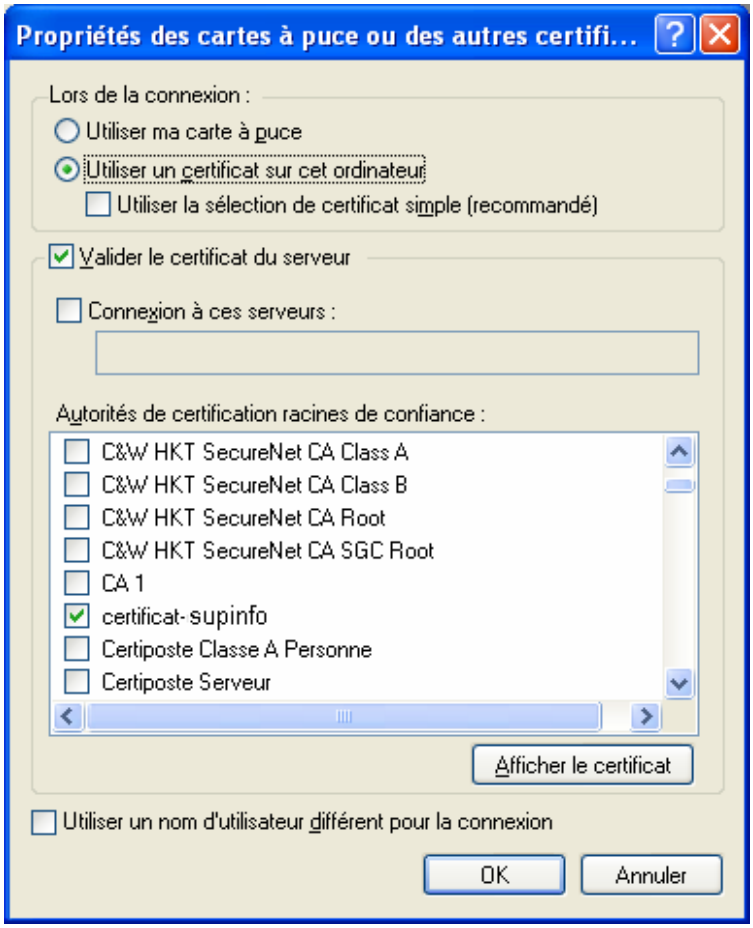


Dans l'onglet authentification sélectionnez activer l'authentification IEEE 802.1X pour ce réseau et cliquez sur propriétés du type EAP (Laissez le type EAP à carte à puce ou autre certificat).

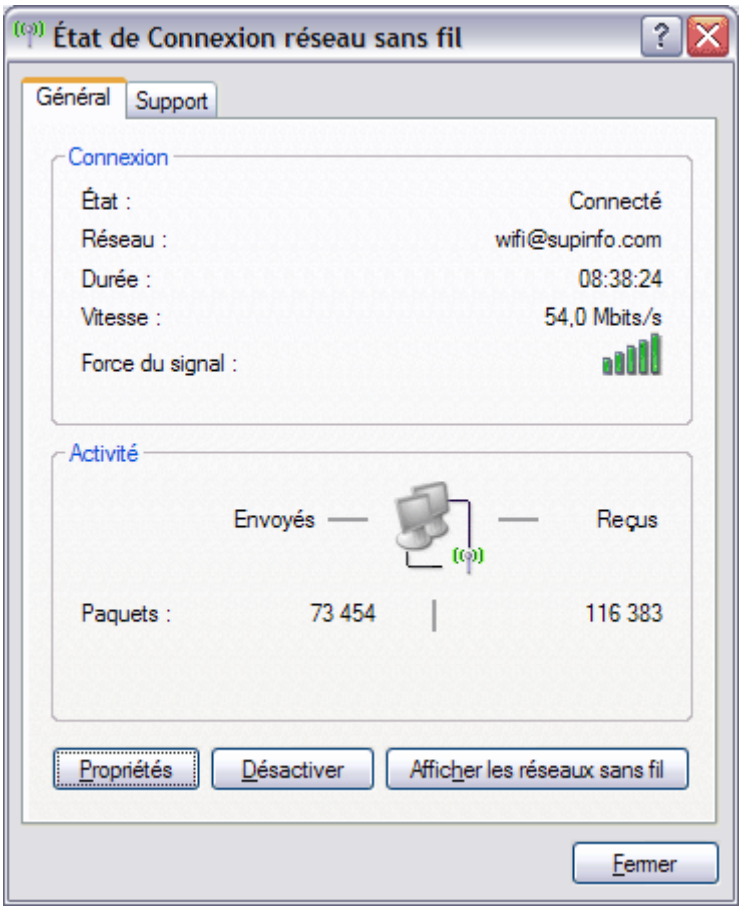


Décochez l'option connexion à ces serveurs.

Puis sélectionner votre serveur de certificat dans la liste des autorités de certification racine de confiance.



Votre connexion est maintenant configurée et opérationnelle, vous pouvez donc vous connectez au réseau sans-fil, mais avant, redémarrer quand même la machine.



- Poste en Windows 2000

Une installation est également pour possible pour un Windows 2000 mais vous devez disposer du service Pack 3 ou plus récent et installer un correctif que vous pouvez trouvez à cette adresse :

http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=6B78EDBE-D3CA-4880-929F-453C695B9637

17.1.8. Conclusion

Nous avons donc tout fait au long de cet article pour mettre en place une infrastructure Wi-Fi la plus sécurisée possible tout en étant compatible avec les exigences des différentes technologies des fabricants.

Vous disposez donc maintenant de la sécurité la plus renforcée pour un réseau sans-fil. Si vous craigniez encore le piratage, il ne vous reste plus qu'à mettre en place des dispositifs de brouillage, mais attention à ne pas détériorer du même coût votre réseau.

De plus cet architecture basée sur un serveur Radius et une authentification de type EAP pourra également vous servir pour mettre en place une politique d'accès distant centralisée et sécurisée.

17.2. Installation et configuration de FreeRadius

17.2.1. Sur RedHat

(Documentation pris du site http://earxtacy.free.fr/doc/radius.pdf)

Cette documentation est à utilisé tel quel, en effet elle est assez incomplète du fait que la plupart des documentations soient en anglais.

L'installation proposé ici à été réalisé sur une distribution RedHat, par conséquent elle est également compatible avec Mandrake (Mandriva (nouveau nom de Mandrake Linux)) par le fait qu'elle utilise des RPM.

Sous REDHAT

17.2.1.1. Télécharger TOUS les packages de MySQL :

```
MySQL-3.23.55-1.i386.rpm
MySQL-client-3.23.55-1.i386.rpm
MySQL-devel-3.23.55-1.i386.rpm
MySQL-shared-3.23.55-1.i386.rpm
```

Une fois cela fait il faut les installer sur la machine

```
rpm –ivh MySQL-3.23.55-1.i386.rpm MySQL-client-3.23.55-1.i386.rpm
MySQLdevel-3.23.55-1.i386.rpm MySQL-shared-3.23.55-1.i386.rpm
```

17.2.1.2. Installation de Freeradius (www.freeradius.org)

Il faut tout d'abord télécharger **freeradius.tar.gz** et ensuite il va falloir le compiler correctement.

```
tar zxvf freeradius.tar.gz
```

Une fois la décompression faite , il faudra se mettre dans le repertoire freeradius…. créé :

```
./configure
make
make install
```

17.2.1.3. Configuration de Freeradius :

Le serveur radius fonctionne avec, de base, 4 fichiers de configuration. Ceux ci sont à modifier comme suit pour notre exemple.

/usr/local/etc/raddb/clients.conf :

```
# Client pour test local
client 127.0.0.1 {
            secret = testradius #secret partagé
            shortname = localhost
            nastype = other
}
# Client pour test depuis votre LAN en 192.168.5.0/24
client 192.168.5.0/24 {
            secrect = testradius
            shortname = private-network-1
}
```

/usr/local/etc/raddb/users :

Ce fichier etant commenté et n'etant utiliser que pour les premiers tests je ne m'etendrai pas dessus. Nous utiliserons l'utilisateur Steve.

```
steve Auth-Type := Local, User-Password == "testing"
      Service-Type = Framed-User,
      Framed-Protocol = PPP,
      Framed-IP-Address = 172.16.3.33,
      Framed-IP-Netmask = 255.255.255.0,
      Framed-Routing = Broadcast-Listen,
      Framed-Filter-Id = "std.ppp",
      Framed-MTU = 1500,
      Framed-Compression = Van-Jacobsen-TCP-IP
```

/usr/local/etc/raddb/realms :

Rajoutons DEFAULT et LOCAL pour ne pas avoir a se poser la question dans quel domaine le client se connecte.

```
# Realm           Remote server [:port]   Options
#---------------- --------------------- -------
#isp2.com         radius.isp2.com         nostrip
#company.com      radius.company.com:1600
#bla.com          LOCAL
#replicateme      radius2.company.com     notrealm
#foo.com               192.168.1.39
DEFAULT           LOCAL
```

/usr/local/etc/raddb/radiusd.conf :

Ce fichier est très long je sais, il s'étend de la page 5 à la page 25 (pour ceux qui désirerait imprimer sans cette partie). Les modifications

```
##
## radiusd.conf -- FreeRADIUS server configuration file.
##
##    http://www.freeradius.org/
##    $Id: radiusd.conf.in,v 1.123 2002/11/12 20:22:48 aland Exp $
##
#     The location of other config files and
#     logfiles are declared in this file
#
#     Also general configuration for modules can be done
#     in this file, it is exported through the API to
#     modules that ask for it.
#
#     The configuration variables defined here are of the form ${foo}
#     They are local to this file, and do not change from request to
#     request.
#
#     The per-request variables are of the form %{Attribute-Name}, and
#     are taken from the values of the attribute in the incoming
#     request. See 'doc/variables.txt' for more information.

prefix = /usr/local
exec_prefix = ${prefix}
sysconfdir = ${prefix}/etc
localstatedir = ${prefix}/var
sbindir = ${exec_prefix}/sbin
logdir = ${localstatedir}/log/radius
raddbdir = ${sysconfdir}/raddb
radacctdir = ${logdir}/radacct

# Location of config and logfiles.
```

```
confdir = ${raddbdir}
run_dir = ${localstatedir}/run/radiusd

#
# The logging messages for the server are appended to the
# tail of this file.
#
log_file = ${logdir}/radius.log

#
# libdir: Where to find the rlm_* modules.
#
# This should be automatically set at configuration time.
#
# If the server builds and installs, but fails at execution time
# with an 'undefined symbol' error, then you can use the libdir
# directive to work around the problem.
#
# The cause is usually that a library has been installed on your
# system in a place where the dynamic linker CANNOT find it. When
# executing as root (or another user), your personal environment MAY
# be set up to allow the dynamic linker to find the library. When
# executing as a daemon, FreeRADIUS MAY NOT have the same
# personalized configuration.
#
# To work around the problem, find out which library contains that
symbol,
# and add the directory containing that library to the end of 'libdir',

# with a colon separating the directory names. NO spaces are allowed.
#
# e.g. libdir = /usr/local/lib:/opt/package/lib
#
# You can also try setting the LD_LIBRARY_PATH environment variable
# in a script which starts the server.
#
# If that does not work, then you can re-configure and re-build the
# server to NOT use shared libraries, via:
#
# ./configure --disable-shared
# make
# make install
#
libdir = ${exec_prefix}/lib
# pidfile: Where to place the PID of the RADIUS server.
#
# The server may be signalled while it's running by using this
# file.
#
# This file is written when ONLY running in daemon mode.
#
# e.g.: kill -HUP `cat /var/run/radiusd/radiusd.pid`
#
pidfile = ${run_dir}/radiusd.pid
# user/group: The name (or #number) of the user/group to run radiusd as.
#
# If these are commented out, the server will run as the user/group
# that started it. In order to change to a different user/group, you
# MUST be root ( or have root privleges ) to start the server.
#
# We STRONGLY recommend that you run the server with as few permissions
```

```
# as possible. That is, if you're not using shadow passwords, the
# user and group items below should be set to 'nobody'.
#
# On SCO (ODT 3) use "user = nouser" and "group = nogroup".
#
# NOTE that some kernels refuse to setgid(group) when the value of
# (unsigned)group is above 60000; don't use group nobody on these systems!
#
# On systems with shadow passwords, you might have to set 'group = shadow'
# for the server to be able to read the shadow password file. If you can
# authenticate users while in debug mode, but not in daemon mode, it may
be
# that the debugging mode server is running as a user that can read the
# shadow info, and the user listed below can not.
#
#user = nobody
#group = nobody
# max_request_time: The maximum time (in seconds) to handle a request.
#
# Requests which take more time than this to process may be killed, and
# a REJECT message is returned.
#
# WARNING: If you notice that requests take a long time to be handled,
# then this MAY INDICATE a bug in the server, in one of the modules
# used to handle a request, OR in your local configuration.

#
# This problem is most often seen when using an SQL database. If it takes
# more than a second or two to receive an answer from the SQL database,
# then it probably means that you haven't indexed the database. See your
# SQL server documentation for more information.
#
# Useful range of values: 5 to 120
#
max_request_time = 30
# delete_blocked_requests: If the request takes MORE THAN
'max_request_time'
# to be handled, then maybe the server should delete it.
#
# If you're running in threaded, or thread pool mode, this setting
# should probably be 'no'. Setting it to 'yes' when using a threaded
# server MAY cause the server to crash!
#
delete_blocked_requests = no
# cleanup_delay: The time to wait (in seconds) before cleaning up
# a reply which was sent to the NAS.
#
# The RADIUS request is normally cached internally for a short period
# of time, after the reply is sent to the NAS. The reply packet may be
# lost in the network, and the NAS will not see it. The NAS will then
# re-send the request, and the server will respond quickly with the
# cached reply.
#
# If this value is set too low, then duplicate requests from the NAS
# MAY NOT be detected, and will instead be handled as seperate requests.
#
# If this value is set too high, then the server will cache too many
# requests, and some new requests may get blocked. (See 'max_requests'.)
#
# Useful range of values: 2 to 10
#
```

```
cleanup_delay = 5
# max_requests: The maximum number of requests which the server keeps
# track of. This should be 256 multiplied by the number of clients.
# e.g. With 4 clients, this number should be 1024.
#
# If this number is too low, then when the server becomes busy,
# it will not respond to any new requests, until the 'cleanup_delay'
# time has passed, and it has removed the old requests.
#
# If this number is set too high, then the server will use a bit more
# memory for no real benefit.
#
# If you aren't sure what it should be set to, it's better to set it
# too high than too low. Setting it to 1000 per client is probably
# the highest it should be.
#
# Useful range of values: 256 to infinity
#
max_requests = 1024
# bind_address: Make the server listen on a particular IP address, and
# send replies out from that address. This directive is most useful
# for machines with multiple IP addresses on one interface.

#
# It can either contain "*", or an IP address, or a fully qualified
# Internet domain name. The default is "*"
#
bind_address = *
# port: Allows you to bind FreeRADIUS to a specific port.
#
# The default port that most NAS boxes use is 1645, which is historical.
# RFC 2138 defines 1812 to be the new port. Many new servers and
# NAS boxes use 1812, which can create interoperability problems.
#
# The port is defined here to be 0 so that the server will pick up
# the machine's local configuration for the radius port, as defined
# in /etc/services.
#
# If you want to use the default RADIUS port as defined on your server,
# (usually through 'grep radius /etc/services') set this to 0 (zero).
#
# A port given on the command-line via '-p' over-rides this one.
#
port = 0
# hostname_lookups: Log the names of clients or just their IP addresses
# e.g., www.freeradius.org (on) or 206.47.27.232 (off).
#
# The default is 'off' because it would be overall better for the net
# if people had to knowingly turn this feature on, since enabling it
# means that each client request will result in AT LEAST one lookup
# request to the nameserver. Enabling hostname_lookups will also
# mean that your server may stop randomly for 30 seconds from time
# to time, if the DNS requests take too long.
#
# Turning hostname lookups off also means that the server won't block
# for 30 seconds, if it sees an IP address which has no name associated
# with it.
#
# allowed values: {no, yes}
#
hostname_lookups = no
```

```
# Core dumps are a bad thing. This should only be set to 'yes'
# if you're debugging a problem with the server.
#
# allowed values: {no, yes}
#
allow_core_dumps = no
# Regular expressions
#
# These items are set at configure time. If they're set to "yes",
# then setting them to "no" turns off regular expression support.
#
# If they're set to "no" at configure time, then setting them to "yes"
# WILL NOT WORK. It will give you an error.
#
regular_expressions = yes
extended_expressions = yes
# Log the full User-Name attribute, as it was found in the request.
#

# allowed values: {no, yes}
#
log_stripped_names = no
# Log authentication requests to the log file.
#
# allowed values: {no, yes}
#
log_auth = yes
# Log passwords with the authentication requests.
# log_auth_badpass - logs password if it's rejected
# log_auth_goodpass - logs password if it's correct
#
# allowed values: {no, yes}
#
log_auth_badpass = yes
log_auth_goodpass = yes
# usercollide: Turn "username collision" code on and off. See the
# "doc/duplicate-users" file
#
usercollide = no
# lower_user / lower_pass:
# Lower case the username/password "before" or "after"
# attempting to authenticate.
#
# If "before", the server will first modify the request and then try
# to auth the user. If "after", the server will first auth using the
# values provided by the user. If that fails it will reprocess the
# request after modifying it as you specify below.
#
# This is as close as we can get to case insensitivity. It is the
# admin's job to ensure that the username on the auth db side is
# *also* lowercase to make this work
#
# Default is 'no' (don't lowercase values)
# Valid values = "before" / "after" / "no"
#
lower_user = no
lower_pass = no
# nospace_user / nospace_pass:
#
# Some users like to enter spaces in their username or password
# incorrectly. To save yourself the tech support call, you can
```

```
# eliminate those spaces here:
#
# Default is 'no' (don't remove spaces)
# Valid values = "before" / "after" / "no" (explanation above)
#
nospace_user = no
nospace_pass = no
# The program to execute to do concurrency checks.
checkrad = ${sbindir}/checkrad
# SECURITY CONFIGURATION
#
# There may be multiple methods of attacking on the server. This

# section holds the configuration items which minimize the impact
# of those attacks
#
security {
#
# max_attributes: The maximum number of attributes
# permitted in a RADIUS packet. Packets which have MORE
# than this number of attributes in them will be dropped.
#
# If this number is set too low, then no RADIUS packets
# will be accepted.
#
# If this number is set too high, then an attacker may be
# able to send a small number of packets which will cause
# the server to use all available memory on the machine.
#
# Setting this number to 0 means "allow any number of attributes"
max_attributes = 200
#
# delayed_reject: When sending an Access-Reject, it can be
# delayed for a few seconds. This may help slow down a DoS
# attack. It also helps to slow down people trying to brute-force
# crack a users password.
#
# Setting this number to 0 means "send rejects immediately"
#
# If this number is set higher than 'cleanup_delay', then the
# rejects will be sent at 'cleanup_delay' time, when the request
# is deleted from the internal cache of requests.
#
# Useful ranges: 1 to 5
reject_delay = 1
#
# status_server: Whether or not the server will respond
# to Status-Server requests.
#
# Normally this should be set to "no", because they're useless.
# See: http://www.freeradius.org/rfc/rfc2865.html#Keep-Alives
#
# However, certain NAS boxes may require them.
#
# When sent a Status-Server message, the server responds with
# and Access-Accept packet, containing a Reply-Message attribute,
# which is a string describing how long the server has been
# running.
#
status_server = no
}
```

```
# PROXY CONFIGURATION
#
# proxy_requests: Turns proxying of RADIUS requests on or off.
#
# The server has proxying turned on by default. If your system is NOT
# set up to proxy requests to another server, then you can turn proxying
# off here. This will save a small amount of resources on the server.
#
# If you have proxying turned off, and your configuration files say
# to proxy a request, then an error message will be logged.

#
# To disable proxying, change the "yes" to "no", and comment the
# $INCLUDE line.
#
# allowed values: {no, yes}
#
proxy_requests = no
$INCLUDE ${confdir}/proxy.conf
# CLIENTS CONFIGURATION
#
# Client configuration is defined in "clients.conf".
#
# The 'clients.conf' file contains all of the information from the old
# 'clients' and 'naslist' configuration files. We recommend that you
# do NOT use 'client's or 'naslist', although they are still
# supported.
#
# Anything listed in 'clients.conf' will take precedence over the
# information from the old-style configuration files.
#
$INCLUDE ${confdir}/clients.conf
# SNMP CONFIGURATION
#
# Snmp configuration is only valid if you enabled SNMP support when
# you compiled radiusd.
#
$INCLUDE ${confdir}/snmp.conf
# THREAD POOL CONFIGURATION
#
# The thread pool is a long-lived group of threads which
# take turns (round-robin) handling any incoming requests.
#
# You probably want to have a few spare threads around,
# so that high-load situations can be handled immediately. If you
# don't have any spare threads, then the request handling will
# be delayed while a new thread is created, and added to the pool.
#
# You probably don't want too many spare threads around,
# otherwise they'll be sitting there taking up resources, and
# not doing anything productive.
#
# The numbers given below should be adequate for most situations.
#
thread pool {
# Number of servers to start initially --- should be a reasonable
# ballpark figure.
start_servers = 5
# Limit on the total number of servers running.
#
# If this limit is ever reached, clients will be LOCKED OUT, so it
```

```
# should NOT BE SET TOO LOW. It is intended mainly as a brake to
# keep a runaway server from taking the system with it as it spirals
# down...

#
# You may find that the server is regularly reaching the
# 'max_servers' number of threads, and that increasing
# 'max_servers' doesn't seem to make much difference.
#
# If this is the case, then the problem is MOST LIKELY that
# your back-end databases are taking too long to respond, and
# are preventing the server from responding in a timely manner.
#
# The solution is NOT do keep increasing the 'max_servers'
# value, but instead to fix the underlying cause of the
# problem: slow database, or 'hostname_lookups=yes'.
#
# For more information, see 'max_request_time', above.
#
max_servers = 32
# Server-pool size regulation. Rather than making you guess
# how many servers you need, FreeRADIUS dynamically adapts to
# the load it sees, that is, it tries to maintain enough
# servers to handle the current load, plus a few spare
# servers to handle transient load spikes.
#
# It does this by periodically checking how many servers are
# waiting for a request. If there are fewer than
# min_spare_servers, it creates a new spare. If there are
# more than max_spare_servers, some of the spares die off.
# The default values are probably OK for most sites.
#
min_spare_servers = 3
max_spare_servers = 10
# There may be memory leaks or resource allocation problems with
# the server. If so, set this value to 300 or so, so that the
# resources will be cleaned up periodically.
#
# This should only be necessary if there are serious bugs in the
# server which have not yet been fixed.
#
# '0' is a special value meaning 'infinity', or 'the servers never
# exit'
max_requests_per_server = 0
}
# MODULE CONFIGURATION
#
# The names and configuration of each module is located in this section.
#
# After the modules are defined here, they may be referred to by name,
# in other sections of this configuration file.
#
modules {
# PAP module to authenticate users based on their stored password
#
# Supports multiple encryption schemes
# clear: Clear text
# crypt: Unix crypt
# md5: MD5 ecnryption
# sha1: SHA1 encryption.
# DEFAULT: crypt
```

```
pap {
encryption_scheme = crypt
}
# CHAP module
#
# To authenticate requests containing a CHAP-Password attribute.
#
chap {
authtype = CHAP
}
# Pluggable Authentication Modules
#
# For Linux, see:
# http://www.kernel.org/pub/linux/libs/pam/index.html
#
pam {
#
# The name to use for PAM authentication.
# PAM looks in /etc/pam.d/${pam_auth_name}
# for it's configuration. See 'redhat/radiusd-pam'
# for a sample PAM configuration file.
#
# Note that any Pam-Auth attribute set in the 'authorize'
# section will over-ride this one.
#
pam_auth = radiusd
}
# Unix /etc/passwd style authentication
#
unix {
#
# Cache /etc/passwd, /etc/shadow, and /etc/group
#
# The default is to NOT cache them.
#
# For FreeBSD, you do NOT want to enable the cache,
# as it's password lookups are done via a database, so
# set this value to 'no'.
#
# Some systems (e.g. RedHat Linux with pam_pwbd) can
# take *seconds* to check a password, from a passwd
# file containing 1000's of entries. For those systems,
# you should set the cache value to 'yes', and set
# the locations of the 'passwd', 'shadow', and 'group'
# files, below.
#
# allowed values: {no, yes}
cache = no
# Reload the cache every 600 seconds (10mins). 0 to disable.
cache_reload = 600
#
# Define the locations of the normal passwd, shadow, and
# group files.
#
# 'shadow' is commented out by default, because not all
# systems have shadow passwords.

#
# To force the module to use the system password functions,
# instead of reading the files, leave the following entries
```

```
# commented out.
#
# This is required for some systems, like FreeBSD,
# and Mac OSX.
#
# passwd = /etc/passwd
# shadow = /etc/shadow
# group = /etc/group
#
# Where the 'wtmp' file is located.
# This should be moved to it's own module soon.
#
# The only use for 'radlast'. If you don't use
# 'radlast', then you can comment out this item.
#
radwtmp = ${logdir}/radwtmp
}
# Extensible Authentication Protocol
#
# For all EAP related authentications
eap {
# Invoke the default supported EAP type when
# EAP-Identity response is received
# default_eap_type = md5
# Default expiry time to clean the EAP list,
# It is maintained to co-relate the
# EAP-response for each EAP-request sent.
# timer_expire = 60
# Supported EAP-types
md5 {
}
## EAP-TLS is highly experimental EAP-Type at the moment.
# Please give feedback on the mailing list.
#tls {
# private_key_password = password
# private_key_file = /path/filename
# If Private key & Certificate are located in the
# same file, then private_key_file & certificate_file
# must contain the same file name.
# certificate_file = /path/filename
# Trusted Root CA list
#CA_file = /path/filename
# dh_file = /path/filename
#random_file = /path/filename
#
# This can never exceed MAX_RADIUS_LEN (4096)
# preferably half the MAX_RADIUS_LEN, to
# accomodate other attributes in RADIUS packet.
# On most APs the MAX packet length is configured

# between 1500 - 1600. In these cases, fragment
# size should be <= 1024.
#
# fragment_size = 1024
# include_length is a flag which is by default set to yes
# If set to yes, Total Length of the message is included
# in EVERY packet we send.
# If set to no, Total Length of the message is included
# ONLY in the First packet of a fragment series.
#
# include_length = yes
```

```
#}
}
# Microsoft CHAP authentication
#
# This module supports SAMBA passwd file authorization
# and MS-CHAP, MS-CHAPv2 authentication. However, we recommend
# using the 'passwd' module, below, as it's more general.
#
mschap {
# Location of the SAMBA passwd file
# passwd = /etc/smbpasswd
# authtype value, if present, will be used
# to overwrite (or add) Auth-Type during
# authorization. Normally should be MS-CHAP
authtype = MS-CHAP
# If ignore_password is set to yes mschap will
# ignore the password set by any other module during
# authorization and will always use the SAMBA password file
# ignore_password = yes
# if use_mppe is not set to no mschap will
# add MS-CHAP-MPPE-Keys for MS-CHAPv1 and
# MS-MPPE-Recv-Key/MS-MPPE-Send-Key for MS-CHAPv2
# use_mppe = no
# if mppe is enabled require_encryption makes
# encryption moderate
# require_encryption = yes
# require_strong always requires 128 bit key
# encryption
# require_strong = yes
}
# Lightweight Directory Access Protocol (LDAP)
#
# This module definition allows you to use LDAP for
# authorization and authentication (Auth-Type := LDAP)
#
# See doc/rlm_ldap for description of configuration options
# and sample authorize{} and authenticate{} blocks
ldap {
server = "ldap.your.domain"
# identity = "cn=admin,o=My Org,c=UA"
# password = mypass
basedn = "o=My Org,c=UA"

filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
# set this to 'yes' to use TLS encrypted connections
# to the LDAP database by using the StartTLS extended
# operation.
start_tls = no
# set this to 'yes' to use TLS encrypted connections to the
# LDAP database by passing the LDAP_OPT_X_TLS_TRY option to
# the ldap library.
tls_mode = no
# default_profile = "cn=radprofile,ou=dialup,o=My Org,c=UA"
# profile_attribute = "radiusProfileDn"
access_attr = "dialupAccess"
# Mapping of RADIUS dictionary attributes to LDAP
# directory attributes.
dictionary_mapping = ${raddbdir}/ldap.attrmap
# ldap_cache_timeout = 120
# ldap_cache_size = 0
ldap_connections_number = 5
```

```
# password_header = "{clear}"
# password_attribute = userPassword
# groupname_attribute = cn
# groupmembership_filter =
"(|(&(objectClass=GroupOfNames)(member=%{Ldap-
UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-UserDn})))"
# groupmembership_attribute = radiusGroupName
timeout = 4
timelimit = 3
net_timeout = 1
# compare_check_items = yes
# access_attr_used_for_allow = yes
}
# passwd module allows to do authorization via any passwd-like
# file and to extract any attributes from these modules
#
# parameters are:
# filename - path to filename
# format - format for filename record. This parameters
# correlates record in the passwd file and RADIUS
# attributes.
#
# Field marked as '*' is key field. That is, the parameter
# with this name from the request is used to search for
# the record from passwd file
#
# Field marked as ',' may contain a comma separated list
# of attributes.
# authtype - if record found this Auth-Type is used to authenticate
# user
# hashsize - hashtable size. If 0 or not specified records are not
# stored in memory and file is red on every request.
# allowmultiplekeys - if few records for every key are allowed
# ignorenislike - ignore NIS-related records
# delimiter - symbol to use as a field separator in passwd file,
# for format ':' symbol is always used. '\0', '\n' are
# not allowed
#

#passwd etc_smbpasswd {
# filename = /etc/smbpasswd
# format = "*User-Name::LM-Password:NT-Password:SMB-Account-CTRLTEXT::"
# authtype = MS-CHAP
# hashsize = 100
# ignorenislike = no
# allowmultiplekeys = no
#}
# Similar configuration, for the /etc/group file. Adds a Group-Name
# attribute for every group that the user is member of.
#
#passwd etc_group {
# filename = /etc/group
# format = "Group-Name:::*,User-Name"
# hashsize = 50
# ignorenislike = yes
# allowmultiplekeys = yes
# delimiter = ":"
#}
# Realm module, for proxying.
#
# You can have multiple instances of the realm module to
```

```
# support multiple realm syntaxs at the same time. The
# search order is defined the order in the authorize and
# preacct blocks after the module config block.
#
# Two config options:
# format - must be 'prefix' or 'suffix'
# delimiter - must be a single character
# 'username@realm'
#
realm suffix {
format = suffix
delimiter = "@"
}
# 'realm/username'
#
# Using this entry, IPASS users have their realm set to "IPASS".
realm realmslash {
format = prefix
delimiter = "/"
}
# 'username%realm'
#
realm realmpercent {
format = suffix
delimiter = "%"
}
# rewrite arbitrary packets. Useful in accounting and
authorization.
#
## This module is highly experimental at the moment. Please give
## feedback to the mailing list.
#

# The module can also use the Rewrite-Rule attribute. If it
# is set and matches the name of the module instance, then
# that module instance will be the only one which runs.
#
# Also if new_attribute is set to yes then a new attribute
# will be created containing the value replacewith and it
# will be added to searchin (packet, reply or config).
# searchfor,ignore_case and max_matches will be ignored in that case.
#
#attr_rewrite sanecallerid {
# attribute = Called-Station-Id
# may be "packet", "reply", or "config"
# searchin = packet
# searchfor = "[+ ]"
# replacewith = ""
# ignore_case = no
# new_attribute = no
# max_matches = 10
# ## If set to yes then the replace string will be appended to
the original string
# append = no
#}
# Preprocess the incoming RADIUS request, before handing it off
# to other modules.
#
# This module processes the 'huntgroups' and 'hints' files.
# In addition, it re-writes some weird attributes created
# by some NASes, and converts the attributes into a form which
```

```
# is a little more standard.
#
preprocess {
huntgroups = ${confdir}/huntgroups
hints = ${confdir}/hints
# This hack changes Ascend's wierd port numberings
# to standard 0-??? port numbers so that the "+" works
# for IP address assignments.
with_ascend_hack = no
ascend_channels_per_line = 23
# Windows NT machines often authenticate themselves as
# NT_DOMAIN\username
#
# If this is set to 'yes', then the NT_DOMAIN portion
# of the user-name is silently discarded.
with_ntdomain_hack = no
# Specialix Jetstream 8500 24 port access server.
#
# If the user name is 10 characters or longer, a "/"
# and the excess characters after the 10th are
# appended to the user name.
#
# If you're not running that NAS, you don't need
# this hack.
with_specialix_jetstream_hack = no
# Cisco sends it's VSA attributes with the attribute
# name *again* in the string, like:

#
# H323-Attribute = "h323-attribute=value".
#
# If this configuration item is set to 'yes', then
# the redundant data in the the attribute text is stripped
# out. The result is:
#
# H323-Attribute = "value"
#
# If you're not running a Cisco NAS, you don't need
# this hack.
with_cisco_vsa_hack = no
}
# Livingston-style 'users' file
#
files {
usersfile = ${confdir}/users
acctusersfile = ${confdir}/acct_users
# If you want to use the old Cistron 'users' file
# with FreeRADIUS, you should change the next line
# to 'compat = cistron'. You can the copy your 'users'
# file from Cistron.
compat = no
}
# Write a detailed log of all accounting records received.
#
detail {
# Note that we do NOT use NAS-IP-Address here, as
# that attribute MAY BE from the originating NAS, and
# NOT from the proxy which actually sent us the
# request. The Client-IP-Address attribute is ALWAYS
# the address of the client which sent us the
# request.
```

```
#
# The following line creates a new detail file for
# every radius client (by IP address or hostname).
# In addition, a new detail file is created every
# day, so that the detail file doesn't have to go
# through a 'log rotation'
#
# If your detail files are large, you may also want
# to add a ':%H' (see doc/variables.txt) to the end
# of it, to create a new detail file every hour, e.g.:
#
# ..../detail-%Y%m%d:%H
#
# This will create a new detail file for every hour.
#
detailfile = ${radacctdir}/%{Client-IP-Address}/detail-%Y%m%d
#
# The Unix-style permissions on the 'detail' file.
#
# The detail file often contains secret or private
# information about users. So by keeping the file
# permissions restrictive, we can prevent unwanted
# people from seeing that information.
detailperm = 0600

}
# Create a unique accounting session Id. Many NASes re-use or
# repeat values for Acct-Session-Id, causing no end of
# confusion.
#
# This module will add a (probably) unique session id
# to an accounting packet based on the attributes listed
# below found in the packet. See doc/rlm_acct_unique for
# more information.
#
acct_unique {
key = "User-Name, Acct-Session-Id, NAS-IP-Address, Client-IPAddress,
NAS-Port-Id"
}
# Include another file that has the SQL-related configuration.
# This is another file solely because it tends to be big.
#
# The following configuration file is for use with MySQL.
#
# For Postgresql, use: ${confdir}/postgresql.conf
# For MS-SQL, use: ${confdir}/mssql.conf
#
$INCLUDE ${confdir}/sql.conf
# Write a 'utmp' style log file, of which users are currently
# logged in, and where they've logged in from.
#
radutmp {
filename = ${logdir}/radutmp
# Set the file permissions, as the contents of this file
# are usually private.
perm = 0600
callerid = "yes"
}
# "Safe" radutmp - does not contain caller ID, so it can be
# world-readable, and radwho can work for normal users, without
# exposing any information that isn't already exposed by who(1).
```

```
#
# This is another instance of the radutmp module, but it is given
# then name "sradutmp" to identify it later in the "accounting"
# section.
radutmp sradutmp {
filename = ${logdir}/sradutmp
perm = 0644
callerid = "no"
}
# attr_filter - filters the attributes received in replies from
# proxied servers, to make sure we send back to our RADIUS client
# only allowed attributes.
attr_filter {
attrsfile = ${confdir}/attrs
}
# This module takes an attribute (count-attribute).

# It also takes a key, and creates a counter for each unique
# key. The count is incremented when accounting packets are
# received by the server. The value of the increment depends
# on the attribute type.
# If the attribute is Acct-Session-Time or an integer we add the
# value of the attribute. If it is anything else we increase the
# counter by one.
#
# The 'reset' parameter defines when the counters are all reset to
# zero. It can be hourly, daily, weekly, monthly or never.
# It can also be user defined. It should be of the form:
# num[hdwm] where:
# h: hours, d: days, w: weeks, m: months
# If the letter is ommited days will be assumed. In example:
# reset = 10h (reset every 10 hours)
# reset = 12 (reset every 12 days)
#
#
# The check-name attribute defines an attribute which will be
# registered by the counter module and can be used to set the
# maximum allowed value for the counter after which the user
# is rejected.
# Something like:
#
# DEFAULT Max-Daily-Session := 36000
# Fall-Through = 1
#
# You should add the counter module in the instantiate
# section so that it registers check-name before the files
# module reads the users file.
#
# If check-name is set and the user is to be rejected then we
# send back a Reply-Message and we log a Failure-Message in
# the radius.log
#
# The counter-name can also be used like below:
#
# DEFAULT Daily-Session-Time > 3600, Auth-Type = Reject
# Reply-Message = "You've used up more than one hour today"
#
# The allowed-servicetype attribute can be used to only take
# into account specific sessions. For example if a user first
# logs in through a login menu and then selects ppp there will
# be two sessions. One for Login-User and one for Framed-User
```

```
# service type. We only need to take into account the second one.
#
# The module should be added in the instantiate, authorize and
# accounting sections. Make sure that in the authorize
# section it comes after any module which sets the
# 'check-name' attribute.
#
counter {
filename = ${raddbdir}/db.counter
key = User-Name
count-attribute = Acct-Session-Time
reset = daily
counter-name = Daily-Session-Time
check-name = Max-Daily-Session
allowed-servicetype = Framed-User
cache-size = 5000
}

# The "always" module is here for debugging purposes. Each
# instance simply returns the same result, always, without
# doing anything.
always fail {
rcode = fail
}
always reject {
rcode = reject
}
always ok {
rcode = ok
simulcount = 0
mpp = no
}
#
# The 'expression' module current has no configuration.
expr {
}
# ANSI X9.9 token support. Not included by default.
# $INCLUDE ${confdir}/x99.conf
}
# Instantiation
#
# This section orders the loading of the modules. Modules
# listed here will get loaded BEFORE the later sections like
# authorize, authenticate, etc. get examined.
#
# This section is not strictly needed. When a section like
# authorize refers to a module, it's automatically loaded and
# initialized. However, some modules may not be listed in any
# of the following sections, so they can be listed here.
#
# Also, listing modules here ensures that you have control over
# the order in which they are initalized. If one module needs
# something defined by another module, you can list them in order
# here, and ensure that the configuration will be OK.
#
instantiate {
#
# The expression module doesn't do authorization,
# authentication, or accounting. It only does dynamic
# translation, of the form:
#
```

```
# Session-Timeout = `%{expr:2 + 3}`
#
# So the module needs to be instantiated, but CANNOT be
# listed in any other section. See 'doc/rlm_expr' for
# more information.
#
expr
}
# Authorization. First preprocess (hints and huntgroups files),
# then realms, and finally look in the "users" file.
#
# The order of the realm modules will determine the order that

# we try to find a matching realm.
#
# Make *sure* that 'preprocess' comes before any realm if you
# need to setup hints for the remote radius server
authorize {
#
# The preprocess module takes care of sanitizing some bizarre
# attributes in the request, and turning them into attributes
# which are more standard.
#
# It takes care of processing the 'raddb/hints' and the
# 'raddb/huntgroups' files.
#
# It also adds a Client-IP-Address attribute to the request.
preprocess
#
# The chap module will set 'Auth-Type := CHAP' if we are
# handling a CHAP request and Auth-Type has not already been set
chap
#
# If the users are logging in with an MS-CHAP-Challenge
# attribute for authentication, the mschap module will find
# the MS-CHAP-Challenge attribute, and add 'Auth-Type := MS-CHAP'
# to the request, which will cause the server to then use
# the mschap module for authentication.
mschap
# counter
# attr_filter
# eap
suffix
sql
# files
# etc_smbpasswd
# The ldap module will set Auth-Type to LDAP if it has not already been set
# ldap
}
# Authentication.
#
# This section lists which modules are available for authentication.
# Note that it does NOT mean 'try each module in order'. It means
# that you have to have a module from the 'authorize' section add
# a configuration attribute 'Auth-Type := FOO'. That authentication type
# is then used to pick the apropriate module from the list below.
#
# The default Auth-Type is Local. That is, whatever is not included
inside
# an authtype section will be called only if Auth-Type is set to Local.
#
```

```
# So you should do the following:
# - Set Auth-Type to an appropriate value in the authorize modules above.
# For example, the chap module will set Auth-Type to CHAP, ldap to LDAP,
etc.
# - After that create corresponding authtype sections in the
# authenticate section below and call the appropriate modules.

authenticate {
#
# PAP authentication, when a back-end database listed
# in the 'authorize' section supplies a password. The
# password can be clear-text, or encrypted.
authtype PAP {
pap
}
#
# Most people want CHAP authentication
# A back-end database listed in the 'authorize' section
# MUST supply a CLEAR TEXT password. Encrypted passwords
# won't work.
authtype CHAP {
chap
}
#
# MSCHAP authentication.
authtype MS-CHAP {
mschap
}
# pam
#
# See 'man getpwent' for information on how the 'unix'
# module checks the users password. Note that packets
# containing CHAP-Password attributes CANNOT be authenticated
# against /etc/passwd! See the FAQ for details.
#
unix
# Uncomment it if you want to use ldap for authentication
# authtype LDAP {
# ldap
# }
# eap
}
# Pre-accounting. Look for proxy realm in order of realms, then
# acct_users file, then preprocess (hints file).
preacct {
preprocess
suffix
files
}
# Accounting. Log to detail file, and to the radwtmp file, and maintain
# radutmp.
accounting {
acct_unique
detail
# counter
unix # wtmp file
sql

radutmp
# sradutmp
}
```

```
# Session database, used for checking Simultaneous-Use. Either the radutmp
# or rlm_sql module can handle this.
# The rlm_sql module is *much* faster
session {
radutmp
# sql
}
# Post-Authentication
# Once we KNOW that the user has been authenticated, there are
# additional steps we can take.
post-auth {
# Get an address from the IP Pool.
#main_pool
}
```

17.2.1.4. Test de fonctionnement :

Une fois ces fichiers configurés nous pouvons lancer le démon radius avec :
`/usr/local/sbin/radiusd -X`
le –X permet de voir ce que le démon traite (mode de debuggage en quelque sorte).
Pour tester la validité de notre configuration il existe 2 programmes :
Radtest : fourni avec freeradius et fonctionnant exclusivement sous Linux
NTRadPing : fonctionnant sous Windows et téléchargeable sur MasterSoft.com

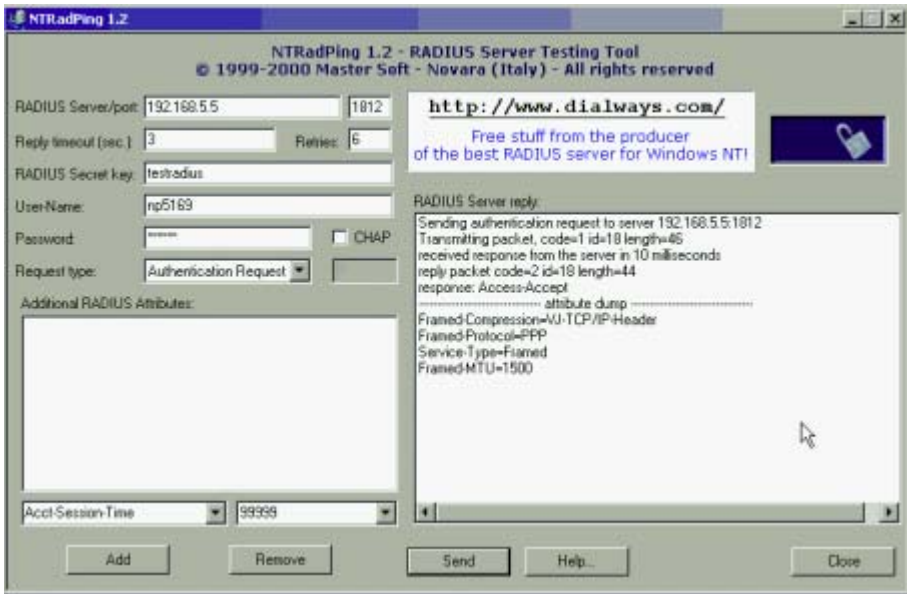
17.2.1.5. Sous radtest :

La syntaxe est la suivante :
`radtest username password servername port secret`
username : nom de l'utilisateur autorisé a se connecté (différents des users du système)
password : password assigné à l'utilisateur
servername : nom du server radius
port : port de connexion, anciennement 1645 et actuellement 1812 (UDP)
secret : clef de secret partagé défini dans les fichiers de configuration.
ce qui donne pour notre exemple :
`radtest steve testing 127.0.0.1 1812 testradius`

```
[root@BRUTUS root]# radtest np5169     127.0.0.1 1812 testradius
Sending Access-Request of id 252 to 127.0.0.1:1812
        User-Name = "np5169"
        User-Password = "h\035ad\035\313}k\r\334\266,\305\223\002\213"
        NAS-IP-Address = BRUTUS
        NAS-Port = 1812
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=252, length=44
        Framed-Compression = Van-Jacobson-TCP-IP
        Framed-Protocol = PPP
        Service-Type = Framed-User
        Framed-MTU = 1500
```

17.2.1.6. Sous NTRadPing :

Le résultat quelque soit la méthode utilisée est le retour d'un message :
Rad_recv : Access-Accept …..
A partir de la, cela veut dire que votre serveur radius fonctionne correctement en authentification par fichier texte.



17.2.1.7. Migration vers une authentification MySQL :

Nous allons mettre tous les user/pass et les methodes de connection dans une base de données qui nous permettra de simplifier l'administration des users.

Outils :

Pour ma part j'utilise MySQLcc sous Windows pour me connecter à la base Mysql.
Je ne ferais pas ici de laïus sur comment installer et configurer une bdd.
Il faut donc créer une base répondant au doux nom de « radius ».
Ensuite il faut remplir cette base nouvellement créée avec des tables. Freeradius est livré avec un script de création fort pratique (db_mysql_sql) :

```
mysql -u root radius <
/rep…decomp…freeradius/src/modules/rlm_sql_mysql/db_mysql.sql
```

17.2.1.8. Configuration liaison Freeradius--MySQL :

A ce stade les tables sont créées dans la base.
Il faut maintenant lier freeradius à cette base de données grâce a un changement dans un fichier de configuration :

```
vi /usr/local/etc/raddb/sql.conf
```

Voici le fichier avec les modifications apportées en gras :

```
#
# Configuration for the SQL module, when using MySQL.
#
# The database schema is available at:
#
# src/radiusd/src/modules/rlm_sql/drivers/rlm_sql_mysql/db_mysql.sql
#
# If you are using PostgreSQL, please use 'postgresql.conf', instead.
# If you are using Oracle, please use 'oracle.conf', instead.
# If you are using MS-SQL, please use 'mssql.conf', instead.
#
# $Id: sql.conf,v 1.26 2002/11/18 15:32:03 aland Exp $
```

```
#
sql {
# Database type
# Current supported are: rlm_sql_mysql, rlm_sql_postgresql,
# rlm_sql_iodbc, rlm_sql_oracle, rlm_sql_unixodbc, rlm_sql_freetds
driver = "rlm_sql_mysql"
# Connect info
server = localhost # l'adresse ou le nom de votre serveur
login = ++++++++ # votre login de connexion a la base
password = XXXXXXXXX #votre mot de passe de connexion a la base
# Database table configuration
radius_db = "radius" # nom de la base ou le radius doit aller
```

Le reste du fichier est à laisser tel quel.
Une fois cela fait, nous devons remplir la bdd avec les données des users.
Il ne reste plus qu'à recopier ce qui suit dans vos tables ou alors de faire un script ou une page en php pour le faire.

```
mysql> select * from radius.usergroup
    -> ;
+----+----------+-----------+
| id | UserName | GroupName |
+----+----------+-----------+
|  1 | np5169   | dynamic   |
+----+----------+-----------+
```

```
mysql> select * from radius.radcheck;
+----+----------+-----------+----+--------+
| id | UserName | Attribute | op | Value  |
+----+----------+-----------+----+--------+
|  1 | np5169   | Password  | == | np5169 |
+----+----------+-----------+----+--------+
```

```
mysql> select * from radius.radgroupcheck;
+----+-----------+-----------+----+-------+
| id | GroupName | Attribute | op | Value |
+----+-----------+-----------+----+-------+
|  1 | dynamic   | Auth-Type | := | Local |
+----+-----------+-----------+----+-------+
```

```
mysql> select * from radius.radgroupreply;
+----+-----------+--------------------+----+---------------------+------+
| id | GroupName | Attribute          | op | Value               | prio |
+----+-----------+--------------------+----+---------------------+------+
|  1 | dynamic   | Framed-Compression | := | Van-Jacobsen-TCP-IP |    0 |
|  2 | dynamic   | Framed-Protocol    | := | PPP                 |    0 |
|  3 | dynamic   | Service-Type       | := | Framed-User         |    0 |
|  4 | dynamic   | Framed-MTU         | := | 1500                |    0 |
+----+-----------+--------------------+----+---------------------+------+
```

17.2.1.9. Test de fonctionnement :

Refaite un test avec NTRadPing ou radtest. Cela doit vous retourner le même message que lors du premier test.
Si cela n'est pas le cas reprendre l'install.
Si c'est le cas il ne nous reste plus qu'a lier pppoe-server a du radius, mais la je n'ai pas encore réussi donc à votre bon coeur.

17.2.1.10. Liens utiles :

http://www.frontios.com/freeradius.html
http://www.wireless-fr.org
http://www.freeradius.org
http://www.mysql.com
http://www.roaringpenguin.com (Rp-pppoe)
http://www.mastersoft-group.com/download (NTRadPing)
http://www.redhat.com

Test d'Accounting :
Sous NT RadPing :

Par rapport à la methode normal de test, changez juste le port de 1812 en 1813.
Il faut aussi rajouter un argument supplementaire qui est :
`Acct-Session-Time 99999`
Choisissez aussi en type de requete :
`Accounting-Stop`
Lancez ensuite le test et regardez dans votre base la table radacct qui a du enregistré votre accounting de test.

17.2.2. Sur Debian

17.2.2.1. Installation de Freeradius

```
# apt-get install freeradius
# apt-get install freeradius-dialupadmin
# apt-get install freeradius-mysql
```

17.2.2.2. Installation de MySQL

```
# apt-get install mysql-server
# apt-get install mysql-client
```

17.2.2.3. Configuration de MySQL

```
# echo "create database radius;" | mysql -u root -p
# echo "grant all on radius.* to radius@'%' identified by 'motdepasse_sql';
flush privileges;" | mysql -u root -p
# zcat /usr/share/doc/freeradius/examples/db_mysql.sql.tgz | mysql -u root
-p radius
```

17.2.2.4. Créer un nouvel utilisateur

```
# echo "INSERT INTO radcheck(UserName,Attribute,op,Value) VALUES
('wifiseb2','User-Password',':=','motdepasse');" | mysql -u root -p radius
```

Configuration de Freeradius

17.2.2.5. Modifier le fichier /etc/freeradius/sql.conf

```
sql {
        driver = "rlm_sql_mysql"
        server = "localhost"
        login = "radius"
        password = "motdepasse_sql"
        radius_db = "radius"
        [...]
}
```

17.2.2.6. Modifier le fichier */etc/freeradius/radiusd.conf*

```
        $INCLUDE ${confdir}/sql.conf
authorize {
        [...]
        sql
        [...]
}
accounting {
        [...]
        sql
        [...]
}
```

17.2.2.7. Installation de Freeradius DialupAdmin

... en attendant la documentation, voici quelques screenshots de l'utilisation de Freeradius+MySQL et ChilliSpot

Statistics

Online Users

User Statistics