REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET D'INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

Du diplôme de MASTER en électronique

Option: Réseaux et Télécommunications

Thème :

Etude sur les mécanismes de sécurité d'un réseau Wi-Fi

Proposé et dirigé par :

- **Mme L.AKROUR**
- **Mr M.LAHDIR**

Présenté par :

- **Mr AMINI Hocine**
- **Melle GUERMAH Nabila**

Promotion 2012-2013

Remerciements

Dieu merci de nous avoir donner la santé et les moyens qui nous ont permis d'aller au bout du tavail qui nous a été confié.

Nous adressons nos remerciements les plus vifs aux membres du jury d'avoir accepté de juger notre travail.

Nous remercions vivement l'enssemble des enseignants du département d'électronique pour leur encadrement tout le long de notre formation.

Nous tenons à exprimer notre vive reconnaissance et nos sincères remerciements à Monsieur LAHDIR Mourad et Madame AKROUR Leila, d'avoir accepté de nous proposer ce thème de projet de fin d'étude, et de nous avoir accorder leurs confiance tout au long de ce travail.

Dédicaces

Je dédie ce mémoire à :

- *Mes chers parents.*
- *Mes sœurs et mon frère Yanis.*
- *Mon neveu Nael.*
- *Toute la famille GUERMAH.*
- *Tous mes amis.*

Et à tous ceux qui font partie de ma vie.

M^{elle} GUERMAH NABILA

Dédicaces

Je dédie ce modeste travail :

- *A ma source d'amour et d'affection, à ma mère et ma tante qui ont toujours veillé à ce que je sois heureux, jamais je pourrai les remercier autant.*
- *A mes grands-parents.*
- *A mon oncle AMINI Ali*
- *A mon frère: Mohammed.*
- *A toute ma famille et mes amis (es) et en particulier :Nacer-eddine, Achour, Farida, et à mon binôme Nabila.*

M^{r} AMINI Hocine

Sommaire

Introduction Générale

Chapitre I :Technologies des réseaux Wi-Fi

1.Introduction……1

2.Architecture Wi-Fi……1

2.1 Les topologies de la normes802.11……1

2.1.1 Le mode infrastructure ……2

2.1.2 Le mode ad-hoc……2

2.2 Les couches de l'IEEE 802.11……3

2.2.1 La couche physique……3

2.2.2 La couche de liaison de données……3

2.3 Les technique d'accès au support radio……4

2.3.1 Le protocole CSMA/CA……4

2.3.2 Mécanisme de réservation du support RTS/CTS……7

3. Normes associées à l'IEEE 802.11……7

3.1 Les normes physiques……7

3.1.1 La 802.11b……7

3.1.2 La 802.11a……8

3.1.3 La 802.11g……8

3.2 Les normes d'amelioration……8

3.2.1 L'IEEE 802.11e :la qualité de service……8

3.2.2 L'IEEE 802.11f :les handovers……8

3.2.3 L'IEEE 802.11n :le haut débit……9

3.2.4 L'IEEE 802.11i :la sécurité……9

3.2.5 L'IEEE 802.11d……9

3.2.6 L'IEEE 802.11h……..10

4.Conclusion……..10

Chapitre II: Les mécanismes de sécurités des réseaux Wi-Fi

1.Introduction……..11

2.Généralités sur la sécurité……..11

2.1.Risques et attaques……..11

2.1.1. Les risques……..11

2.1.2. Les attaques……12

2.1.2.1. Les attaques passives……..12

2.1.2.2. Les Attaque actives……..12

2.1.2.3. Autre attaques……14

3. Service de sécurité……..15

3.1. Confidentialité……..15

3.1.1. Chiffrement……..15

3.1.1.1. Clé symétrique……..15

3.1.1.2. Clé asymétrique……16

3.1.1.3. Clé mixte……18

3.1.2. Certificats……18

3.2. Service d'authentification……20

3.3. L'intégrité des données……22

3.4 Non répudiation……22

3.5. Contrôle d'accès……22

4. Sécurisation du Wi-Fi……23

4.1.Sécurités des points d'accès……23

4.1.1. Eviter les valeurs par défaut……23

4.1.2. Filtrage par adresse MAC……23

4.2. Etude des protocoles de sécurité liés aux Wi-Fi……24

4.2.1. Le protocole WEP……24

4.2.1.1. Clé WEP……24

4.2.1.2. Principe du WEP……24

4.2.2. Le protocole WPA……25

4.2.2.1. Fonctionnement du WPA……25

4.2.2.2. TKIP……26

4.2.3. Le protocole WPA2/802.11i……26

4.2.3.1. Description techniqhes des clés utilisées par WPA/WPA2……27

4.2.3.2. Description technique du handShake WPA/WPA2……28

4.3. Les réseaux VPN……28

4.3.1. Concept VPN……28

4.3.2. Fonctionnement du VPN……29

4.3.3. Le certificat numérique……29

4.3.4. Les protocoles de tunnelisation……29

4.4. Le protocole 802.1X……30

4.4.1. Mécanisme générale……31

4.4.2. EAP……32

4.4.2.1. Composition du paquet EAP……32

4.4.2.2. Méthodes d'authentification associée à EAP……33

4.5. Le protocole RADIUS……35

4.5.1. Présentation……35

4.5.2. Principe de fonctionnement du RADIUS……36

5.Conclusion……38

Chapitre III: Analyse des failles et des attaques dans les réseaux Wi-Fi

1.Introduction……39

2.Faiblesses et contournements des mécanismes préliminaire de sécurité……..39

2.1. Utilisation d'ESSID fermés……..39

2.2. Filtrage par adresse MAC……39

3. Les failles du protocole WEP……..40

3.1. Les faiblesses conceptuelles du protocole WEP……40

3.1.1. Mécanisme défaillant de génération des clés WEP :RC4……..40

3.1.2. Collision des vecteurs d'initialisations……41

3.1.3. Contrôle d'intégrité inadapté……41

3.1.4. Clé unique : taille faible et gestion statique ……..42

3.2. Les attaques contre le protocole WEP……..42

3.2.1. Attaque par force brute……43

3.2.2. Attaque inductive à texte clair connu : injection du trafic……..43

3.2.3. Attaque bit flipping sur le CRC……44

3.2.4. Attaque FMS……44

4. Les failles du protocole 802.1x……45

4.1 les faiblesses conceptuelles du protocole IEEE 802.1x……45

4.1.1. Authentification à sens unique……45

4.1.2. Absence de synchronisation entre les machines à état……45

4.1.3. Manque d'intégrité dans les messages de contrôle 802.1x……..45

4.2. Les attaques sur le protocole 802.1x……46

4.2.1. Attaquede l'homme au milieu sur la couche physique……46

4.2.2. Attaque de l'homme au milieu sur lacouche de liaison de données……47

4.2.3. Attaque de l'homme au milieu sur SSL……48

5. Les failles de la norme WPA/WPA2……48

5.1. Attaque par dictionnaire sur la clé PSK……48

5.2. Attaque DOS sur l'échange 4 Way-Handshake……49

6.Conclusion……49

Chapitre IV : Architecture d'un réseau Wi-Fi sécurisée

1.Introduction……50

2.Approches principales de sécurisation des architectures Wi-Fi……50

2.1. Approche VLAN……50

2.2.Approche VPN……50

3.Principe de l'architecture Wi-Fi sécurisé……51

4. configuration d'un VLAN……55

4.1.Première étape : la configuration de l'USG 100……55

4.2.Deuxième étape : la configuration du switch GS191048……57

4.3. Troisième étape : la configuration du GS22008HP……59

4.4.Quatrième étape : configuration du point d'accès NWA3160N……65

5.Conclusion……71

Conclusion génerale

Bibliographie

Introduction générale

Introduction générale

Nous assistons aujourd'hui à un fort développement de l'effectif nomade dans les entreprises, dont l'organisation devient de moins en moins hiérarchisée. En effet, les employés sont équipés d'ordinateurs portables et passent plus de temps à travailler au sein d'équipes plurifonctionnelles, et géographiquement dispersées.
De ce fait, nous avons assisté ces dernières années à la montée en puissance des réseaux locaux sans fil ou encore Wi-Fi, qui sont en passe de devenir l'une des principales solutions de connexion pour de nombreuses entreprises. Le marché du sans fil se développe rapidement dès lors que les entreprises constatent les gains de productivité qui découlent dela disparition des câbles.

Ainsi avec cette évolution rapide de ce type dématérialisé de réseaux, les exigences en termes de sécurité deviennent de plus en plus sévères.en effet, pour garantir la pérennité etl 'essor de cette technologie, il est primordial de recourir à des méthodes avancées d'authentification, de gestion et de distribution de clés entre les différentes entités communicantes, ceci tout en respectant les contraintes imposées par les réseaux sans fil, telles que la capacité de l'interface radio qui représente le goulot d 'étranglement du trafic pour ce Beaucoup de travaux et d'efforts ont été consentis ces dernières années afin d'aboutir àdes solutions pour sécuriser les échanges dans ces réseaux.

Toutefois, des vulnérabilités persistent encore dans ces solutions et il est toujours possible de monter des attaques plus oumoins facilement. Notamment contre le dernier né des protocoles de sécurité Wi-Fi, à savoirle WPA2, qui bien qu'étant plus robuste sur le plan conceptuel que les générations précédentes, fait face au problème majeur de son incompatibilité matérielle avec lesprécédents protocoles. En effet, WPA2 exige de nouveaux équipements matériels, ce quiconstitue un surcoût économique énorme pour les entreprises ayant déjà déployé des équipements Wi-Fi d'anciennes générations.

Dans ce mémoire, nous nous intéressons à la problématique de sécurité des réseaux Wi-Fi dans l'entreprise. Compte tenu des vulnérabilités des standards de sécurité Wi-Fi, et face à toutes les failles de sécurité et la diversité des attaques qu'il est possible de monter contre les mécanismes de sécurité dans les réseaux 802.11, Comment assurer une sécurité optimale, compte tenu de l'hétérogénéité des équipements Wi-Fi (WEP, WPA, WPA2), excitants actuellement dans les entreprises.

Le présent mémoire est structuré comme suit :

Dans le premier chapitre, nous nous consacrons à l'étude des technologies employées au niveau de la couche physique et la couche liaison de données, ainsi qu'aux diversesfonctionnalités offertes par la norme Wi-Fi, ou encore IEEE 802.11.

Dans le second chapitre, nous focalisons sur les mécanismes etles standards de sécurité de la normeIEEE 802.11. Nous nous concentrerons sur l'aspect analyse de cette évolution, montrant àchaque fois, les caractéristiques et le fonctionnement de chaque protocole.

Le troisième chapitre, sur le volet faiblesses et vulnérabilités. En effet, ce chapitre, présente une analyse desvulnérabilités de chaque génération de protocole de sécurité Wi-Fi, ainsi que les détails de fonctionnement desprincipales attaques.

Dans le quatrième chapitre, Nous proposonsune approche architecturale de sécurisation des réseaux Wi-Fi, et nous configurons à la fin un VLAN avec une topologie multi SSID.

Finalement, ce mémoire se termine par une conclusion généralequi fait la synthèse de ce qui aété vu tout au long de cette étude et donne un aperçu sur les perspectives de travaux derecherche futurs.

Chapitre I

1. Introduction :

La norme IEEE 802.11 est un standard international décrivant les caractéristiques d'un réseau local sans fil. Le nom Wi-Fi correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance, l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11.

A travers ce chapitre nous montrons les différentes topologies de ces réseaux, ainsi que les caractéristiques des couches physiques et liaisons de données. Ensuite, nous présentons les techniques d'accès et de réservation du support employées. Enfin, nous esquissons les diverses orientations de recherche et les problématiques qui restent à résoudre afin de garantir 1 'essor de cette technologie.

2. Architecture Wi-Fi :

Un réseau 802.11 est composé de plusieurs regroupements de terminaux, munis d'une carte d'interface réseau 802.11. Ces regroupements sont des cellules Wi-Fi. Dans ce qui suit, nous montrons qu'ils peuvent être de différentes topologies.

2.1. Les topologies de la norme 802.11 :

A la base, les réseaux sans fil 802.11 peuvent être vus comme un ensemble de technologies permettant d'établir un réseau local sans l'utilisation du câblage pour les liaisons entre les ordinateurs. En effet, le câblage est remplacé par des liaisons hertziennes. Les principales technologies permettant de développer des réseaux sans fil ou WLAN sont celles appartenant aux normes IEEE 802.11. La norme la plus populaire de WLAN est le 802.11 b.

Ainsi, tel que le montre la figure I.1 la norme Wi-Fi définit deux modes opératoires :

- le mode infrastructure dans lequel les clients sans fil sont connectés à un point d'accès. Il S'agit généralement du mode par défaut des cartes réseaux 802.11.

- le mode ad hoc dans lequel les clients sont connectés les uns aux autres sans aucun point d'accès.

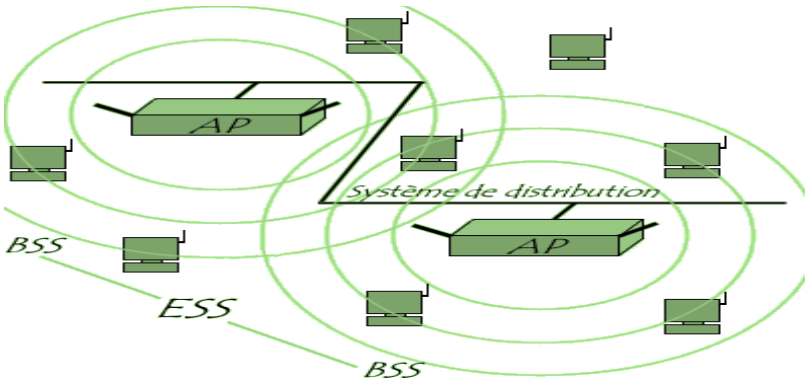
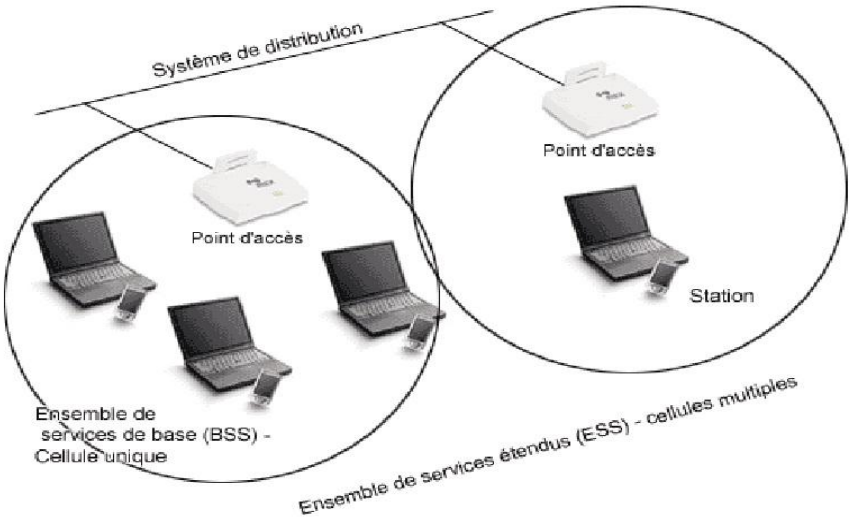


Figure I.1 : Topologies des réseaux de la norme IEEE 802.11

2.1.1. Le mode infrastructure :

Un réseau 802.11 est un ensemble de cellules de base (BSS). Chaque cellule BSS comporte un point d'accès matérialisé par un dispositif d'émission/réception. Les cellules sont reliées par une infrastructure de communication fixe et interconnectées par un système de distribution afin de former un ESS

• Cette infrastructure incorpore un portail permettant d'assurer l'interface avec un réseau local, tel que le montre la figure 1.2.



FigureI.2 Mode infrastructure

Chaque BSS est identifié par un BSSID. Dans le mode infrastructure, le BSSID correspond à l'adresse physique (adresse MAC) du point d'accès.

2.1.2. Le mode ad-hoc :

Ce mode représente un ensemble de stations 802.11 qui communiquent entre elles sans avoir recours à un point d'accès. Chaque station peut établir une communication avec n'importe quelle autre station dans la cellule que l'on appelle cellule indépendante IBSS, tel qu'illustré dans la figure I.3.

Dans les deux modes infrastructure et ad hoc, chaque réseau de service est identifié par un identificateur de réseau SSID. Par conséquent, toute station désirant se connecter à un réseau de service particulier doit connaître au préalable la valeur de son SSID.

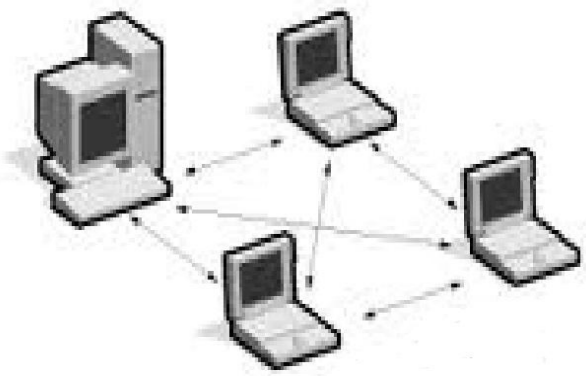


Figure I.3 : Mode AD HOC

2.2. Les couches de l' IEEE 802.11 :

L'IEEE 802.11 implémente de nouvelles couches physiques et de nouvelles techniques d'accès au support, au niveau de la couche de liaison de données. Dans ce qui suit, nous donnons un aperçu sur les nouvelles caractéristiques des couches physiques et de liaison de données, relatives à la norme 802.11.

2.2.1. La couche physique :

Au niveau de la couche physique, les normalisateurs ont opté pour deux sous-couches, à savoir PLCP (Physical Layer Convergence Protocol) et PMD (Physical Medium Dependent). La sous-couche PLCP concentre les fonctionnalités d'encodage des données, alors que la seconde sous-couche PMD se charge de l'écoute du support et fournit un service de signalisation à la couche MAC, en lui notifiant l'état du support soit occupé ou libre.

Pour l'encodage des données, la sous-couche PLCP utilise plusieurs techniques de modulation et de codage binaire. Cette diversité de techniques de codage et de modulation a donné naissance à plusieurs sous-normes avec des débits et des portées différentes, telles que 802.11b, 802.11a et 802.11g. Parmi ces techniques, nous citons la CCK (Complementary Code Keying), le codage DSSS (Direct Sequence Spread Spectrum), l'OFDM (Orthogonal Frequency Division Multiplexing) et la FHSS (Frequency Hopping Spread Spectrum).

2.2.2. La couche de liaison de données :

La couche de liaison de données de la norme 802.11 est subdivisée en deux sous couches : la sous-couche LLC (Logical Link Control) et la sous-couche MAC. La première sous-couche est commune à tous les standards du groupe 802. Quant à la sous-couche MAC 802.11, son rôle primaire est l'écoute de la porteuse avant l'émission des données. Elle intègre en plus un grand nombre de fonctionnalités que l'on ne trouve pas dans la version 802.3 (Ethernet) de cette même sous-couche.

Les normalisateurs ont en effet défini deux méthodes d'accès différentes au niveau de la couche MAC 802.11. La première est le DCF (Distributed Coordination Function), qui correspond à une méthode supportant le best-effort. Le DCF a été conçu principalement pour le transport de données asynchrones. Ainsi, cette méthode garantit à tous les utilisateurs qui veulent transmettre des données la même probabilité d'accès au support.

La seconde méthode d'accès est le PCF (Point Coordination Function). Elle se base sur l'interrogation séquentielle des stations, sous la supervision du point d'accès. Ainsi, la méthode PCF est conçue essentiellement pour la transmission de données sensibles, qui sollicitent une gestion serrée des délais. Cette méthode d'accès est utilisée pour le transport de grosses trames pour lesquelles une retransmission serait trop coûteuse en termes de bande passante.

2.3. Les techniques d'accès au support radio :

La technique DCF pour l'accès au support de transmission constitue la technique d'accès par défaut. Elle permet la transmission de données en mode asynchrone et best-effort, sans aucune exigence de priorité. La technique DCF s'appuie sur le protocole CSMA/CA qui est la variante sans fil du traditionnel CSMA/CD du monde Ethernet. Dans ce qui suit, nous donnons les caractéristiques principales du protocole CSMA/CA, ainsi que le mécanisme de réservation du support hertzien.

2.3.1. Le protocole CSMA/CA :

Dans le monde filaire d'Ethernet, le protocole CSMA/CD régule les accès au support et se charge de la détection et du traitement des collisions qui se produisent. Dans les réseaux Wi-Fi, la détection des collisions n'est pas possible, due à la nature même du support de transmission. En effet, la détection de collision exige de la station la simultanéité de l'émission et de la réception. Or les liaisons radio ne sont jamais en bidirectionnel simultané (full duplex). Ainsi, la station étant incapable d'écouter sa propre transmission, si une collision se produit, la station continuera à transmettre la trame au complet, ce qui entraîne une forte baisse de performance du réseau.

Le protocole CSMA/CA doit donc éviter les collisions, à défaut de pouvoir les détecter. CSMA/CA se base principalement sur. Les espaces inter trames ou encore IFS pour l'évitement de collisions. Ces IFS sont les intervalles de temps séparant la transmission de trames consécutives et qui correspondent à des périodes d'inactivité sur le support de transmission. Le standard défini trois types d'IFS différents :

1. SIFS (Short IFS) : SIFS est utilisé pour séparer les transmissions de trames consécutives au sein d'une même transmission (envoi de données, ACK, etc.). Durant cet intervalle, il n'y a qu'une seule station pouvant transmettre.

2. PIFS (PCF IFS) : PIFS est utilisé par le point d'accès pour accéder avec priorité au support.

3. DIFS (DCF IFS) : DIFS est utilisé lorsqu'une station veut commencer une nouvelle transmission.

Ainsi, lors de l'envoi d'une trame par la station source, les autres stations entendent cette transmission et pour éviter une collision, incrémentent la valeur d'un compteur, appelé NAV (Network Allocation Vector), qui sert à retarder toutes les transmissions prévues de toutes les stations. La· valeur d'incrémentation du NAV est calculée par rapport au champ durée de vie, ou TTL, contenu dans les trames qui passent sur le support. Ensuite, le compteur NAV est décrémenté jusqu'à atteindre la valeur 0, instant signalant à la station l'autorisation de transmettre ses données, après un intervalle DIFS. Le principe de fonctionnement de CSMA/CA moyennant les IFS et le compteur NAV est illustré par la figure I.4.

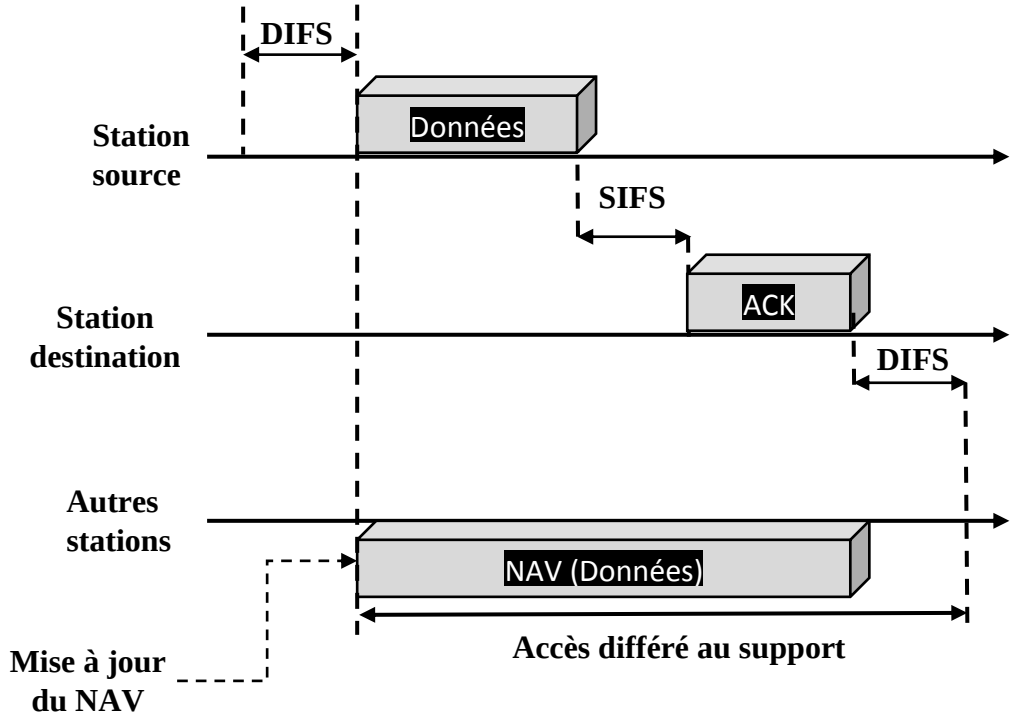


Figure I.4 : Processus de transmission des trames

Comme le montre la figure I.4, une station voulant transmettre des données écoute le support. Si aucune activité n'est détectée pendant une période DIFS, elle transmet ses données immédiatement. La station destination attend pendant un intervalle SIFS et émet un ACK pour confirmer la bonne réception des données. Si l'ACK n'a pas été détecté par la station source ou si les données ne sont pas reçues correctement, on suppose qu'une collision s'est produite et la trame est retransmise.

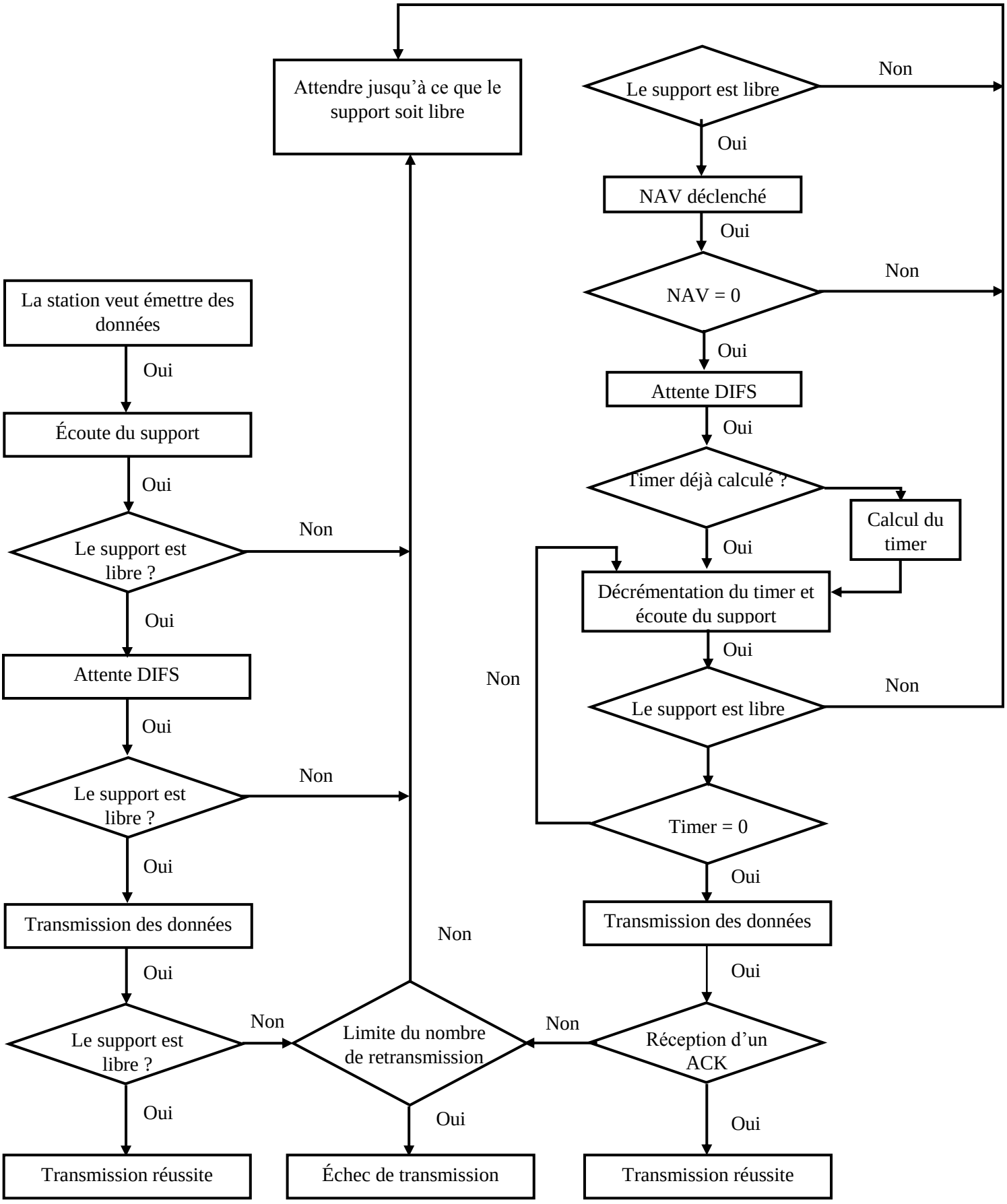


Figure I.5 : Mécanisme du CSMA/CA

2.3.2. Mécanisme de réservation du support RTS/CTS :

Les normalisateurs ont inclus dans le standard IEEE 802.11 un mécanisme permettant de réserver le support pour une transmission particulière. Ce mécanisme n'est pas actif par défaut dans le standard, mais il est activé optionnellement par la station souhaitant réserver le support exclusivement pour sa transmission. Ce mécanisme n'est autre que VCS localisé au niveau de la couche MAC. VCS se base sur l'émission de trames RTS/CTS entre une station source et une station destination, précédant toute transmission de données.

Ainsi, une station source voulant transmettre des données émet une trame RTS. Toutes les stations de la cellule BSS détectant le RTS lisent son champ TTL et mettent à jour leur valeur de NAV. La station destination ayant reçu le RTS réplique par un CTS, en temporisant sa transmission pendant un SIFS. Les autres stations détectent le CTS, lisent le champ TTL de celui-ci et mettent à nouveau à jour leur NAV.

Après réception du CTS, la station source est assurée que le support est stable et réservé exclusivement pour sa transmission de données. De cette manière, la station source peut transmettre ses données ainsi que recevoir l'ACK sans collision. Ce mécanisme de réservation est surtout utilisé pour l'envoi de grosses trames pour lesquelles une retransmission serait trop coûteuse en bande passante.

3. Normes associées à l'IEEE 802.11 :

Les réseaux Wi-Fi ont suscité un engouement incomparable chez la communauté scientifique, ainsi que chez les industriels, vu l'énorme potentiel que représente une telle technologie. D'un autre côté, la technologie Wi-Fi renferme une grande complexité et pose plusieurs problématiques, souvent divergentes.

Dans ce qui suit, nous donnons une description des principales problématiques traitées par les groupes de travail de 1' IEEE 802.11.

3.1. Les normes physiques :

La première version normalisée par l'IEEE fût la 802.11. Elle utilisait la modulation DSSS sur la bande 2.4 GHz. Cette norme n'était pas compatible entre constructeurs. De plus, elle offrait un débit très faible (2 Mbps), comparés aux débits que proposait la norme Ethernet filaire. L'IEEE développa de nouvelles générations de réseaux sans fil : la 802.11b, la 802.11a et la 802.11g.

3.1.1. La 802.11b ou Wi-Fi 2 :

C'est la première norme Wi-Fi interopérable. Avec un débit de 11 Mbps, elle permet une portée de 300 mètres dans un environnement dégagé. Elle utilise la bande des 2.4 GHz avec 3 canaux radios disponibles. Cette norme Wi-Fi a connu beaucoup d'extensions et chacune

d’entre elles, visant à apporter une amélioration soit au niveau du débit, soit au niveau de la bande passante ou même de la sécurité, de la qualité de service ou de la capacité du canal.

3.1.2. La 802.11 a :

Encore appelé Wi-Fi 5, cette norme permet d’obtenir du haut débit (54 Mbit/s) tout en spécifiant 8 canaux. Mais elle n’est pas compatible avec la 802.11b. Elle utilise la technique de modulation OFDM.

3.1.3. La 802.11g :

La 802.11a offre un débit assez élevé mais la portée est plus faible et son usage en extérieur est souvent interdit. Pour répondre à ces problèmes, l’IEEE développe la nouvelle norme 802.11g, offrant le même débit que le Wi-Fi 5, tout en restant compatible avec le Wi-Fi 2 (bande de fréquences de 2.4 GHz) .Cette norme vise aussi à remplacer Wi-Fi 2 sur la bande 2.4 GHz mais avec un débit plus élevé pouvant atteindre les 54 Mbits/s. Elle utilise la technique de modulation OFDM.

3.2. Les normes d’amélioration

3.2.1. L'IEEE 802.11e : la qualité de service

L'IEEE a chargé le groupe de travail 802.11e d'améliorer la couche MAC 802.11 pour y inclure des mécanismes de qualité de service, afin de permettre un meilleur support des applications sensibles aux phénomènes de latence, telles que les applications de voix ou vidéo. Le groupe de travail a réussi de mettre en œuvre quelques solutions intermédiaires intéressantes, tel qu’EDCF qui réalise un contrôle d'admission simple et efficace. Les efforts se poursuivent encore afin d'aboutir à un ensemble d'outils pratiques et efficaces qui permettent d'étendre et de développer les applications Wi-Fi.

3.2.2. L'IEEE 802.11f : les handovers

L'objectif du groupe 802.11fest de développer la technologie permettant la mobilité inter-cellules des stations Wi-Fi, tout en préservant les performances du réseau et en maintenant la connectivité des stations lors du déplacement.

Ainsi, la plupart des réseaux sans fil pourront désormais jouer le rôle de réseaux mobiles, en adoptant la norme 802.11f, qui équipe actuellement la plupart des interfaces Wi-Fi. Ces dernières permettent de réaliser des handovers ou relève intercellulaire qui désigne la possibilité de passer d'une cellule à une autre sans interruption de la communication. Le protocole retenu par le groupe de travail 802.11f est IAPP qui fait communiquer les différents points d'accès d'un même réseau ESS, de façon à permettre à un utilisateur mobile de passer d'une cellule à une autre sans perte de connexion.

Toutefois, le standard 802.11f ne garantit pas une mobilité sécurisée et rapide. C'est pourquoi, l'IEEE vient de mettre en place un nouveau groupe de travail, l'IEEE 802.11r, afin de développer une nouvelle norme garantissant la sécurité et la rapidité des handovers.

3.2.3. L'IEEE 802.11n : le haut débit

L'IEEE 802.11n est un groupe de travail au sein de l'IEEE, mis en place en 2003. Les raisons qui ont suscité la création de ce groupe sont les suivantes :

- Les réseaux Wi-Fi (standards 802.11b, g et a) offrent une portée limitée.
- Les réseaux Wi-Fi sont très sensibles aux phénomènes de réflexion d'ondes, ainsi qu'aux interférences ayant comme origine d'autres unités sans fil.
- Les réseaux Wi-Fi sont beaucoup plus lents, en termes de débits, qu'Ethernet.

Cette unité de recherche travaille sur la mise en œuvre d'une norme devant résoudre les problèmes cités ci-dessus. En effet, 802.l1n est censé permettre d'atteindre un débit minimal de l00 Mbps, et un débit théorique utile maximal de 540 Mbps. Ce pré-standard se base sur une technologie radio innovante, nommée MIMO qui se base sur l'utilisation de plusieurs antennes à l'émission et pareillement à la réception. De plus, l'IEEE a mis comme exigence à la mise en œuvre d'une telle technologie la rétrocompatibilité et l'interopérabilité complètes avec les standards actuels (802.11b, g et a).

3.2.4. L'IEEE 802.11i : la sécurité

Dans les réseaux Wi-Fi, le support est partagé. Tout ce qui est transmis peut donc être intercepté. L'incapacité de garantir un trafic aussi sécurisé que dans les réseaux fixes constitue un obstacle pour l'essor de la technologie Wi-Fi. C'est pourquoi l'IEEE a mis en place le groupe de travail IEEE 802.11i, dont la mission est la mise au point d'une architecture de sécurité robuste, qui prend en compte les spécificités des réseaux sans fil.

Parmi les groupes de travail de l'IEEE, le 802.11i est certainement le groupe de travail le plus actif et le plus sollicité par les industriels. Les réseaux Wi-Fi dans leur conception originelle n'intégraient pas la sécurité comme contrainte majeure à couvrir, ce qui a eu comme conséquence une grande difficulté à l'intégrer par la suite.

3.2.5. L'IEEE 802.11d :

En permettant aux différents équipements d’échanger des informations sur les plages de fréquences et les puissances autorisées dans le pays d’origine du matériel, cette norme permet l’adaptation des couches physiques afin de fournir une conformité aux exigences de certains pays particulièrement strictes, exemple France et Japon.

3.2.6. La 802.11h :

Elle gère le spectre de la norme 802.11a et vise à améliorer la sous couche MAC, afin de rendre compatible les équipements 802.11a avec les infrastructures Hiperlan2. Enfin, elle s'occupe de l'assignation automatique de fréquences du point d'accès et du contrôle automatique de la puissance d'émission, afin d'éliminer les interférences entre points d'accès.

4. Conclusion

Dans ce chapitre on a bien vu que lors du déploiement d'un réseau sans fil, le Wi-Fi (802.11) semble être la solution répondant au mieux aux besoins des réseaux locaux sans fil grâce à l'avantage qu'elle procure, qui est son interopérabilité avec les réseaux de type Ethernet. Cette technologie, est fréquemment utilisée dans les entreprises désirant accueillir des utilisateurs mobiles ou souhaitant une alternative au réseau filaire tout en conservant des performances quasi identiques. Contrairement le Wi-Fi a beaucoup de problèmes de sécurité, dans le chapitre qui suit, on va détailler les mécanismes utilisé pour mettre au point une stratégie de sécurité.

Chapitre II

1. Introduction

Le point crucial lors d'une installation réseau, qu'elle soit filaire ou sans fil, est la mise en place d'éléments de protection. La sécurité a toujours été le point faible des réseaux Wi-Fi à cause principalement de sa nature physique : les ondes radio étant un support et s'introduire dans la zone de couverture peut écouter un support de transmission partage quiconquese trouvant dans la zone de couverture peut écouter le support et s'introduire dans le réseau. On peut même grâce à des antennes amplifiées, se trouver hors de portée de la couverture radio pour pénétrer ce réseau .ces problèmes de sécurité se posent aussi pour des réseaux câblés mais l'écoute passive nécessite une intrusion physique car toute personne possédant quelques notions d'informatique et un peu de matériel peut facilement trouver les informations et les programmes pour écouter et percer des réseaux Wi-Fi. En plus de ces faiblesses intrinsèques aux ondes radio, un réseau Wi-Fi doit se protéger des attaques classiques. Ces failles de sécurité ont porté un préjudice certain à son développement en entreprise Car elles deviennent les points d'accèsau réseau interne sur lequel il est connecté. Il existe des moyens de sécurité implantes de base sur le matériel Wi-Fi (carte et pointd'accès) permettant un premier niveau de protection. Mais ces moyens de sécurisation sont facilement contournable. Dans ce chapitre, on va présenter d'une part une analyse des différentes attaques susceptibles d'atteindre un réseauWi-Fi, d'autre part une série de notions utilisé qui répondent aux trois principes élémentaires de sécurité qui sont : codage, authentification et intégrité, permettant à leurs administrateurs et usagers de mieux contrôler et si possible réduire les risques.

2. Généralités sur la sécurité

2.1. Risques et attaques

2.1.1. Les risques

Les risques dépendentdes paramètres que l'on peut maitriser. Contrairement au réseau câblé, le contrôle des accès physiques au réseau sans fils est difficile, voir impossible.
Il existe deux types de risques :

- **Risque structurel** : dépend de l'organisation de l'entreprise.
- **Risque accidentel** : indépendant de tous les facteurs de l'entreprise.

On peut classifier les risques en quatre niveaux :

a. Acceptables : pas de conséquences graves pour les utilisateurs du réseau.
Exemple : panne électrique, perte de liaison, engagement…
b. Courants : pas de préjudices graves au réseau, on peut réparerfacilement
Exemple : gestion du réseau, mauvaise configuration, erreur utilisateur.
c. Majeurs : dus à des facteurs graves et qui causent de gros dégâts mais récupérables.
Exemple : foudre qui tombe sur le routeur.
d. Inacceptables : fatals pour l'entreprise, ils peuvent entrainer son dépôt de bilan.
Exemple : perte ou corruption des informations importante.

2.1.2.Les attaques

Les attaques ont pour but :

- **Interruption:** vise la disponibilité des informations.
- **Interception :** vise la confidentialité des informations.
- **Modification :** vise l'intégrité des informations.
- **Fabrication :** vise l'authenticité des informations.

On peut classifier les attaques en deux groupes principaux : les attaques passives et lesattaques actives, qui sont bien évidemment plus dangereuses.

2.1.2.1. Attaques passives

Elles ne modifient pas le comportement du système, et peuvent ainsi passer inaperçues.

- ***Attaques sur la confidentialité :***

  Objectifs : obtention d'informations sur un système, sur un utilisateur ou un projet.

La zone de couverture radio d'un point d'accèsdéborde du domaine privé d'une entreprise ou d'un particulier. L'attaque passive la plus répandueest la recherche du point d'accès .cette attaque (appelée Wardriving) est devenu le jeu favori de nombreux pirates informatique. Les points d'accès sont facilement détectablesgrâce à un scanner(portable équipé d'une carte WIFI et d'un logicielspécifique de recherchede PA).Ces cartes Wi-Fi sontéquipées d'antennes directives permettant d'écouter le trafic radio à distance hors de la zone de couverture du point d'accès. Il existe deux types de scanners, lespassifs (Kismet, wifiscanner, prsmstumber…) ne laissant pas de traces (signatures).quasiment indétectables et les actifs (Netstumbler, dstumbler) détectables en cas d'écoute, ils envoient des probe request.

Une première analyse du trafic permet de trouver le SSID (nom du réseau), l'adresse MAC du point d'accès, ledébit, l'utilisation du cryptage WEP et la qualité du signal. Associéà un GPS. Ces logiciels permettent de localiser (latitude longitude) ces point d'accès .A un niveau supérieur des logiciels (type Aisnot ou Wepcrack) permettent, en quelques heures (suivant le trafic), de déchiffrer les clés WEPet ainsi avec des outils d'analyse de réseaux conventionnels la recherche d'informations peut aller plus loin. Le pirate peut passer à une attaque dite active

2.1.2.2. Attaques actives

Elles modifient le contenu des informations du système ou le comportement du système. Elles sont en général plus critique que les passives.

- ***Attaques sur l'intégrité :***

  Objectifs : modification ou destruction de données ou de configurations.

- ***Attaques sur l'authentification :***

  Objectifs : utilisation des ressources de façon clandestine sur un système.

- ***Attaques sur la disponibilité :***
  Objectifs : perturbation d'un échange par le réseau, d'un service ou d'un accès à un service.

Nous allons revoir, assez succinctement, les différentes attaques connues par les réseaux filaires et qui touchent bien évidemment, le monde du Wi-Fi.

- **Dos (Denial of Service)**

Le déni de services réseau est souvent l'alternative à d'autre formes d'attaques car dans beaucoup de cas il est plus simple à mettre en œuvre, nécessite moins de connaissances et est moins facilement traçable qu'une attaque directe visant à entrer dans un système pour en prendre le contrôle. Cette attaque a pour but d'empêcher des utilisateurs légitimes d'accéder à des services en saturant de fausses requêtes ces services. Elle base généralement sur des bugs logiciels. Dans le milieu Wi-Fi, cela consiste notamment à bloquer des points d'accès soit en l'inondant de requêtes de désassociassions ou des authentifications, ou plus simplement en brouillant les signaux hertzien.

- **Spoofing (usurpation d'identité)**

Le spoofing IP est une technique permettant à un pirate d'envoyer à une machine des paquets semblant provenir d'une adresse IP autre que celle de la machine du pirate. Le spoofing IP n'est pas pour autant un changement d'adresse IP. Plus exactement il s'agit d'une mascarade (il s'agit du terme technique) de l'adresse IP au niveau des paquets émis, C'est-à-dire que les paquets envoyés sont modifiés afin qu'ils semblent parvenir d'une machine.

- **Man in the middle (homme au milieu)**

Cette attaque consiste. Pour un réseau Wi-Fi, à disposer un point d'accès étranger dans proximité des autre PA légitimes. Les stations désirant se connecter au réseau livreront au PA "félon" leurs informations nécessaires à la connexion. Ces informations pourront être utilisées par une station pirate. Il suffit tout simplement à une station pirate écoutant le trafic. De récupérer l'adresse MAC d'une station légitime et son PA, et de s'intercaler au milieu.

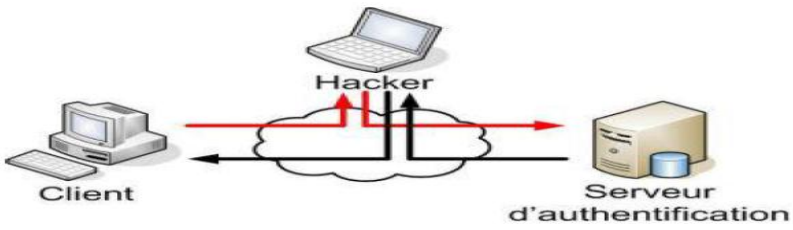


Figure II.1 : Attaque MITM

2.1.2.3. Autres attaques

- **Craquage du mot de passe**

Cette méthode est souvent le dernier de recours, elle consiste à faire beaucoup d'essais pour déterminer un mot de passe. On distinguera deux grandes méthodes :

- L'utilisation du dictionnaire : la plus part des mots de passes ne sont pas des chaines aléatoires mais des mots ou des phrases faciles à retenir. Cela permet d'écarter une très grande possibilité.
- La force brute consiste à essayer toutes les combinaisons possibles. Elle est rapidement Efficace sur les petites chaînes (moins de 8 caractères) mais devient rapidement trop longue à exécuter quand la longueur du mot de passe augmente (plus de16 caractères).

- **Backdoors**

Quand un pirate arrive à accéder à un système et qu'il veut pouvoir y accéder plus facilement par la suite, il crée une "Backdoors" ou porte de derrière. Cela pourra se traduire par :

- Le rajout d'un nouveau compte au serveur avec le mot de passe choisi par le pirate
- La modification du firewall pour qu'il accepte une IP définie (une que le pirate pourra spoofer facilement) ou qu'il ouvre certains ports.

-la création d'un compte FTP.

-L'utilisation d'un troyen.

- **Virus, vers et chevaux de Troie**

Un virus est un programme capable de se cacher dans un autre et qui peut se reproduire en infectant d'autres programmes ou d'autres ordinateurs. Les dégâts pourront aller d'un simple affichage à l'écran à une mise hors service d'un système. On recense plusieurs catégories :

- Les vers capables de se propager dans le réseau.
- Les chevaux de Troie ou troyens créant des failles dans un système.
- Les bombes logiques se lançant suite à un évènement du système
- Les hoax qui sont des canulars envoyés par mail.

- **Le sniffing**

Ce type d'attaque est basé sur l'interception de données émises sana précaution à toutes les parties comme lors des diffusions. Il suffit d'être présent sur le réseau pour

intercepter tout le trafic et récupérer n'importe quelles données transitant sur le réseau si celles-ci ne sont pas cryptées.

3. service de sécurité

Les services de sécurité représentent les logiciels et matériels mettant en œuvre les mécanismes dans le but de mettre à la disposition des utilisateurs des fonctions de sécurité dont ils ont besoin.
Il existe cinq notions fondamentales de la sécurité :

3.1. Confidentialité

Le service de confidentialité garantie aux communicants à être les seuls à pouvoir comprendre les données échangées. Ceci implique la mise en œuvre des algorithmes de chiffrement en mode flux, c'est-à-dire octet par octet, ou en mode bloc. Un message écrit en clair est transformé en un message chiffré, appelé « cryptogramme » grâce aux algorithmes de chiffrement. Cette transformation est fondée sur une ou plusieurs clés.

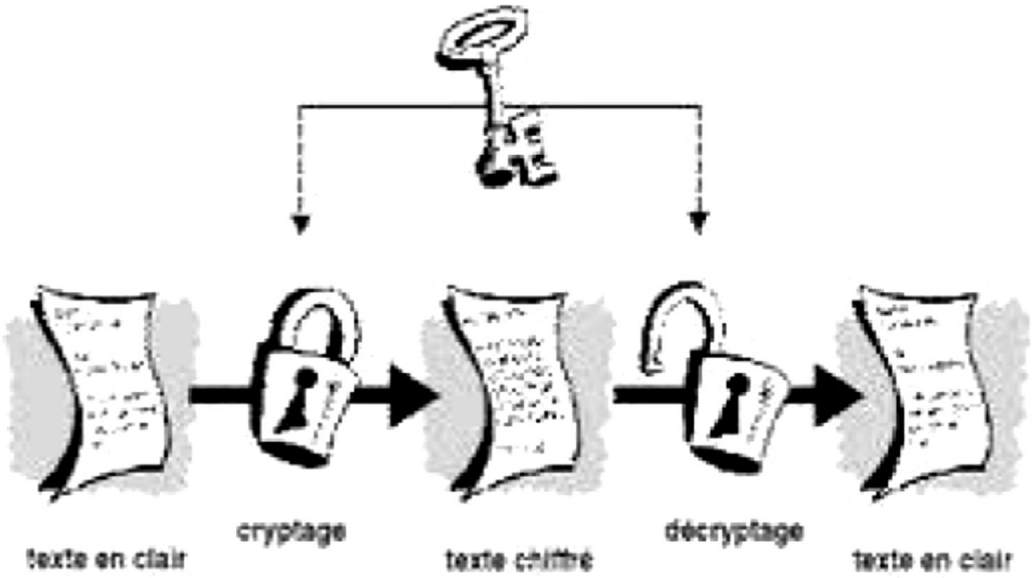
3.1.1. Chiffrement (la cryptographie)

Le chiffrement consiste à rendre un texte incompréhensible en le codant. On code (crypte ou chiffre) le texte en effectuant une opération sur le texte en clair à partir d'une règle appelé clé de chiffrement. Le texte codé (cryptogramme) peut alors être envoyé à son destinataire. La cryptanalyse consiste à déchiffrer un texte codé en effectuant sur ce texte avec une clé. Il existe trois méthodes de chiffrement : à clé symétrique, à clé asymétrique (ou clé publique), à clé mixte.

3.1.1.1. Clé symétrique

La clé de chiffrement est identique à la clé de déchiffrement. Ainsi c'est la même clé qui va nous permettre à la fois de chiffrer le message et de permettre aux destinataires de le déchiffrer. Cela ne va pas sans poser un problème majeur : l'échangeprêtable de la clé entre les protagonistes. Or, ceci est particulièrement difficile à réaliser, tant que la clé n'est pas transmise, il n'existe pas de moyen sûr d'échange d'information, en dehors d'une rencontre physique qui n'est pas forcément possible.

Le deuxième problème est le nombre de clés nécessaire pour sécuriser un ensemble de relations. En effets, si l'on désire que chaque utilisateur d'un réseau puisse communiquer avec un autre utilisateur de manière sécurisée, une clé différente est alors utilisée pour chaque paire d'utilisateur du réseau. Le nombre total de clés croît alors suivant un polynôme quadratique.Ainsi, un groupe de 10 utilisateurs met en jeu 45 clés différentes et 100 utilisateurs, 4950 clés.



FigureII.2 : Chiffrementsymétrique

Les principes algorithmes de chiffrement symétrique sont :

- **DES (Data Encryptions Standard)** : a été le plus utilisé, mais n'est plus utilisé depuis 1998. Considéré peu sûr. Clé de 40 à56 bits.
- **IDEA** (**International Data Encryptions Algorithme)** : est utilisé par PGP (Pretty Good Privary).Le logiciel de cryptographie le plus utilisé au monde, clé de 128 bits.
- **Séries RC (Ron's Code) RC2 à RC6** : algorithme développé par Ron Rivest, la version RC4 est utilisé dans le protocole WEP d'IEEE 802.11.
- **AES (Advanced EncryptionsStandard)** : remplaçant du DES dans l'administration américaine et du RC4 dans la norme 802.11 avec 802.11i.

3.1.1.2. Clé asymétrique

Dans ce cas, les clés de chiffrement et de déchiffrement sont distinctes, et généralement symétriques entre elles : la clé de chiffrement permet de déchiffrer ce qui a été chiffré avec la clé de déchiffrement. Et vice versa. Le possesseur d'une telle paire de clés. En rend une (au choix) publique. C'est-à-dire qu'il la donne à tout le monde, dans une sorte d'annuaire. Tout correspondant qui veut envoyer un message. Chiffre son message à l'aide de la clé publique du destinataire. Seul le possesseur de la clé secrète correspondant à cette clé publique pourra déchiffrer le message. Les algorithmes de chiffrement à clé publique permettent aussi à l'envoyeur de signer son message. En effet, il lui suffit de chiffrer le message (ou une partie de ce message) avec sa propre clé secrète. Le destinataire déchiffrera cette fonction avec la clé publique de l'envoyeur et sera ainsi certain de l'identité de l'expéditeur, puisqu'il est le seul à posséder la clé secrète qui permet de faire un tel chiffrement. Ainsi cette méthode permet de réaliser une communication confidentielle sans échanger auparavant de code secret.Le principal inconvénient de ce type

d'algorithme est la lenteur à laquelle s'effectuent les opérations de chiffrement et de déchiffrement.

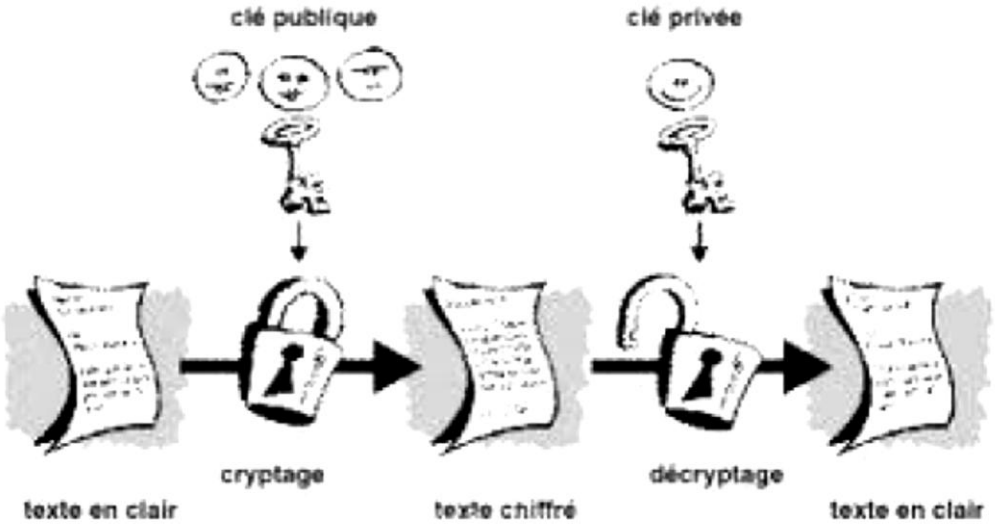


Figure II.3 : chiffrement asymétrique

RSA (Ruverst, Shamir, Adelam) : comme le plus connu de ces algorithmes. La sécurité du RSA réside dans l'impossibilité pratique de factoriser un grand nombre de quelques centaines de chiffres en un temps raisonnable. Qui plus est pour assurer sa pérennité il est toujours possible d'augmenter la longueur de la clé qui varie entre 1024 et 2048 bits. En résumé, unesynthèse de ces deux méthodes de cryptographie est décrite dans le tableau Ci-après.

Type de crypto système	**Avantages**	**Inconvénients**
Clé symétrique	*Rapide *Peut être facilement réalisé sur une puce	*Difficultés de distribuer les clés *Ne permet pas de signature électronique
Clé asymétrique	*Utilise deux clés différentes *Fournit des garanties d'intégrité et non répudiation par signature électronique	*Lent et demandant beaucoup de calculs

Tableau II.1 : comparaison des deux types de chiffrement

Finalement comme nous avons pu le voir précédemment, les deux systèmes de base de la cryptographie souffrent de problèmes complémentaires. Ainsi l'intérêt pour augmenter la sécurité des systèmes de cryptage passe certainement par l'utilisation combinée de ces deux techniques, ce que l'on nomme la cryptographie mixte.

3.1.1.3. Clé mixte

Ce principe fait appel aux deux techniques précédentes, à clé symétrique et à clé publique, combinant les avantages des deux tout en évitant leurs inconvénients, le principe Générale consiste à effectuer le chiffrement des données avec des clés symétriques, mais en ayant effectué au départ l'envoi de la clé symétrique par un algorithme à clé publique. L'un de ces algorithmes est PGP.

- **PGP (Pretty Good Privacy)**

PGP est un système de cryptographiehybride, utilisant une combinaison des fonctionnalités de la cryptographie clé publique et de la cryptographie symétrique.
Lorsqu'un utilisateur chiffre un texte avec PGP. Les données sont d'abord compressées. Cette compression des données permet de réduire le temps de transmission par tout moyen de Communication, d'économiser l'espace disque et, surtout, de renforcer la sécurité cryptographique.
La plupart des cryptanalyses exploitent les modèles dans le texte en clair pour casser le chiffrement. La compression réduit ces modèles dans le texte en clair, améliorant par conséquent considérablement la résistance à la cryptanalyse.
Ensuite, l'opération de chiffrement se fait principalement en deux étapes :

- Le PGP crée une clé secrète IDEA d'une manière aléatoire, et chiffre les donnés avec cette clé
- PGP crypte la clé secrète IDEA et la transmet au moyen de clé RSA publique du destinataire.

L'opération de décryptage se fait également en deux étapes :

- PGP déchiffre la clé secrète IDEA au moyen de la clé RSA privé.
- PGP déchiffre les données avec la clé secrète IDEA précédemment obtenue.

Cette méthode de chiffrement associe la facilité d'utilisation du cryptage de clé publique à la vitesse du cryptage conventionnel. Le chiffrement conventionnel est environ 1000 fois plus rapide que les algorithmes de chiffrement à clé publique. Le chiffrement à clé publique résout le problème de la distribution des clés. Utilisées conjointement, ces deux méthodes améliorent la performance et la gestion des clés, sans pour autant compromettre la sécurité.

3.1.2. Certificats

Un certificat permet d'associer une clé publique à une entité (une personne, une machine) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé autorité de certification (souvent notée CA pour Certificat Authority). L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits

alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date encas de compromission de la clé (ou du propriétaire).

- **Structure d'un certificat**

Les certificats sont des petits fichiers divisés en deux parties :

- La partie contenant les informations.
- La partie contenant la signature de l'autorité de certification.

La structure des certificats est normalisée par le standard X.509 de l'UIT (plus exactement.509v3), qui définit les informations contenues dans le certificat :

- La version de X.509 à laquelle le certificat correspond.
- Le numéro de série du certificat.
- L'algorithme de chiffrement utilisé pour signer le certificat.
- Le nom (DN, pour Distinguished Name) de l'autorité de certification émettrice
- La date de début de validité du certificat.
- La date de fin de validité du certificat.
- L'objet de l'utilisation de la clé publique.
- La clé publique du propriétaire du certificat.
- La signature de l'émetteur du certificat.

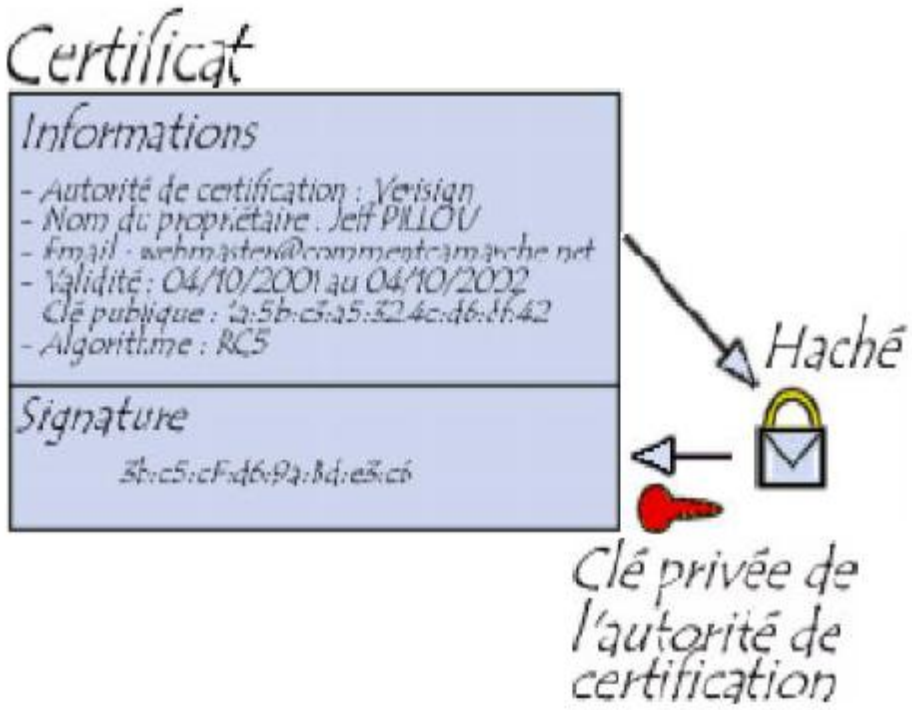


Figure II.4 : Certificat

L'ensemble de ces informations (informations +clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification, la clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification. Lorsqu'un utilisateur désire communiquer avec une autre personne. Il lui suffit de se procurer le certificat du destinataire. Ce certificat contient le nom du destinataire, ainsi que sa clé publique est signé par l'autorité de certification. Il est donc possible de vérifier la validité du message en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière, et en comparant ces deux résultats.

3.2. Service d'authentification

L'authentification a pour but de garantir l'identité des correspondantes. Parmi les solutions simples qui existent, l'utilisation d'un identificateur et d'un mot de passe, une méthode de défi basé sur une fonction cryptographique et un secret, l'authentification peut s'effectuer par un numéro d'identification personnel, comme le numéro inscrit dans une carte à puce, ou le code PIN.

L'authentification peut être simple ou mutuelle. Elle consiste surtout à comparer les données provenant de l'utilisateur qui se connecte à des informations, stockées dans un site protégé susceptibles de piratage. Les sites mémorisant les mots de passe.

- **Les protocoles**

Un protocole d'authentification est un moyen de contrôle d'accès caractérisépar les 3 A (AAA): Authentication, Autorisation, Accounting.

La signification de ces termes est la suivante :

- Authentication: consiste à vérifier qu'une personne équipement est bien celle qu'elle prétend être.
- Autorisation : consiste à permettre l'accès à certains services ou ressources.
- Accounting : le serveur AAA a la possibilité de collecter des informations sur l'utilisation des ressources

- **Diameter**

Diameter est un protocole d'Authentification conçu pour servir de support à l'architecture AAA, successeur du protocole Radius. Ce protocole est défini par la RFC 3588.Il a repris les principales fonctions de Radius (Diameter est compatible avec Radius) et en rajouté de nouvelles pour s'adapter aux nouvelles technologies (IPv4 Mobile, NASREQ…)

etplus particulièrement offrir des services aux applications mobiles. Ce protocole se situe au niveau de la couche transport. Il utilise le port 3868 via le protocole TCP ou bien SCTP.

- **TACACS+**

TACACS+ (Terminal Access Controller Access Control System Plus) est un protocole de sécurité inventé la fin des années 90 par SISCO Systems. Même s'il a fini par remplacer les protocoles TACACS et XTACACS, TACACS+ n'est pas basé sur ces derniers. Ce protocole se situe au niveau de la couche transport. Il utilise le port 46 via le protocole TCP.

TACACS+ permet de vérifier l'identité des utilisateurs distants mais aussi, grâce au modèle AAA, d'autoriser et de contrôler leurs actions.

- **PAP**

Le protocole PAP (Password Authentication Protocol) utilise des mots de passe en texte brut et constitue le protocole d'authentification le moins sécurisé. Il est généralement négocié lorsque le client distant et le serveur d'accès distant ne disposent d'aucun moyen de validation plus sûr.

- **CHAP**

Le protocole CHAP (Challenge Handshaken Authentication Protocol) est un protocole D'authentification par stimulation-réponse, qui utilise le modèle de hachage MD5 (Message Digest 5) standard pour crypter la réponse. CHAP est utilisé par de nombreux fournisseurs de clients et de serveurs d'accès réseau. Un serveur exécutant routage et accès distant prend en charge CHAP pour que les clients d'accès distant exigeant CHAP soient authentifiés. Dans la mesure où CHAP exige l'utilisation d'un mot de passe crypté à l'envers, vous devez envisager un autre protocole d'authentification comme MSCHAP version 2.

- **Kerberos**

Kerberos est un protocole de sécurité originaire du monde Unix, il a pris un niveau départ lorsqu'il a été choisi par Microsoft pour remplacer NTLM (NT Lan Manager) dans Windows 2000. Kerberos a pour objectif :

- D'authentifier les utilisateurs.
- De leurs allouer des droits d'accès à des applications (sur un serveur) sur le réseau sous forme
- De ticket ou jetons d'accès périssables dans le temps.
- La transmission sécurisée de ces tickets ou jetons d'accès vers les applications et ressources demandées, de protéger les échanges entre les utilisateurs et les applications.

3.3. L'intégrité des données

Dans certains cas, il peut être nécessaire d'assurer simplement sont intégrés, c'est-à-dire qu'elles n'elles n'ont pas été au passage falsifiées par un intrus. Ces données restent claires, au sens où elles ne sont pas secrètes.

3.4. Nonrépudiation

Elle fournit au récepteur/émetteur une preuve qui empêche l'émetteur/récepteur de l'envoi du message.

3.5. contrôle d'accès

De nos jours, toutes les entreprises possédant un réseau local et aussi un accès internet, afin d'accéder aux informations disponibles sur le réseau, et pouvoircommuniquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable et dangereuse en même temps.

Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise, et y accomplir des actions douteuses, pour cela une architecture sécurisée est nécessaire.

Le cœur d'une telle architecture est basé sur un firewall. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion. Cela représente une sécurité supplémentaire rendant le réseau ouvert sur internet beaucoup plus sûr. De plus, il peut Permettre de restreindre l'accès interne de l'extérieur et l'accès vers l'extérieur de l'intérieur.

En effet, des employés peuvent s'abonner à des activités (exemple : les jeux en ligne) que l'entreprise ne cautionne pas. En plaçant un firewall, on peut limiter et au même temps interdire l'accès à ces services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte.

Le firewall propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécurisé de gérer le trafic réseau, et ainsi d'utiliser le réseau de façon pour laquelle il a été prévu et sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données. Mais il ne fournit pas les services de sécurité.

4. Sécurisation du wifi

Installer un réseau sans fil sans le sécuriser peut permettre à des personnes non autorisées d'écouter, de modifier et d'accéder à ce réseau. Il est donc indispensable de sécuriser les réseaux sans fil dès leur installation.il est possible de sécuriser son réseau de façon plus ou moins forte selon les objectifs de sécurité et les ressources que l'on y accorde. La sécurité d'un réseau sans fil peut-être réalisée à différents niveaux : configuration des équipements et choix des protocoles.

4.1. Sécurités des points d'accès

La première chose à faire lors de la mise en place d'un réseau sans fil consiste positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir. Eviter les murs extérieurs mais choisir plutôt un emplacement central, en se promenant autour de l'immeuble, on peut établir le périmètre à l'intérieur duquel la borne est accessible. Il n'est toutefois pas rare que la zone effectivement couverte soit largement plus grande que souhaitée, auquel cas il est possible de réduire la puissance de la borne d'accès afin d'adapter sa portée à la zone à couvrir.

4.1.1. Éviter les valeurs par défaut

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut. Y compris en ce qui concerne le mot de passe de l'administrateur. Un grand nombre d'administrateurs en herbe considèrent qu'à partir du moment où le réseau fonctionne, il est inutile de modifier la configuration du point d'accès. Toutefois les paramètres par défaut sont tels que la sécurité est minimale, ilest donc impératif de se connecter à l'interface d'administration notamment pour définir un mot de passe d'administration.D'autre part, afin de se connecter à un point d'accès il est indispensable de connaîtreL'identifiant du réseau(SSID). Ainsi il est vivement conseillé de modifier le nom du réseau par défaut et de désactiver la diffusion (broadcast) de ce dernier sur le réseau .le changement de l'identifiant réseau par défaut est d'autant plus important qu'il peut donner aux pirates des éléments d'information sur la marque ou le modèle du point d'accès utilisé. L'idéal est même de modifier régulièrement le nomSSID.il faudrait même éviter de choisir des mots reprenant l'identité de l'entreprise ou sa localisation, qui sont susceptibles d'être plus facilement devinés.

4.1.2. Filtrageparadresse MAC

Chaque adaptateur réseau possède une adresse physique qui lui est propre, les point d'accès permettent généralement dans leur interface de configuration de gérer une liste de droits d'accès (appelée ACL) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil. Cette précaution un peu contraignante permet de limiter l'accès au réseau à un certain nombre de machines. En contrepartie cela ne résout pas le problème de la confidentialité des échanges.

Remarque : certains adaptateurs permettent de modifier leurs adresses et donc de se faire passer pour d'autres adaptateurs se trouvant sur d'autres postes.

4.2. Etude des protocoles de sécurité liés aux Wi-Fi

De nombreuses évaluations protocolaires ont rythmé la sécurité des réseaux wifi. Les objectifs sont les suivants :

- Assurer la confidentialité des données.
- Permettre l'authentification des clients.
- Garantir l'intégrité des données.

4.2.1. Le protocole WEP (Wired Equivalent Privacy)

Le WEP est un protocole conçu pour sécuriser les réseaux sans fil de type Wi-Fi. Les réseaux sans fil diffusant les messages échangés par ondes radioélectriques, sont particulièrement sensible aux écoutes clandestines. Le WEP tient son nom du fait qu'il devait fournir aux réseaux sans fil une confidentialité comparable à celle d'un réseau local filaire classique.

4.2.1.1. Clé WEP

La clé de session partagée par toutes les stations est statique, c'est-à-dire pour déployer un grand nombre de stations Wi-Fi, il est nécessaire de les configurer en utilisant la même clé de session. Ainsi la connaissance de la clé est suffisante pour déchiffrer les communications. De plus, 24 bits de la clé servent uniquement pour l'initialisation, ce qui signifie que seuls 40 bits de la clé de 64 bits servent réellement à chiffrer et 104 bits pour la clé de 128 bits.

4.2.1.2. Principe du WEP

Le principe du WEP consiste à définir dans un premier temps la clé secrète. Cette clé doit être déclarée au niveau du point d'accès et des clients. Elle sert à créer un nombre pseudo-aléatoired'une longueur égale à la longueur de la trame. Chaque transmission de donnée est ainsi chiffrée en utilisant le nombre pseudo-aléatoire comme masque grâce à un OU Exclusif entre ce nombre et la trame.

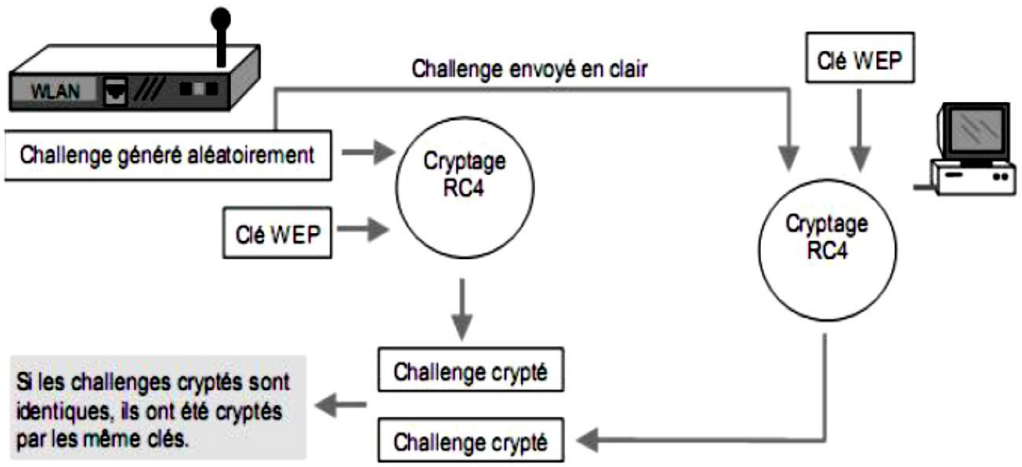


Figure II.5 : le principe du WEP

4.2.2. Le protocole WPA (Wi-FiProtected Access)

Le WPA, développé par l'IEEE, est un autre protocole de sécurisation des réseaux sans fil offrant une meilleure sécurité que le WEP car il est destiné à combler les faiblesses. En effet, le WPA permet un meilleur cryptage de données qu'avec le WEP car il utilise des clés TKIP (Temporal Key Integrity Protocol) qui permet l'authentification des utilisateurs. Ainsi, le WPA permet d'utiliser une clé par station connectée à un réseau sans fil, alors que le WEP lui utilisait la même clé pour tout le réseau sans fil. Les clés WPA sont en effet générées et distribuées de façon automatique par le point d'accès sans fil qui doit être compatible avec le WPA.

De plus, un vérificateur de données permet de vérifier l'intégrité des informations reçues pour être sûr que personne ne les a pas modifiées.

4.2.2.1. Fonctionnement du WPA

WPA, lui est plus évolué avec un nombre IV de 48 bits : ce qui veut dire qu'il prendra beaucoup plus de temps avant que le nombre IV ne soit recyclé. Il faut également noter que dans la manière, WPA est supérieur dans sa méthode de connexion lorsque des utilisateurs sont connectés, ils sont authentifiés par des clés pré-partagées, ou bien par des configurations plus sophistiquées, par une authentification (LDAR, RADIUS).

Une fois qu'un utilisateur est membre d'un réseau, une clef WPA est crée. Périodiquement, WPA va générer une nouvelle clé par utilisateur. Combiné la longueur du nombre IV, ceci rend très difficile le piratage. Sur la transmission de chaque paquet, WPA

ajoute un code de vérification d'intégrité de 4bit(ICV)afin de les vérifier. On peut donc conclure que l'utilisation de WPA est renforcée par rapport à la vérification WEP.

Néanmoins un problème ici reste évident : un attaquant peut intercepter la transmission, modifier le Payload, recalculer le code d'intégrité, et le retransmettre sans que personne ne s'en aperçoive. WPA résout ce problème avec un message d'intégrité 8 bits : un payload crypté et des facteurs dans le calcul de l'ICV réduise fortement les possibilités de forge de paquets (l'usurpation d'adresses IP sources).

4.2.2.2. TKIP (Temporal Key Integrity Protocol)

Protocole permettant le cryptage et le contrôle d'intégrité des données. Ce protocole utilise toujours le RC4 (d'où sa comptabilité avec le WEP) comme algorithme de cryptage avec une clé de 128 bits, par contre l'IV passe à 48 bits. De plus il ya une clé par station (etnon une pour tout le réseau avec le WEP), cette clé est générée et changer automatiquement de façon périodique. Le contrôle d'intégrité des données s'effectue par un code de hachage de 8 octets appelé MIC (Message Integrity Code).Ce code porte aussi les adresses MAC, ce qui évite de modifier ou forger des trames. De plus, il utilise un numéro de séquence sur les paquets, permettant un bon contrôle de séquence.

4.2.3. Le protocole WPA2 /802.11i

La dernière évolution en juin 2004, est la ratification de la norme IEEE 802.11i, aussi appelé WPA2 dans la documentation grand public. Ce standard repend la grande majorité des principes et protocoles apportés par WPA, avec ne différence notoire dans le cas du chiffrement : l'intégration de l'algorithme AES. Les protocoles de chiffrement WEP et TKIP sont toujours présents. Deux autres méthodes de chiffrement sont aussi inclus dans IEEE 802.11i en plus des chiffrements WEP et TKIP :

WRAP (Wireless Robust Authenticated Protocol) s'appuyant sur le mode opératoire OCB(Offset Code Book) de AES, CCMP (Counter with CBC Mac Protocol) : s'appuyant sur le mode opératoire CCM (Counter with CBC-MAC) de AES, le chiffrement CCMP est le chiffrement recommandé dans le cadre de la norme IEEE 802.11i. Il s'appuie sur AES, en utilisant des clés de 128 bits avec un vecteur d'initialisation de 48 bits. Ces mécanismes cryptographiques sont assez récents et peu de produits disponible sont certifiés WPA2. Le recul est donc faible quant aux vulnérabilités potentielles de cette norme. Même si ce recul existe pour l'algorithme AES, le niveau de sécurité dépend de l'utilisation et la mise en œuvre d'AES.

La norme IEEE802.11i définit deux modes de fonctionnement :

- **WPA Personnel :** le mode « WPA personnel » permet de mettre en œuvre une infrastructure sécurisée basée sur le WPA sans mettre en œuvre de serveur

d'authentification. Le WPA personnel repose sur l'utilisation d'une clé partagée, appelées PSK pour Pré-Shared Key, renseignée dans le point d'accès ainsi que dans les postes clients. Contrairement au WEP, il n'est pas nécessaire de saisir une clé de longueur prédéfinie.

En effet, le WPA permet de saisir une phrase secrète, traduite en PSK par un algorithme de hachage.

- **WPA Entreprise :** le mode entreprise impose l'utilisation d'une infrastructure un serveur RADIUS et d'un contrôleur réseau (le point d'accès). Cette solution est actuellement ce qu'il y a de plus sûr en termes de sécurité d'authentification forte. Mais attention, toutefois, rien n'est acquis et il y a fort à parier que cette solution ne restera pas à l'abri des hackers très longtemps.

4.2.3.1. Description technique des clés utilisées par WPA/WPA2

Le protocole WPA/WPA2 utilise une série de clé de cryptage qui sont généralisées et aléatoire tout au long du protocole. De plus, la durée de vie des clés aléatoire est aussi limitée. Cette méthode rend impossible la détection d'une clé WPA/WPA2 contrairement au protocole WEP.

En terme clair, même si on écoute sur un réseau qui utilise l'encryption WPA/WPA2,nous n'augmentons pas nos chances pour autant(c'est techniquement une demi vérité).

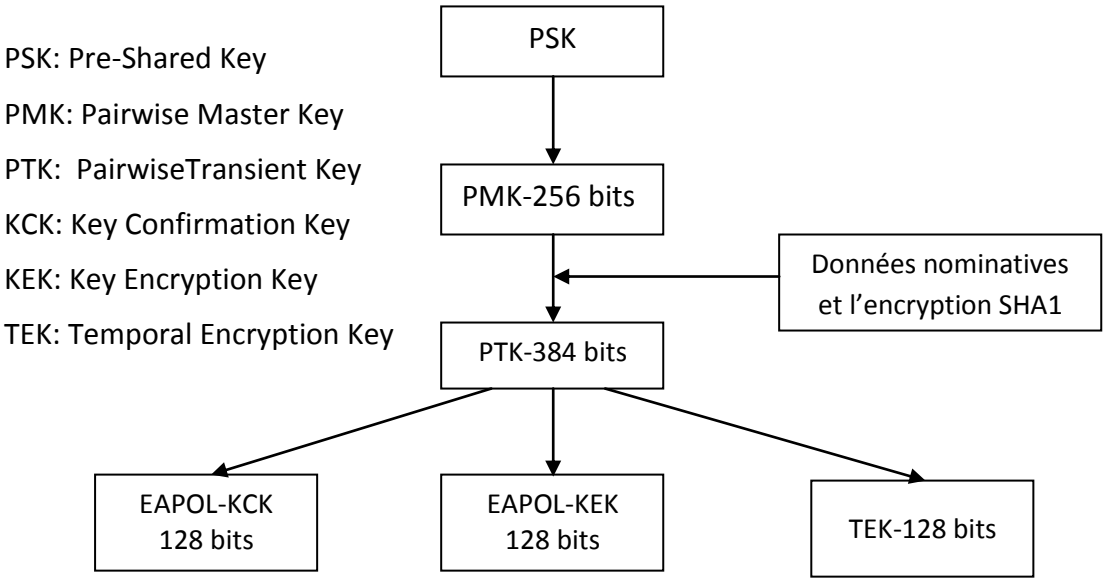


Figure II.6 : Description des clés généralisées et aléatoire

- PSK correspond à la Pre-Shared Key, soit la clé alphanumérique que WPA2 utilise.
- PMK correspond à la PSK.

- PTK correspond à la combinaison de la PMK, suivi de l'adresse MACdu Access Point(Routeur), l'adresse MAC du client, nombre aléatoire côté Acces Point (ANonce), nombre aléatoire côté client (SNonce) le tout crypté avec l'algorithme SHA1.
- La clé PTK est en fait séparée en 3 clés distinctes.
- KCK correspond à la clé de confirmation qui est en fait la clé d'authentification des messages (MIC).
- KEK correspond à la clé qui est utilisée pour encrypter les données lors du Handshake.
- TEK correspond à la clé qui est utilisée pour encrypter les données après le Handshake.

4.2.3.2. Description technique du HandShake WPA/WPA2

Le protocole utilise un 4 Way-HandShake pour pouvoir démarrer une communication sécurisée entre un client et un AP. En effet, c'est le seul moment dans la communication ou il s'échange des informations pour pouvoir se connecter avec succès et c'est la partie la plus importante du protocole et surtout la plus compliquée. Le 4 Way-HandShake se compose de 4 parties :

- Accord au niveau du protocole de sécurité utilise (Agreeing on the security policy)
- Authentification
- Génération des clés et distributions (Key hierarchy and distribution)
- Confirmation (RSNA data condentiality and integrity).

4.3. Les réseaux VPN (réseau privé virtuel)

Pour toutes les communications nécessitant un haut niveau de sécurisation. Il est préférable de recourir à un chiffrement fort des données en mettant en place un réseau privé virtuel.

4.3.1. Concept de VPN

Une solution consiste à utiliser le réseau Wi-Fi comme support de transmission en utilisant un protocole d'encapsulation, c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de réseau privé virtuel le VPN pour désigner le réseau ainsi artificiellement créé. Le système de VPN permet donc d'obtenir une liaison sécurisée à moindre coût. Si ce n'est la mise en œuvre des équipements terminaux.

4.3.2. Fonctionnement

Un réseau privé virtuel repose sur un protocole, appelé protocole «tunneling », il permet aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie. Le terme"tunnel" est utilisé pour symboliser le fait que entre

l'entrée et la sortie du VPN les données sont chiffrées (cryptées) et donc incompréhensible pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN, l'élément chiffrant et déchiffrant les données du coté de l'organisation.

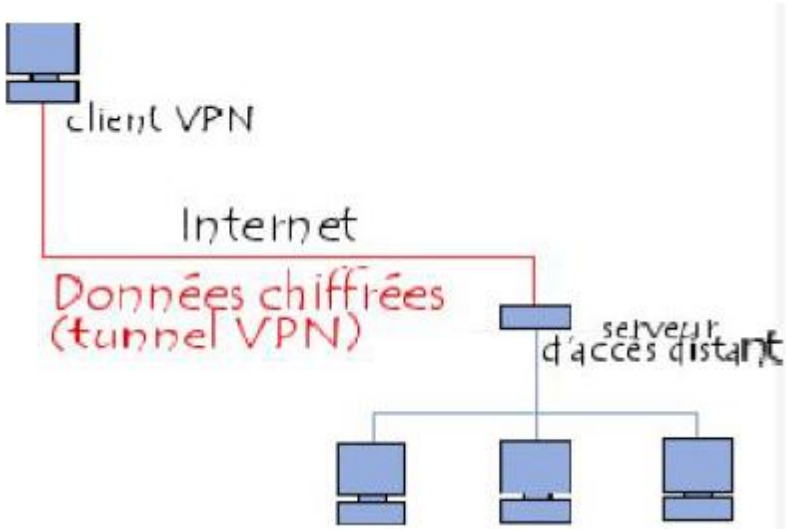


Figure II.7 : le principe du VPN

4.3.3. Le certificat numérique

La sécurité du VPN repose sur l'utilisation de certificat numérique et la plupart des solutions actuelles du marché prévoient de stocker le certificat de l'utilisateur sur le disque dur de la machine, d'autre abrite ces certificats dans un support amovible. Le certificat n'est donc plus associé à une machine mais à l'utilisateur. Lors de l'établissement de la connexion, l'utilisateur doit s'authentifier en introduisant sa clé dans le connecteur USB ou sa carte dans un lecteur, puis en saisissant son code secret.

4.3.4. Les protocoles de tunnelisation

Les principaux protocoles de tunnelisation sont les suivants :

-**PPTP** (point to point tunneling protocol) est un protocole de niveau 2 développé par Microsoft ,3Com, Ascend, US Robotics.

-**L2F** (layer Two Forwarding) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète.

-**L2TP** (layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP et L2F. il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.

-**IPSec** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.

4.4. Le protocole 802.1x

Le protocole 802.1x est une solution de sécurisation d'un réseau mis au point par l'organisme de standardisation IEEE en 2001. Il a pour but de contrôler l'accès à un réseau filaire ou sans fil grâce à un serveur d'authentification. Le standard permet de mettre en relation le serveur d'authentification et le système à authentifier par des séquences par des échanges EAP. Le protocole 802.1x va donc unifier les différentes méthodes d'authentification sous la même bannière : le protocole EAP.

Laprincipale innovation amenée par le standard 802.1x consiste à scinder le port logique, qui est connecté en parallèle sur le port physique. Le premier port logique est dit « contrôle », et peut prendre deux états "ouvert" ou "fermé". Le deuxième port logique est lui toujours accessible mais il ne gère que les trames spécifique à 802.1x. cela permet de gérer le dialogue nécessaire à l'authentification au préalable à une connexion réseau.la connexion initiale est donc limitée à un usage de sécurité qui ouvre ultérieurement le canal des données en cas d'authentification réussie.

802.1x est aussi appelé Port-based Network Access Control, c'est-à-dire qu'il introduit une notion de port contrôlé par l'authentification. Une station ne pourra accéder aux ressources d'un LAN que si elle a été auparavant authentifiée. Le protocole fonctionne à partir de trois éléments :

- **Le client (supplicant) :**c'est le système à authentifier c'est-à-dire l'élément qui désire se connecter sur le réseau.
- **Le contrôleur (point d'accès) :** ou systèmes authentificateur c'est-à- dire l'élément qui va demander l'authentification.
- **Le serveur d'authentification :** ce serveur d'authentification est en général un serveur Radius. Selon la requête du supplicant, ce serveur détermine les services auxquels le demandeur a accès (serveur placé sur le LAN).

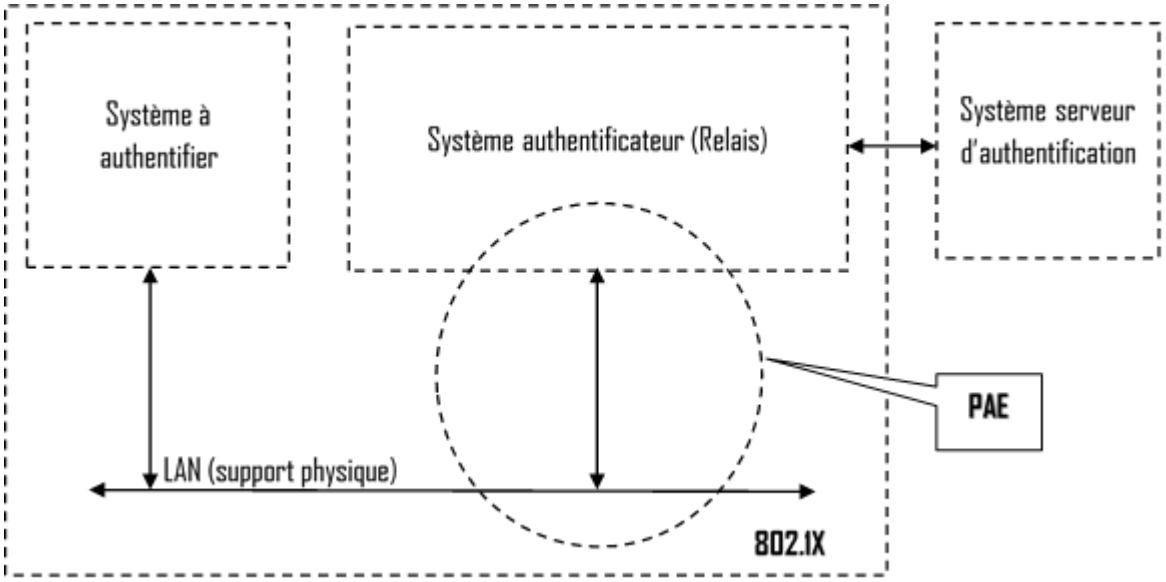


Figure II.8 : les trois entités qui interagissent dans le 802.1x

La communication entre ces éléments fait intervenir différents protocoles suivants un principe de fonctionnement spécifique.

4.4.1. Mécanisme générale

Le supplicant souhaite accèder aux ressources du réseau, mais pour cela il va devoir s'authentifier. Le système authentificateur gère cet ccès via le PAE(Port Access Entity) ; ce PAE est divisé en deux ports, un portcontrôlé (connexion ouverte ou fermée) donnant accès à la ressource en cas de suuccès de l'authentification, et un port non contrôlé (connexion toujours ouverte) servant à l'authentification ou tout autre trafic est rejeté.

Le port contrôlépeut être ouvert ou fermé suivant le contrôle qui a été défini u moyen d'une variable (Auth Controlled Port Control). Cette variable peut prendre trois états :

- **Force Unauthorized** :l'accès au port contrôlé est interdit (connexion toujours ouverte).
- **Force Authorized** : l'accès au port contrôlé est autorisé (connexion toujours fermée).
- **Auto (par défaut)** :l'accès dépend du résultat de l'authentification.

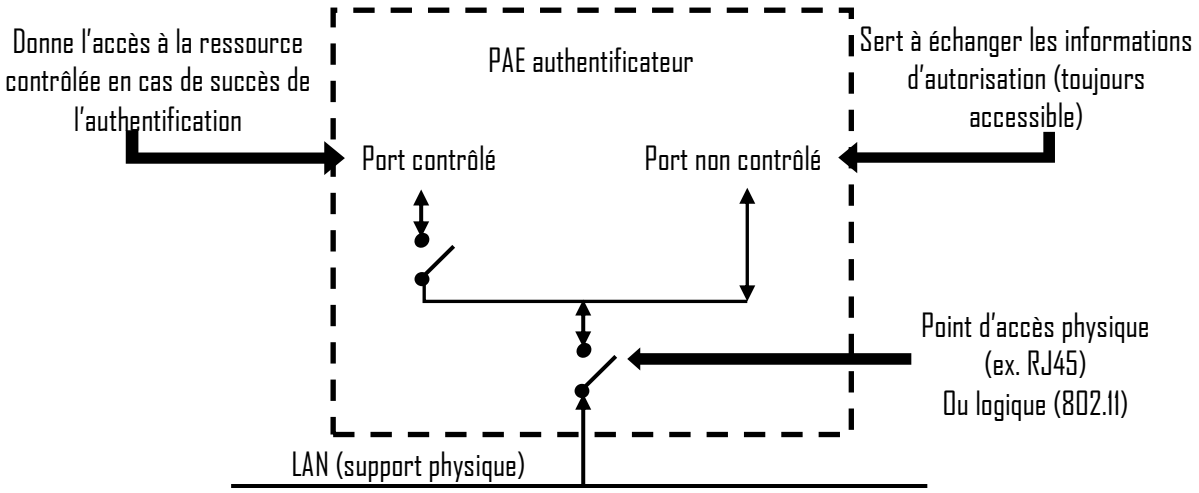


Figure II.9 :PAE

L'utilisation du 802.1x en wifi permettra l'authentification du demandeur, le contrôle d'accès aux bornes et la distribution des clés WEP. Mais attention, il faut que le 802.1x soit bien implémenté sur les différentes machines. Si les implémentations sur les bornes et serveurs sont disponibles, il n'en est pas de même chez les postes clients. Le 802.1x est maintenant de plus en plus intégré avec le système d'exploitation.

4.4.2. EAP (Extensible Authentification Protocol)

EAP est une extension de PPP définie par la RFC 2284. Il permet l'authentification des utilisateurs du lien selon de nombreuses méthodes possible. En somme, on peut dire que l'EAP est une sorte de protocole ''parapluie'' pour l'authentification : il détermine un schéma d'authentification (Kerberos, mot de passe jetable, PKA).

Une extension d'EAP s'appelle EAPOL pour ''EAP Over Lan''. Celle-ci permet de faire transiter des requêtes EAP à travers un réseau LAN en direction d'un serveur compétent qui se chargera de passer la requête EAPOL en EAP.

4.4.2.1. Composition du paquet EAP

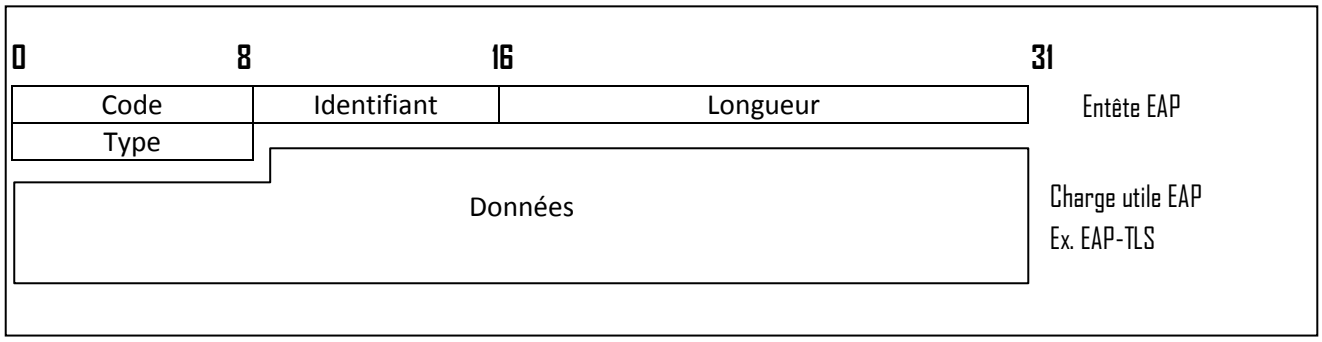


Figure II.10 : Paquet EAP

- **Champ code**

Dans l'en-tête du paquet EAP, le champ code correspond au premier octet.
Il en existe 4 types :

- Request : le système authentificateur émet une requête d'information auprès du supplicant.
- Réponse : le supplicant répond à la requête du système authentificateur.
- Success : le système authentificateur informe le supplicant de l'échec de la demande d'authentification.
- Failure : le système authentificateur informe le supplicant de l'échec de la demande d'authentification.

- **Champ identifiant**

Codé sur 2 octets également, il sert à identifier une session d'authentification. Ce champ change pour chaque nouvelle requête ou réponse. Si une duplication d'une requête doit être faite, l'identifiant ne change pas.

- **Champ longueur**

Codé sur 2 octets, il indique la langueur de l'ensemble du paquet EAP, il prend donc encompte la longueur des données mais aussi des longueurs des autres champs de l'entête comme le type, le code.Ainsi on connaîtra la taille des données utiles même en cas de bourrage par la couche liaison.Champ type

Ce champ est codé sur un octet et définit le type de données qui contient le paquet EAP. Logiquement, requête et réponse des trames de même type.

Nous allons particulièrement nous intéresser au champ type lors des communications requête/réponse.

4.4.2.2. Méthode d'authentification associée à EAP

Le standard 802.1x ne propose pas une seule méthode d'authentification mais un canevas sur lequel sont basés plusieurs types d'authentification. Ainsi, une méthode d'authentification EAP utilise différents éléments pour identifier un client :

- Login/mot de passe.
- Certificats.
- Carte à puce ou calculette.

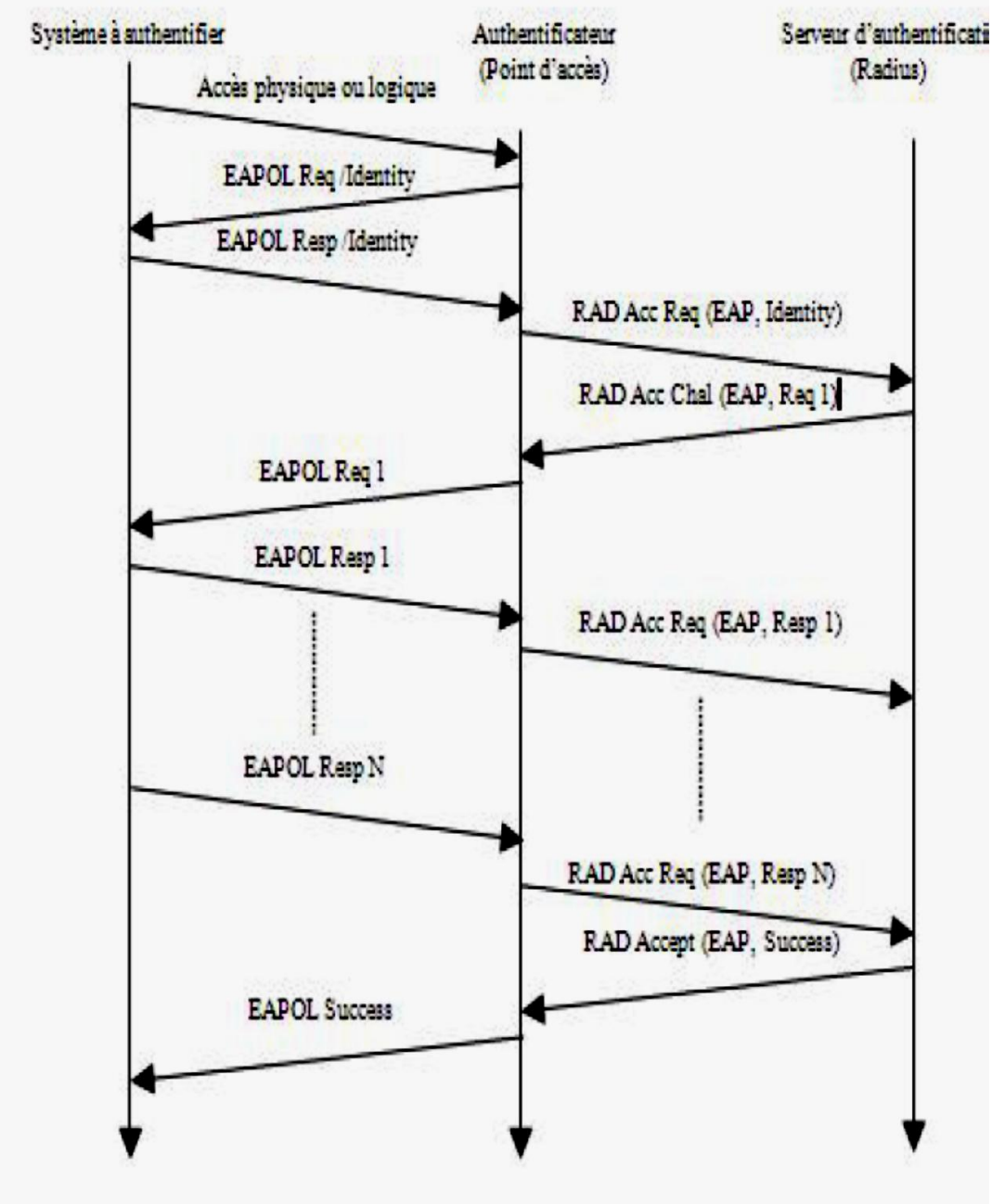


Figure II.11: Séquence d'authentification 802.1x

- **Méthodes basées sur les mots de passes**

LEAP :(Lightweight Extensible Authentification Protocol) c'est la méthode la plus utilisée pour les points d'accès. Il gère la distribution dynamique de clés WEP. C'est aussi à la base une solution propriétaire de Cisco mais qui a aussi été implémenté par la suite par d'autres constructeurs.

EAP-MD5 :(EAP-Message Digest 5) il est souvent utilisé pour les informations d'authentification des clients, par un système basé sur le nom d'utilisateur et le mot de passe. Il n'existe pas d'authentification du serveur. Une machine qui se fait passer pour un

serveur peut ainsi facilement récupérer les authentifiant (login, mot de passe) de la machine qui cherche à s'authentifier.

EAP-SKE :(EAP-Shared Key Exchange) il permet une authentification mutuelle ainsi qu'une itinérance entre les réseaux de plusieurs fournisseurs d'accès Internet.

EAP-SRP : (EAP-Secure Remote Password) il s'agit de l'adaptation du protocole SRP (RFC2945) à l'EAP.

- **Méthodes basées sur les certificats**

EAP-TLS : (EAP-Transport Layer Security) utilise les mécanismes d'authentification à clé publique de TLS. Clients et serveur doivent posséder un certificat. Permet l'authentification mutuelle, l'échange des clés (WEP dynamique ou TKIP), la fragmentation et le réassemblage, la connexion rapide.

EAP-TTLS : méthode du tunnel TLS. Fournit une séquence d'attributs inclus dans le message. En incluant un attribut de type RADIUS, EAP peut fournir les mêmes

Fonctionnalités que PEAP. Cependant, si un mot de passe RADIUS ou CHAP est encapsulé, il est chiffré par TLS. Cette méthode est moins utilisée que PEAP qui rend les mêmes services.

PEAP : (Protocol EAP) authentification sans certificat. Ajoute une couche TLS sur EAP, permet d'authentifier le serveur au client. Offre les services d'authentification (impossible de falsifier ou insérer des messages EAP), de chiffrement, d'échange de clé (WEP dynamique ou TKIP), fragmentation et réassemblage, reconnexion rapide.

PEAP Microsoft : supporte l'authentification du client via MS-CHAP v2 uniquement réduisant ainsi le champ d'utilisation au domaine NT et ADS.

- **Méthodes basées sur les cartes à puces**

EAP-SIM : (EAP-Subsciber Identity Module) utilisé pour les points d'accès public (hot spot), utilise la carte à puce SIM du GSM, permet la mise en place de la facturation.

EAP-AKA :(EAP-Authentification and Key Agreement) utilise le système d'authentification de la carte SIM de l'UMTS, il est compatible avec le GSM.

4.5. Protocole Radius

4.5.1. Présentation

RADIUS (Remote Authentification Dial In User Service) est un protocole d'authentification client/serveur habituellement utilisé pour l'accès à distance, défini par la RFC 2865. Ce protocole permet de sécuriser les réseaux contre des accès à distance non autorisés. Ce protocole est indépendant du type de support utilisé.

Le protocole Radius repose principalement sur un serveur (serveur Radius), relié à une base d'identification (fichier local, base de données, annuaire LDAP, etc.)et un client Radius, Appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. Le mot de passe servant à authentifier les transactions entre le client Radius et le serveur Radius est chiffré et authentifier grâce à un secret partagé.

4.5.2. Principe de fonctionnement

Le fonctionnement de Radius est basé sur un scénario proche de celui-ci :

- Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance.
- Le NAS achemine la demande au serveur Radius.
- Le serveur Radius consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur Radius retourne ainsi une des quatre réponses suivantes :

  - **ACCEPT :** l'identification a réussi.
  - **REJECT** : l'identification a échoué.
  - **CHALLANGE :** le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un «défi».
  - **CHANGE PASSWORD :** le serveur Radius demande à l'utilisateur un nouveau mot de passe.

Suite à cette phase d'authentification débute une phase d'autorisation ou le serveur retourne les autorisations aux utilisateurs.

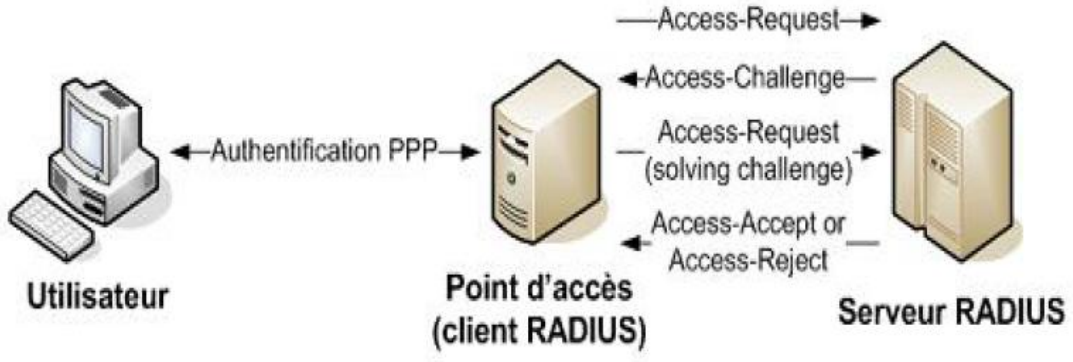


Figure II.12: Principe de fonctionnement du RADIUS

- **Paquets Radius**

Un paquet Radius est inclus dans un et un seul paquet UDP. Le schéma suivant représente un paquet Radius standard, les unités étant exprimé es en octets :

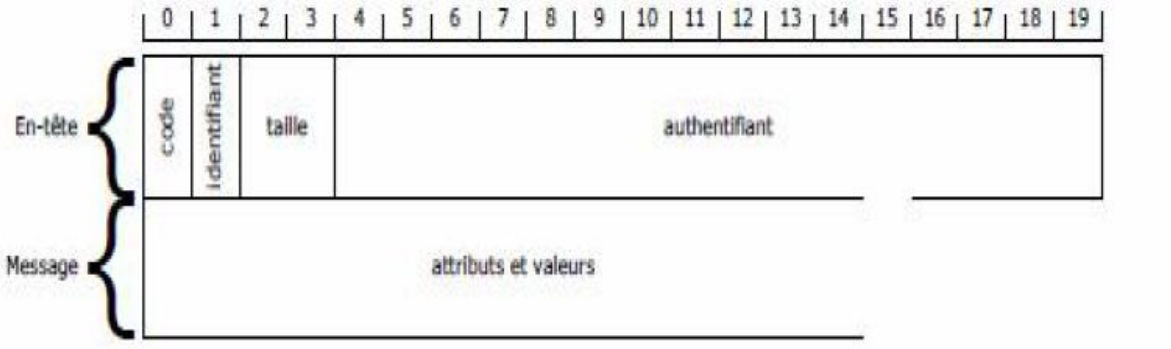


Figure II.13 : Paquet Radius

Le code : identifie le type de message.

Code	Description
Access-Request	Demande accès à un service
Access-Accept	Réponse favorable à la demande du client
Access-Reject	Réponse négative au client
Accounting-Request	Demande les informations d'authentification
Accounting-Reponse	Informations d'authentification
Access-Challenge	Sollicite des informations supplémentaires pour l'autorisation du client

Tableau II.2 : Description du champ code.

- **Identifiant** : permet de reconnaitre les messages (requêtes et réponses) d'une même session d'authentification.
- **Longueur (taille)** : définie la longueur de la trame.
- **Authentificateur** : permet au client d'authentifier la réponse de serveur Radius et de protégé les mots de passes. Il contient également la méthode d'authentification à utiliser avec le client.
- **Attributs** : ce champ est utilisé pour véhiculer toutes les informations nécessaires, il a pour format :

Type	Longueur	Valeur

Figure II.14: formats des attributs Radius

5. Conclusion

Le WEP avait à sa création pour but avoué (prétention) de proposer une solution de confidentialité équivalente au réseau filaire en s'appuyant uniquement sur un algorithme réputé sûr : RC4. A partir de cette certitude infondée, la simplicité d'utilisation a alors été privilégiée pour promouvoir le développement de ce protocole. Cette « négligence » de la sécurité n'a pas été sans conséquence. Sa conception on ne l'a constaté pas a été exemple de failles.

Le développement exponentiel de l'Internet a chamboulé les données du point de vue de la sécurité des réseaux. La découverte constante, au cours de ces dernières années, de ces nombreuses failles devrait mettre un terme à l'utilisation du protocole WEP qui est tout bonnement à proscrire en entreprise et à utiliser avec parcimonie en environnement domestique. C'est pour cela qu'il est progressivement remplacé par des solutions qu'on croyait plus performantes telles que le 802.1x, WPA et WPA2, à la fin des comptes on constate que chaque protocole a ses faiblesses.

Donc dans notre prochain chapitre on tient à analyser et étudier les failles et les attaquesde ces protocoles de sécurisation àfin d'améliore et d'assurer la sécurité du réseau Wi-Fi.

Chapitre III

1. Introduction

Dans ce chapitre, nous présentons une étude détaillée des vulnérabilités des protocoles de sécurité que nous avons passés en revue au chapitre précédent. Ainsi, dans ce dernier nous concentrerons sur les faiblesses de chaque protocole et les types d'attaques qu'il est possible de monter en tirant profit de ces vulnérabilités.

Alors nous détaillons les attaques relatives à chaque protocole de sécurité Wi-Fi.

Mais Avant d'aborder les failles de sécurité des protocoles que nous avons présentés au chapitre précédent (WEP, 802. l x, ...), nous présentons dans cette section la première ligne de défense préliminaire des réseaux Wi-Fi.

2. Faiblesses et contournements des mécanismes préliminaires de sécurité

2.1. Utilisation d'ESSID fermés

Afin d'accéder à tout réseau Wi-Fi, il est nécessaire de connaître son identifiant, c'est-à-dire son ESSID. Au début du développement des réseaux Wi-Fi, l'ESSID était transmis en clair périodiquement par le point d'accès dans des trames balises (beacon frames). De cette façon, il était très facile de s'associer avec n'importe quel réseau Wi-Fi, en récupérant l'ESSID à l'aide d'un renifleur (sniffer) qui permet de récupérer tout le trafic réseau qui circule. De nombreux outils de surveillance et d'analyse de trafic pour les réseaux sont disponibles sur Internet. Parmi les plus célèbres, citons Kismet, AirTraf, Mogne et Wifi Scanner.

Afin de parer à cette faiblesse, une nouvelle fonctionnalité a été mise en place. Elle permet d'éviter que l'ESSID ne soit transmis en clair sur le réseau. Ce mécanisme, appelé Closed Network, ou réseau fermé, interdit la transmission de I'ESSID par l'intermédiaire de trames balises. Ainsi, pour s'associer à un réseau Wi-Fi implémentant un ESSID fermé, il est indispensable d'entrer l'ESSID à la main. Toutefois, même avec la mise en place d'un tel mécanisme, l'ESSID est transmis quand même en clair durant la phase d'association d'un client légitime à son point d'accès. Ainsi, pour contourner ce mécanisme de défense préliminaire, il suffit d'écouter le trafic réseau durant la phase d'association d'un client légitime et de récupérer l'ESSID en clair.

2.2. Filtrage par adresse MAC

Outre l'utilisation de l'ESSID fermé, les points d'accès permettent d'établir un filtrage par adresse MAC, ou encore des listes de contrôle d'accès (ACL). Ainsi, le point d'accès autorise uniquement les stations ayant une adresse MAC qui figure dans la liste ACL.

La première vulnérabilité de ce filtrage est qu'il s'agit d'un mécanisme optionnel, rarement activé dans les faits. Outre cette vulnérabilité, le filtrage par adresse MAC peut être facilement contourné, en usurpant l'adresse MAC d'un hôte légitime du réseau cible.

En effet, il suffit à un attaquant d'écouter le trafic du réseau cible et d'identifier les adresses MAC des hôtes légitimes, car elles transitent en clair. Une fois qu'un client cible est

identifié par l'attaquant, il suffit alors d'usurper son adresse MAC (quasiment toutes les cartes sans fil permettent le changement d'adresses MAC) et de s'associer au point d'accès.

Avant de pouvoir s'associer au point d'accès, il faut soit attendre que le client légitime se déconnecte du réseau, soit l'obliger à le quitter.

Pour obliger un client légitime à se désassocier du réseau auquel il est rattaché, il suffit d'usurper l'adresse MAC du point d'accès et inonder le client victime de trames de désassociation. Une fois le client légitime désassocié, il est possible de s'associer au réseau à sa place sans problèmes.

3. Les failles du protocole WEP

3.1. Les faiblesses conceptuelles du protocole WEP

Le protocole WEP constitue le premier protocole de sécurité des réseaux Wi-Fi. Toutefois, depuis sa sortie ce standard n'a cessé de créer la polémique autour de lui, à cause de plusieurs défaillances et vulnérabilités inhérentes à sa conception.

L'ensemble des mécanismes de sécurité du WEP comportent des faiblesses. Les failles ne sont pas tant liées à l'algorithme de chiffrement RC4 qu'à la façon dont les mécanismes sont mis en œuvre, comme le vecteur d'initialisation ou le contrôle d'intégrité. Chacun de ces mécanismes comporte des défauts, qui ajoutés les uns aux autres, permettent de casser le WEP.

3.1.1. Mécanisme défaillant de génération des clés WEP : RC4

Le standard comporte une faille profonde, qui est intrinsèquement liée à l'utilisation de l'algorithme de chiffrement RC4. La clé utilisée par RC4 dans WEP est une concaténation de l'IV (Initialization Vector) et de la clé secrète partagée. Il existe des classes de clés RC4 faibles, dans lesquelles un motif dans les trois premiers octets de la clé engendre un motif équivalent décelable dans les premiers octets de la suite chiffrante, ou KeyStream (KS).

En effet, parmi les IVs utilisés pour composer la clé RC4 du WEP, certains ont des valeurs dites résolvantes. Environ 60 IVs ayant des valeurs résolvantes suffisent à retrouver un octet du secret partagé (PSK).

Cette faille facilite la déduction de la clé par des attaques statistiques, en interceptant le maximum de trames chiffrées avec une classe spécifique d'IV. Le KeyStream obtenu avec ces IV révèle des informations sur la clé secrète PSK. En traitant suffisamment de paquets chiffrés, un attaquant peut la déterminer complètement. C'est cette faille qui est exploitée par l'outil AirSnort pour casser des clés WEP.

3.1.2. Collision des vecteurs d'initialisations

Outre la faiblesse du mécanisme de génération des clés avec RC4, WEP utilise des vecteurs d'initialisations de 24 bits pour réaliser une différenciation de chiffrement (sans IV, toutes les trames seront chiffrées avec la même clé), vu que c'est la même clé secrète de 40 ou 104 bits qui est utilisée par toutes les stations de la même cellule (les clés WEP de 40 bits ne sont quasiment plus employées actuellement).

L'utilisation des vecteurs d'initialisation telle qu'elle est réalisée avec le chiffrement WEP présente deux vulnérabilités. D'abord, la taille de ces vecteurs d'initialisation, qui n'est que de 24 bits. En effet, la clé secrète partagée (PSK) définie dans le WEP est statique et ne change pratiquement jamais. L'IV est concaténé avec cette clé de façon à créer des flux de chiffrement différents. L'IV étant sur 24 bits, il peut y avoir jusqu'à 2^{24}, soit exactement 16777216 clés différentes. Après les 2^{24} transmissions chiffrées, il y aura une réinitialisation des IVs et la même séquence d'IV sera réutilisée, causant une collision (2 trames chiffrées avec la même clé WEP : même IV et même PSK). Ainsi, il y aura une réutilisation des mêmes flux de chiffrement, puisqu'il s'agit des mêmes IVs et de la même clé secrète partagée qui ne change pas.

La seconde vulnérabilité relative à l'utilisation des vecteurs d'initialisation dans WEP est la transmission en clair du vecteur d'initialisation utilisé pour le chiffrement. En effet, il suffit d'écouter le trafic pendant un certain temps, pour se constituer progressivement un ensemble de trames chiffrées avec le même IV et donc la même suite chiffrante KS.

Une première solution qui pourrait venir à l'esprit pour corriger le problème de collision des vecteurs d'initialisions est d'augmenter la taille des IV. Toutefois, cette dernière n'est pas une solution fiable, vu qu'un réseau modérément occupé peut épuiser l'espace des IVs. Une seconde solution serait de changer la clé secrète partagée, à toutes les 2^{24}trames, afin d'éviter la collision. Malheureusement, le protocole WEP tel qu'il a été conçu ne comprend aucun mécanisme central de mise à jour de cette clé secrète.

3.1.3. Contrôle d'intégrité inadapté

Généralement en sécurité, un contrôle d'intégrité est assuré par des fonctions non linéaires, à sens unique et sans brèche tel que MD5.

Ces fonctions de très performantes permettent, à partir d'un message donné, de générer une empreinte quasiment irréversible. Une des principales propriétés de ces fonctions est certainement la non-linéarité.

Le contrôle d'intégrité dans WEP est réalisé par la fonction CRC32. Le CRC sert plutôt à la détection d'erreur, mais n'a jamais été considéré crypto-graphiquement sûr pour le contrôle d'intégrité, principalement à cause de sa linéarité.

3.1.4. Clé unique : taille faible et gestion statique

Le standard d'origine définit une taille de clé de 40 bits ou 104 bits. Cette clé étant d'une taille insuffisante pour contrer les attaques par force brute.

Outre l'insuffisance de la taille de la clé, le protocole WEP ne prévoit pas de mécanisme de mise à jour ou de génération et de distribution dynamique de la clé secrète partagée. En effet, la gestion des clés est statique et manuelle, une seule clé secrète est partagée par toutes les stations du réseau et le point d'accès.

3.2. Les attaques contre le protocole WEP

Plusieurs études ont révélés les défaillances du WEP et les cryptanalyses s'en sont donné à cœur joie à monter des attaques contre ce protocole, qui ne satisfait en rien ses objectifs de sécurité. Le tableau suivant montre la chronologie de la mort du WEP.

Date	Description
Septembre 1995	Vulnérabilité potentielle dans RC4 (Wagner)
Octobre 2000	Première publication sur les faiblesses du WEP : Unsafe at any key size; An analysis of the WEP encapsulation(Walker)
Mai 2001	An inductive chosen plaintext attack against WEP/WEP2(Arbaugh)
Juillet 2001	Attaque bit flippingsur le CRC – Intercepting Mobile Communications : The Insecurity of 802.11(Borisov, Goldberg, Wagner)
Août 2001	- Attaques FMS – Weaknesses in the Key Scheduling Algorithm of RC4(Fluhrer, Mantin, Shamir) - Sortie d'AirSnort
Février 2002	Optimisation de l'attaque FMS
Août 2004	- Attaque de KoreK (IVs uniques) - sortie de chopchop et chopper
Juillet/Août 2004	Sortie d'Aircrack (Devine) et WepLab (Sanchez) implémentant l'attaque de KoreK.

Tableau III.1 : la chronologie de la mort du WEP

3.2.1. Attaque par force brute

Puisque le protocole WEP base sa sécurité sur le secret de la clé utilisée, une des attaques les plus simples à mettre en œuvre est certainement l'attaque par force brute. En effet, avant de passer à des attaques utilisant des outils sophistiqués d'attaques statistiques, un attaquant peut tenter de casser la clé WEP en opérant des attaques par force brute. Le principe le plus simple est d'essayer toutes les clés binaires possibles pour une clé WEP donnée. Il existe une panoplie d'outils implémentant des attaques par force brute, les plus performants étant WepLab et WepCrack.

Pour monter des attaques par dictionnaire, l'attaquant devra avoir une connaissance du matériel déployé dans le réseau cible. En effet, il faut tenir compte de la méthode utilisée pour la transformation de la clé WEP en clé binaire. Ces méthodes sont au nombre de deux : la première et la plus commune se base sur l'utilisation de la fonction MD5, la seconde, moins fréquente, utilise la méthode «Nullterminatedraw ASCII». Les meilleurs outils permettant de mettre en œuvre des attaques par dictionnaires sur WEP sont WepLab et WepAttack.

Les attaques par force brute et par dictionnaires sont des attaques purement passives dans le sens où elles n'impliquent ni altération du contenu des messages, ni déni de service, ni de rejoue de paquets dans le réseau cible ou encore de mascarade, comme dans le cas des attaques de l'homme au milieu.

3.2.2. Attaque inductive à texte clair connu: injection de trafic

Il s'agit d'une attaque active mise en place par W.Arbaugh. Cette attaque se base sur l'injection de trafic dans le réseau. En effet, elle tire profit des faiblesses de WEP au niveau du chiffrement en mode flux utilisé avec RC4, ainsi que des collisions d'IV et de l'absence d'un mécanisme anti rejoue (deux trames avec le même IV peuvent se trouver sur le réseau). Cette attaque se décompose en trois phases :

- **Phase 1:** Récupération des n premiers octets de la suite chiffrante (KeyStream).
- **Phase 2:** Découverte de la totalité de la suite chiffrante (KeyStream).
- **Phase 3:** Construction de la table de correspondance

Une fois que l'attaquant dispose d'un KeyStream complet pour un IV particulier, il devient possible d'injecter au réseau des paquets chiffrés en utilisant ce même IV. Au bout de cette dernière phase, l'attaquant disposera d'une table de correspondance complète, entre IV et Key Stream correspondant. À la fin de cette attaque, l'attaquant sera dans la possibilité de déchiffrer tous les paquets transitant sur le réseau, vu qu'il dispose de tous les KeyStream (2^{24}KeyStream). La seule condition pour empêcher cette attaque est la mise en place d'un mécanisme de changement de clés secrètes PSK permettant de mettre à jour la clé au plus à tous les 2^{24} paquets.

3.2.3. Attaque bit flipping sur le CRC (Bit Flip)

L'attaque bit flipping publié par Borisov, Goldberg et Wagner tire profit de la faille conceptuelle de WEP inhérente au contrôle d'intégrité qui se fait au moyen de la fonction CRC32. Il s'agit d'une attaque active, vu qu'elle vise à apporter des modifications illicites dans les trames 802.11 du réseau Wi-Fi cible.

3.2.4. Attaque FMS

Une des attaques les plus célèbres pour craquer la clé WEP est certainement l'attaque FMS, du nom de ses créateurs Fluhrer, Mantin et Shamir. L'attaque FMS est une attaque

passive dans le sens où elle n'influe pas sur le comportement du réseau cible. En effet, FMS est une attaque crypto-analytique statistique apparue en 2001. FMS a d'abord été mise en œuvre dans l'outil WepCrack, puis dans AirSnort.

Cette attaque exploite deux failles majeures :

- Faiblesses RC4: l'utilisation de certains IVs, dits faibles, permettent de révéler quelques bits de la clé secrète partagée. Ceci en plus d'une faiblesse au niveau de l'algorithme KSA, implémenté dans RC4. Cette dernière, dite faiblesse d'invariance, permet de déterminer les octets de clé les plus probables, parmi les octets du flux de sortie de RC4.
- Les quatre premiers octets du flux de sortie de RC4 sont toujours prévisibles, car ils contiennent l'entête du protocole SNAP.

3.2.5. Attaque ChopChop de KoreK

Cette attaque est basée sur la preuve de concept publiée par un pirate informatique surnommé KoreK. Cette attaque appelée ChopChop, ou encore Chopper (Découpeur) peut décrypter un paquet chiffré avec le protocole WEP sans avoir connaissance de la clé. Il s'agit d'une attaque cryptanalytique statistique, qui contrairement à l'attaque FMS, permet de casser une clé WEP avec quelques centaines de milliers de paquets.

Contrairement à l'attaque FMS et l'attaque inductive d'Arbaugh, l'attaque ChopChop de KoreK ne dépend pas des IV faibles et est plus performante, vu qu'elle permet de déchiffrer n'importe quel paquet indépendamment de la classe d'IV employée pour son chiffrement.

Ainsi, avec cette attaque il n'est plus nécessaire d'analyser des millions de paquets, ni de détecter les IVs faible, afin de casser la clé WEP. D'ailleurs, c'est ce qui fait de ChopChop, l'attaque la plus innovante et la plus performante du moment, vu qu'elle tire profit de quasiment toutes les attaques précédentes. Tous les experts de la sécurité des réseaux sans fil sont unanimes sur la mort de WEP depuis la sortie de cette attaque.

4. Les failles du protocole 802.1x

4.1. Les faiblesses conceptuelles du protocole IEEE 802.1x

Le protocole 802.1x est un protocole d'authentification utilisé au départ dans les réseaux filaires commutés qui a été ensuite intégré au mécanisme de sécurité des réseaux Wi-Fi. L'utilisation de ce protocole vient répondre principalement à la problématique d'authentification centralisée et de distribution dynamique des clés de chiffrement dans ce type de réseaux. Ainsi, 802.1x vient encadrer l'authentification dans les réseaux Wi-Fi.

Toutefois, certaines spécificités des réseaux Wi-Fi ne sont pas prises en compte par ce protocole.

4.1.1. Authentification à sens unique

Dans l'architecture 802.lx, les points d'accès sont considérés à tort comme des entités de confiance. Cette façon de faire provient de l'origine d'utilisation de ce protocole dans les réseaux filaires, où les commutateurs étaient l'équivalent des points d'accès dans les réseaux Wi-Fi. Toutefois, les commutateurs étaient enfermés dans des salles informatiques sécurisées et pour y accéder il fallait s'y connecter physiquement, alors que dans les réseaux Wi-Fi, les points d'accès peuvent être localisés n'importe où.

De ce fait, le protocole 802.lx ne fournissait pas une authentification mutuelle entre les clients et le point d'accès. Toute la sémantique du protocole se basait sur une authentification unilatérale allant du point d'accès vers le client.

4.1.2. Absence de synchronisation entre les machines à état

Les machines à état de 802.11 et 802.1x ne sont pas corrélées, vu qu'elles ont été conçues de façon complètement indépendante. Ce manque de synchronisation laisse la porte ouverte à bon nombre d'attaques qui utilisent cette défaillance afin de détourner des sessions.

4.1.3. Manque d'intégrité dans les messages de contrôle 802.1x

Outre l'authentification mutuelle et l'absence de synchronisation entre les machines à état du client et du point d'accès, plusieurs messages de signalisation de 802.1x sont dépourvus de mécanismes de vérification d'intégrité. En particulier, les messages Disassociate, Deauthenticate, EAP Success et EAP failure ne sont pas protégés. De ce fait, il est possible de dissocier et dés authentifier les clients légitimes ou même de monter des attaques DoS contre eux en les inondant de ces messages.

4.2. Les attaques sur le protocole 802.1x

Les attaques sur le standard 802.1 x sont toutes des attaques du type homme au milieu, mais qui s'opèrent à des niveaux différents. Le but ultime de ces attaques est de s'intercaler dans les connexions entre les clients 802.11 et le point d'accès et donc de subtiliser la session sécurisée établie entre les pairs légitimes.

4.2.1. Attaque de l'homme au milieu sur la couche physique

Cette attaque consiste à mettre en place un point d'accès pirate, dont le rôle est de brouiller le signal émis par un point d'accès légitime, en émettant un signal fort et clair. Ce signal devrait être bien supérieur à la puissance de rayonnement autorisée sur la majorité des réseaux sans fil déployés, soit 1 Watt. Le brouillage peut être réalisé à l'aide d'un dispositif de brouillage spécifique ou en inondant de trafic factice le canal du point d'accès de trafic factice. Il existe une panoplie d'utilitaires permettant de générer un tel trafic, citons FakeAP ou File2air.

Le brouillage aura pour incidence de forcer les hôtes du point d'accès victime de se dissocier de leur WLAN, pour s'associer avec le point d'accès pirate, dont la puissance de rayonnement est relativement élevée.

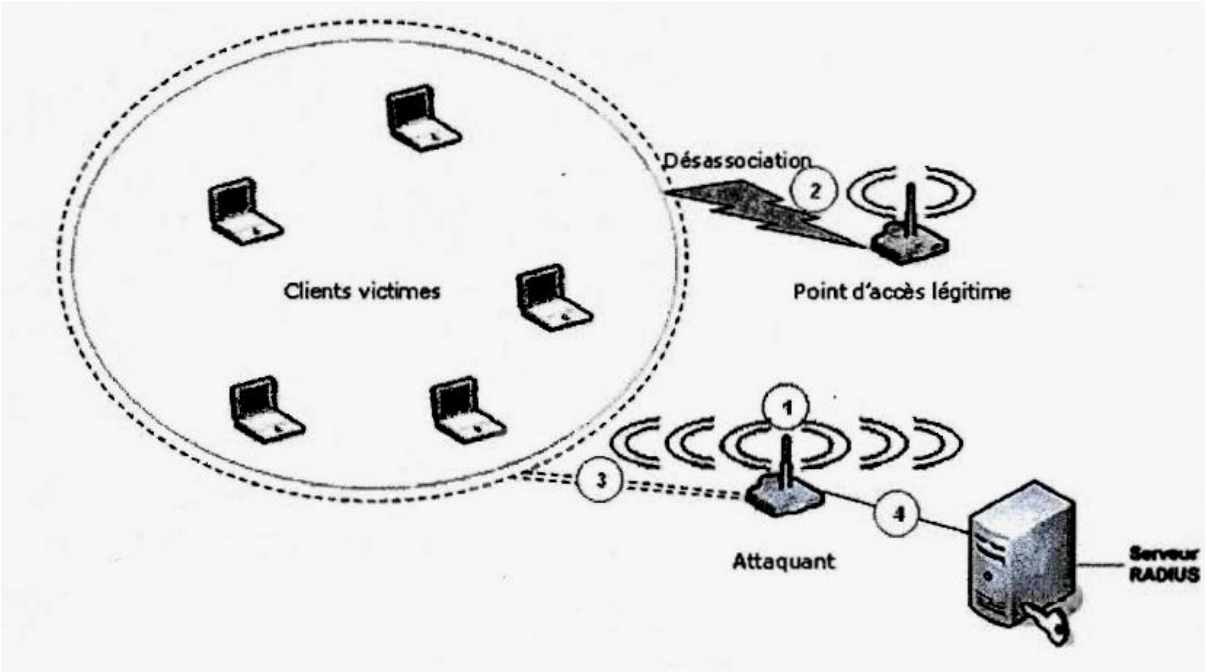


Figure III.1 : Attaque de l'homme au milieu sur la couche

Étapes de l'attaque :

1- Brouillage du signal du point d'accès légitime.
2- Déassociation des clients de leur point d'accès légitime
3- Association avec les clients victimes
4- Authentification contrefaite avec serveur RADIUS malveillant

Il est à signaler que ce type d'attaques n'est faisable que contre les systèmes d'authentification 802.lx unilatéraux, utilisant une méthode d'authentification unilatérale, notamment, EAP-MD5.

4.2.2. Attaque de l'homme au milieu sur la couche de liaison de données

Cette attaque, également appelée détournement de sessions, consiste à détourner une session sécurisée établie entre un point d'accès et un client. Elle se déroule comme le montre la figure suivante :

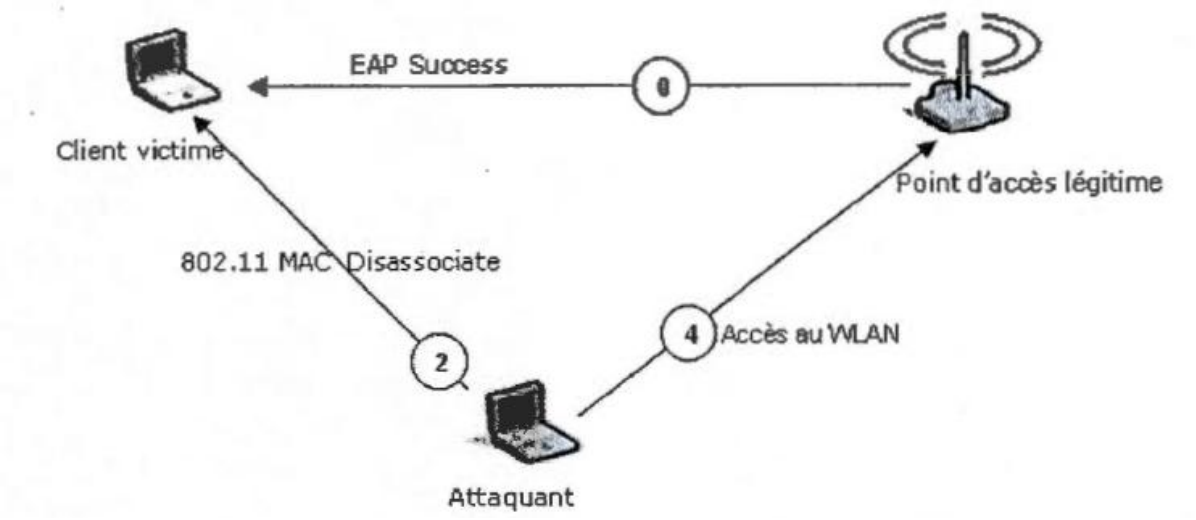


Figure III.2 : Attaque de l'homme au milieu sur la couche de liaison de données

Cette attaque est possible principalement à cause des éléments suivants :

- Absence de mécanisme d'intégrité dans les messages de signalisation 802.11, tel que le message MAC 802.11 Désassociât. Ceci a pour incidence de permettre à l'attaquant de forger son propre message Désassociât et l'envoyer à l'hôte victime de son choix. La faiblesse du mécanisme d'intégrité est valable également pour les messages de contrôle 802.1x tels que les messages EAP-SUCCESS et EAP-FAILURE qui viennent conclure toute procédure d'authentification EAP.
- Absence de synchronisation entre les machines à état du client et du point d'accès.

4.2.3. Attaque de l'homme au milieu sur SSL: Phishing

Cette attaque concerne le cas où le réseau sans fil a recours à une authentification utilisateur 802.1x fondée sur une interface Web (page de login Web), comme le font classiquement les points d'accès publics sans fil, au moyen du protocole de sécurité SSL.

Cette attaque se base sur la technique du Phishing, qui par ailleurs n'est pas spécifique au protocole 802.1x.Il est très facile de monter ce genre d'attaques, en s'aidant d'outils comme AirSnarf.

Finalement, un attaquant peut combiner les attaques de l'homme au milieu explicitées ci-dessus (de la couche physique, liaison de données et sur le protocole SSL), afin de maximiser les chances de réussite de son attaque.

En guise de conclusion sur les failles du protocole 802.1x, nous pouvons dire qu'outre les problèmes d'authentification mutuelle, de manque de synchronisation des machines à état et d'absence de mécanisme d'intégrité des messages de contrôle, le protocole 802.lx

ne résout pas les problèmes de confidentialité liés au WEP. Ainsi, il ya eu un empilement de protocoles malheureusement accompagné d'un empilement de failles, avec pour résultat que les réseaux Wi-Fi ne sont pas plus sécurisés.

5. Les failles de la norme WPA/WPA2

Depuis la sortie de WPA puis de WPA2,il y a eu découverte de deux failles sur trois mécanismes de sécurité.

5.1. Attaque par dictionnaire sur la clé PSK

Cette attaque cible la clé PSK qui, nous le rappelons est l'un des modes de génération des clés de chiffrement et d'intégrité introduits par WPA. En effet, la clé PSK est la clé pré-partagée à partir de laquelle toutes les autres clés sont dérivées. La clé PSK est utilisée comme alternative à l'établissement de clés de chiffrement et d'intégrité avec le protocole 802.1x.

L'attaque par dictionnaire sur la clé PSK a été découverte en novembre 2003. Une clé PSK est d'une taille de 256 bits, une longueur relativement importante. Toutefois, vu que personne ne pourra retenir une chaîne de mot de passe de cette taille, la clé PSK est générée à partir d'une phrase de passe *(Passphrase)* ASCII, d'une taille acceptable (du point de vue de l'utilisateur). Cette phrase de passe est entrée par l'utilisateur.

Ainsi, l'attaquant peut tenter une attaque par dictionnaire sur la valeur de cette clé PSK. Une fois la clé PSK connue, l'attaquant peut dériver la clé PTK et toutes les clés qui en découlent (Rappelons qu'à partir de la clé PTK seront générées les différentes clés de chiffrement TKIP et d'autres clés d'intégrité).

5.2. Attaques DoS sur l'échange 4 Way-Handshake

L'attaque DoS sur l'échange 4-Way Handshake est l'attaque la plus célèbre et la plus percutante que WPA2 ait connu depuis sa sortie. En effet, le premier message de l'échange 4Way-Handshake n'est pas authentifié. De plus, le client conserve chaque premier message jusqu'à réception du troisième message (signé), laissant le client vulnérable à une saturation de mémoire. L'attaque exploite cette faille en inondant le client avec des messages contrefaits (ouverture de plusieurs sessions simultanées), en usurpant l'identité d'un point d'accès légitime. Cela aura pour incidence la saturation de l'espace mémoire du client et le blocage du protocole. Ceci en plus du blocage de l'échange avec le point d'accès légitime: impossible d'établir la clé PTK.

6. Conclusion

Ce chapitre constitue une étude des failles des protocoles de sécurité Wi-Fi. Nous avons ainsi parcouru, protocole par protocole, la quasi-totalité des attaques qu'il est possible de monter en tirant profit des failles conceptuelles de ces protocoles.

En guise de synthèse, nous pouvons dire que WEP est définitivement à éviter. En effet, la durée de vie d'une clé de 128 bits est inférieure à 1 h avec les nouveaux outils, tel qu'AirCrack.

Les points d'accès ne supportant pas WPA doivent impérativement implémenter un mécanisme de rotation des clés au moins à toutes les heures, afin de minimiser les risques liés à WEP. La norme de transition WPA s'impose comme solution pour les points d'accès ne supportant pas le standard WPA2 .Finalement, nous pouvons affirmer que WPA2 est certainement la solution la plus robuste et la plus pérenne. Toutefois, le mode PSK ne garantit pas la confidentialité entre utilisateurs d'une même cellule BSS. De plus, les attaques DoS de bas niveau sont toujours possibles.

Le prochain chapitre s'inscrit dans la suite logique des chapitres précédents en abordant l'une des différentes architectures de sécurité Wi-Fi et proposant une nouvelle approche dans la sécurisation de l'architecture Wi-Fi dans l'entreprise.

Chapitre IV

1. Introduction

Le chapitre précédent met en évidence le manque de sécurité dans les réseaux Wi-Fi, la profusion des attaques qu'il est possible de monter et leur relative simplicité de mise en œuvre. Toutefois, ce manque de sécurité ne devrait pas constituer un obstacle à la mise en place et au déploiement de réseaux Wi-Fi dans l'entreprise. En effet, il est économiquement plus intéressant de mettre en place un réseau local sans fil qu'un réseau local filaire. Un réseau Wi-Fi est beaucoup plus flexible qu'un réseau filaire et peut être désinstallé facilement. Il peut également compléter ou remplacer un réseau local filaire lors d'un contexte de mobilité.

2. Approches principales de sécurisation des architectures Wi-Fi

Le manque de sécurité des réseaux Wi-Fi et l'absence de standards de sécurité 802.11 robuste nous a obligé de faire appel à d'autres technologies afin de renforcer la sécurité de l'extension Wi-Fi des systèmes d'information.

Les technologies employées visaient principalement deux objectifs. D'abord, isoler le trafic Wi-Fi du reste du trafic filaire, ce qui peut être réalisé par le biais des réseaux locaux virtuels (VLAN). Ensuite, sécuriser les liens radio établis entre les clients Wi-Fi et le serveur d'authentification, ce qui peut se mettre en place en utilisant la technologie des réseaux virtuels privés (VPN).

2.1. Approche VLAN

Cette approche consiste à mettre en place un VLAN pour tous les clients 802.11 qui se connectent à un réseau pour l'isolation de ce trafic non sécurisé du reste du trafic qui transite dans le système d'information.

Rappelons qu'un VLAN est un réseau local regroupant un ensemble de machines de façon logique et non physique.

Ainsi, l'allocation d'un VLAN particulier aux clients Wi-Fi permet de définir un nouveau réseau au-dessus du réseau physique, ce qui offre les avantages suivants :

- Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs ;
- Gain en sécurité car les informations sont isolées logiquement du reste du trafic et peuvent éventuellement être analysées ;
- Réduction de la diffusion du trafic sur le réseau.

2.2. Approche VPN

La seconde approche de sécurisation des réseaux Wi-Fi consiste à déployer des réseaux virtuels privés entre les clients 802.11 et le réseau filaire de l'entreprise. En effet, faire face au manque de sécurité des liens radios des réseaux Wi-Fi, les responsables de

sécurité ont opté pour la mise en place de tunnels sécurisés pour protéger le flux d'information qui transite du client sans fil vers le système d'information de l'entreprise. Dans la majorité des cas, cette mise en place de VPN se fait moyennant le protocole de tunnelisation IPSec.

Cette solution a le mérite de renforcer la sécurité des liens radio et de pallier ainsi aux faiblesses des standards de sécurité, notamment le protocole WEP. Ceci d'autant que le protocole IPSec a fait ses preuves et peut être considéré comme étant le meilleur protocole de tunnelisation, en offrant simultanément sécurité et flexibilité.

3. Principe de l'architecture Wi-Fi sécurisé

Pour élaborer notre solution de sécurisation Wi-Fi, nous avons fait appel aux approches traditionnelles mais que nous employons de façon plus élaborée, afin de satisfaire au mieux les besoins spécifiques de sécurité. En effet, nous nous sommes basés sur le principe de différenciation entre les différentes catégories de trafics qui passent sur le réseau d'un organisme. Pour matérialiser cette différenciation, nous avons fait appel aux réseaux locaux virtuels afin d'établir deux niveaux de séparation logique.

Le premier niveau est relatif aux types d'équipements utilisés par les utilisateurs qui se connectent au réseau 802.11 et aux standards de sécurité Wi-Fi supportés (par exemple : WEP, WPA avec TKIP, WPA2 avec AES). Ainsi, nous opérons une première différenciation des utilisateurs selon la catégorie de leurs équipements /standards. Cette différenciation permet d'adapter les mécanismes de sécurité et d'authentification en fonction des vulnérabilités des standards implantés sur le matériel.

Nous opérons un second niveau de différenciation qui vient à la suite de l'authentification des clients 802.11. Ce second niveau de différenciation vient établir un VLAN par profil d'utilisateur (ex : permanents et visiteurs).

Nous faisons appel au protocole IPSec, afin de mettre en place des canaux de communication sécurisés pour les transmissions des clients 802.11 ayant Je protocole WEP comme seul mécanisme de sécurité, ceci afin de pallier au manque de sécurité de ce dernier.

À part les mécanismes de VLAN et de sessions sécurisées avec IPSec, nous mettons en place des zones démilitarisées en se servant de coupe-feu.

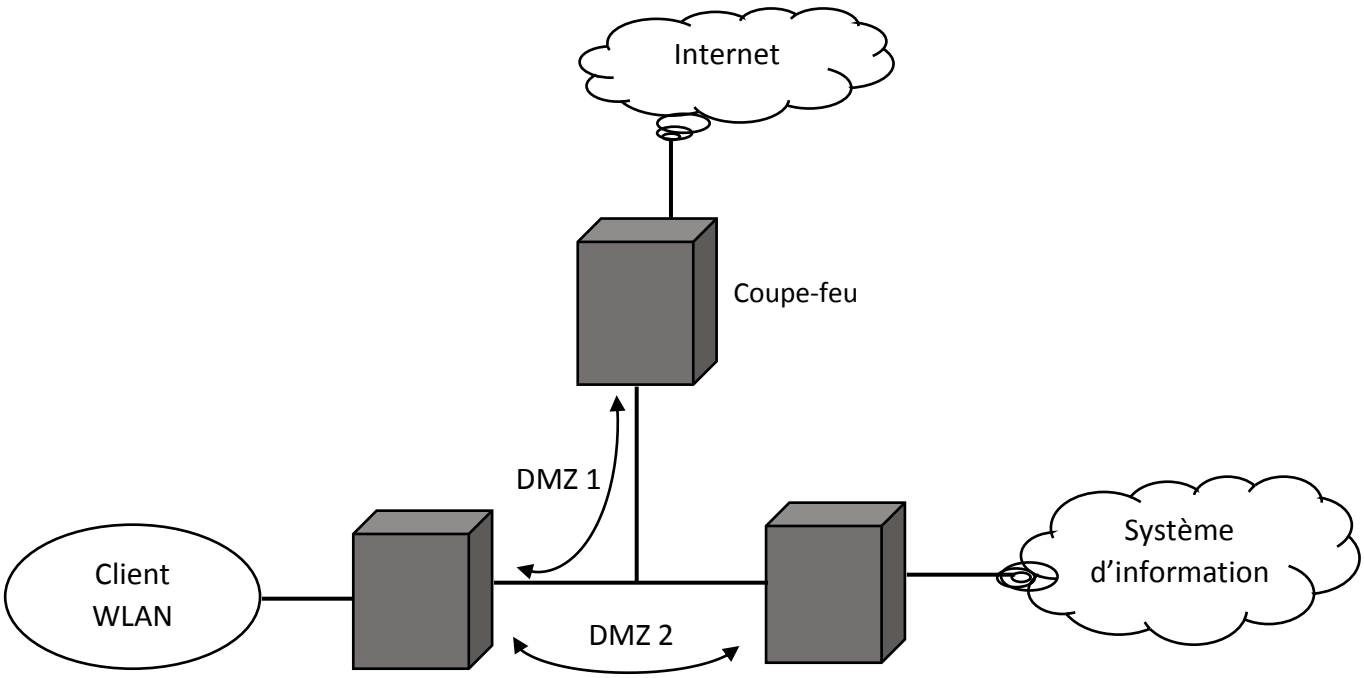


Figure IV.1 : Mise en place de zones démilitarisées

En effet, nous protégeons l'accès depuis le monde Wi-Fi aux serveurs d'authentifications de l'entreprise, à l'aide d'un premier coupe-feu, pour constituer la première zone démilitarisée, qui donne accès à Internet pour les clients Wi-Fi authentifiés en tant que visiteurs. Quant aux permanents, ces derniers seront réacheminés vers une seconde zone démilitarisée.

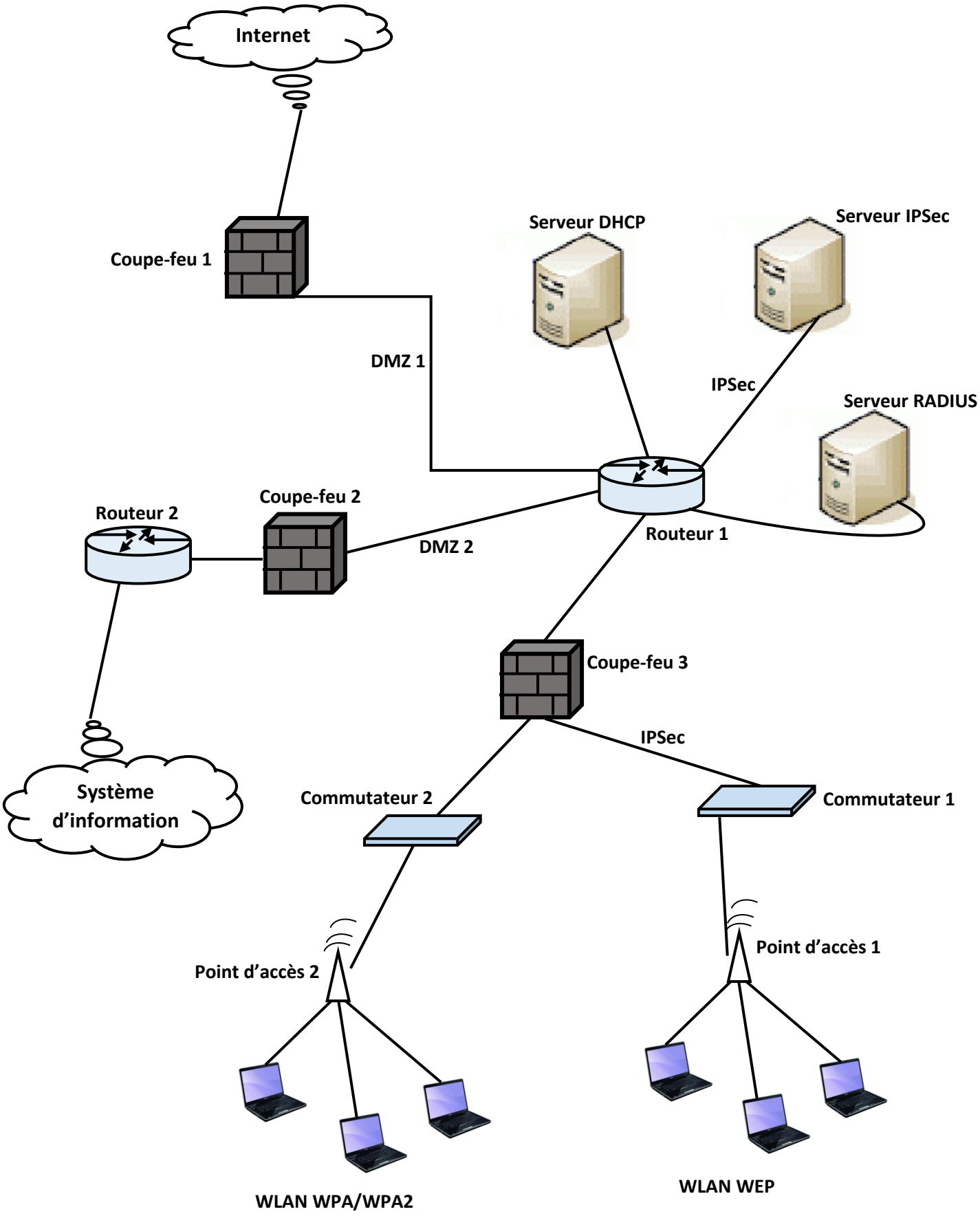


Figure IV.2 : Architecture Wi-Fi sécurisée

Comme illustré dans la figure précédente, nous avons choisi de placer le serveur d'authentification IPSec pour l'établissement du canal IPSec sécurisé avec les clients de la communauté WEP derrière le premier coupe-feu. Ceci en plus d'un serveur RADIUS pour l'authentification des clients de la communauté WPA/WPA2.

De plus, pour pouvoir authentifier les utilisateurs de la communauté WPA/WPA2, il est impératif d'utiliser un serveur RADIUS et pas n'importe lequel : il doit être compatible EAP-RADIUS.

Nous avons également choisi de mettre en place un serveur DHCP pour l'attribution d'adresses IP aux clients 802.11. Ce serveur DHCP permettra de mettre en place un adressage IP dynamique et privé, selon des règles d'adressage par VLAN, de façon à permettre l'identification de chaque client 802.11 par la classe de son adresse IP.

En élaborant cette approche de sécurisation Wi-Fi, nous avions comme objectif de pouvoir supporter plusieurs architectures logiques, sur la même architecture physique. Cela a pu être possible grâce au déploiement de plusieurs VLAN.

En effet, pour la mise en place du premier niveau de différenciation, c'est-à-dire VLAN par famille d'équipements (WEP, WPA/WPA2), il suffit d'associer un nom de réseau (SSID) à un VLAN. Ainsi, chaque SSID/VLAN peut bénéficier d'une authentification spécifique.

Un client Wi-Fi se connectant à un point d'accès avec un SSID particulier se trouvera automatiquement membre d'un VLAN particulier. Il est à rappeler que la majorité des points d'accès supportent les SSID multiples et la correspondance SSID/VLAN. Un point d'accès peut comporter plusieurs SSID, chacun associé à un VLAN particulier.

Dans l'architecture que nous proposons, deux communautés avec deux modes d'accès différents au système d'information se dégagent : la communauté WEP et la communauté WPA/WPA2. Pour avoir accès aux ressources du système d'information depuis le réseau Wi-Fi, les clients 802.11 de la communauté WEP doivent passer par les étapes suivantes :

- Rattachement au point d'accès
- Association au VLAN de la communauté WEP
- Établissement d'une session IPSec
- Authentification WEP
- Établissement d'un canal WEP sécurisé

Quant aux clients 802.11 de la communauté WPA/WPA2, ces derniers devront passer par les étapes suivantes :

- Rattachement au point d'accès
- Association au VLAN de la communauté WPA/WPA 2
- Échanges WPA/WPA 2
- Établissement d'un canal WPA/WPA2 sécurisé.

4. Configuration d'un VLAN

Voici une procédure vous démontrant un exemple de configuration de VLAN avec une topologie Multi SSID.

Dans cet exemple, nous allons utiliser :

- Un routeurZyWALLUSG100 ;
- Un Switch Web-administrable Layer (commutateur) GS1910-48 ;
- Un Switch administrable Layer GS22008H;
- Un point d'accès LAN sans fil NWA3160N.

Il est à signalé que tous les produits utilisés sont de marque ZyXEL.

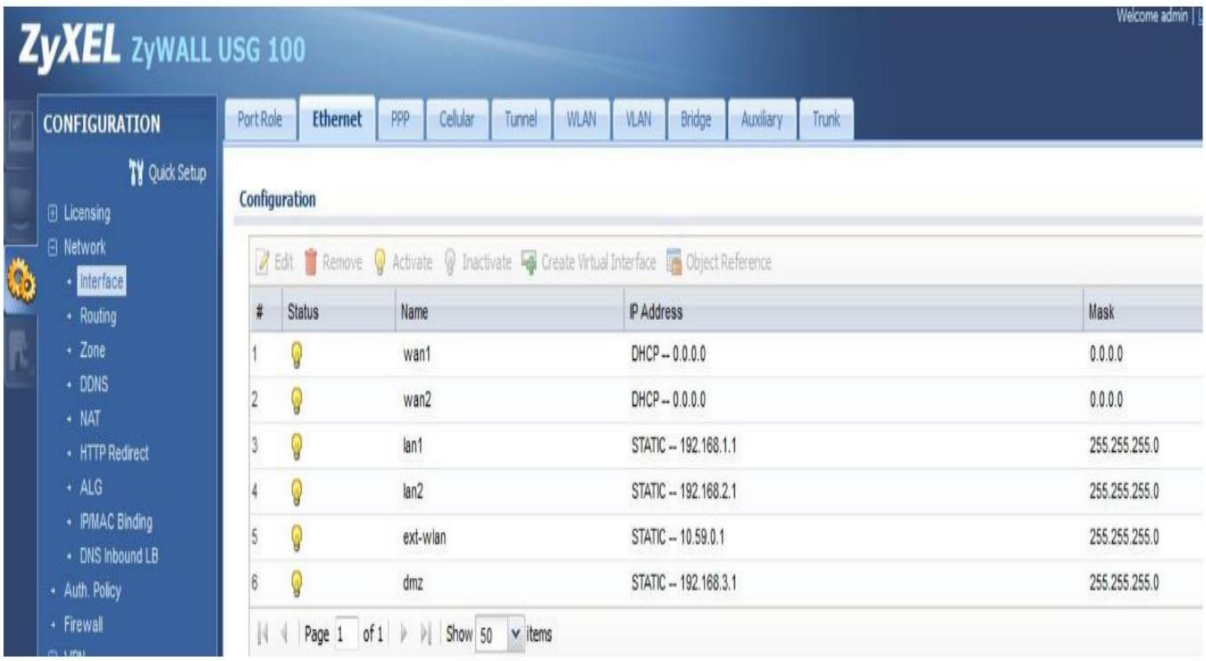
Comme si indiqué dans le principe d'architecture Wi-Fi proposée, Nous allons mettre en place une solution de séparation de deux réseaux : un réseau Interne, qui permettra d'accéder aux ressources, et un réseau Invité, qui permettra à des personnes nomades d'avoir un accès Internet, sans avoir accès au réseau Interne.

4.1. Première étape : la configuration de l'USG 100

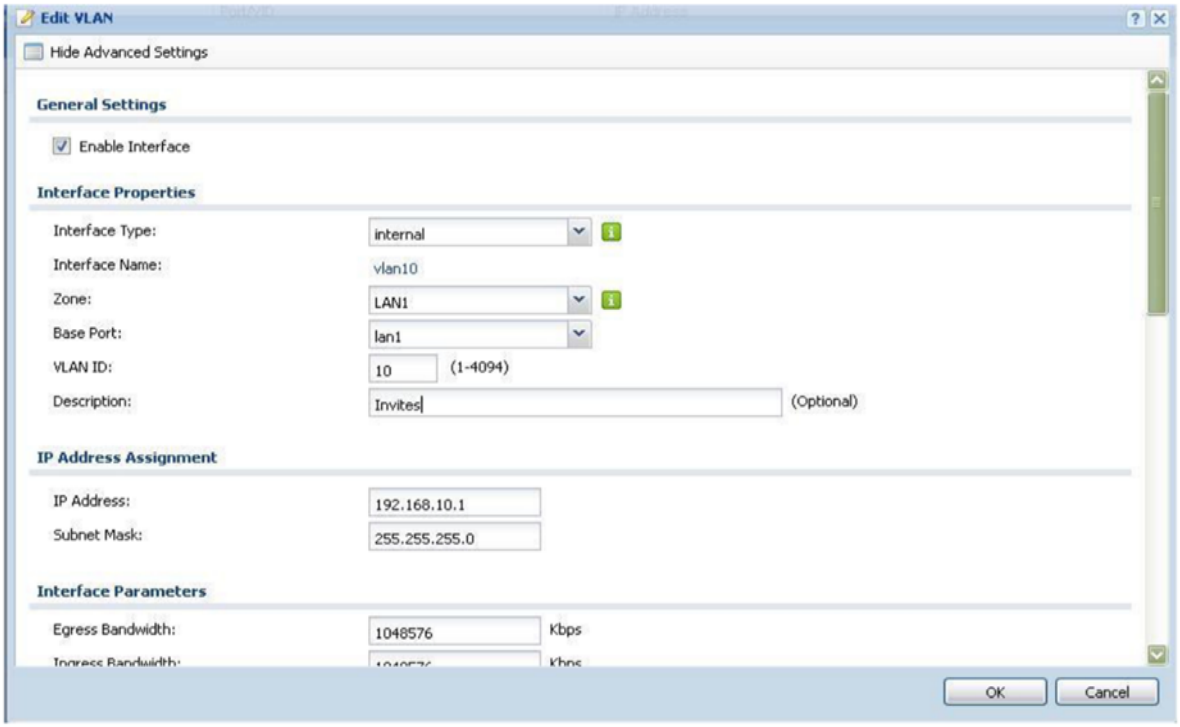
Le routeur doit être configuré pour l'exploitation.

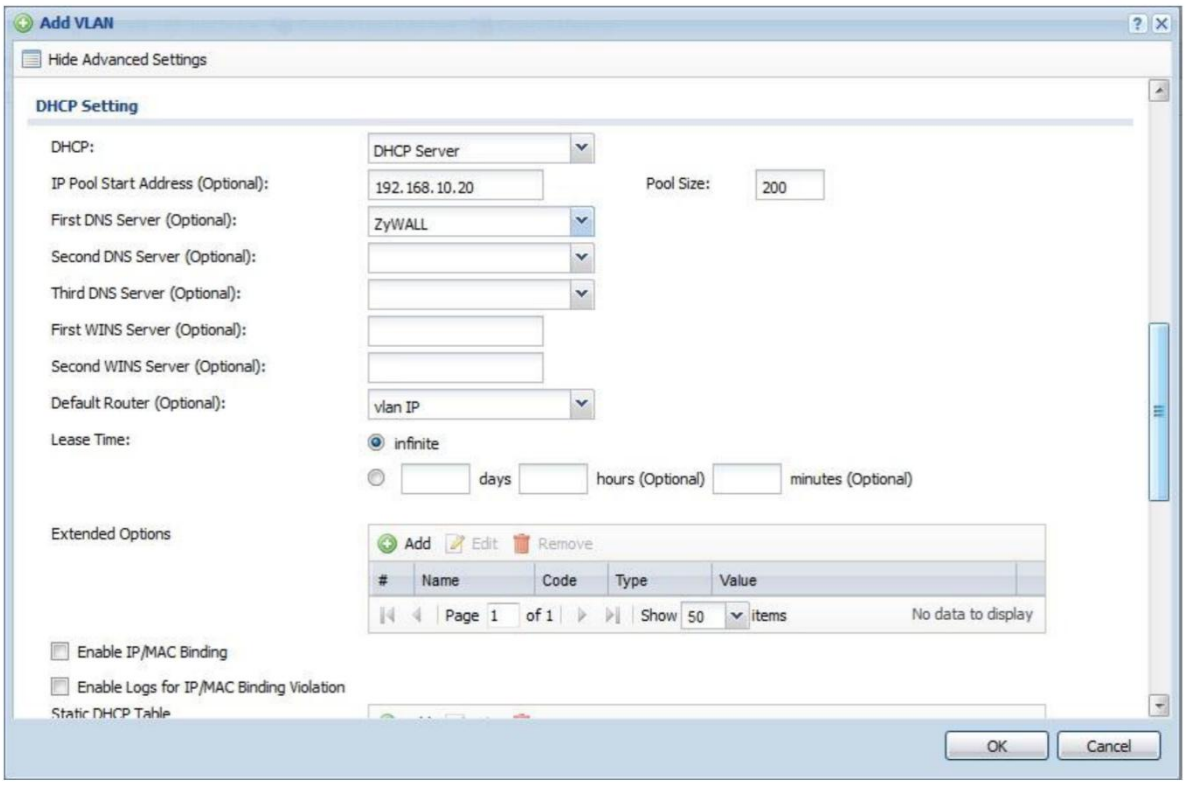
Pour cela il faut utiliser un configurateur web et ont saisi l'adresse par défaut fournit avec le routeur qui est : http://192.168.1.2 par laquelle on va accéder à son software. Ensuite, une fenêtre apparaitre qui nous demande d'insérer un nom d'utilisateur et un mot de passe qui sont respectivement par défaut **admin** et **1234**.

Nous déterminons le réseau LAN en 192.168.1.0/24 :



Nous créons le Vlan10 qui permettra aux invités d'avoir accès Internet : Menu Configuration -->Network -> Interface -> Vlan ->Add :



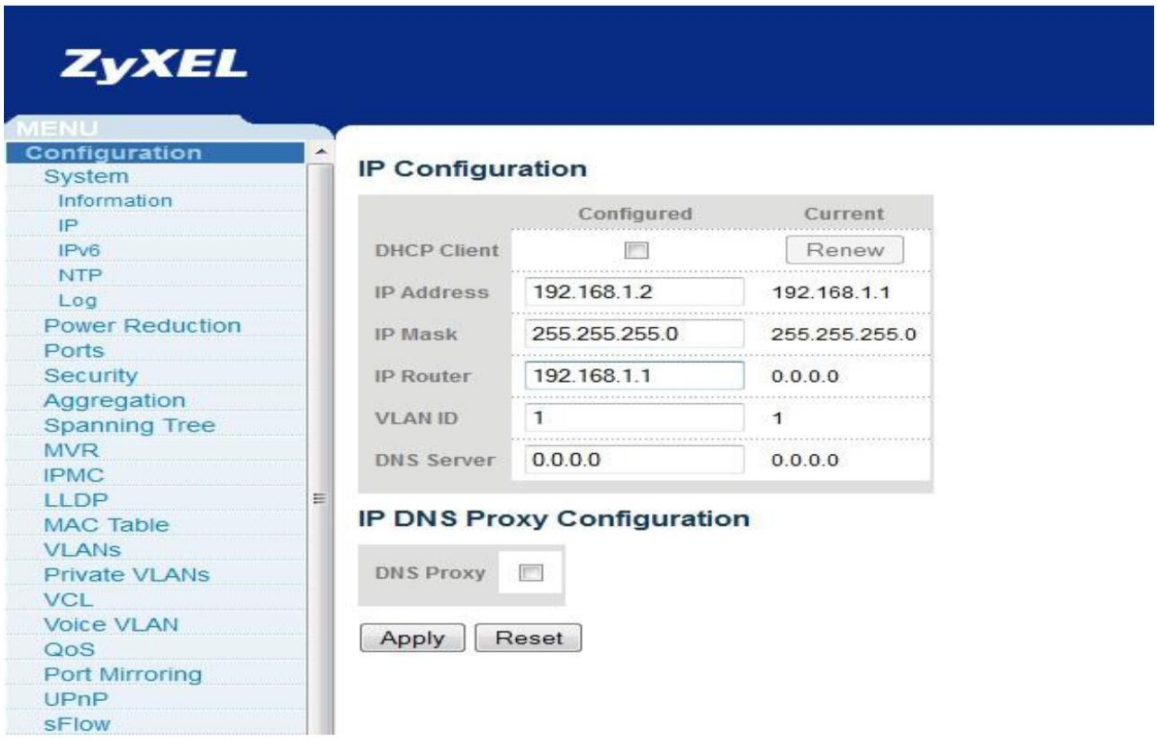


Nous avons indiqué le type d'interface en internal, la zone LAN1, Base port LAN1, un Vlan ID 10, une adresse réseau 192.168.10.1/24, avec un DHCP serveur pour les invités 192.168.10.20, pool 200 IP.

4.2. Deuxième étape : la configuration du switch GS191048

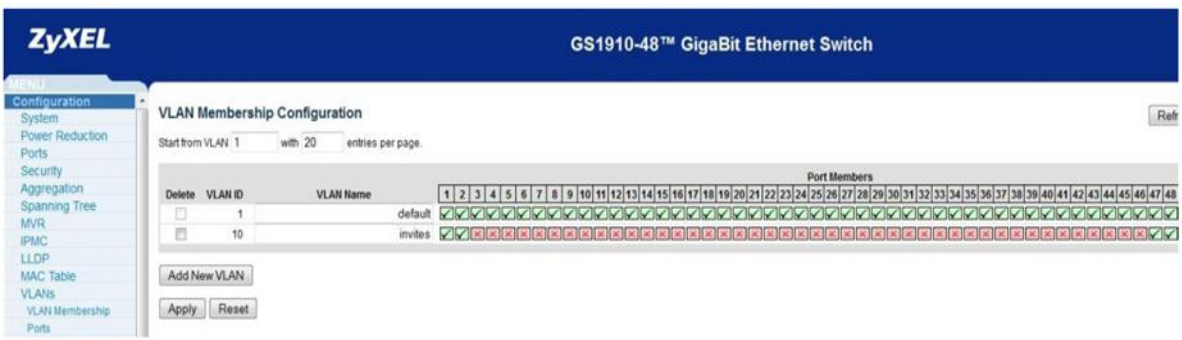
On doit suivre les mêmes étapes que pour le routeur afin d'accéder au software du switch(http://192.168.1.1)

Il faut lui changer son IP dans un premier temps : Menu Configuration -> System -> IP :



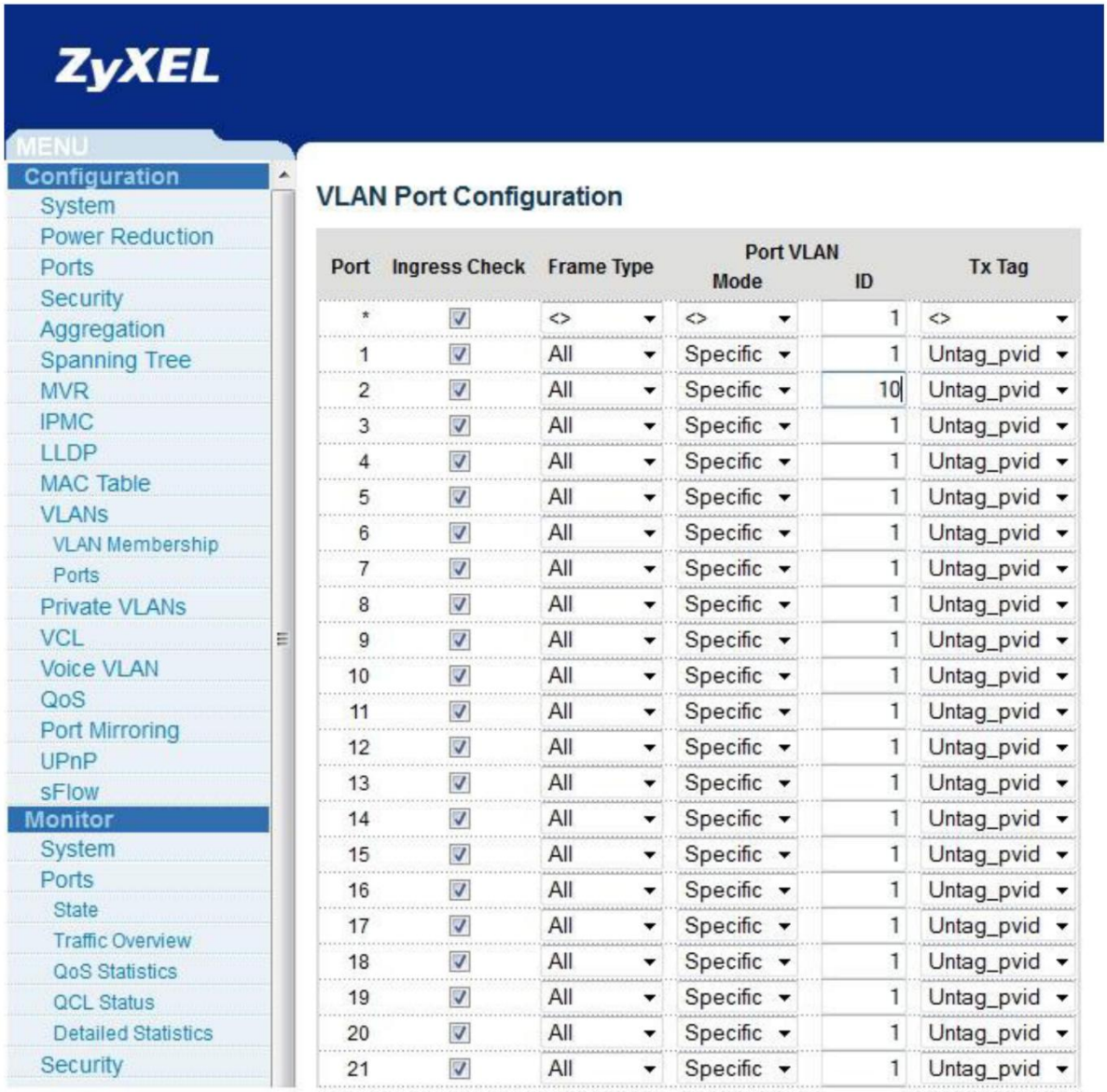
Nous avons déterminé que le port 48 du switch sera relié au LAN 1 de l'USG100, et le port 47 sera connecté sur le SWITCH GS22008HP (port 10).

Nous pouvons créer le Vlan sur le switch : Menu Configuration ->VLANs -> VLAN Membership:



Il a été créé le VLAN invites VLAN ID 10. Sur le port 48 nous avons l'USG, le port 47 le switch GS22008HP. Le port 1 sera relié à un NWA3160N.

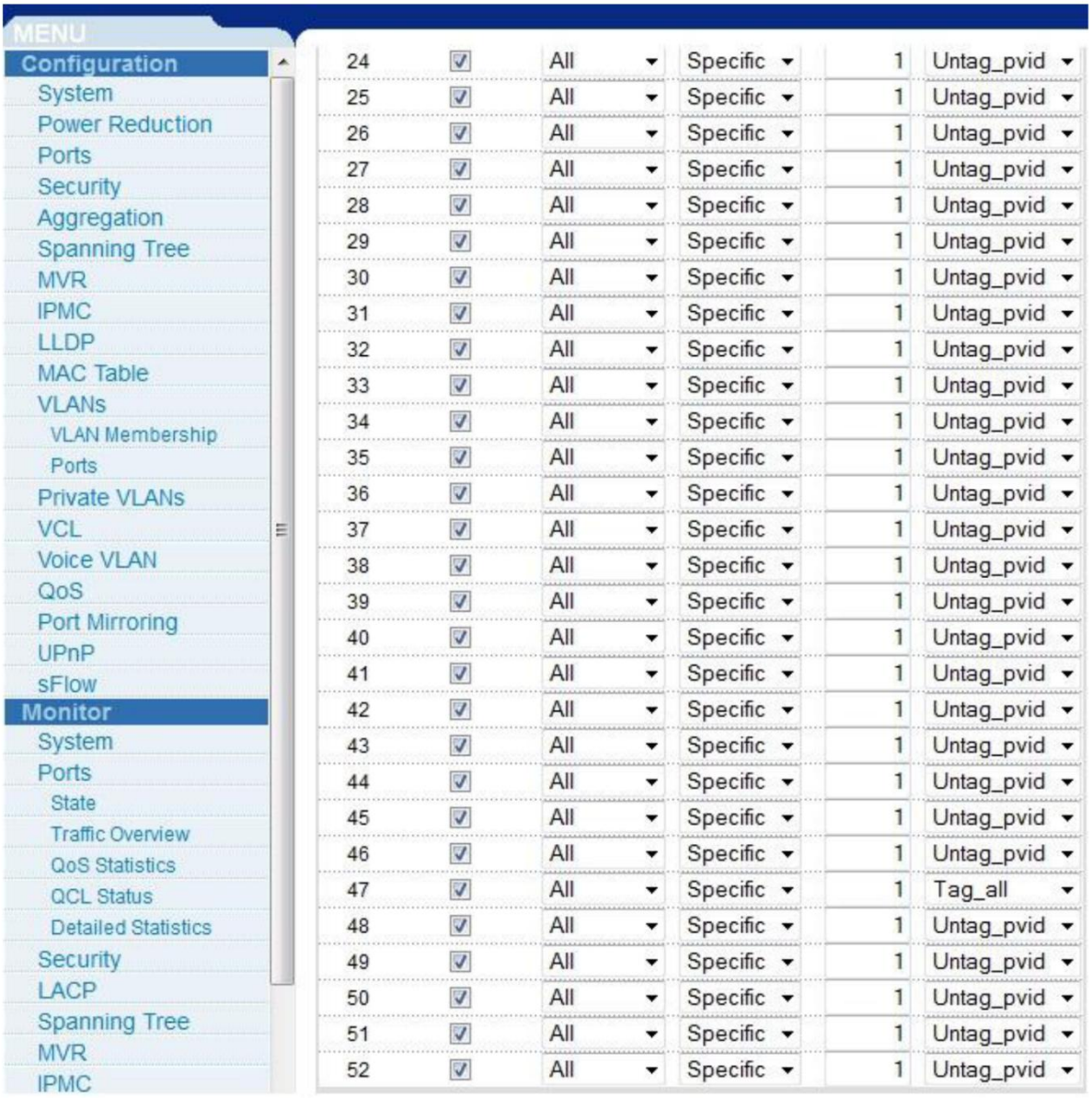
L'entreprise souhaite mettre à disposition un PC fixe pour les nomades sur le port 2. Il faut donc lui fixer un PVID à 10 afin qu'il soit isolé dans le VLAN 10 : Menu Configuration ->VLANs -> Ports :



Sur le switch dans la catégorie **Tx Tag**, trois choix s'offrent à nous.

- **Untag_pvid** signifie que toutes les trames reçues sur ce port sont Tagguées, sauf le PVID.
- **Untag_all** signifie que le switch reçoit uniquement des trames non Tagguées.
- **Tag_all** signifie que toutes les trames sont Tagguées : Souvent utilisé pour les ports d'interconnexion vers d'autres switchs.

Il faut donc indiquer que le Port 47 est en **Tag_all** car nous allons y connecter le GS22008HP :

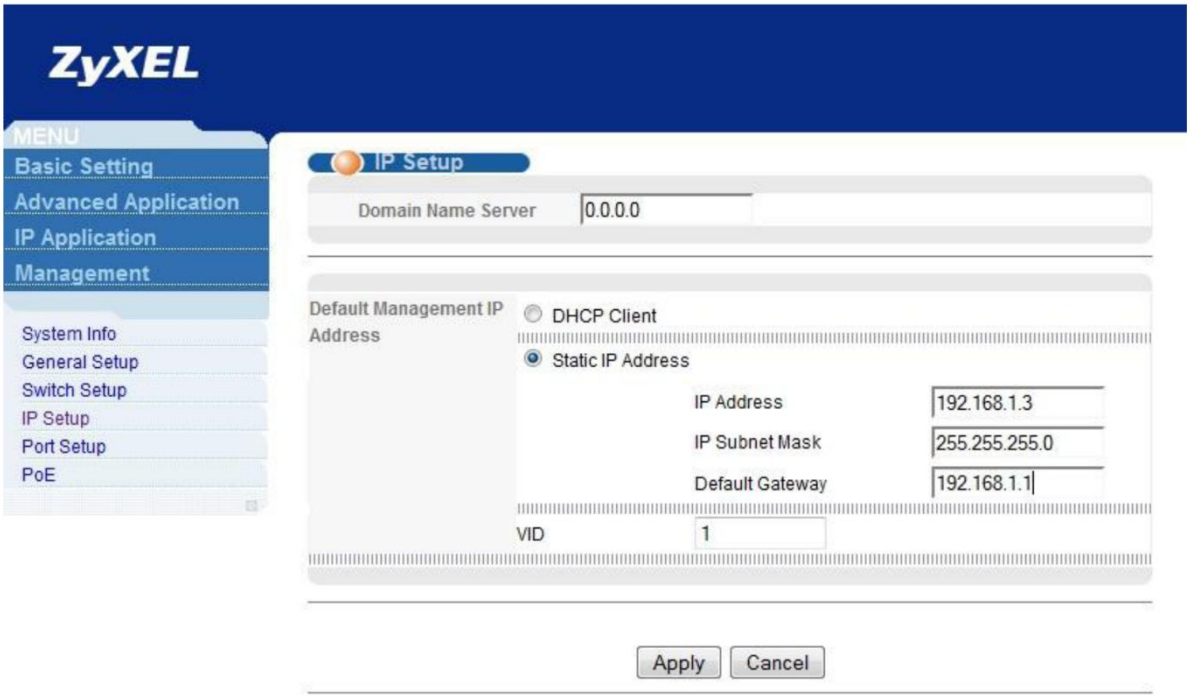


Le port 48 où est connecté l'USG100 est en **Untag_pvid** car notre PVID 1 correspond à notre réseau Interne, et que l'USG ne Tag pas sur le Réseau LAN1. Le Tag s'appliquera uniquement sur le VLAN10.

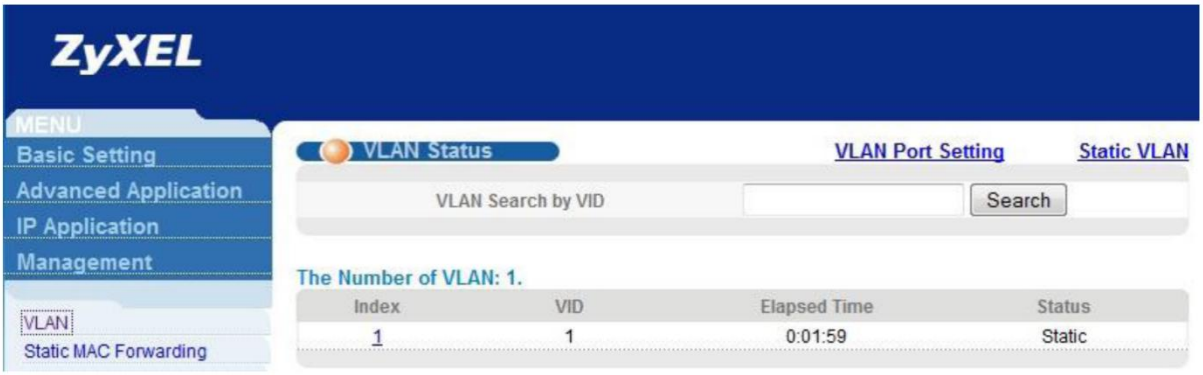
4.3. Troisième étape : la configuration du GS22008HP

On doit suivre les mêmes étapes que pour le routeur afin d'accéder au software du switch (http://192.168.1.1)

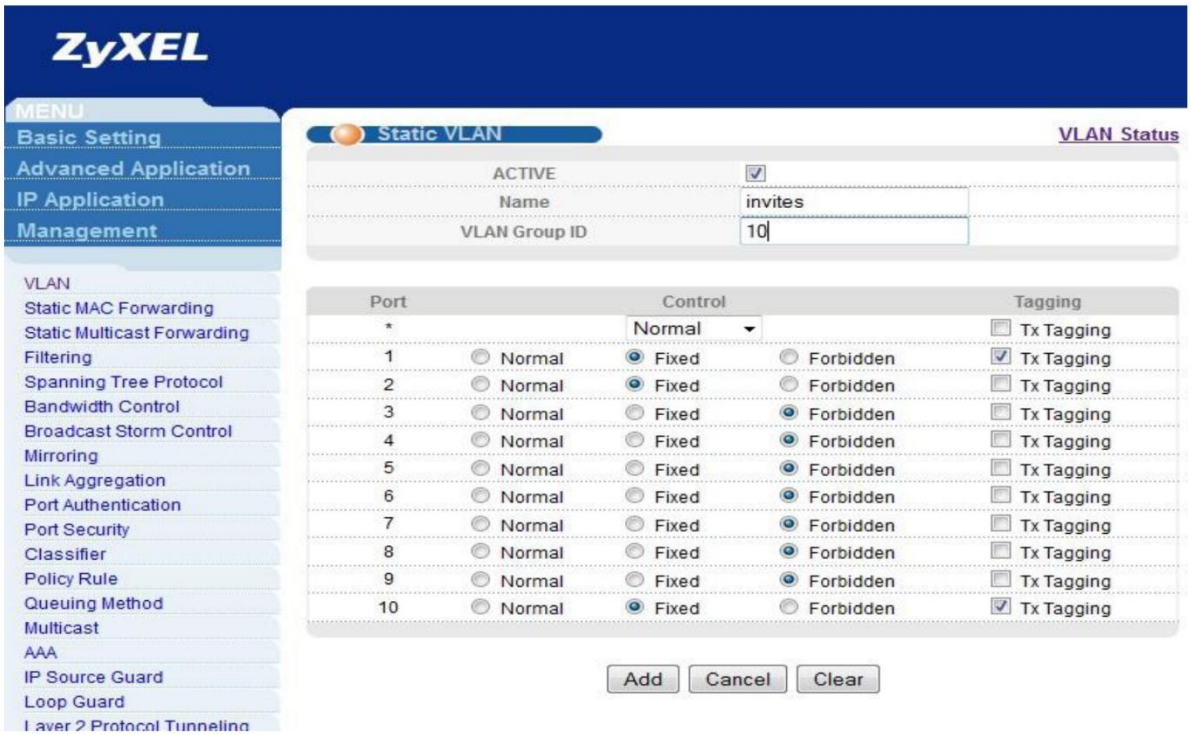
Il faut lui changer son IP dans un premier temps : Menu Basic Setting -> IP Setup :



Nous pouvons créer le Vlan sur le switch : Menu Advanced Application -> Vlan :



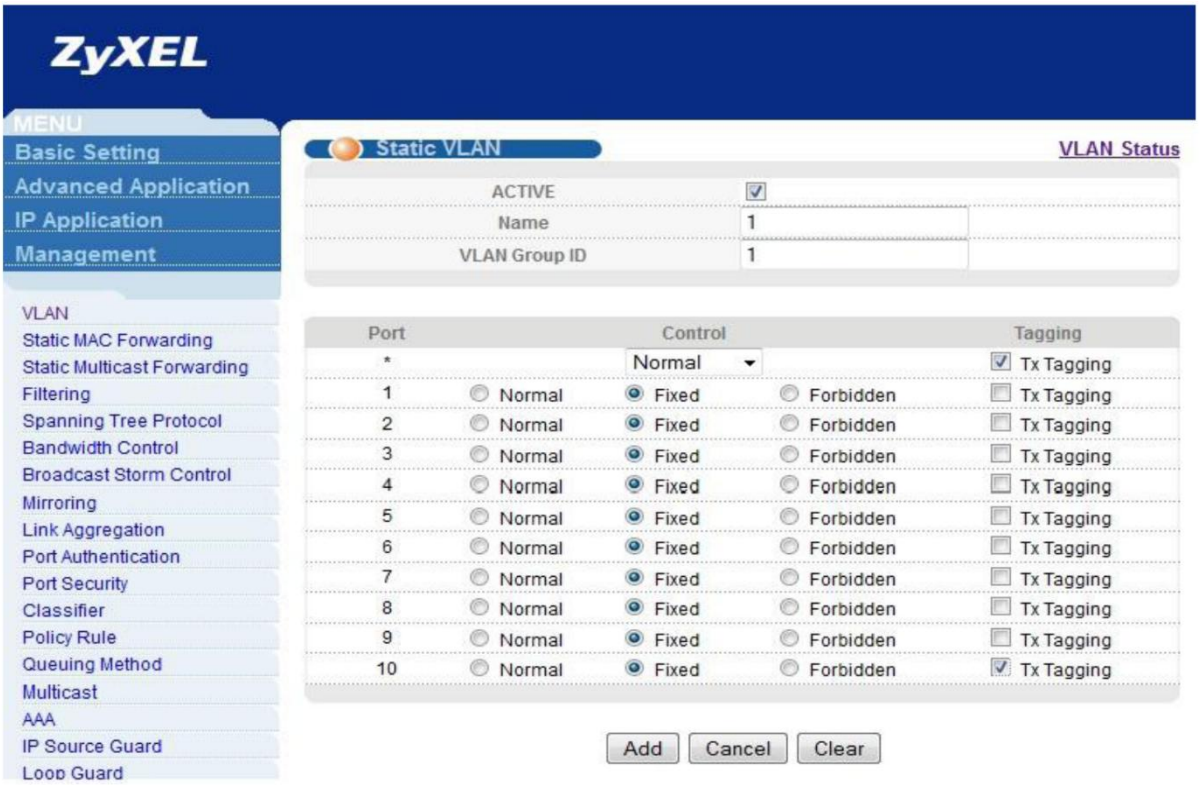
II faut ensuite cliquer sur **Static Vlan** puis créer notre Vlan Invites :



Nous indiquons le VLAN Group ID (VID) : 10

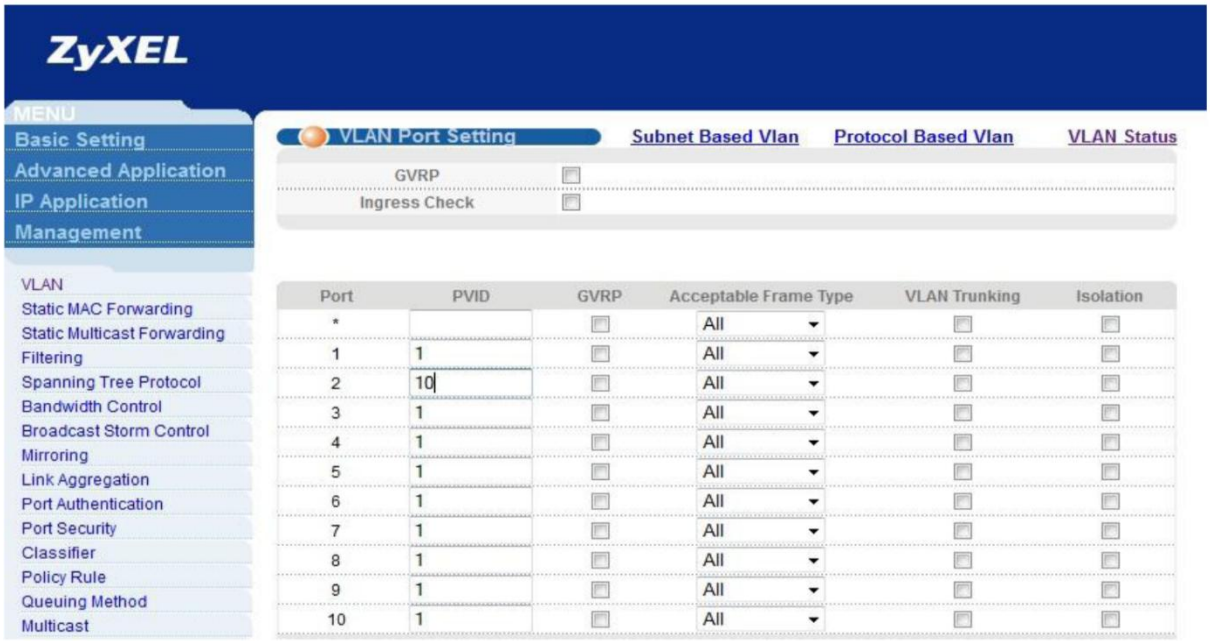
Sur le port 1, nous aurons une NWA3160N, il faut donc que le port soit Taggué dans le VLAN 10, cocher **TxTagging** pour cela.

Il ne faut pas oublier d'aller cocher le TxTagging sur le Vlan 1 pour le port d'interconnexion vers le GS191048 :



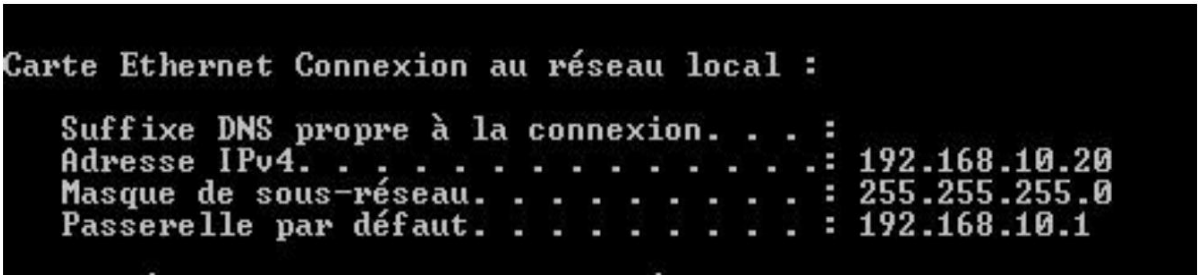
Comme pour le GS191048, l'entreprise met à disposition un PC, qui sera connecté sur le port 2.

Il faut donc aller indiquer le PVID 10 sur le port 2. Le PC envoie des trames non tagguées sur le port, et le switch TAG avec le PVID 10 en sortie : Menu Advanced -> Vlan ->

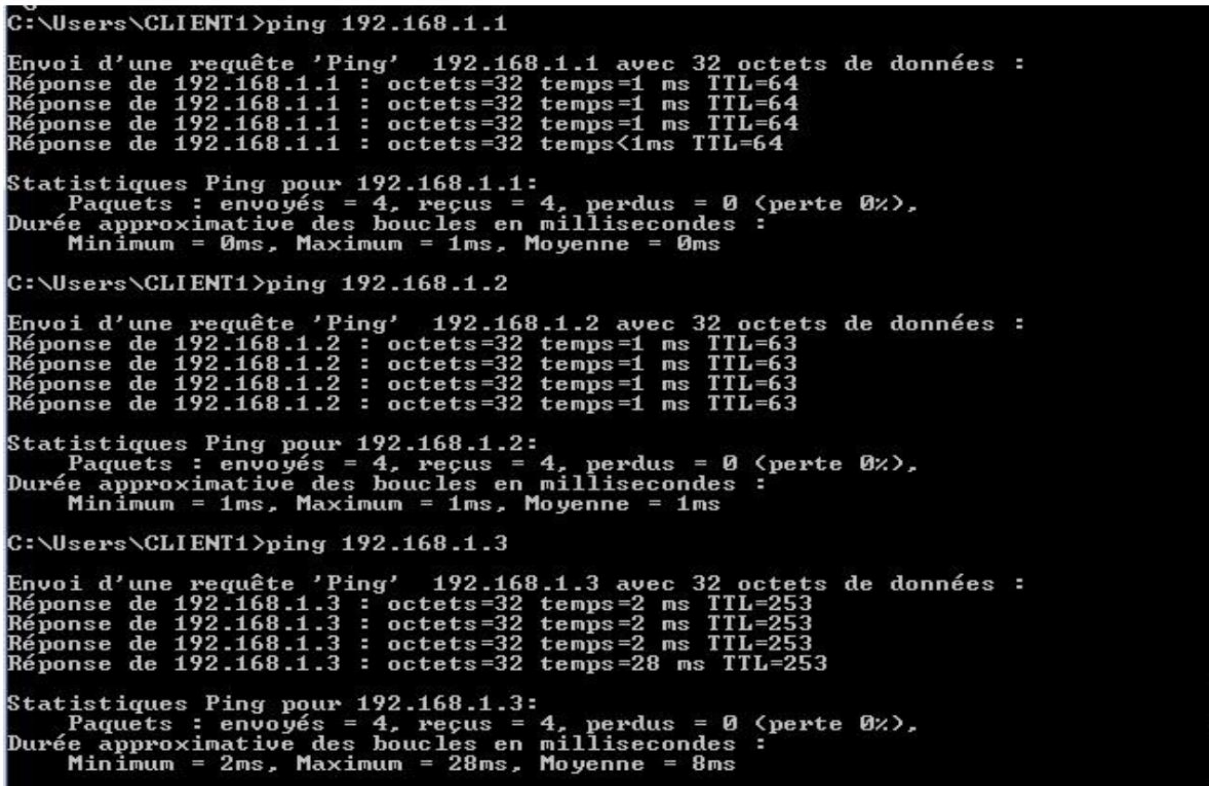


Vlan Port Setting :

Connectons notre PC en DHCP sur le port 2 du GS22008HP afin de voir si nous obtenons bien une IP dans le Vlan 10 :

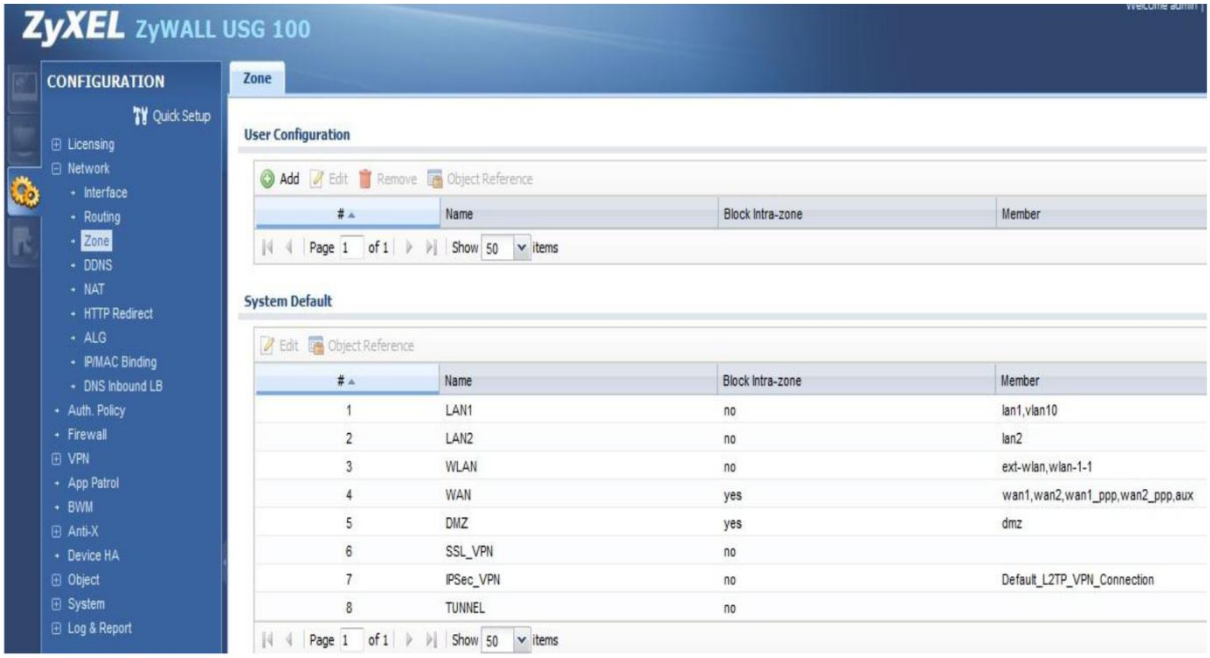


On peut s'apercevoir que l'on arrive à joindre le réseau 192.168.1.0/24 car c'est l'USG qui fait le routage :

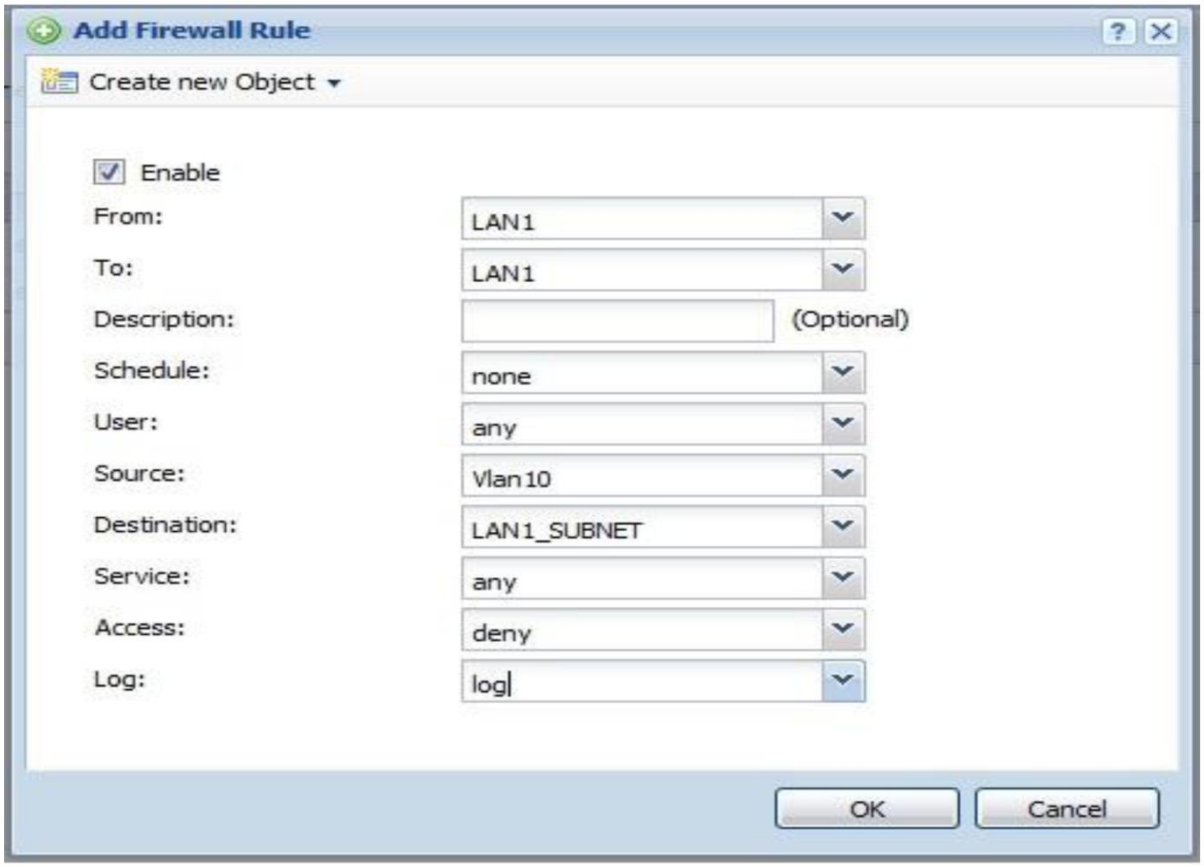


Pour bloquer l'accès entre le Vlan10 et le LAN1, deux possibilités s'offrent à vous :

- Soit d'activer le Block Intra Zone dans l'USG sur la zone LAN1 (LAN1 et VLAN) :



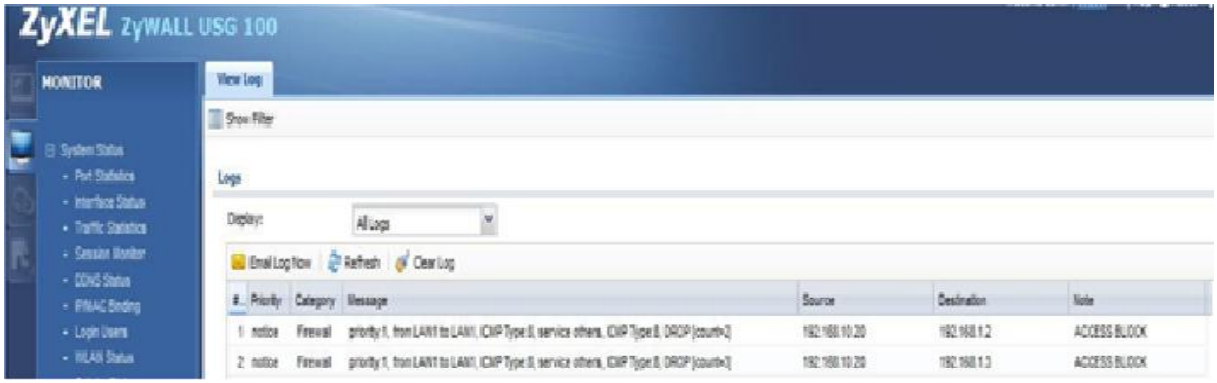
- Soit de faire une règle de firewall : Menu Firewall ->Add :



Testons un ping à présent :

```
C:\Users\CLIENT1>ping 192.168.1.3

Envoi d'une requête 'Ping'  192.168.1.3 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.1.3:
    Paquets : envoyés = 2, reçus = 0, perdus = 2 (perte 100%),
Ctrl+C
^C
C:\Users\CLIENT1>ping 192.168.1.2

Envoi d'une requête 'Ping'  192.168.1.2 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.1.2:
    Paquets : envoyés = 2, reçus = 0, perdus = 2 (perte 100%),
```

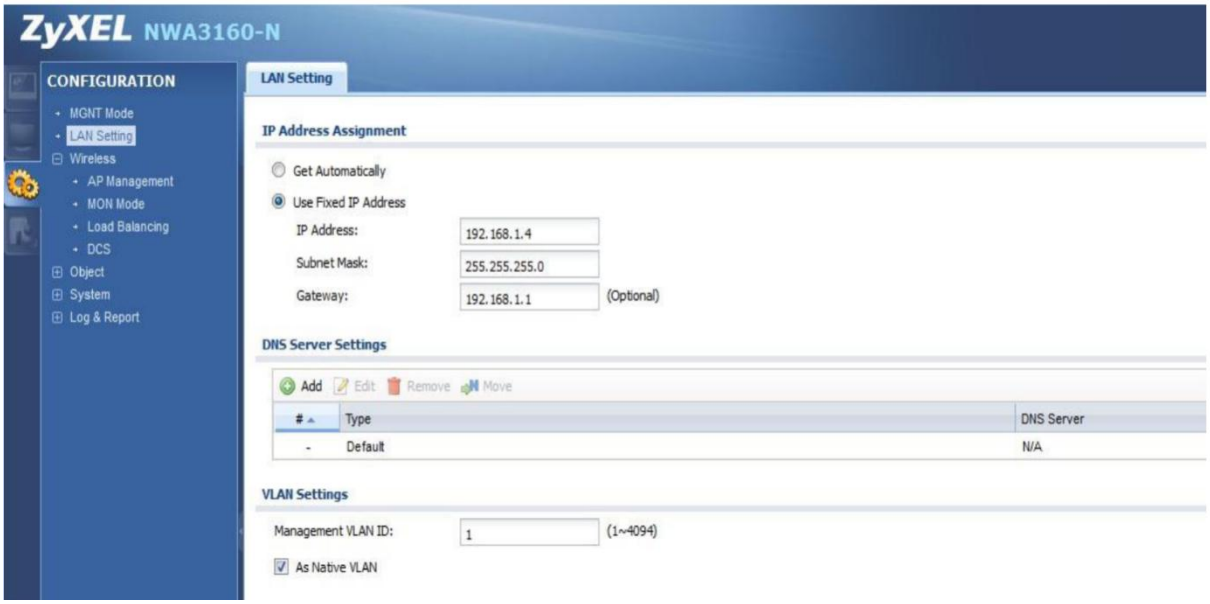
Le ping ne fonctionne plus, et nous avons la confirmation du blocage du trafic dans les logs de l'USG :



4.4. Quatrième étape : configuration du point d'accès NWA3160N

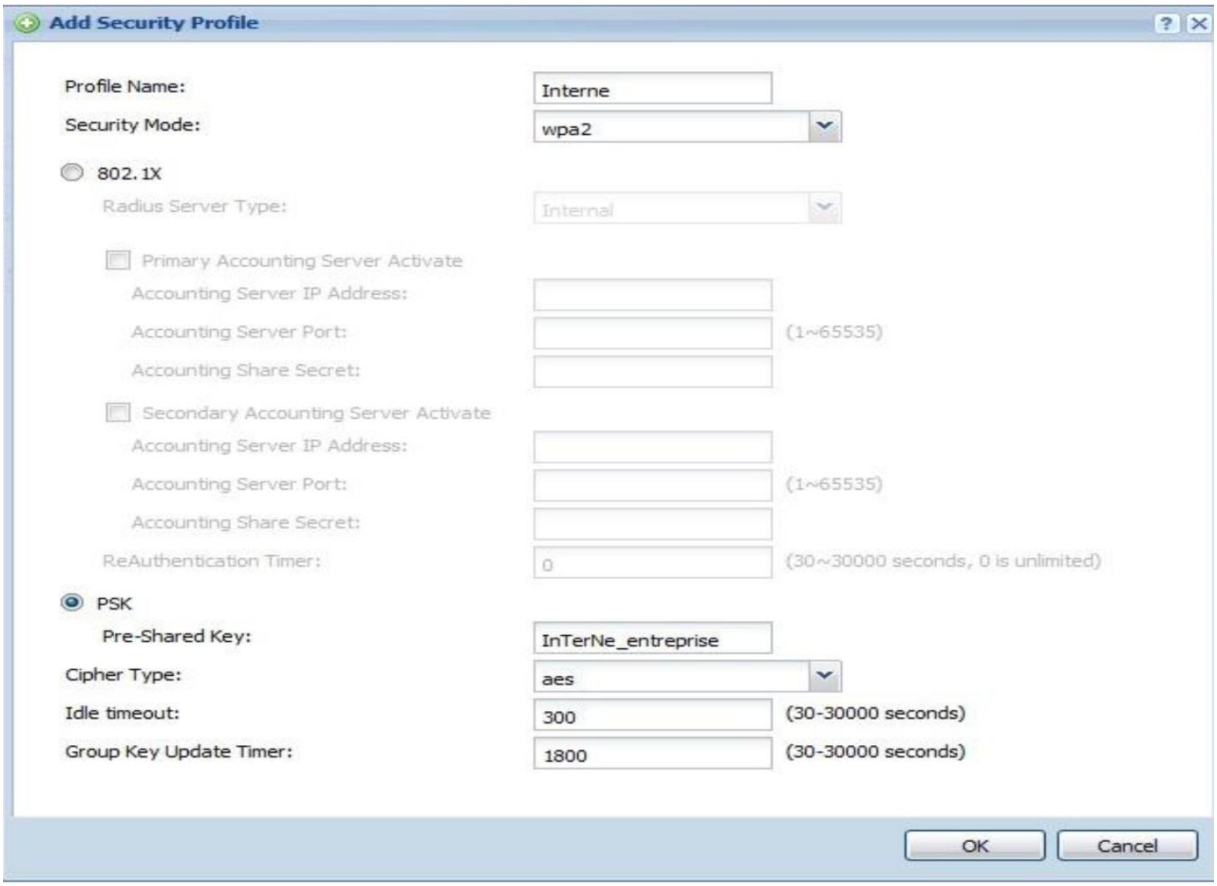
On doit suivre les mêmes étapes que pour le routeur afin d'accéder au software du switch (http://192.168.1.2)

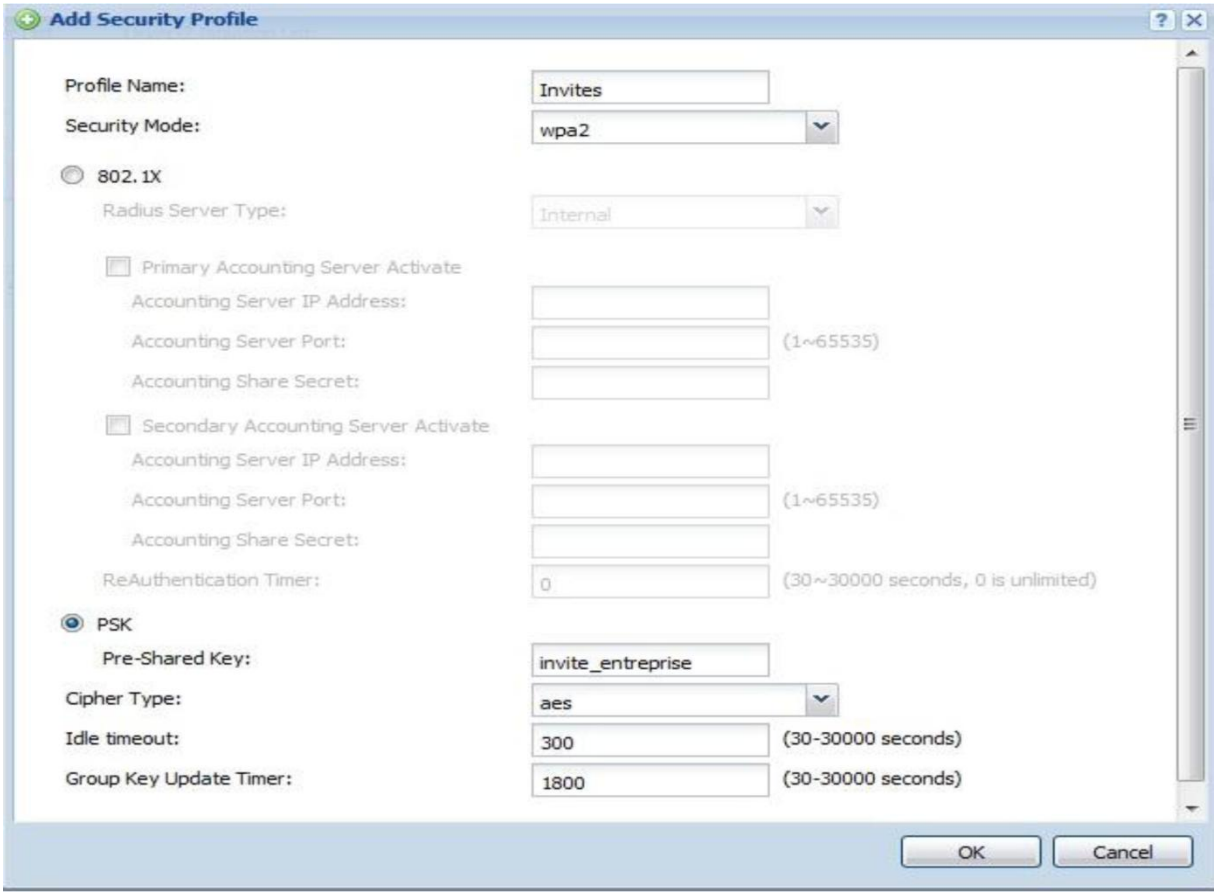
Il faut lui change son IP dans un premier temps.



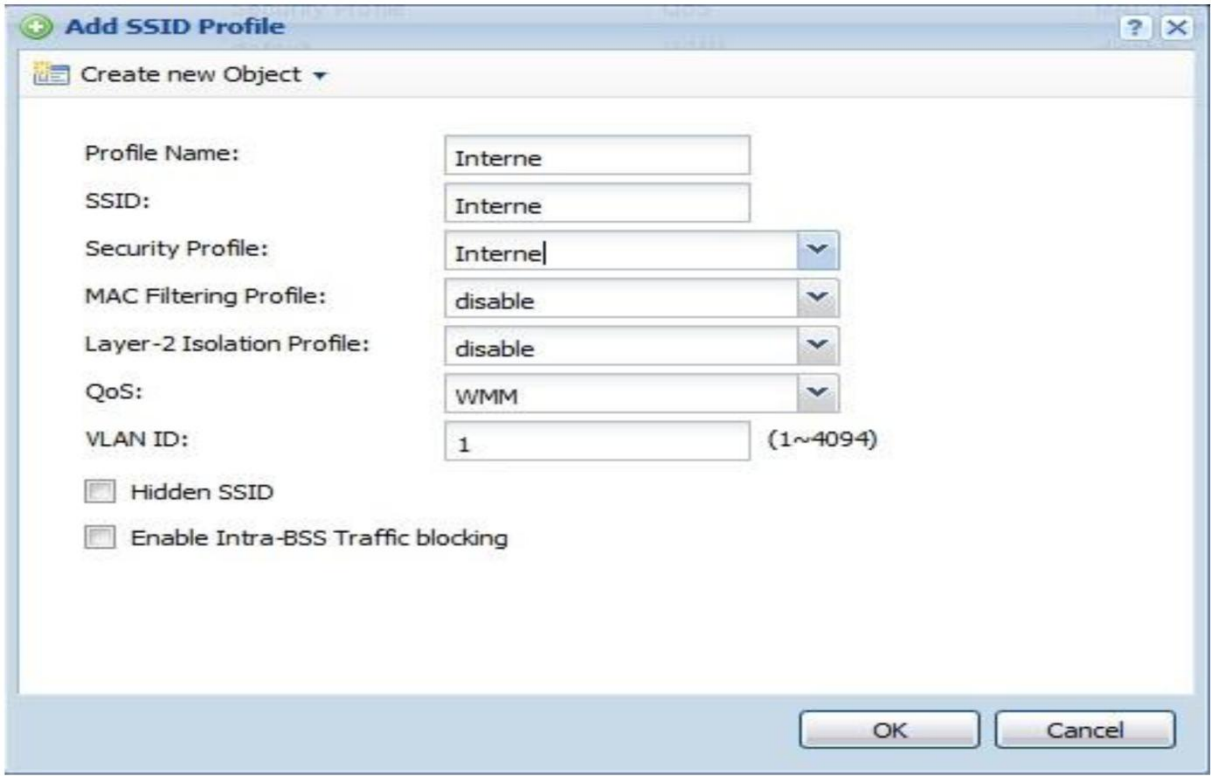
Ensuite on paramètre les profils de sécurité : Menu Object -> AP Profile -> SSID -> Security List ->Add :

Nous aurons deux sécurités, la première pour le réseau interne, et la seconde pour le réseau invité

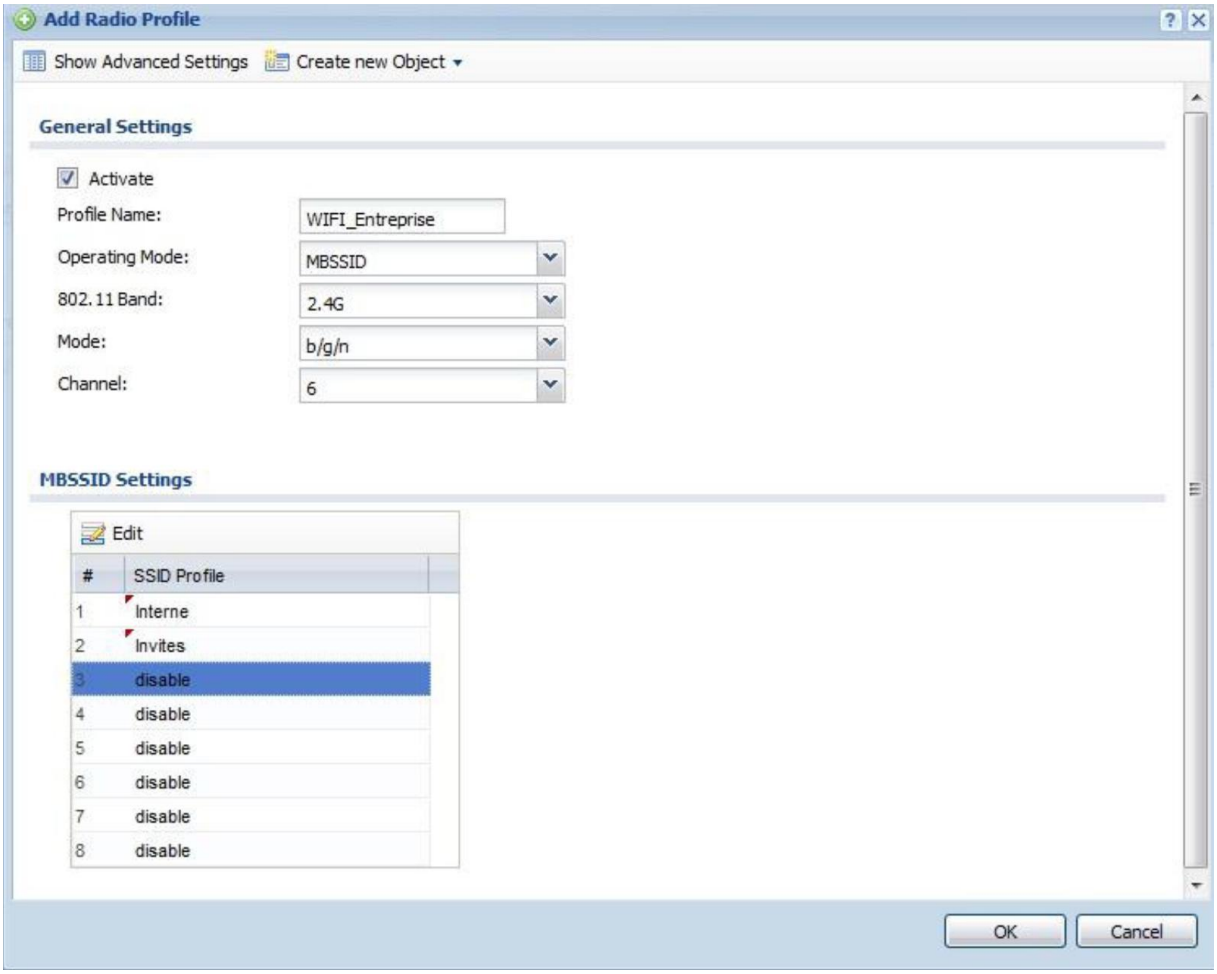

Add Security Profile
Profile Name:
Interne
Security Mode:
wpa2
802.1X
Radius Server Type:
Internal
Primary Accounting Server Activate
Accounting Server IP Address:
Accounting Server Port:
(1~65535)
Accounting Share Secret:
Secondary Accounting Server Activate
Accounting Server IP Address:
Accounting Server Port:
(1~65535)
Accounting Share Secret:
ReAuthentication Timer:
0
(30~30000 seconds, 0 is unlimited)
PSK
Pre-Shared Key:
InTerNe_entreprise
Cipher Type:
aes
Idle timeout:
300
(30-30000 seconds)
Group Key Update Timer:
1800
(30-30000 seconds)
OK
Cancel


Add Security Profile
Profile Name:
Invites
Security Mode:
wpa2
802.1X
Radius Server Type:
Internal
Primary Accounting Server Activate
Accounting Server IP Address:
Accounting Server Port:
(1~65535)
Accounting Share Secret:
Secondary Accounting Server Activate
Accounting Server IP Address:
Accounting Server Port:
(1~65535)
Accounting Share Secret:
ReAuthentication Timer:
0
(30~30000 seconds, 0 is unlimited)
PSK
Pre-Shared Key:
invite_entreprise
Cipher Type:
aes
Idle timeout:
300
(30-30000 seconds)
Group Key Update Timer:
1800
(30-30000 seconds)
OK
Cancel

Ensuite, il faut créer deux profiles SSID, un Interne (avec sécurité Interne et Vlan ID 1) et l'autre invité (avec sécurité Invité et Vlan ID 10) : Menu Object -> AP Profile -> SSID -> SSID List ->Add :

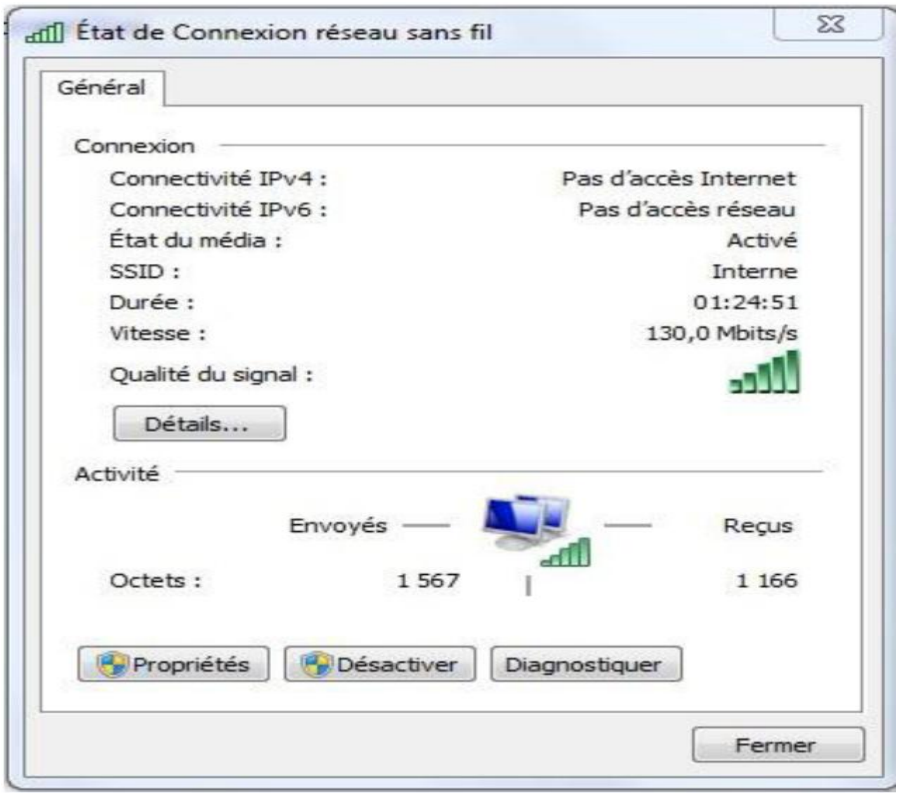


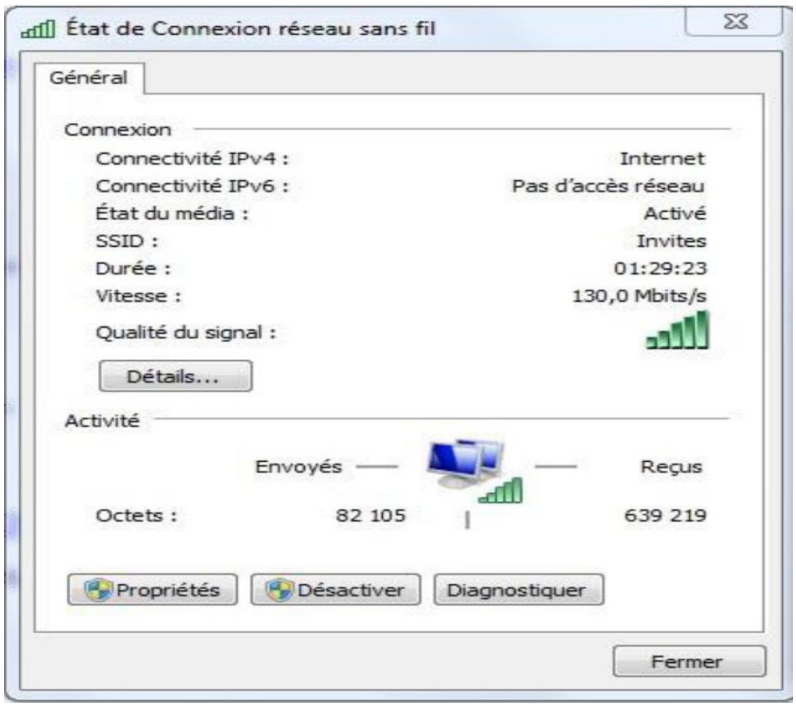
Les deux profils SSID sont créés, il faut désormais les associer à un profil Radio qui sera diffusé par la borne : Menu -> Object -> AP Profile -> Radio ->Add :



Notre profile est complètement configuré, il faut désormais le diffuser sur la borne. Pour se faire, nous allons dans le menu : Wireless -> AP Management et on sélectionne le profile :

Les deux SSID sont bien diffusés par la borne.





5. Conclusion

Dans ce dernier chapitre on a pu nous présenter une nouvelle approche architecturale de sécurisation des réseaux 802.11 dans l'entreprise qui prend en compte l'hétérogénéité des équipements et des standards de sécurité supportés. Cette nouvelle approche a le mérite d'offrir une grande flexibilité ainsi qu'une sécurité renforcée par rapport aux approches traditionnelles. Ainsi on a illustré à la fin par un exemple de configuration d'un VLAN.

Conclusion générale

Conclusion générale

Dans cette étude, nous avons présenté une synthèse de l'état de l'art des réseaux WiFi.

Ensuite, nous sommes passés au volet des standards de sécurité qui a fait l'objet du deuxième chapitre. Ainsi, nous avons montré l'évolution de la normalisation en termes de standards de sécurité 802.11. Nous avons également présenté une étude détaillée sur les vulnérabilités des standards de sécurité et les modes opératoires des différentes attaques qui exploitent ces faiblesses. Cette étude nous a permis de prendre conscience de l'étendue des dégâts qu'il est possible de provoquer sur un réseau Wi-Fi. Finalement, nous avons proposé une nouvelle approche architecturale qui permet d'allier sécurité renforcée, flexibilité et optimisation de l'utilisation des ressources du réseau.

Notre proposition a le mérite de favoriser principalement la flexibilité et de répondre aux besoins spécifiques exprimés aujourd'hui par les administrateurs des réseaux Wi-Fi. Ceci en plus de la prise en compte de l'hétérogénéité des équipements Wi-Fi et des standards de sécurité supportés. L'architecture Wi-Fi sécurisée que nous proposons se base sur une différenciation à plusieurs niveaux. En effet, nous établissons un premier niveau de différenciation relatif au standard de sécurité employé (WEP, WPA, WPA2). Le second niveau de différenciation permet de distinguer les différentes communautés d'utilisateurs Wi-Fi, ainsi nous avons distingués deux communautés d'utilisateurs (invités et interne), dont l'accès aux ressources et les niveaux de sécurité à appliquer sont différents d'une communauté à une autre.

Outre ces niveaux de différenciation, nous avons opté pour l'établissement de sessions sécurisées via le protocole IPSec, afin de sécuriser les liens radios des clients 802.11, ayant le protocole WEP comme seul mécanisme sécuritaire. Ce choix s'explique par la défaillance du protocole WEP et ses vulnérabilités flagrantes.

Il est utile de signaler que notre proposition s'inscrit pleinement dans le contexte actuel qui se caractérise par l'instabilité des standards de sécurité Wi-Fi et la rapidité de leur obsolescence. Cette mouvance rapide entre les différents standards et les diverses technologies inhérentes à la sécurité Wi-Fi, a créé une méfiance vis-à-vis de cette technologie malgré son grand potentiel. Notre solution vient intégrer toutes ces problématiques et propose une nouvelle approche de sécurisation de la technologie Wi-Fi dans l'entreprise.

Nous pouvons dire que ce travail a constitué pour nous, un très bon exercice d'analyse et de conception architecturale dans le contexte de la sécurité des réseaux Wi-Fi. Cela nous a également permis de prendre conscience de l'étendue des potentialités de cette technologie et en même temps, la difficulté d'assurer une sécurité optimale. Le plus difficile étant d'atteindre un compromis entre facilité d'accès et sécurité optimale.

Bien que nous n'ayons pas mis en pratique notre proposition pour des raisons matérielles évidentes, la suite logique de ce travail consisterait à :

- Mettre en œuvre notre architecture Wi-Fi.
- Implantation des systèmes de détection d'intrusion spécifiques aux réseaux Wi-Fi.
- La mise en place d'outils qui permettent de vérifier le niveau de sécurité et la conformité des postes clients 802.11 avec les exigences de sécurité de l'entreprise.

En guise de conclusion, nous pouvons affirmer que les réseaux Wi-Fi présentent de grands potentiels. Toutefois, les services fournis par ces réseaux sont confrontés à de graves problèmes de sécurité, au point de mettre en péril leur développement. Ces risques de sécuritéont tendance à s'atténuer, surtout avec le standard WPA2 qui semble répondre à la majorité des exigences actuelles de sécurité dans les réseaux Wi-Fi. Mis à part cet aspect de sécurité, les réseaux Wi-Fi font face à d'autres défis, parmi lesquels on peut citer la qualité de service et le transfert entre cellules (handover), ou encore la mobilité Wi-Fi.

En effet, selon une étude [1], le service de confidentialité assuré par le WEP fait perdre en moyenne 25% de performances, en induisant de graves failles de sécurité. Quant à TKIP et WPA, étant plus sécuritaires que WEP, ils induisent 30% de baisses de performances. WPA2, le nec plus ultra en matière de sécurité Wi-Fi, améliore un peu les performances mais engendre une perte de 25% de bande passante. De ce fait, il est primordial de trouver un compromis entre les exigences de sécurité et ceux de la qualité de service.

Outre l'aspect qualité de service, les réseaux Wi-Fi se doivent de remporter le défi de la mobilité sécurisée, en assurant un transfert entre cellules Wi-Fi Je plus sécuritaire et le plus rapide possible.

Une fois, tous ces défis relevés, la technologie Wi-Fi sera certainement un pilier majeur pour l'établissement de l'Internet ambiant de demain, offrant sécurité, mobilité, qualité de service et haut débit.

Bibliographie

- [1] G. Pujolle. « Sécurité Wi-Fi ». Edition Eyrolles, 2004.
- G. Pujolle. « Sécurité Wi-Fi ». Edition Eyrolles, 2003.
- Aurélien Géron. « Wi-Fi professionnel » . Edition Dunod, 2011.
- www.commentcamarche.net.
- www.cisco.com.
- www.google.fr