CYBER NETWORKS

LIVRE BLANC
Sécurité des systèmes sans-fil

Version 2.0

Dernière révision : Janvier 2004

22, rue Edouard Nieuport - 92150 Suresnes - Tél. : 01 42 04 95 95 - Fax : 01 42 04 95 87
SA au capital de 74 800 € - RCS Nanterre B 403 366 503 - APE 721Z

Avertissement

Tables de matières

Table des schémas

1. Introduction

Confirmant une révolution technologique et culturelle des systèmes d'information initiée dans les années 2000, la mobilité d'une manière générale et de manière plus spécifique son pendant technique, les réseaux sans-fil, ont commencé à véritablement s'imposer dans le paysage informatique français en 2003.

Ces technologies, porteuses de progrès indéniables, font émerger de nouvelles façons d'accéder aux ressources informatiques et d'échanger des données. Mais cette ouverture des réseaux est à double tranchant car elle peut grandement fragiliser la sécurité du système d'information si elle se fait de manière non maîtrisée ou sans réelle prise en compte des problématiques de sécurité.

A présent, la pression combinée des constructeurs d'équipement et de certaines catégories d'employés fait qu'il est devenu très difficile de tenir totalement à l'écart un système d'information des systèmes sans-fil. Ceci est d'autant plus vrai que les ordinateurs actuellement en vente, en particulier les portables, sont nativement équipés de ces technologies (Centrino par exemple). Il est désormais essentiel que les responsables intègrent ces technologies et les nouvelles problématiques qu'elles posent dans une politique de sécurité globale et mettent en place les solutions techniques et organisationnelles adaptées.

Dans le cadre de cette problématique complexe de la mobilité en entreprise, l'objectif de ce livre blanc est d'aborder les réseaux sans-fil sous l'angle de la sécurité. Après une présentation générale des réseaux sans-fil, nous aborderons donc les problèmes de sécurité et les risques associés pour terminer sur une présentation des solutions de sécurisation.

2. Présentation des réseaux sans-fil

Un réseau sans-fil substitue aux habituels câbles des connexions aériennes via des ondes radios, infrarouges ou éventuellement des faisceaux laser. Cette définition, assez large, nous amène à considérer plusieurs types de réseaux sans-fil.

2.1. Les réseaux sans fil de type infrastructure

Les réseaux de type infrastructure sont des réseaux structurés, basés sur des équipements d'interconnexion faisant office de ponts entre un réseau radio et un réseau câblé permettant ainsi à de nombreux clients mobiles d'accéder à des ressources informatiques.

2.1.1. Les réseaux sans-fil locaux

Les réseaux sans-fil locaux pour terminaux mobiles, et en particulier les réseaux Wi-Fi, sont à la fois les plus répandus et les plus médiatisés à l'heure actuelle.

Note :
Le Wi-Fi (Wireless Fidelity) est à l'origine un label garantissant la compatibilité des terminaux et des infrastructures basé sur la norme 802.11 entre tous les constructeurs. Aujourd'hui le terme Wi-Fi est devenu le nom commercial des systèmes fonctionnant avec le standard 802.11.

Le terme technique pour ces réseaux est WLAN (pour Wireless Local Area Network) par opposition à LAN (Local Area Network) qui désigne un réseau câblé traditionnel.

Un WLAN est constitué de points d'accès équipés d'une antenne et d'une interface réseau Ethernet standard. Chaque point d'accès forme une zone de couverture radio appelée cellule. L'ensemble des cellules constitue le WLAN.

Les terminaux mobiles (PC portable, PDA…) équipés d'adaptateur réseau sans-fil naviguent dans la zone de couverture du WLAN et restent connectés en permanence au réseau de l'entreprise sans contrainte physique. Ils accèdent ainsi aux ressources informatiques situées sur la partie câblée des points d'accès de la même façon que les stations de travail standards : le seul changement vient du lien physique utilisé pour la connexion.

Le passage d'un terminal de cellule en cellule sur un WLAN s'effectue via des mécanismes de roaming (itinérance) proche des systèmes utilisés sur le réseau GSM.

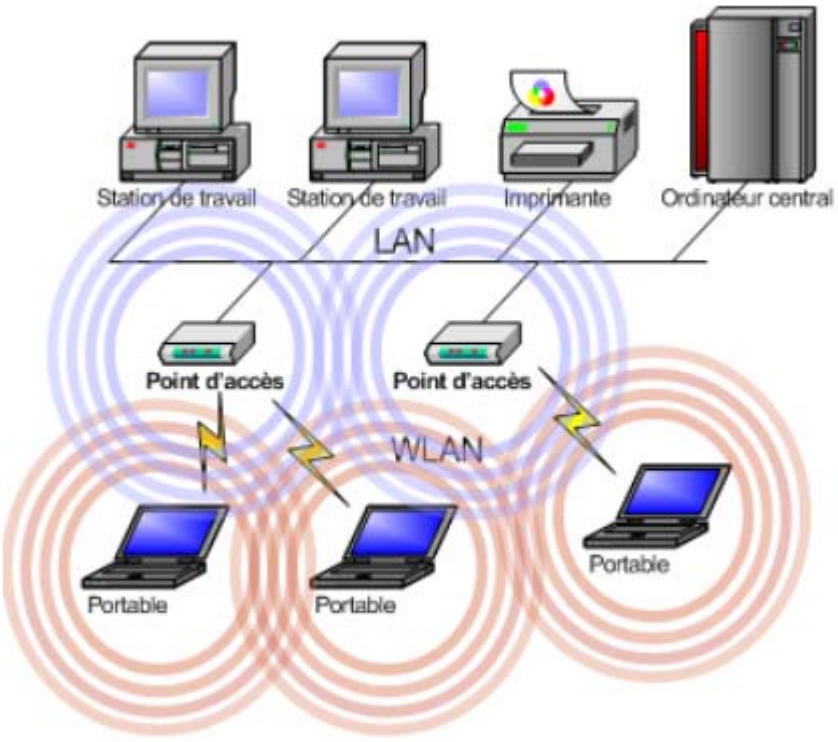


Figure 1 : Exemple de WLAN

Pour rester dans le cadre d'un WLAN, il faut que le réseau respecte deux conditions :

- La zone de couverture utile doit être de l'ordre d'un bâtiment ou d'un site.
- L'infrastructure réseau utilisée doit être contrôlée par l'entreprise.

Selon leur vocation les WLAN peuvent être :

- **Des WLANs privés ou d'entreprise** : les terminaux mobiles servent à des employés dans l'enceinte de l'entreprise pour accéder au système d'information traditionnel.

  Exemple : Dans un hôpital, les médecins vont de chambre en chambre tout en accédant aux dossiers des patients en ligne et aux applications médicales depuis des PC portables.

- **Des WLANs publics ou hot-spots :** les terminaux mobiles appartiennent dans ce cas à des clients accédant à une ressource particulière (le plus souvent un accès à Internet) proposée par le propriétaire du hot-spot.

  Exemple : Des hôtels, des aéroports ou des cyber-cafés mettent à la disposition de leurs clients un accès Internet sans-fil.

- **Des WLANs domestiques :** un particulier forme un réseau sans-fil pour connecter un ou plusieurs PC et son accès Internet (routeur ADSL Wi-Fi par exemple).

Tous ces WLANs utilisent des technologies semblables mais leur intégration est très différente.

2.1.2. Les réseaux sans-fil étendus

Les réseaux sans-fil étendus reposent exactement sur le même principe que les WLANs mais avec des zones de couverture nettement plus larges, allant de la ville au monde entier. Ils sont souvent basés sur des technologies télécoms (GSM, GPRS, UMTS…) ou des normes radios propriétaires.

On parle de WMANs (Wireless Metropolitan Area Network) ou de WWANs (Wireless Wide Area Network) selon les distances.

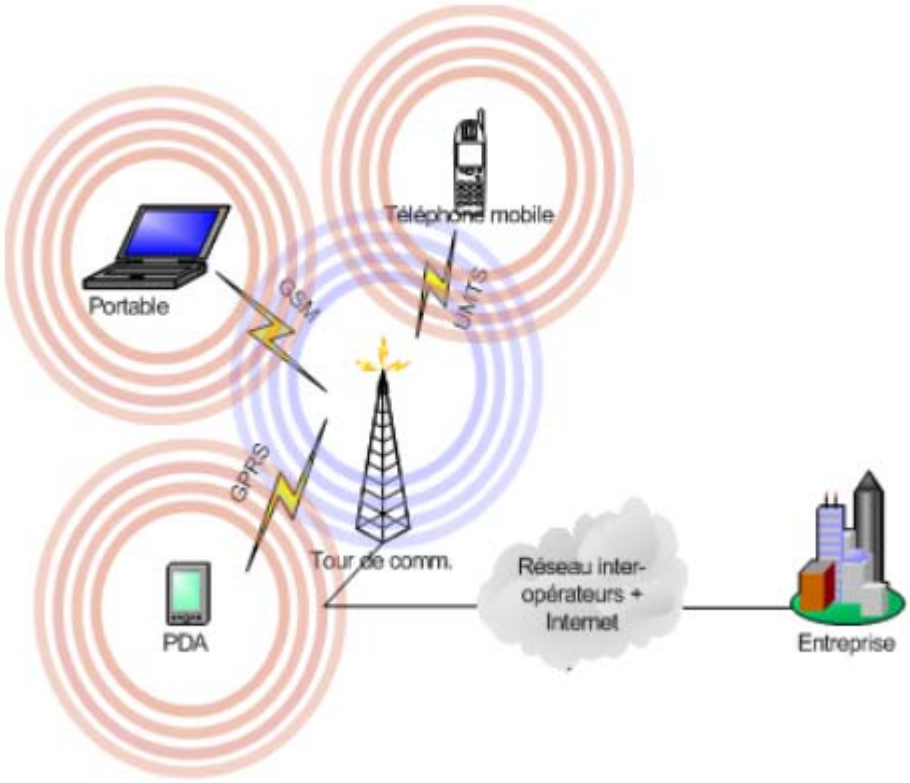


Figure 2 : Exemple de WWAN ou WMAN

Les WWANs peuvent être catégorisés de la façon suivante :

- **Les WWANs publics :** ils sont mis en œuvre par des opérateurs pour offrir des services réseaux à un grand nombre de clients mobiles. Ce sont l'équivalent des hot-spots publics des WLANs mais à plus grande échelle.

  Exemple : Les opérateurs télécoms offrent des accès Internet ou des services de messagerie accessibles sur des téléphones mobiles évolués.

- **Les WWANs privés sur infrastructure publique :** ces WWANs sont mis en place par les entreprises pour relier leurs terminaux mobiles à leurs systèmes d'information via une infrastructure publique de type télécom. Un WWAN de ce type est une véritable extension d'Internet.

Exemple : Les employés nomades accèdent à l'intranet et à la messagerie interne de l'entreprise depuis leurs PDA connectés en GPRS sur Internet.

- **Les WWANs totalement privés :** assez rares dans le secteur civil, les WWANs totalement privés connectent sur de grandes distances les terminaux mobiles d'une entreprise à un central via une infrastructure réseau radio privée.

  Exemple : Une compagnie de taxi connecte par liaison radio dédiée sa flotte de véhicules à son système informatique.

2.1.3. Les réseaux sans-fil spécifiques

Il existe des WLANs particuliers ne concernant pas directement des utilisateurs : par exemple un réseau de caméras de surveillance sans-fil, un réseau connectant des horodateurs ou des distributeurs de boisson avec un serveur… Beaucoup de ces réseaux sont complètement nouveaux ou prennent un nouvel essor grâce aux WLANs.

On peut également considérer les systèmes de téléphones sans-fil radio basés sur DECT comme des WLANs. Une fois que la qualité de service sera mieux implémentée sur les WLANs, le mariage de la voix sur IP et des technologies Wi-Fi donnera des applications VoIPoWLAN intéressantes.

Les réseaux sans-fil de type infrastructure ne se limitent pas aux seuls réseaux de technologie Wi-Fi : tout composant mobile connecté à un point d'accès via un lien aérien est à prendre en considération.

2.2. Les réseaux ad-hoc

Les réseaux ad-hoc sont connus sous le nom de WPAN (Wireless Personal Area Network) ou de réseaux personnels. L'objectif de ces réseaux est de fournir une connectivité sans infrastructure dédiée. Ils sont donc exclusivement point à point et ne comptent en général que deux participants :

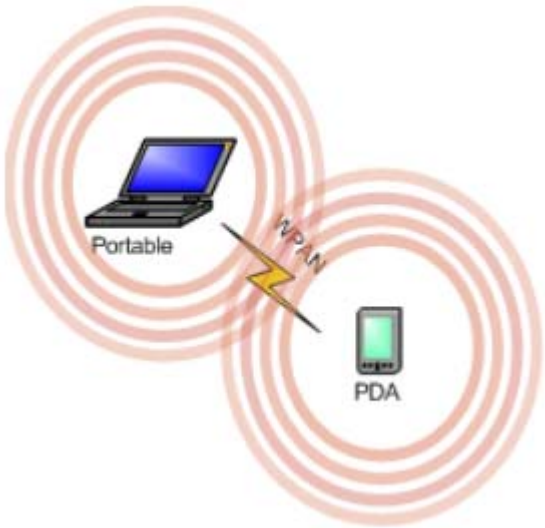


Figure 3 : Exemple de WPAN

Les terminaux mobiles friands de connectivité sans-fil comme les nouveaux téléphones portables et les PDA rassemblent la majeure partie des applications actuelles des WPANs.

Exemples : l'échange de carte de visite ou de fichiers en infrarouge entre deux PDA, la connexion d'un PDA avec un téléphone mobile en Bluetooth pour permettre un accès Internet GPRS, la connexion sans-fil d'un PDA sur une imprimante, …

Les WPANs ont beaucoup d'avenir dans les réseaux dédiés entre des équipements non informatiques, en particulier dans la domotique.

Exemples : les connexions utilisées par les périphériques comme les claviers et les souris sans-fil, la connexion sans-fil Bluetooth entre un lecteur CD portable et le casque audio…

Les WPANs sont exceptionnellement variés et doivent être considérés comme des réseaux sans-fil à part entière, surtout du point de vue de la sécurité.

2.3. Les réseaux point à point

Ce type de réseau sans-fil englobe toutes les liaisons point à point longue distance utilisées pour relier des bâtiments ou des sites distants. Ces réseaux utilisent généralement des équipements spécifiques comme des antennes directionnelles ou des technologies plus pointues (liaison laser par exemple) :

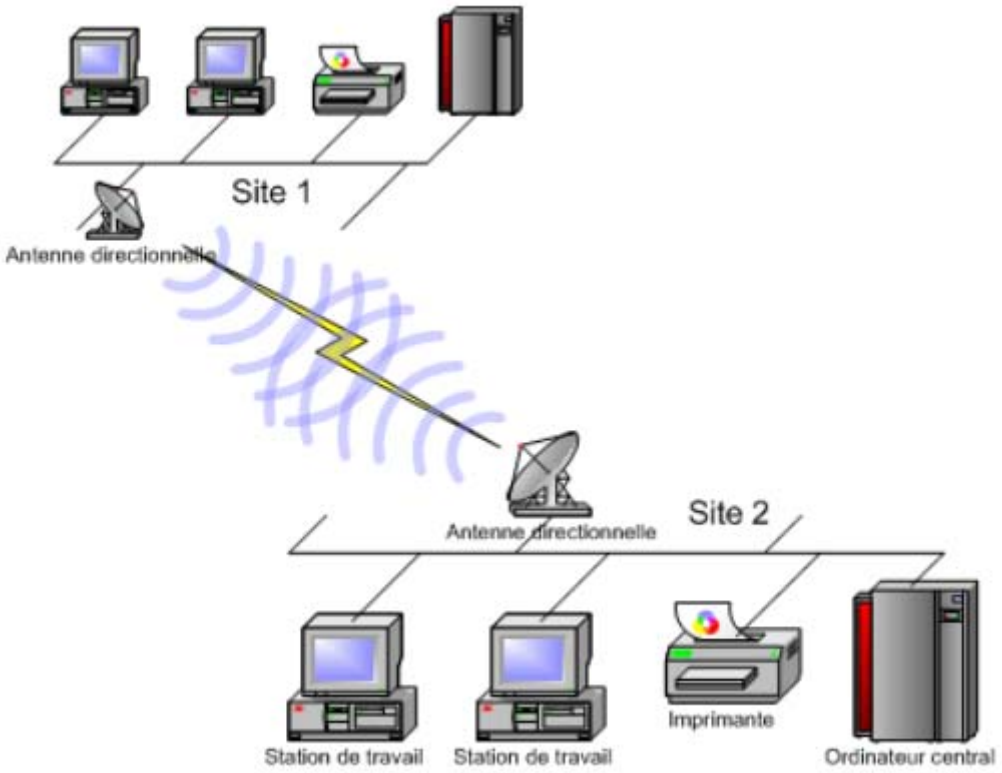


Figure 4 : Exemple de liaison point à point

Ce type de liaison peut encore se heurter à d'importants problèmes légaux : même si l'ART (Autorité de Régulation des Télécommunications, organisme régissant en particulier l'utilisation des fréquences radio en France) assouplit certaines lois, la réglementation reste assez stricte sur les réseaux radio en extérieur.

2.4. Les réseaux point à multipoint

Les réseaux point à multipoints sont semblables à ceux formés par les stations radios ou la télévision hertzienne traditionnelle : un émetteur diffuse une information à un nombre important de récepteurs sur des distances pouvant être étendues. Ces réseaux sans-fil particuliers restent encore très spécialisés.

La montée en puissance des normes pour les accès sans-fil à large bande passante sur de longues distances va probablement ouvrir la voie à de nouvelles applications, informatiques ou non, pour ce type de réseau.

3. Pourquoi utiliser un réseau sans-fil ?

Les motivations pour utiliser un réseau sans-fil ne manquent pas, que ce soit pour améliorer un système d'information existant ou pour mettre en place des applications entièrement nouvelles. Dans tous les cas le retour sur investissement apporté par ces technologies est exceptionnel.

Voici un bref aperçu des différents avantages des solutions sans-fil :

- **Mobilité :** les utilisateurs sont généralement très satisfaits des libertés offertes par les réseaux sans-fil et de fait sont plus enclin à utiliser les moyens informatiques mis à leur disposition. Le gain en productivité est important.

- **Evolutivité** : ces réseaux peuvent être dimensionnés au plus juste et suivre simplement l'évolution des besoins par simple ajout ou suppression de points d'accès par exemple.

- **Souplesse et facilité d'utilisation** : un système sans-fil peut être utilisé dans des installations temporaires (manifestation, salon…), couvrir des zones non accessibles aux câbles et relier facilement des bâtiments ou des sites distants. En étant peu intrusifs, ils permettent des installations dans un monument classé par exemple.

- **Coût réduit :** si leur installation est souvent plus coûteuse que celle d'un réseau câblé, les réseaux sans-fil ont des coûts de maintenance très réduits. Sur le moyen terme, l'investissement est facilement rentabilisé.

4. Aperçu des différentes normes radio

Comme toutes les technologies naissantes, les réseaux sans-fil font l'objet d'un nombre impressionnant de normes en constante évolution et malheureusement pas toujours interopérables… Voici un aperçu rapide des principales normes radio actuellement en vigueur.

4.1. Les normes WLAN

Plusieurs normes concurrentes se partagent aujourd'hui le marché des WLANs. Parmi celles-ci, les normes IEEE 802.11 ont de très bonnes chances de devenir le standard incontesté pour les WLANs.

4.1.1. IEEE 802.11 / Wi-Fi

La Wi-Fi Alliance (anciennement WECA), créée en 1999 pour certifier l'interopérabilité des équipements utilisant 802.11, a été un moteur fort pour l'intégration de la norme 802.11b dans les équipements réseaux et les systèmes sans-fil.

A présent, la majorité des WLANs est actuellement basée sur les normes IEEE 802.11 et en particulier la 802.11b.

De plus, depuis fin 2003, l'ART a assouplit considérablement les conditions d'utilisation de la bande de fréquence des 2,4GHz en France, faisant évoluer le périmètre d'actions des WLAN 802.11 (voir la partie réglementation en 4.1.1.3).

4.1.1.1. Les principales normes de transport 802.11

Il existe aujourd'hui trois grandes variantes de 802.11 définissant trois protocoles de transport bien distincts :

802.11b	**Norme dominante ratifiée en 1999.** Débit théorique de 11Mbps (environ 6Mbps effectif) sur la bande de fréquence des 2.4 GHz (14 canaux dont 13 utilisables en Europe (ETSI) et dont 3 seulement ne se recouvrent pas). Modulation DSSS (nommée séquence directe ou système à spectre dispersé avec séquences continues).
802.11a	**Norme à haut débit ratifiée en 1999.** Débit théorique de 54Mbps (environ 30Mbps effectif) sur la bande de fréquence des 5 GHz (8 canaux avec 52 porteuses). Non compatible avec la norme 802.11g et non utilisable en extérieur en France. Modulation OFDM (Orthogonal Frequency Division Multiplexing)
802.11g	**Norme à haut débit ratifiée en 2003.** Débit théorique de 54 Mbps (environ 30Mbps effectif) sur la même bande de fréquence que le 802.11b (2.4Ghz).

	Modulation OFDM et DSSS (en fonction du data rate). Compatibilité ascendante avec le 802.11b.

Note :
L'IEEE travaille actuellement sur 802.11n, un projet de norme haut débit dans la famille des 802.11. Ce standard devrait permettre dans un premier temps un débit réel de 100Mbps pour puis de 320Mbps. Il travaillerait sur la bande de fréquence des 2.4 GHz et 5GHz. Il serait compatible avec la norme 802.11 et intègrerait les spécifications de sécurité 802.11i, de qualité de service 802.11e et de handover 802.11f. L'IEEE y ajouterait aussi de nouveaux algorithmes de compression et une meilleure gestion des pertes/erreurs et des interférences. 802.11n pourrait devenir le futur standard incontournable pour les WLANs mais des spécifications ne verront probablement le jour qu'en 2006.

4.1.1.2. Les extensions de la norme 802.11

Voici un aperçu des différentes extensions du 802.11 :

- **802.11b.corl :**
  L'objectif de cette extension est de corriger les problèmes liés au MIB (Management Information Base) dans le 802.11b.

- **802.11d :**
  L'objectif de cette extension est l'utilisation à l'échelle internationale des normes 802.11. Elle permet aux différents équipements d'ajuster automatiquement la bande de fréquence entre un client et un point d'accès afin de s'adapter aux réglementations locales du pays. Cette norme est déjà implémentée dans certains équipements.

- **802.11e :**
  802.11e est la norme de qualité de service (QoS) au niveau de la couche liaison de données (L2). Elle permet de définir les besoins des différents paquets en terme de bande passante et de délai de transmission. La QoS est un point important, en particulier pour les applications multimédia (Voix/Téléphone VoWLAN, Vidéo, …). Elle s'applique sur le 802.11 a, b et g.

- **802.11f :**
  Cette extension regroupe les recommandations d'interopérabilité des produits à l'intention des fabricants.

- **802.11h :**
  802.11h modifie légèrement 802.11a pour le rapprocher des normes européennes en intégrant une fonction TPC (Transmission Power Control) permettant d'optimiser la puissance de transmission et une fonction DFS (Dynamic Frequency Selection) permettant de sélectionner le canal radio le plus adéquat par rapport aux interférences possibles avec

les autres équipements. Les équipements compatibles 802.11h sont prévus pour Q1 2004.

- **802.11i :**

  802.11i est le volet sécurité de la norme 802.11 s'appliquant au 802.11 a, b et g. 802.11i est largement détaillé dans la suite de ce document.

4.1.1.3. Cadre réglementaire et technique de déploiement des réseaux sans fil

Depuis le 25 juillet 2003, suite à des négociations entre le Ministère de la Défense et l'ART (Autorité de Régulations des Télécommunications), l'attribution des fréquences sur la bande des 2,4GHz a été modifiée.

Le tableau suivant récapitule les puissances autorisées dans les bandes de fréquence 2,4GHz et 5GHz en France (métropole uniquement). Les puissances sont exprimées en PIRE (puissance isotrope rayonnée équivalente) :

<table>
<tr><th>Puissance autorisée / Bande de fréquences</th><th>Utilisation en intérieur</th><th>Utilisation en extérieur</th></tr>
<tr><td>2400

2454</td><td rowspan="2">100mW</td><td>100mW</td></tr>
<tr><td>

2483,5</td><td>10mW</td></tr>
<tr><td>5150

5250</td><td>200mW</td><td rowspan="2">IMPOSSIBLE</td></tr>
<tr><td>5250

5350</td><td>200 mW avec DFS/TPC ou équivalent
ou 100mW avec DFS uniquement</td></tr>
<tr><td>5470

5725</td><td>IMPOSSIBLE</td><td>IMPOSSIBLE</td></tr>
</table>

Dans le cas d'un déploiement de réseau WLAN ouvert au public, le cadre de réglementation a lui aussi été assoupli depuis le 25 juillet 2003. Un cadre expérimental est maintenu, au moins jusqu'à la fin 2004, pour permettre à des initiatives originales de se développer dans un cadre peu restrictif.

Il est simplement demandé aux opérateurs, dans l'esprit des nouvelles directives, de déclarer leur activité à l'ART, en communiquant notamment une brève description de leur projet, la date prévue pour le lancement, la localisation de l'expérimentation.

4.1.2. Hiperlan et Hiperlan2

La norme Hiperlan2 est une norme européenne standardisée par l'ETSI et concurrente directe du 802.11a. Elle possède les mêmes caractéristiques techniques que le 802.11a : bande de fréquence en 5GHz, débit de 54Mbps, fonctionnalité DFS (Dynamic Frequency Selection) et TPC (Transmit Power Control).

Face à la norme Wi-Fi appuyée par la plupart des industriels, le standard Hiperlan2 a eu du mal à se démarquer. Aujourd'hui les premiers produits sont prêts et présentent quelques avantages non négligeables, en particulier sur la gestion de la qualité de service et sa bonne adaptation avec les contraintes européennes.

A moyen terme, il est probable que les normes Hiperlan soient progressivement abandonnées au profit du 802.11.

4.1.3. HomeRF

Cette technologie évolue sur la bande de fréquence 2,4GHz et est utilisée dans certains réseaux pour particuliers.

Depuis la dissolution du groupe de travail HomeRF en janvier 2003, cette technologie a été quasiment laissée à l'abandon, ce qui a certainement profité au développement du Wi-Fi.

4.2. Les normes WMANs et WWANs

En Europe, la plupart des WWANs actuels sont basés sur des technologies télécoms capables de transporter à la fois des données informatiques et de la voix :

- Le GSM (faible débit et facturation à la durée)
- Le GPRS (basé sur le GSM mais permettant des débits plus élevés et une facturation au volume de données échangées).
- Le futur UMTS qui permettra des applications beaucoup plus évoluées via des débits nettement plus élevés que le GSM / GPRS.

Les autres réseaux étendus civils reposent sur des protocoles radio traditionnels et propriétaires.

Des projets de création de WMANs basés sur des normes WLAN mises en place à l'échelle d'une ville sont actuellement à l'étude sous les groupes de travail IEEE 802.16 (Broadband Wireless Access) et 802.20 (Mobile Broadband Wireless Access).

> **Note :**
> *IEEE 802.16 est également connu sous le nom de WiMAX d'après l'organisation du même nom.*

La couverture de villes par des hot-spots publics étendus basés sur 802.11 pourrait concurrencer sérieusement ou venir en complément des protocoles télécoms, surtout l'UMTS. Une autre application des WMANs 802.11 envisagée est d'offrir un accès Internet haut débit dans des zones non couvertes par l'ADSL.

4.3. Les normes WPANs

Les WPANs reposent également sur des protocoles variés. Les antiques connexions IrDA (Infrarouge) laissent progressivement la place à des technologies radios plus performantes. Plusieurs acteurs se partagent le monde des WPAN avec des applications variées.

4.3.1. IEEE 802.15.1 / Bluetooth

Bluetooth utilise la bande de fréquence 2,4GHz et permet d'atteindre un débit maximal théorique de 1Mbps avec une couverture de quelques mètres.

Du fait de sa faible consommation électrique, cette technologie est devenue le standard de raccordement courte distance sans-fil, soit le standard des WPANs.

Bluetooth est très utilisé pour les claviers/souris sans fil, les kits main libre ou écouteur, le tranfert de données entre un PC et les PDA/téléphones/Smartphones…

4.3.2. IEEE 802.15.3 / UWB (Ultra Wide Band)

Cette norme permettra de faire une connexion haut débit (de plusieurs centaines de Mbits à un Gbits) sur une courte distance.

4.3.3. IEEE 802.15.4 / ZigBee

Cette norme permettra de faibles débits (100kbps environ) mais avec une consommation électrique extrêmement réduite.

4.3.4. IEEE 802.11 / Wi-Fi

En plus de son mode infrastructure, la norme 802.11 peut être utilisée en mode ad hoc pour une utilisation proche du Bluetooth.

5. Les problématiques associées aux systèmes sans-fil

En faisant tomber la barrière de l'isolement physique sur lequel reposait la majeure partie de la sécurité interne des systèmes d'information, les réseaux sans-fil ont fait émerger des problématiques sécurité entièrement nouvelles.

En dépit de la variété des réseaux sans-fil, on retrouve dans tous les cas les mêmes problématiques mettant en péril le DICP (Disponibilité, Intégrité, Confidentialité, Preuve) des systèmes d'information :

Utilisation d'un système sans-fil
=
Perte du confinement physique de l'information
→ Risque d'espionnage
+
Perte de l'isolement physique des systèmes d'information
→ Risque d'intrusion
+
Perte de la fiabilité des liens câblés
→ Risque de dénis de service

5.1. La perte du confinement physique de l'information

Les systèmes sans-fil fonctionnent généralement en mode diffusion : les ondes radios se propagent sur toute la zone de couverture de l'émetteur. Tout récepteur adapté situé à portée est en mesure de capter ces ondes, donc le trafic réseau, et de l'analyser.

La portée utile des émetteurs est très variable en fonction de la technologie utilisée, du matériel et de l'environnement : quelques mètres pour Bluetooth, une petite centaine de mètres pour un point d'accès 802.11b.

Cependant il faut absolument faire la distinction entre la portée utile et la porté d'attaque : un simple amplificateur étend grandement la portée d'un récepteur. Ces amplificateurs sont courants, peu coûteux et une simple boite de biscuits peut servir de base à un amplificateur artisanal !

Pour un attaquant la zone de couverture radio réellement utile d'un WLAN s'étend largement au-delà de la zone de contrôle physique d'une entreprise : pour peu que des points d'accès sans-fil non sécurisés existent dans son réseau, son système d'information peut être facilement espionné à distance par un simple PC portable équipé d'une carte sans-fil passive.

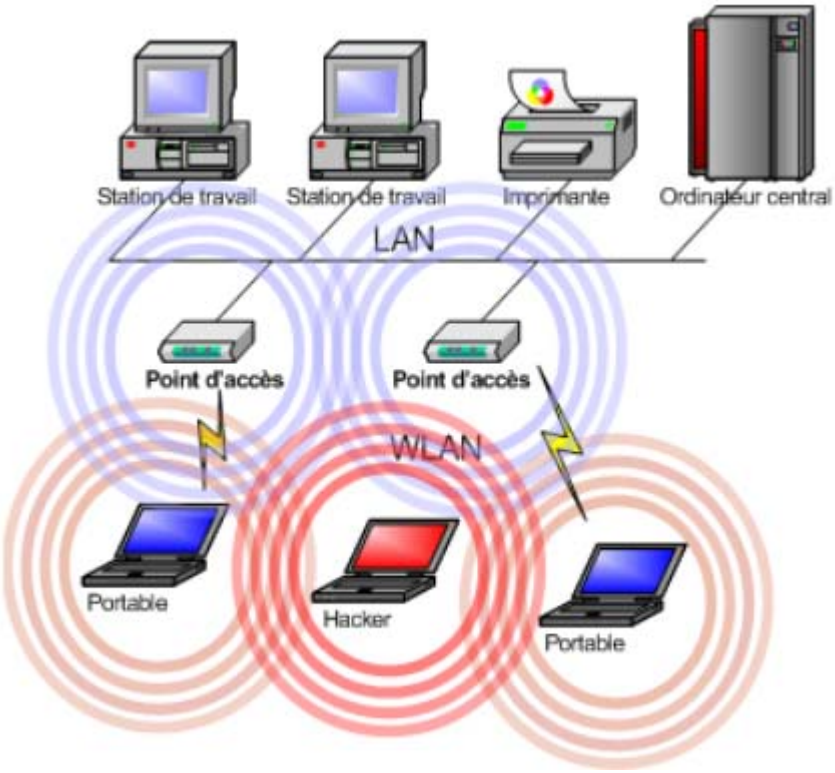


Figure 5 : Espionnage d'un WLAN

La mobilité des terminaux et les WPANs entraînent fréquemment la création de réseaux non sécurisés en dehors de l'entreprise. Un commercial synchronisant son PDA avec son portable en Bluetooth dans le train diffuse dans tout le wagon des informations parfois très critiques…

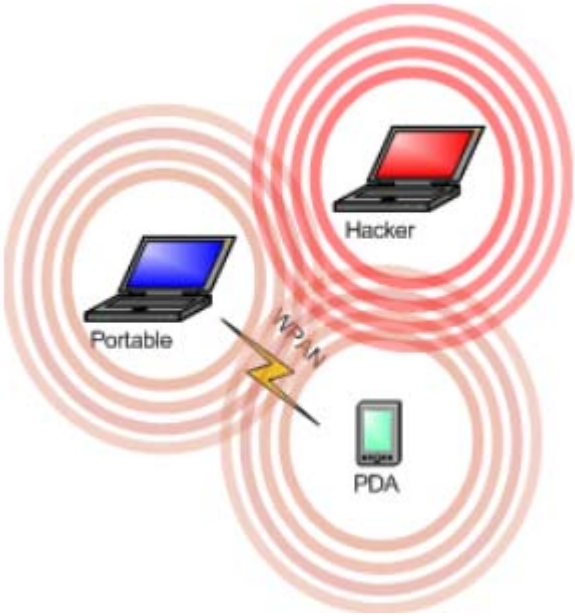


Figure 6 : Espionnage d'un WPAN

Les WPANs spécifiques sont également dangereux pour la confidentialité du système d'information : par exemple toutes les données saisies sur un clavier

sans-fil standard, dont les mots de passe, sont diffusées en clair dans tout le bâtiment !

En configuration par défaut presque aucun système sans-fil n'offre un chiffrement satisfaisant du trafic sur le segment radio. Pour les réseaux Wi-Fi, le trafic passe tout simplement en clair avec une configuration par défaut ! Pire, les solutions de chiffrements proposées en standard dans le 802.11 comme le WEP sont notoirement inefficaces.

L'utilisation d'un système sans-fil non chiffré expose fortement la confidentialité des données. L'espionnage à distance de ce type de réseau est facile et sans risque pour l'attaquant.

5.2. La perte de l'isolement physique des systèmes d'information

Les systèmes sans-fil remettent en question les politiques de sécurité classiques. En effet, la plupart des entreprises sont actuellement des villes fortifiées : des murailles bien conçues (firewalls, proxy…) et bien gardées (système de détection d'intrusion) isolent de l'extérieur les ressources internes critiques. Les défenses périphériques sont fortes mais, une fois dans la ville, les systèmes de sécurité sont faibles ou inexistants : le réseau interne est une zone considérée à tort comme sécurisée de nature (zone de confiance).

Tout équipement disposant d'une interface sans-fil active, que ce soit un point d'accès Wi-Fi ou un terminal utilisateur équipé d'un adaptateur réseau Bluetooth actif par exemple, est attaquable directement depuis l'extérieur. Ces équipements constituent alors autant de portes potentielles vers les ressources informatiques auxquelles ils sont connectés par le réseau câblé.

Les défenses périphériques de l'entreprise ne sont plus à même de sécuriser seules les ressources internes contre les intrusions : elles peuvent se retrouver complètement court-circuitées depuis l'extérieur. Dans le cas des équipements mobiles, ces défenses ne rentrent même plus en ligne de compte.

Une attaque contre un équipement via son interface sans-fil peut être menée sans équipement spécifique depuis n'importe quel point de la zone de couverture radio utile, donc depuis des zones non contrôlées physiquement par l'entreprise.

Le facteur aggravant est que la majorité des systèmes sans-fil est conçue dans un esprit d'ouverture et de connectivité : dans les configurations par défaut, tout est pensé pour faciliter l'accès au réseau au détriment de la sécurité.

5.2.1. L'ouverture sur l'extérieur des réseaux internes

En standard, les points d'accès d'un WLAN 802.11 ne demandent pas d'authentification : les paramétrages par défaut sont pensés pour faciliter au maximum la vie des utilisateurs. En d'autres termes si un point d'accès est sorti de sa boite et branché sur le réseau, il va commencer à se signaler au niveau radio et à diffuser toutes les informations nécessaires pour que les

cartes sans-fil à portée se connectent. Toute demande de connexion sera acceptée sans autre forme de procès et le point d'accès ira jusqu'à chercher sur le serveur DHCP de l'entreprise des adresses IP libres pour les nouveaux venus !

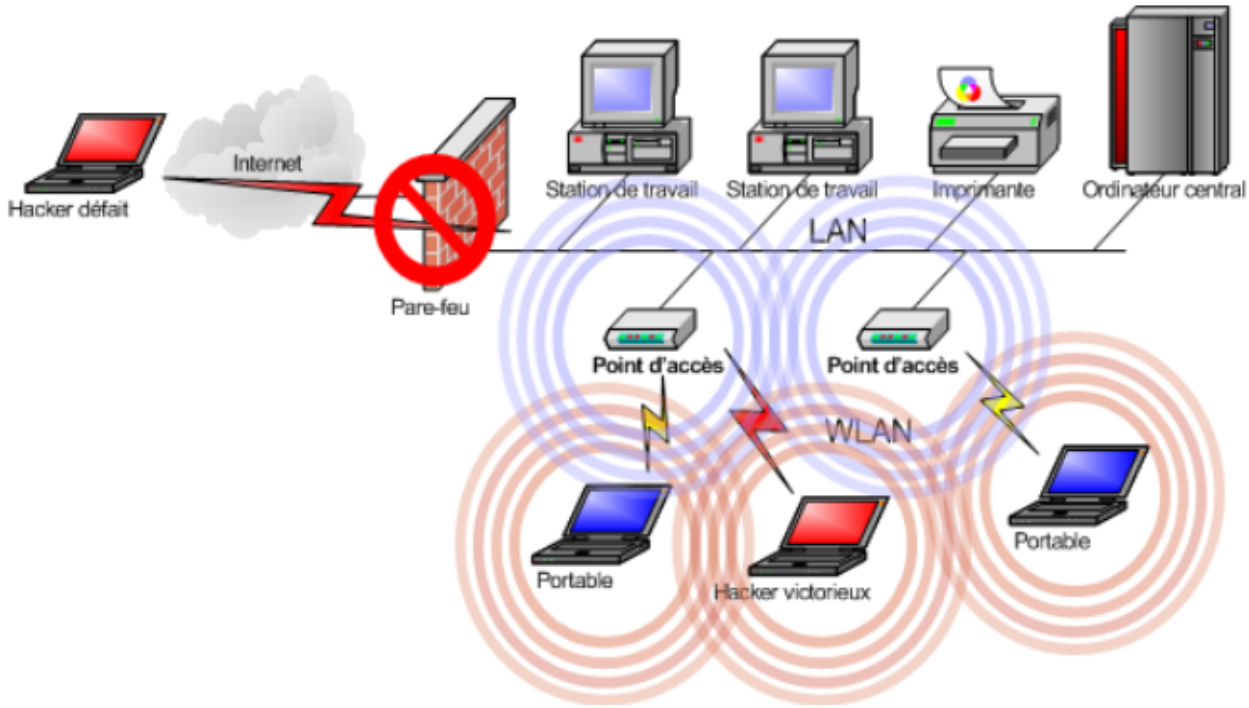


Figure 7 : Intrusion sur un LAN via un WLAN

Le pire est que les points d'accès constituant un WLAN sont généralement connectés sans précaution directement sur le LAN interne de l'entreprise et donnent donc accès au cœur des ressources informatiques internes peu sécurisées…

Un WLAN non sécurisé rend réellement triviale une intrusion à distance sur le réseau interne de l'entreprise et revient schématiquement à installer dans la rue des prises réseau brassées sur le LAN !

5.2.2. L'ouverture sur l'extérieur d'équipements utilisateurs

Un attaquant peut tenter de se connecter directement sur tout équipement disposant d'une interface sans-fil active en mode ad-hoc en établissant un WPAN pirate entre sa victime et sa propre machine. S'il y parvient, il lui est possible d'attaquer l'équipement lui-même et toutes les ressources qui lui sont connectées !

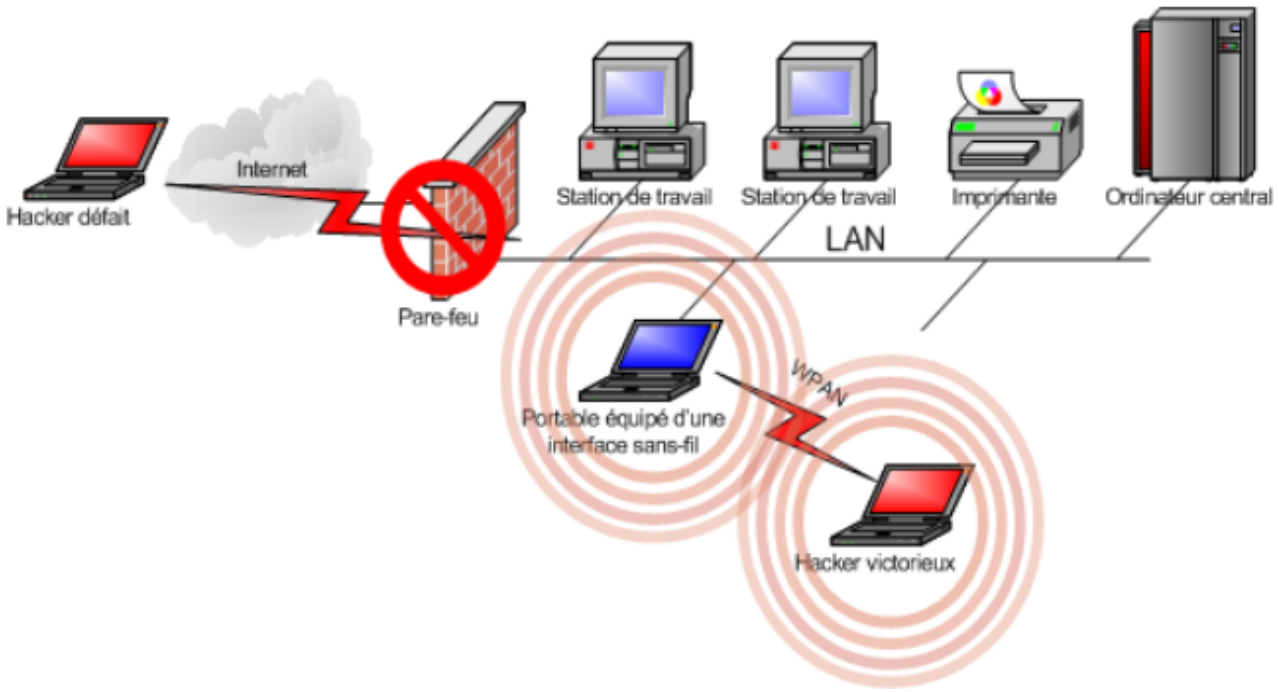


Figure 8 : Intrusion sur un LAN via un WPAN

Les équipements ciblés sont en grande partie des postes ou des terminaux utilisateurs, mobiles ou non. Ces derniers ne sont pas préparés à ce type de menace : jusqu'à présent une attaque informatique directe contre ces équipements présupposait une intrusion physique, un vol…

Il est devenu excessivement dangereux de se reposer exclusivement sur des défenses périphériques, même si elles sont fortes, pour prévenir les intrusions informatiques. L'ouverture sur l'extérieur des ressources internes à travers des systèmes sans-fil doit s'accompagner de la mise en place de mesures de sécurité adaptées comme par exemple :

- **L'intégration des systèmes sans-fil dans des architectures sécurisées (cloisonner les WLAN du LAN par exemple).**
- **La mise en place de solutions d'authentification des utilisateurs et des équipements matériels.**
- **La sécurisation des terminaux mobiles ou fixes exposés.**
- **Le renforcement de la sécurité interne générale du système d'information.**

5.2.3. La maîtrise délicate de l'espace radio

Si un WLAN mal intégré remet en cause la sécurité de l'entreprise, que dire des dispositifs sans-fil connectés au LAN à l'insu des responsables informatiques ?

En interne, cela peut être un point d'accès connecté au réseau par un utilisateur inconscient ou plus couramment encore par un informaticien faisant quelques tests. Ces points d'accès, généralement qualifiés de renégats, sont bien plus courants dans les entreprises que l'on pourrait l'imaginer et ne

sont bien sûr jamais sécurisés. On retrouve l'épineuse problématique des modems non contrôlés…

Nous estimons qu'actuellement environ 35% des entreprises françaises hébergent au minimum un point d'accès Wi-Fi renégat.

La plupart des équipements connectés au LAN câblé standard d'une entreprise et disposant d'une interface sans-fil sont également éligibles au rang de point d'accès renégat : un PC sur le LAN avec une carte 802.11b active en mode had-hoc est une véritable passerelle vers les ressources informatiques internes.

Le problème est que ces interfaces sans-fil, d'ailleurs rarement utilisées et intégrées dans la politique de sécurité, prolifèrent littéralement sur les PC portables, les PDA et même les stations de travail.

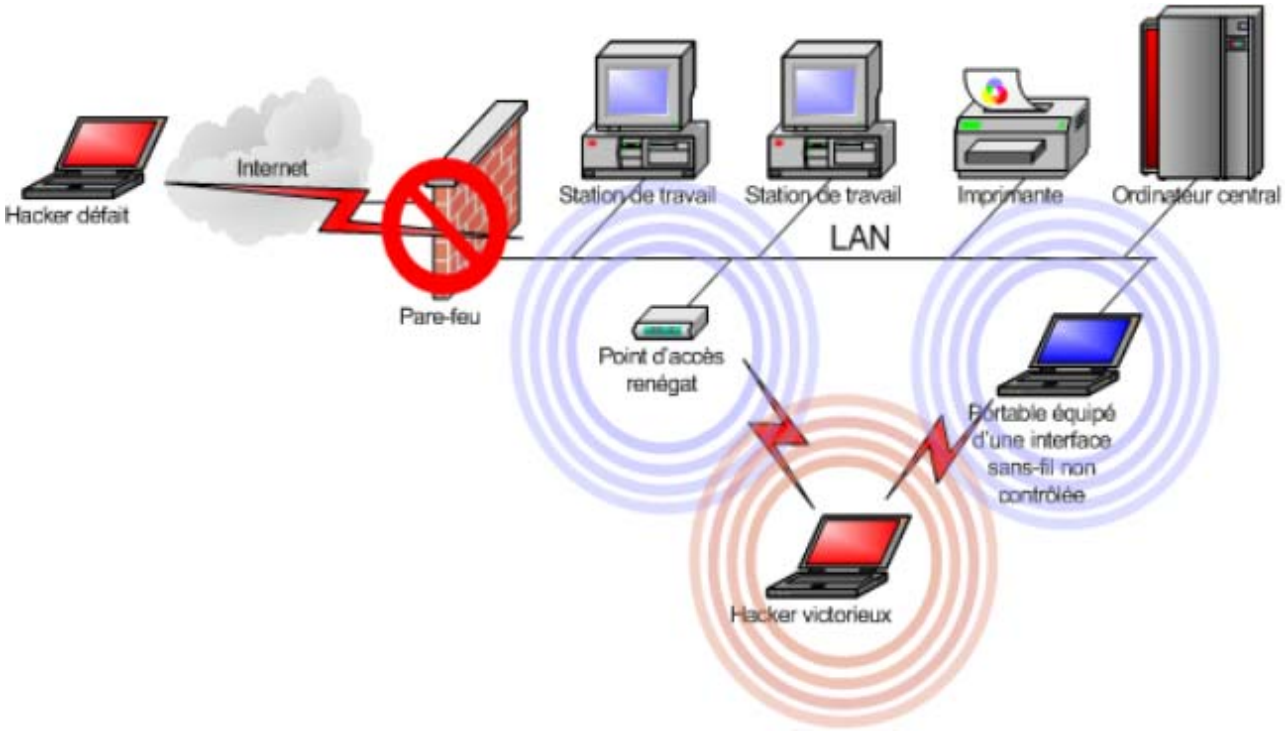


Figure 9 : Intrusion sur un LAN via un système sans-fil renégat

Il faut donc bien être conscient que les problématiques sécurité des réseaux sans-fil sont à prendre en compte dans toutes les entreprises, même dans celles n'ayant pas comme projet d'utiliser un WLAN.

Enfin, la baisse des prix et la miniaturisation des équipements sans-fil font que les pirates n'hésitent plus à utiliser des points d'accès comme vecteur d'attaque. Plusieurs attaques sont envisageables, par exemples :

- L'installation d'un point d'accès Wi-Fi renégat directement sur le réseau câblé de leurs victimes.
- L'insertion à distance dans un WLAN d'un point d'accès pirate via les mécanismes de chaînage d'équipement ou de mise en haute disponibilité.

- La création d'un WLAN pirate parallèle sur lequel les utilisateurs vont se connecter automatiquement en pensant être sur le réseau de l'entreprise.

L'audit régulier de l'espace radio de l'entreprise est important pour détecter les équipements non autorisés et faire le point sur la sécurité des systèmes sans-fil.

5.3. La perte de la fiabilité des liens câblés

La qualité de service sur un réseau sans-fil est un point sensible. Si elle a été relativement bien maîtrisée dans le cadre de la téléphonie mobile, elle reste un sujet à problème pour les WLANs ou les liaisons point à point.

En effet, la qualité finale d'une connexion réseau radio est influencée par de nombreux paramètres extérieurs très divers : la distance entre l'émetteur et le récepteur, la pollution de la bande de fréquence utilisée, le nombre d'utilisateurs se partageant la bande passante du point d'accès… Maintenir une qualité de service optimale dans des conditions de production normales nécessite une infrastructure réellement bien pensée et adaptée aux besoins.

Cependant cela devient nettement plus complexe quand il faut prendre en compte la disponibilité de l'infrastructure et les risques d'atteinte volontaire à la qualité du service.

Les communications radio ont un long historique, particulièrement militaire, en matière d'attaque par déni de service. Les guerres récentes ont démontré que les armées modernes sont capables de mettre rapidement et à distance une véritable chape de plomb sur toutes les communications radio de l'ennemi. Les principes issus des techniques militaires de déni de service (DoS) radio sont tout à fait utilisables dans le milieu civil.

Il est impossible de faire le tri dans les ondes avant que celles-ci n'atteignent les équipements radio : dès lors créer une interruption ou une perturbation du service est relativement aisé, qu'elle soit temporaire (simple brouillage par pollution de bande de fréquence) ou de longue durée (destruction à distance des équipements radio : bombes électromagnétiques artisanales par exemple).

En plus des attaques orientées radio, de nombreuses attaques DoS réseaux ou logiques sont dès à présent opérationnelles et faciles à mettre en œuvre sans équipement spécifique pour perturber le fonctionnement des réseaux sans-fil.

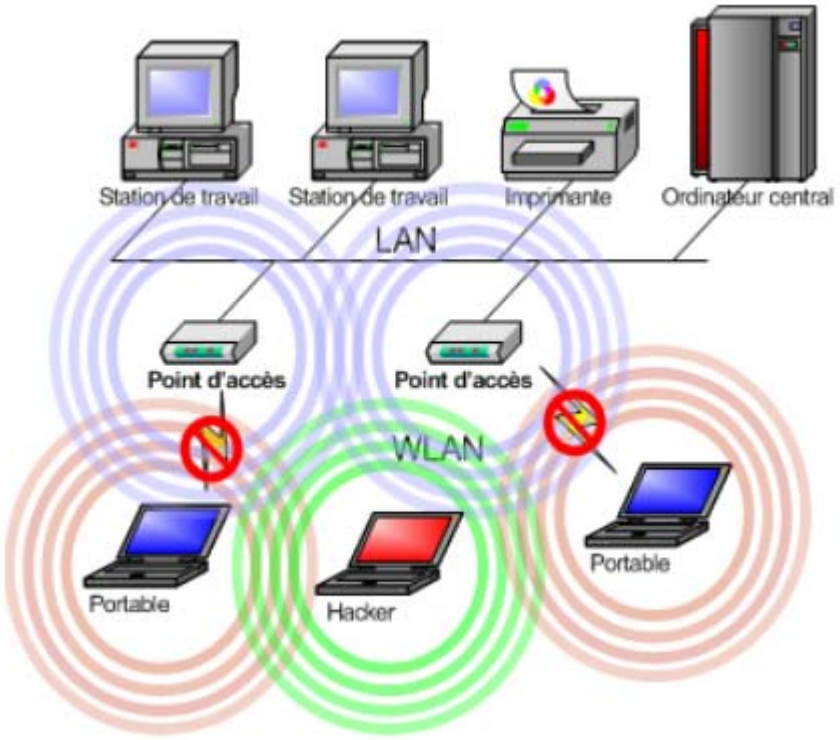


Figure 10 : Dénis de service sur un WLAN

Les architectures sans-fil doivent être bien étudiées pour optimiser la qualité de service et réduire les conséquences d'attaques par déni de service. Dans les situations où la disponibilité du service est primordiale, l'utilisation des technologies sans-fil civiles actuelles doit faire suite à une étude approfondie.

6. La menace

Mal intégrés, les systèmes sans-fil ouvrent une voie royale aux pirates informatiques. Ces derniers ne s'y sont d'ailleurs pas trompés : leurs communautés sont en pleine ébullition. A présent nous estimons que les attaques réussies portées via les systèmes sans-fil ont largement dépassé en nombre les attaques via les accès Internet, et pour cause :

- **La prise de risque est faible** : Prendre d'assaut un réseau sans-fil fait prendre très peu de risque à l'attaquant, voir aucun dans le cas du simple espionnage : les actions sont menées à distance et ne laissent pas de traces exploitables pour remonter jusqu'au coupable.

- **Le gain potentiel est énorme** : Quel que soit l'objectif du pirate, espionnage, intrusion ou simple déni de service, son "retour sur investissement" peut être très important, d'autant plus que contrairement aux attaques Internet, les grandes entreprises ou organisations gouvernementales sont encore très vulnérables.

- **Les compétences nécessaires sont minimes** : Un simple portable, voir un PDA, équipé d'une carte 802.11b et un logiciel trouvé sur Internet peut pirater automatiquement 80% des points d'accès et donner accès aux LANs…

Ce n'est donc pas un hasard si le war-driving (détection et piratage automatisé de réseaux sans-fil vulnérables à bord d'une voiture) devient une véritable mode dans les centres urbains. Aux Etat-Unis, certains sont même passés au war-flying (même principe à bord d'un hélicoptère) ou mettent en place un système de tag fait à la craie (war-chalking) indiquant la proximité et les caractéristiques d'un point d'accès :

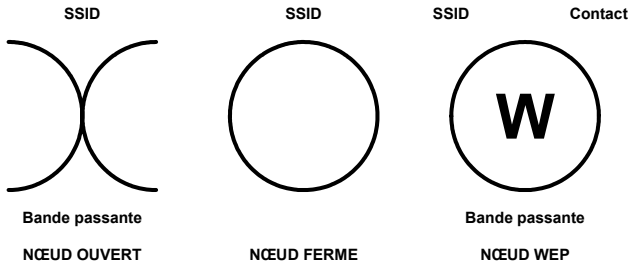


Figure 11 : Exemple de war-chalking

La problématique sécurité des systèmes sans-fil est bien réelle et ne relève pas de la paranoïa aiguë : les failles existent, sont faciles à exploiter et des milliers de pirates n'ont de cesse de s'y engouffrer, par jeu ou pour des raisons plus malsaines : espionnage, intrusion, déni de service…

7. Les méthodes de sécurisation

S'il est clair que les problématiques de sécurité posées par les réseaux sans-fil sont réelles et complexes, elles ne restent heureusement pas sans réponse. En effet, des systèmes éprouvés, venus en grande partie du monde de la sécurité LAN et Internet, permettent de sécuriser simplement et efficacement les systèmes sans-fil ou de se prémunir d'une utilisation néfaste.

La première et principale solution est de bien prendre en compte les technologies sans-fil dans la réflexion sur la sécurité globale de l'entreprise.

Les réseaux sans-fil pouvant avoir des formes et des applications très variées, il est impossible de parler de solution de sécurité clé en main. Il est évident que l'on ne sécurise pas un WLAN comme un WPAN ou un réseau privé comme un hot-spot public. Chaque projet est réellement unique et doit être étudié puis intégré avec soin.

Cependant il est possible de dégager des concepts généraux qui sont autant de guides dans la définition des stratégies et des solutions de sécurité.

Note :
Dans la suite de cette partie, nous avons volontairement mis fortement l'accent sur la sécurité des WLANs 802.11.

7.1. La chaîne de sécurité d'un système sans-fil

La sécurité d'un système sans-fil ne se limite pas à la sécurisation des points d'accès. Il est en effet essentiel de prendre en compte tous les éléments qui forment la « chaîne de sécurité » du système, à savoir :

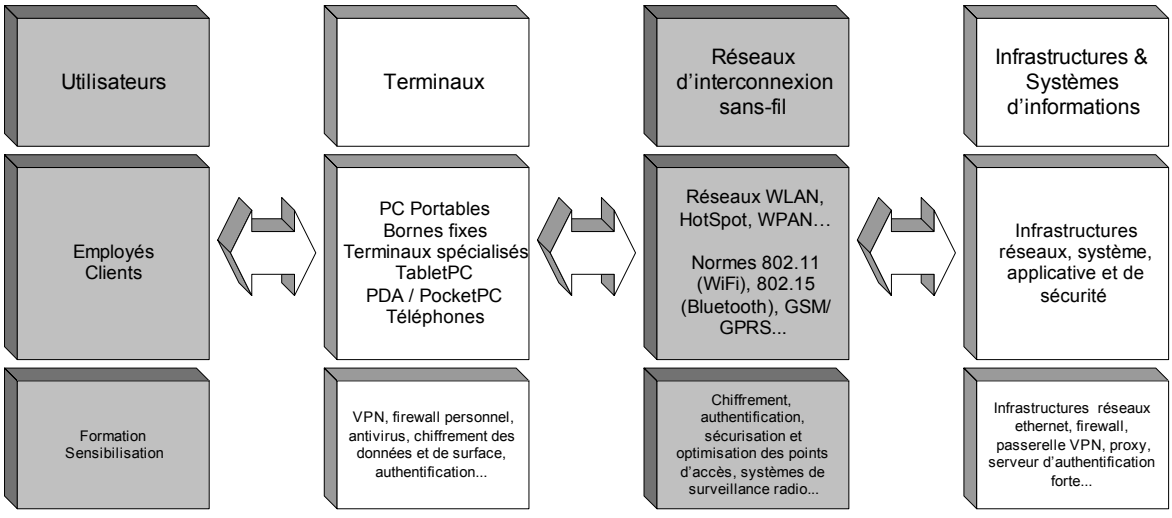


Figure 12 : Chaîne de sécurité

7.2. Les utilisateurs

Les utilisateurs sont au cœur des technologies sans-fil, domaine dans lequel ils sont d'ailleurs souvent moteurs au sein de l'entreprise. Généralement peu formés aux problématiques de sécurité informatique, ils font une utilisation intensive et parfois inconsciente de système sans-fil qui mettent gravement en péril la sécurité de leurs données, voir le système d'information de leur entreprise.

Aussi, les solutions techniques mises en place pour sécuriser un système sans-fil sont inutiles si elles ne sont pas accompagnées d'une forte sensibilisation et d'une formation sécurité de tous les acteurs : utilisateurs, administrateurs, responsables…

Cette sensibilisation est également indispensable dans les entreprises n'ayant pas de système sans-fil propre : en effet la plupart des employés sont ou seront à court terme des utilisateurs de systèmes sans-fil, que ce soit via un PDA, un PC portable, un hot-spot ou encore une installation Wi-Fi à leur domicile !

Un exemple classique : Le cadre non informé utilisant un modem ADSL/Wi-Fi domestique non sécurisé pour accéder à Internet quand il travaille chez lui avec son PC portable professionnel met en danger des données confidentielles et l'intégrité du système d'information !

7.3. Les terminaux mobiles

Les terminaux mobiles, et en particulier ceux équipés d'une interface sans-fil active, doivent être considérés avec une grande attention par les responsables de la sécurité de l'entreprise et ce pour deux raisons :

- Ils contiennent des données confidentielles (messagerie, agenda mais aussi fichiers…)
- Ils permettent d'accéder directement ou non au système d'information de l'entreprise.

La sécurité des terminaux mobiles doit répondre à trois objectifs :

- Empêcher un attaquant de monter une attaque réseau contre le terminal ou d'utiliser le terminal comme vecteur d'attaque.
- Limiter les conséquences d'un vol ou d'une perte.
- Imposer des limites techniques à l'utilisateur pour éviter les comportements à risque sans pour autant « brimer » l'utilisateur.

Les solutions techniques à mettre en œuvre, qui doivent correspondre à la politique de sécurité de l'entreprise, varient également selon les terminaux mobiles utilisés : téléphones mobiles ou PDA basiques basés sur des systèmes très propriétaires, PC portables, PDA type PocketPC…

7.3.1. Sécurité réseau

7.3.1.1. Firewall personnel

La mise en place d'un firewall personnel sur un terminal mobile permet de contrôler les connexions réseaux. La politique de sécurité implémentée doit permettre de :

- Protéger le terminal mobile des connexions entrantes non autorisées (extérieur vers terminal mobile) pour limiter les possibilités d'attaque, d'infection par un vers, cheval de Troie,…
- Limiter les possibilités de connexion sortante (terminal mobile vers l'extérieur) pour autoriser par exemple uniquement les connexions vers le système d'information de l'entreprise ou interdire les logiciels de P2P (Peer to Peer, protocoles souvent utilisés de plus pour le transfert de fichiers illégaux (musiques, films,…)) .

Il est important que le firewall personnel soit géré par un système de management centralisé permettant de distribuer les politiques de sécurité et des mises à jour.

A présent les systèmes de firewall personnels intègrent souvent un système de détection d'intrusion et/ou un client VPN.

7.3.1.2. Interfaces réseau sans-fil

Les interfaces réseaux sans-fil du terminal mobile doivent impérativement être configurées pour interdire l'établissement automatique de WPAN et ne pas s'associer automatiquement à des WLANs étrangers.

7.3.2. Sécurité système

La sécurité du système d'exploitation et des applications sur les postes utilisateurs est généralement délaissée au profit des défenses périphériques. Les technologies sans-fil remettant en cause cette stratégie, il devient important de sécuriser et de maîtriser la partie système et applicative sur tous les équipements concernés.

Là encore, la sécurité système doit être pensée pour répondre à deux objectifs :

- Protéger le terminal mobile d'attaques externes.
- Limiter les possibilités d'un utilisateur de mettre en danger sa propre sécurité : installation de logiciels à risque, modification du paramétrage…

7.3.3. Sécurité anti-virale

L'antivirus sur le poste de travail est une brique indispensable, en particulier pour lutter contre les chevaux de Troie (trojan). En effet un terminal mobile faisant l'aller retour entre l'extérieur et le LAN d'une entreprise constitue en

soit un excellent cheval de Troie. Des mesures doivent être prises pour empêcher l'utilisation de ce type d'équipement comme vecteur d'attaque contre le LAN.

L'antivirus doit pouvoir se mettre à jour très régulièrement dans un environnement variable et déconnecté, ce qui nécessite un système parfaitement adapté.

7.4. Infrastructure des réseaux sans-fil

L'infrastructure des réseaux sans-fil représente l'ensemble des équipements réseau radio et câblés permettant l'interconnexion entre les terminaux mobiles et les ressources du système d'information. Pour la plupart des entreprises, le périmètre se limite aux seuls WLAN.

7.4.1. Sécurité physique des équipements du WLAN

Contrairement à un LAN qui se matérialise dans les zones « publiques » uniquement par le biais de prises Ethernet, un système sans-fil a une composante physique très exposée : les antennes et les points d'accès. Aussi, la sécurité physique de l'infrastructure est un aspect à prendre en compte.

La sécurité physique d'un WLAN doit :

- Limiter les risques de vol des équipements
- Limiter les risques de dégradation des équipements
- Limiter les possibilités de piratage par attaque physique

7.4.1.1. Limiter le vol d'équipements

Le vol des équipements est le problème principal dans la plupart des entreprises mais il peut être adressé de plusieurs façons :

7.4.1.1.1. Rendre le vol plus difficile

D'un point de vue architecture radio, seule la position de l'antenne est réellement importante. En utilisant une antenne déportée reliée au point d'accès via un câble à faible perte, il est souvent possible de monter le point d'accès dans un endroit moins exposé (faux plafond, dans un local derrière un mur…). La principale limitation vient de la longueur du câble car les pertes sont très importantes.

Si le point d'accès ne peut être placé dans un environnement sécurisé, il est généralement possible de le rendre nettement plus difficile à voler : montage fixe cadenassé, coffret de sécurité, alarme couplé à un petit détecteur de mouvement attaché au point d'accès…

7.4.1.1.2. Minimiser les tentations de vol

La tentation du vol vient essentiellement du fait que ces équipements sont facilement réutilisables à son domicile. L'utilisation de points d'accès légers

(thin access point) (voir partie 7.4.2.2.2) est une solution radicale : les points d'accès légers ne sont pas utilisables de façon autonome mais nécessitent un switch WLAN ou une appliance WLAN pour fonctionner, ce qui rend impossible toute utilisation personnelle.

7.4.1.2. Limiter les risques de dégradation des équipements

Les risques de dégradation des équipements sont à prendre en compte lorsque des antennes ou des points d'accès vont être montés dans des zones publiques à risque.

Contrairement au vol, en terme de dégradation, les antennes sont aussi exposées que les points d'accès. Ce paramètre doit être pris en compte dans la conception de l'architecture radio, au même titre que la zone de couverture et les performances à offrir, pour placer au maximum les équipements dans des endroits sûrs.

L'utilisation d'équipements robustes renforcés par des mesures de sécurité physique type coffret blindé pour les points d'accès peut venir en complément.

7.4.1.3. Limiter les possibilités de piratage par attaque physique

Les vols et les dégradations sont des problèmes importants mais qui ne mettent généralement pas en danger le système d'information de l'entreprise (à l'exception notable de la qualité de service du WLAN). Par contre si ces attaques physiques sont commises par un pirate informatique dans le cadre d'une action de plus grande envergure, la menace prend une tout autre ampleur.

Un pirate qui vole un point d'accès a comme objectif d'analyser la configuration de l'équipement pour récupérer des informations importantes : adressage IP, mot de passe, clé de chiffrement WEP statique… Pour limiter les conséquences d'un tel vol, l'utilisation de points d'accès légers est une solution radicale : toute « l'intelligence wireless » étant déportée sur le switch WLAN, aucune information importante n'est stockée physiquement sur le point d'accès.

L'attaque physique des équipements peut également prendre la forme d'une connexion sur le port série ou en câble croisé sur l'interface ethernet. La sécurité intrinsèque du point d'accès prend alors toute son importance : mot de passe blindé, limitation d'accès à l'interface d'administration, désactivation ou démontage physique des interfaces inutiles.

7.4.2. Architecture et sécurité de la partie LAN des systèmes sans-fil

Tout WLAN a une partie LAN qu'il est également très important de sécuriser. Le principe de base est de cloisonner le WLAN du système d'information en imposant aux flux de passer par des points de contrôle : firewall et système de détection ou de prévention d'intrusion par exemple. Ainsi, même en cas

d'intrusion sur le WLAN, les ressources internes de l'entreprise sont encore protégées par des niveaux de sécurité.

A noter que la plupart des points d'accès supportent désormais les VLANs et sont capables de tagguer les paquets réseau en 802.1q selon le SSID. Cela permet de gérer plusieurs populations d'utilisateurs sur le WLAN avec des politiques de sécurité différentes.

7.4.2.1. Positionnement du WLAN par rapport au LAN

D'une manière générale le WLAN peut être intégré en surcouche d'un LAN câblé ou comme un réseau indépendant.

> **Note :**
> *Dans la suite de ce document, il sera fait fréquemment référence aux termes L2 et L3 correspondant aux définitions suivantes :*
> ***L2 (Layer 2)** : couche 2 (liaison de donnée) du modèle OSI. Les switchs et les adresses MAC par exemple opèrent au niveau L2.*
> ***L3 (Layer 3)** : couche 3 (réseau) du modèle OSI. Les routeurs IP en général opèrent au niveau L3.*

7.4.2.1.1. WLAN en surcouche du LAN

Dans ce cas l'infrastructure L2/L3 du LAN sert de support au WLAN.

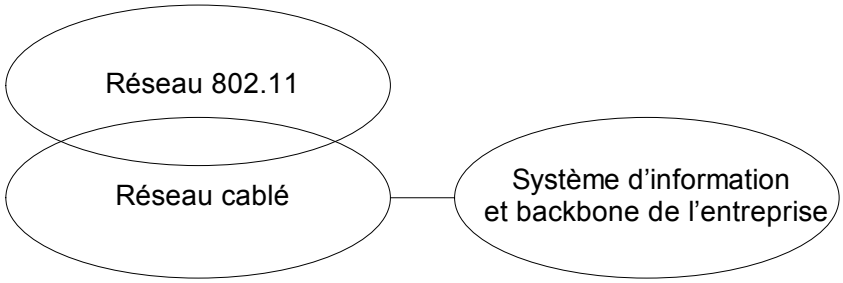


Figure 13 : WLAN en surcouche du LAN

7.4.2.1.2. WLAN indépendant

Dans ce cas le WLAN est déployé sur une infrastructure L2/L3 dédiée, comme une DMZ d'une plate-forme firewall par exemple.

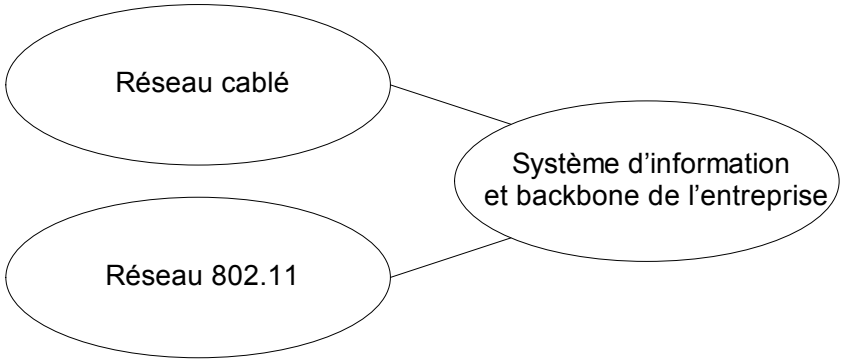
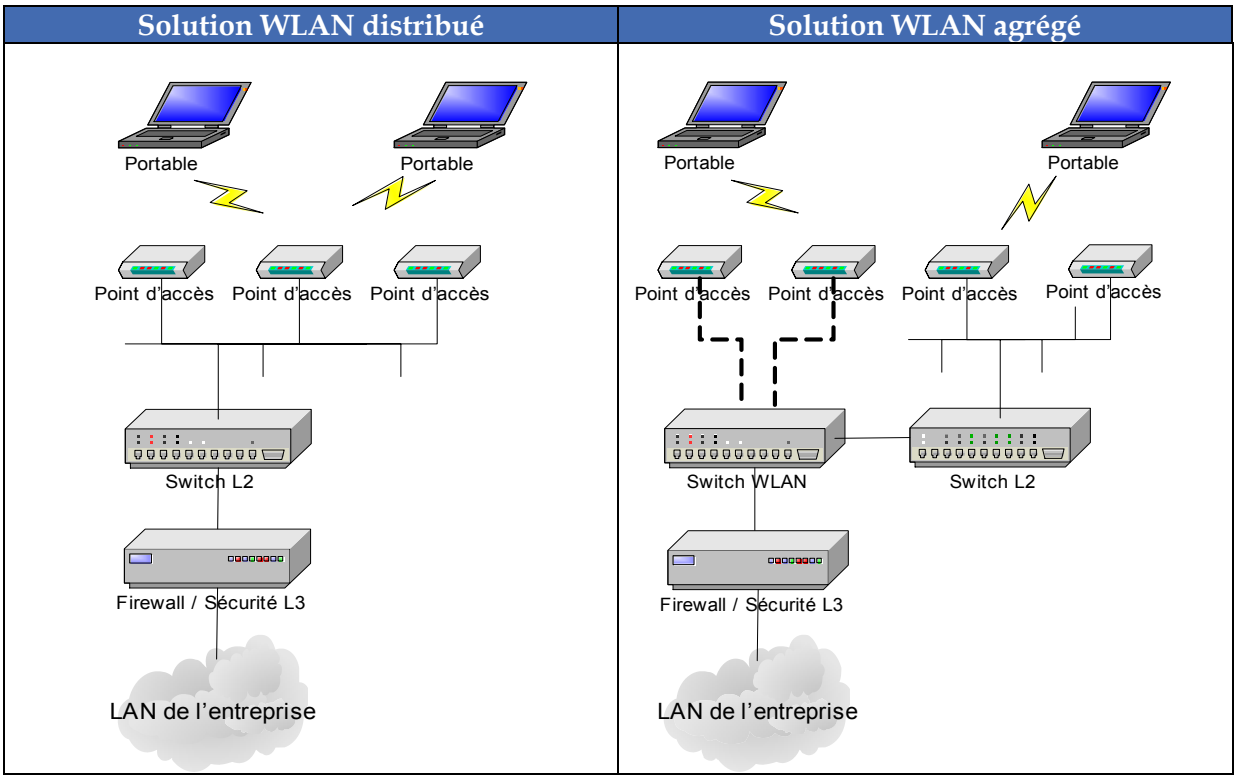


Figure 14 : WLAN indépendant

Le cloisonnement peut être implémenté de différentes façons en fonction de l'environnement réseau, de la topologie du WLAN et des équipements utilisés. Il peut être basé sur un réseau L2 dédié, des VLANs ou l'utilisation de switch WLAN, de firewall, de passerelle VPN mais ne doit pas être un goulet d'étranglement.

7.4.2.2. Style d'architecture du WLAN : distribué ou agrégé

Il existe principalement deux styles d'architectures pour les WLANs :



7.4.2.2.1. Solution WLAN distribué

Les solutions « WLAN distribué » reposent sur l'utilisation de points d'accès lourds autonomes. Chaque équipement intègre toutes les fonctionnalités radio, réseau et sécurité nécessaires et est connecté sur une architecture L2 classique.

Les points d'accès doivent être isolés par un firewall du reste du réseau et des ressources (critiques) de l'entreprise. Selon l'environnement réseau en place, ce cloisonnement peut être implémenté de différentes façons :

7.4.2.2.1.1. Architecture L2 dédiée

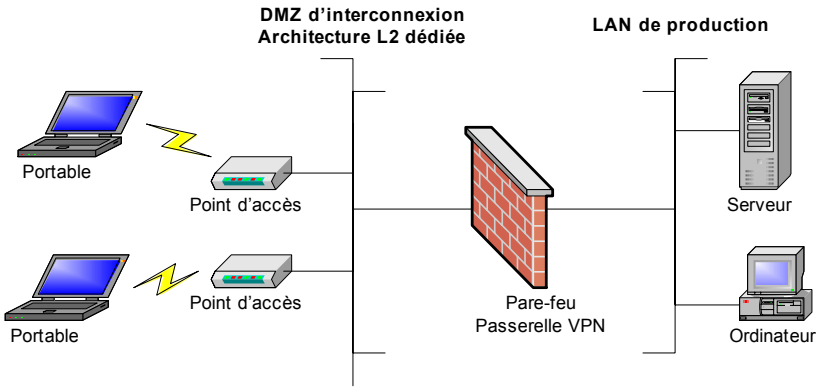


Figure 13 : WLAN distribué avec architecture L2 dédiée

Une architecture L2 dédiée à l'interconnexion des points d'accès dans une DMZ d'un firewall représente la solution idéale : l'étanchéité du cloisonnement entre cette DMZ et le LAN de production est alors uniquement dépendante du firewall. De plus, elle permet l'utilisation de switch supportant le PoE (Power over Ethernet) pour gérer l'alimentation des points d'accès.

Cependant, si le nombre et la répartition des points d'accès est élevé ou s'il est nécessaire d'unifier plusieurs sites sur une même plate-forme firewall, ce type de cloisonnement peut être abandonné au profit d'une architecture L2 mutualisée.

7.4.2.2.1.2. Architecture L2 mutualisée

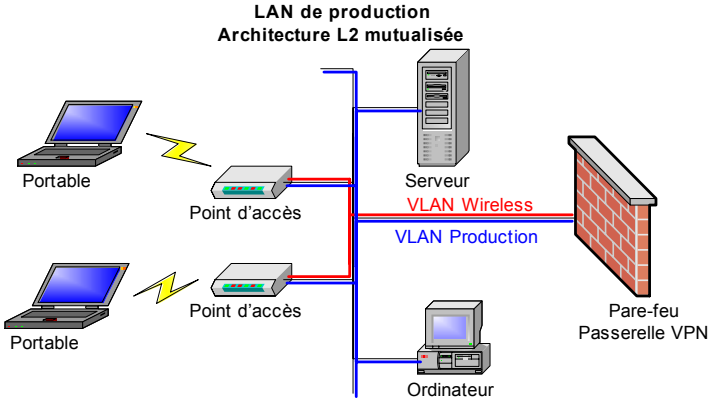


Figure 14 : WLAN distribué avec architecture L2 mutualisée

L'utilisation de VLANs permet d'implémenter le cloisonnement réseau tout en mutualisant une architecture L2 préexistante.

La mise en place de ce type d'architecture nécessite un environnement réseau L2 capable de gérer les VLANs. Cette gestion peut être statique ou utiliser 802.1q. A noter que les points d'accès avancés sont capables de tagguer les paquets IP en 802.1q et de gérer ainsi plusieurs populations d'utilisateurs mobiles (un SSID radio = un VLAN réseau).

7.4.2.2.2. Solution WLAN agrégé

Les solutions « WLAN agrégé » reposent sur l'utilisation de switchs/appliances WLAN spécialisés permettant de centraliser les points d'accès du WLAN et fédérer les fonctionnalités radio, réseau et sécurité. Ces derniers sont connectés soit en direct sur le switch WLAN, soit via une architecture L2/L3 classique.

Toute « l'intelligence » du WLAN et la gestion de la sécurité sont alors déportés sur le switch spécialisé. Les points d'accès ne sont plus que des modules radio transmettant le trafic 802.11 au switch qui se charge du traitement.

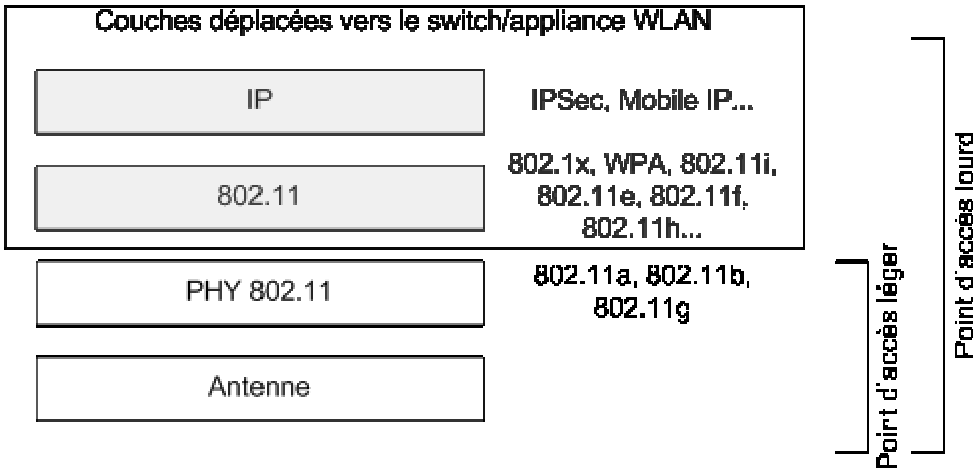


Figure 15 : Principe du WLAN agrégé

Les switchs/appliances WLAN disposent de fonctionnalités qui permettent de gérer la sécurité réseau du WLAN avec des performances élevées (performance type switch) et sans avoir nécessairement recours à une DMZ et un firewall dédié pouvant devenir un goulet d'étranglement. Cependant, dans une architecture WLAN hautement sécurisée et si les débits le permettent, il est envisageable de connecter tous les switchs et appliances WLAN sur une DMZ d'une plateforme de sécurité (firewall, sonde de détection d'intrusion…).

Les points d'accès sont connectés au switch soit en brassage direct, soit sur une appliance via le LAN et une architecture L2/L3 classique. Ces deux modes de connexion sont complémentaires et peuvent être utilisés simultanément dans une architecture :

7.4.2.2.2.1. Connectivité directe

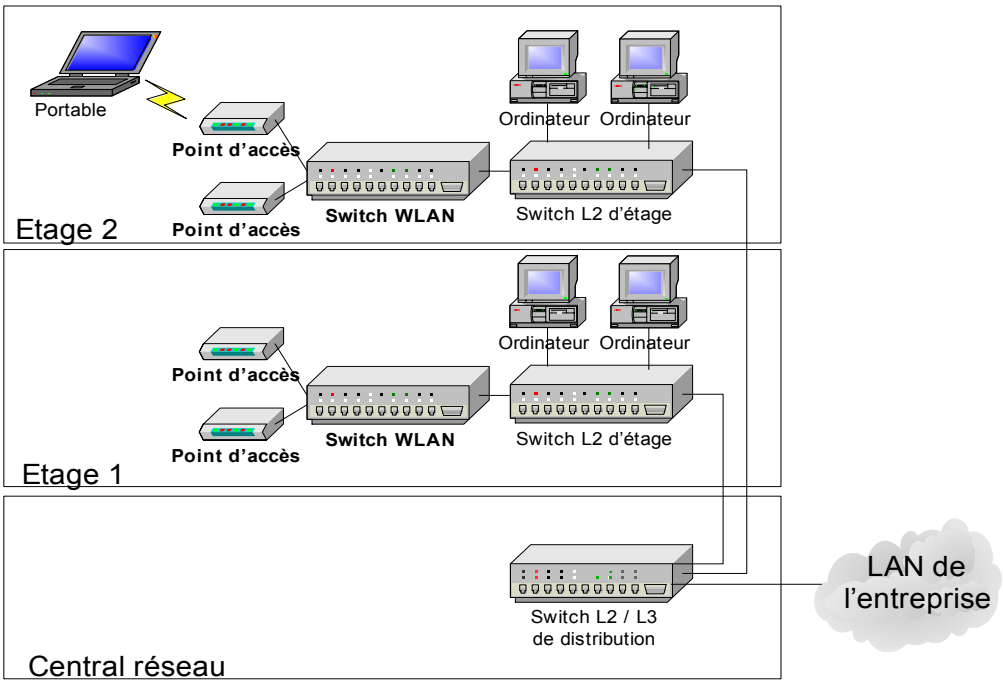


Figure 16 : WLAN agrégé en connectivité directe

Les switchs WLANs sont utilisables directement dans les locaux techniques d'un étage avec des points d'accès brassés en direct. Cela permet entre autre l'utilisation du PoE (Power over Ethernet) pour alimenter les points d'accès et faciliter ainsi leur déploiement.

7.4.2.2.2.2. Connectivité L2/L3

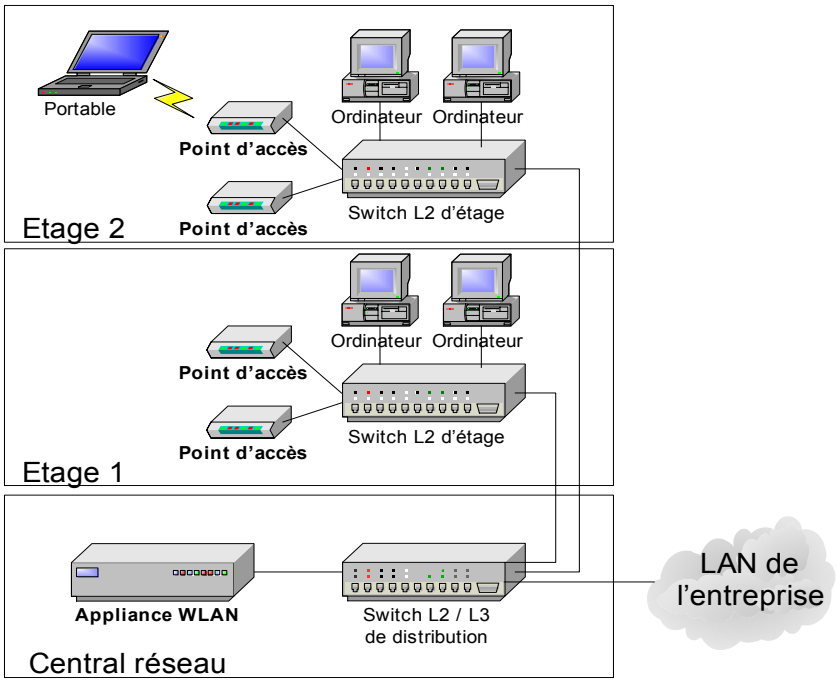


Figure 17 : WLAN agrégé en connectivité L2/L3

En connectivité L2/L3, les points d'accès forwardent tout le trafic 802.11 au switch via un tunnel type GRE, le protocole Light Weight Access Point Protocol (LWAPP) ou encore une connexion propriétaire.

Cette connectivité étant transparente, il est possible de traverser sans problème un environnement réseau L2/L3 sans forcément recourir à des VLANs (l'utilisation de VLANs peut cependant assurer un cloisonnement supplémentaire).

7.4.2.3. Supervision de l'infrastructure

Lors d'un déploiement WLAN, toute entreprise aspirant à délivrer une haute disponibilité de service se doit de maîtriser chaque élément de son infrastructure.

Pour cela il est nécessaire de mettre en place une surveillance constante des points d'accès et switch/appliance WLAN à l'aide d'une plate-forme de supervision standard ou d'appliances spécifiques de supervision WLAN.

Les solutions de WLAN agrégé intègrent pour la plupart une solution de supervision centralisée sur le switch/appliance WLAN performante (toutes les informations étant concentrées au même endroit, le traitement est plus aisé).

7.4.2.4. Valider la sécurité d'un système existant

Il est important de valider régulièrement l'architecture et les configurations mises en place afin de connaître les vulnérabilités éventuelles du système et pouvoir y pallier avant qu'un pirate ne les exploite. Si les outils sont souvent spécifiques aux réseaux sans-fil, les méthodes sont classiques : tests de pénétration, étude des configurations, …

7.4.3. Sécurité L2 des réseaux sans-fil

La mise en place de sécurité L2 n'est envisageable que sur des réseaux dont l'entreprise maîtrise la couche L2, ce qui limite en pratique le périmètre aux seuls WLANs. En effet dans le cadre de réseau type GSM ou GPRS, c'est l'opérateur qui a complètement en charge cet aspect de la sécurité, ce qui peut d'ailleurs amener une entreprise cliente à se baser sur des sécurités L3 pour garder un certain contrôle (voir partie 7.4.4).

Nous nous limiterons principalement dans ce document à aborder la sécurité L2 des WLANs basés sur les normes 802.11.

7.4.3.1. Authentification sur un WLAN

Que ce soit sur un WLAN d'entreprise pour s'assurer que seuls les employés autorisés accèdent au réseau ou sur un WWAN GSM d'un opérateur pour pouvoir facturer les clients, il est nécessaire de mettre en place des solutions d'authentification des utilisateurs.

Il est également très important de mettre en place des solutions permettant aux terminaux mobiles d'authentifier les réseaux sur lesquels ils se connectent, principalement pour contrer certaines attaques où un attaquant va par exemple faire basculer les terminaux mobiles sur un « faux » réseau qu'il contrôle.

Ce document traite essentiellement des systèmes de contrôle d'accès sur les réseaux sans-fil en mode infrastructure. En effet pour les WPANs les systèmes d'authentification restent très limités (généralement à l'utilisation d'une chaîne de caractère servant de secret partagé entre les différentes machines).

7.4.3.1.1. L'authentification basique sur les réseaux 802.11

Par défaut, aucune authentification n'est demandée pour l'accès à un WLAN 802.11.

Cependant, trois options sont disponibles sur pratiquement tous les points d'accès 802.11 :

- L'utilisation d'un SSID (identifiant de réseau sans-fil) non trivial qui devra être connu du client pour se connecter sur le point d'accès. Il est préférable de désactiver la diffusion du SSID dans les balises (beacons) émises par les points d'accès pour éviter les associations automatiques. Le SSID n'est cependant pas un secret partagé (il est transmit en clair dans les phases d'association) et ne constitue aucunement une mesure de sécurité : c'est un mécanisme de gestion du chevauchement de WLAN.

- L'utilisation d'une clé WEP statique unique entrée « en dur » sur tous les clients et tous les points d'accès. Cette clé agit alors comme un secret partagé global en plus du chiffrement WEP statique standard. C'est une solution lourde à gérer, peu sécurisée mais qui peut compléter à moindre coût une solution plus avancée comme l'utilisation de tunnels VPN IPSec.

- Le filtrage par adresse MAC. La plupart des points d'accès sont capables de gérer une liste des adresses MAC des cartes réseaux autorisées à accéder au WLAN. La gestion de ces listes, si elle n'est pas effectuée en central sur un serveur RADIUS, est très fastidieuse et le spoofing (usurpation) d'adresse MAC permet de contourner facilement cette sécurité.

Les solutions 802.11 basiques ne sont clairement pas suffisantes pour sécuriser l'accès à un WLAN.

7.4.3.1.2. WPA et les solutions 802.1x/EAP pour WLAN

Les constructeurs ont rapidement été obligés de proposer sur leurs matériels des systèmes d'authentification palliant les faiblesses des standards WLANs.

Dans un premier temps, la plupart se sont inspirés des projets de l'IEEE pour le 802.11i et ont donc proposé des implémentations propriétaires de 802.1x/EAP adaptées aux WLANs. A présent, 802.1x/EAP est stabilisé et forme la composante authentification de la norme WPA (Wi-Fi Protected Access).

802.1x est un système de contrôle d'accès réseau par port disponible sur tous les réseaux 802 (donc LAN ou WLAN). Basiquement les ports d'un équipement d'interconnexion (point d'accès ou switch) utilisant 802.1x ont deux états possibles :

- **Fermé** : c'est l'état par défaut. Un port fermé permet uniquement les flux d'authentification entre le client, l'équipement d'interconnexion et un système d'authentification (serveur RADIUS). Une fois que le client s'est authentifié avec succès, le port s'ouvre.

- **Ouvert** : cet état demande que le client connecté se soit authentifié avec succès. Un port ouvert laisse passer tout le trafic et se referme dès que le client se déconnecte.

802.1x sert de support pour EAP (Extensible Authentication Protocol). EAP n'est pas un système d'authentification en soi mais un protocole de transport de l'authentification. EAP s'appuie donc obligatoirement sur une ULA (Upper Layer Authentication) pour l'authentification proprement dite. Les ULA sont basées sur une vérification de couples login/password, un système de certificats, un système de cartes SIM…

Le couple 802.1x/EAP est le socle du système d'authentification (ULA). De l'ULA utilisée découlent les principales implémentations de EAP. Selon les cas l'authentification est simple (le réseau authentifie le client) ou double (le réseau authentifie le client et le client authentifie le réseau). Voici les principales implémentations EAP actuelles :

- **LEAP (Lightweight EAP)** : EAP développé par Cisco de type challenge-response basé sur un serveur RADIUS et un login/password.

- **EAP-TLS (EAP with Transport Layer Security)** : EAP basés sur des certificats gérés manuellement coté clients et coté serveurs.

- **PEAP (Protected EAP)** : EAP utilisant un certificat coté serveur et une authentification par login/password de l'utilisateur.

- **EAP-TTLS (EAP with Tunneled Transport Layer Security)** : EAP très similaire au PEAP.

- **EAP-SIM :** EAP utilisant le système d'authentification par carte SIM développé pour le GSM.

L'implémentation de 802.1x/EAP requiert systématiquement un serveur d'authentification type RADIUS s'appuyant sur une source d'authentification intégrée ou externe (service d'authentification forte, annuaire LDAP…). Certaines implémentations nécessitent également une infrastructure simplifiée de gestion des certificats (PKI).

Le processus d'authentification 802.1x/EAP est indispensable au système type TKIP pour la génération des clés WEP de chiffrement dynamiques (voir partie 7.4.3.2.2). En effet TKIP utilise les informations issues du processus d'authentification pour dériver les informations cryptographiques servant à créer les clés de chiffrement sur le client et le point d'accès.

Le niveau de sécurité offert par une implémentation de ce type de solution varie beaucoup selon l'ULA utilisée et son implémentation. Une implémentation conforme au standard WPA garantit une bonne sécurité pour le WLAN, une grande interopérabilité avec les terminaux mobiles et une évolution facilitée vers la future norme 802.11i.

A noter que WPA est également utilisable pour les particuliers ou dans certains cas dans un mode ne nécessitant pas de serveur d'authentification : il s'agit du « Pre-Shared Key Mode » qui permet une authentification simple entre le point d'accès et le terminal mobile et sert de base au mécanisme de chiffrement dynamique de WPA (voir partie 7.4.3.2.2).

7.4.3.2. Chiffrement du trafic

La perte du confinement physique de l'information fait qu'il est impossible d'empêcher un espion de récupérer le trafic réseau transitant sur un lien sans-fil. Afin de sauvegarder la confidentialité et l'intégrité des données circulant sur ce type de lien, il est indispensable de chiffrer le trafic de telle sorte qu'il ne soit intelligible que par les destinataires légitimes.

Les techniques de saut de fréquence radio comme FHSS (Frequency Hopping Spread Spectrum) implémentées sur les WLANs sont parfois présentées comme un atout sécurité contre l'espionnage. Ce n'est pas le cas dans les réseaux civils car contrairement aux implémentations FHSS sécurisées utilisées par les militaires, la séquence de saut sur un WLAN est facilement ou volontairement calculable par les récepteurs !

Il est donc indispensable de mettre en place un système de chiffrement au niveau réseau pour sécuriser le trafic sur la partie radio :

7.4.3.2.1. WEP (Wired Equivalent Privacy)

Par défaut le trafic sur un WLAN n'est pas chiffré : devant cet état de fait particulièrement critique, les initiateurs du 802.11 ont conçu le protocole WEP (Wired Equivalent Privacy) qui est censé offrir un niveau de sécurité équivalent à celui obtenu par une connexion câblée.

Le WEP utilise l'algorithme de chiffrement RC4 avec une clé unique et statique connue de tous les points d'accès et des clients. Cette clé, véritable secret partagé dans tout le WLAN, sécurise le trafic uniquement sur la partie radio, entre les terminaux mobiles et les points d'accès.

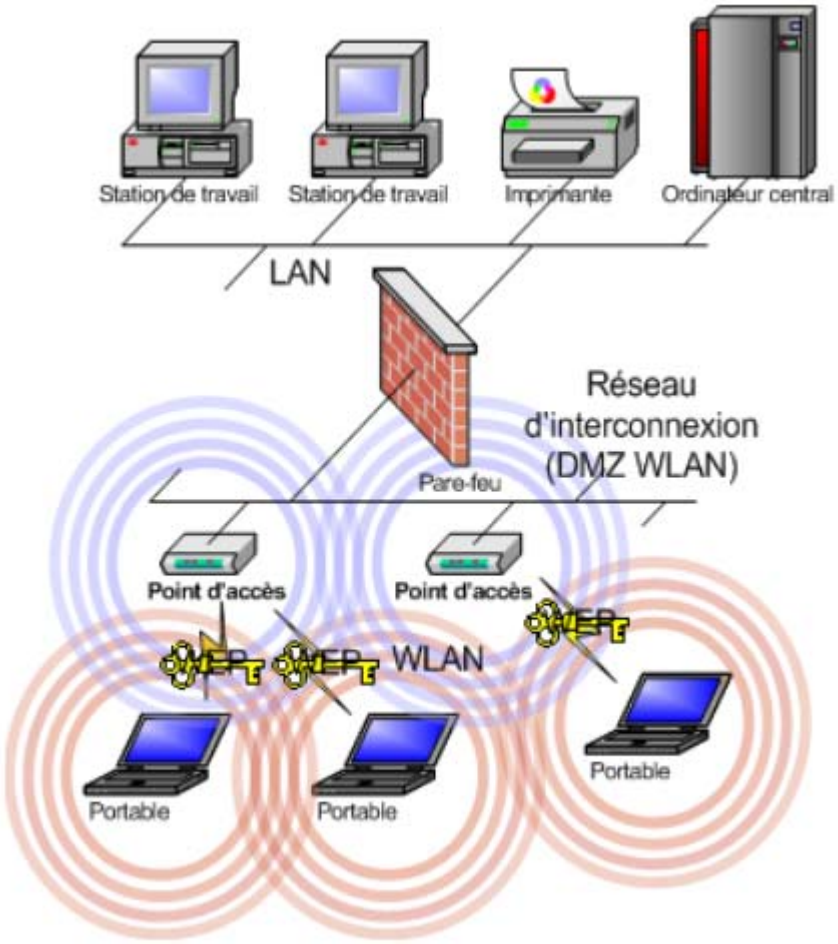


Figure 18 : Chiffrement pour WLAN via WEP

Le WEP basique souffre de plusieurs graves failles de sécurité qui le rendent totalement inefficace :

- L'implémentation de RC4 utilisée par le WEP est extrêmement peu sécurisée. Les clés de chiffrement sont statiques, très exposées par le protocole cryptographique (failles exploitant les vecteurs d'initialisation IV) et ne permettent au final qu'une confidentialité très limitée pour les données et ce quelque que soit leurs longueurs (128bits en général). Un attaquant analysant le trafic réseau sécurisé par le WEP peut casser sans peine le chiffrement en quelques heures d'écoute. Ces attaques sont d'ailleurs automatisées dans plusieurs logiciels de hack dont, par exemple, Airsnort.

- Le WEP n'implémente aucun contrôle d'intégrité des paquets : il est possible de changer des bits dans un paquet chiffré sans que ce soit détecté par le protocole.

- Le WEP ne dispose pas de mécanisme anti-rejeu. Il est possible pour un attaquant de rejouer plusieurs fois une séquence enregistrée.

Toutes ces faiblesses ont été découvertes très rapidement après la sortie du WEP. Depuis elles sont exploitées de manière complètement automatisée dans de nombreux outils de piratage.

Sous peine de prendre du retard, les constructeurs n'ont pas pu attendre la standardisation de la norme de sécurité 802.11i palliant les faiblesses du WEP. Ils ont donc tout d'abord librement amélioré le protocole par des évolutions propriétaires en gardant comme base WEP et RC4, seul algorithme de chiffrement compatible avec la puissance de calcul des équipements actuels.

Ces améliorations se sont généralement basées sur les travaux du groupe de travail IEEE 802.11i (volet sécurité pour le 802.11) et sont désormais regroupée sous le standard WPA.

Les améliorations classiques proposées par les améliorations propriétaires du WEP sont :

- La mise en place de systèmes de management des clés de chiffrement WEP type TKIP (Temporal Key Integrity Protocol) pour doter le WEP de clés dynamiques et uniques pour chaque utilisateur. Ces systèmes nécessitent un processus d'authentification 802.1x/EAP (voir la partie 7.4.3.1.2 sur l'authentification) pour dériver le matériel cryptographique servant à générer la clé de base et un protocole de renouvellement des clés.

- L'ajout de contrôles d'intégrité type MIC (Message Integrity Check) et de systèmes de vérification des séquences pour éviter qu'un attaquant puisse forger ou rejouer facilement des paquets.

Ces améliorations adressent la majeure partie des vulnérabilités du WEP. Bien implémentées, la plupart de ces solutions constructeurs « WEP amélioré » offrent un niveau de sécurité satisfaisant pour des environnements où la confidentialité absolue n'est pas vitale. Elles sont cependant très dépendantes des matériels utilisés donc peu interopérables et dans l'ensemble peu pérennes.

A présent il est nécessaire de mettre en place des solutions basées sur WPA pour le chiffrement L2 d'un WLAN.

7.4.3.2.2. WPA (Wi-Fi Protected Access)

Partant de ce principe de remplacement du WEP, la Wi-Fi Alliance s'est concentrée dès 2002 sur le développement d'un nouveau standard de sécurité. Les principaux objectifs étaient de mettre à disposition pour les fabricants courant 2003, un standard de chiffrement sûr, efficace et interopérable, facile à mettre en œuvre et ne nécessitant pas une évolution matérielle.

Cette démarche a été effectuée en accord avec l'IEEE et a abouti à une norme de sécurité intérimaire dérivée des futurs principes du 802.11i nommée WPA (Wi-Fi Protected Access).

Dans WPA, la partie authentification type 802.1x/EAP (voir partie 7.4.3.1.2) sert de base à un système de chiffrement type TKIP. Le chiffrement de WPA est basé sur du WEP amélioré avec des clés dynamiques (donc au final toujours sur l'algorithme de chiffrement RC4) :

- L'augmentation de la taille du vecteur d'initialisation (IV) à 48bits avec ajout de règles de séquence.
- La gestion dynamique des clés de chiffrement WEP en dérivant la première clé de l'authentification : chaque frame 802.11 possède une clé unique de chiffrement.
- Code d'intégrité du message : système Michael qui spécifie l'utilisation d'un code MIC (Message Integrity Code) permettant de vérifier l'intégrité de la trame. Ce code de 8 octets est ajouté à la valeur de vérification d'intégrité (ICV) de 4 octets déjà présente dans le WEP. Le champ MIC est crypté avec les données de trame et la valeur ICV. Michael fournit également une protection contre le rejeu avec l'utilisation de compteurs spécifiques.

WPA possède une compatibilité ascendante avec le 802.11i. Il nécessite une simple mise à jour des parties logicielles des différents composants de l'architecture WLAN pour pouvoir être utilisé.

7.4.3.2.3. Les futures solutions de chiffrement 802.11

La prochaine évolution prévue pour le chiffrement est WPA2. Identique au WPA sur la partie authentification, WPA2 propose une refonte complète de la partie chiffrement sur la base des systèmes développés pour 802.11i.

WPA2 utilise le chiffrement AES (Advanced Encryption Standard) et le protocole CCM (composé de CTR (Counter Mode Encryption), CBC (Cipher Block Chaining) et MAC (Message Authentication Code)). WPA2 n'utilise plus RC4 et efface donc toute trace du WEP. CCM assure des fonctionnalités équivalentes à TKIP.

WPA2 nécessite un changement hardware de tous les équipements ne disposant pas de la puissance de calcul nécessaire pour exécuter AES, ce qui est le cas de la plupart des points d'accès lourds des architectures WLAN distribuées. Les WLANs agrégés ont un net avantage car WPA2 est géré sur le switch ou l'appliance WLAN, équipement qui dispose de toute la puissance nécessaire. WPA2 ne remplacera pas immédiatement WPA, surtout si ce protocole et RC4 ne sont pas cassés prochainement.

A noter que les premières implémentations de WPA2 et d'AES commencent à être disponibles sur certains équipements. Il est cependant conseillé de conserver WPA pour le moment sur les WLANs en production.

WPA2 sera très proche du futur standard de sécurité pour les réseaux 802.11 : le volet 802.11i de la norme, attendu courant 2005. Par rapport à WPA et WPA2, 802.11i apportera par exemple des solutions pour la sécurité des WPANs (voir partie 7.4.3.2.5) ou la sécurisation des mécanismes de dé-authentification et dé-association.

7.4.3.2.4. Chiffrement pour les WWANs

Dans le cadre des WWANs, et en particulier ceux sur infrastructure télécom publique, la sécurité L2 est gérée par l'opérateur.

Il est important de garder à l'esprit que le chiffrement sur une communication type GSM ou GPRS est assurée par les systèmes de sécurité L2 uniquement sur la partie radio, entre le terminal mobile et l'antenne. En revanche, sur le réseau filaire entre l'antenne et la destination finale (le réseau de l'entreprise), le trafic traverse parfois des zones publiques peu ou pas sécurisées (réseaux inter-opérateurs, Internet…).

Pour maîtriser le chiffrement, il faut utiliser des sécurités L3 (type VPN, voir 7.4.4) ou du chiffrement au niveau applicatif (utilisation de SSL (Secure Sockets Layer) ou SSH (Secure Shell) par exemple).

7.4.3.2.5. Chiffrement pour les WPANs

La gestion de la confidentialité des données échangées sur un réseau ad-hoc n'a pas encore de solution satisfaisante : en effet, les possibilités de chiffrement offertes par les normes WPANs sont généralement très limitées et peu paramétrables.

Bluetooth propose un système de chiffrement relativement efficace mais optionnel et donc peu utilisé par les équipements. La norme 802.11 actuelle et la majorité des WPANs propriétaires ne proposent quant à eux aucun système de chiffrement correct.

En attendant les prochaines solutions de chiffrement pour WPAN qui seront implémentées dans Bluetooth2 et le 802.11i, la meilleure protection est encore de faire en sorte qu'aucune donnée sensible ne circule sur un WPAN. La sécurité passe donc plus par la sensibilisation des utilisateurs que par un moyen technique.

7.4.3.3. Continuité de service

La continuité du service d'un réseau sans-fil peut être attaquée non seulement sur un plan physique et radio mais également au niveau L2. Les attaques par dénis de service au niveau réseau (du simple flood à l'attaque logique bloquant un point d'accès ou déconnectant des clients) sont un problème important.

La plupart des systèmes de sécurité L2 pour les WLANs 802.11, y compris WPA, présentent des vulnérabilités de dénis de service par attaque logique. 802.11i devrait apporter des réponses à ce niveau.

7.4.4. Sécurité L3 des réseaux sans-fil

Dans certains cas, la sécurité d'un réseau sans-fil ne peut pas être exclusivement basée sur des sécurités L2 : soit ces dernières n'offrent pas le niveau de sécurité nécessaire (chiffrement WEP sur un WLAN par exemple) ou ne sont pas maîtrisées par l'entreprise (réseau GPRS par exemple).

Il est alors possible d'utiliser des sécurités de type L3 comme les VPN IPSec et ce en complément ou en remplacement de sécurité L2. Un VPN IPSec permet en effet de garantir une très forte confidentialité des données échangées entre le terminal mobile et une passerelle située dans le réseau de l'entreprise. De plus, l'établissement du tunnel étant soumis à authentification de la part de l'utilisateur sur la passerelle VPN (authentification login/password, authentification forte…), cette solution assure également un contrôle d'accès efficace.

La sécurisation par tunnel VPN nécessite qu'une passerelle VPN soit montée en coupure entre les terminaux mobiles et les ressources du système d'information. Cette passerelle VPN peut être montée sur les firewalls segmentant le réseau, sur les switchs/appliances WLAN ou sur des points d'accès disposant des fonctionnalités nécessaires. La partie radio et le réseau d'interconnexion des points d'accès sont alors considérés comme une zone pratiquement publique.

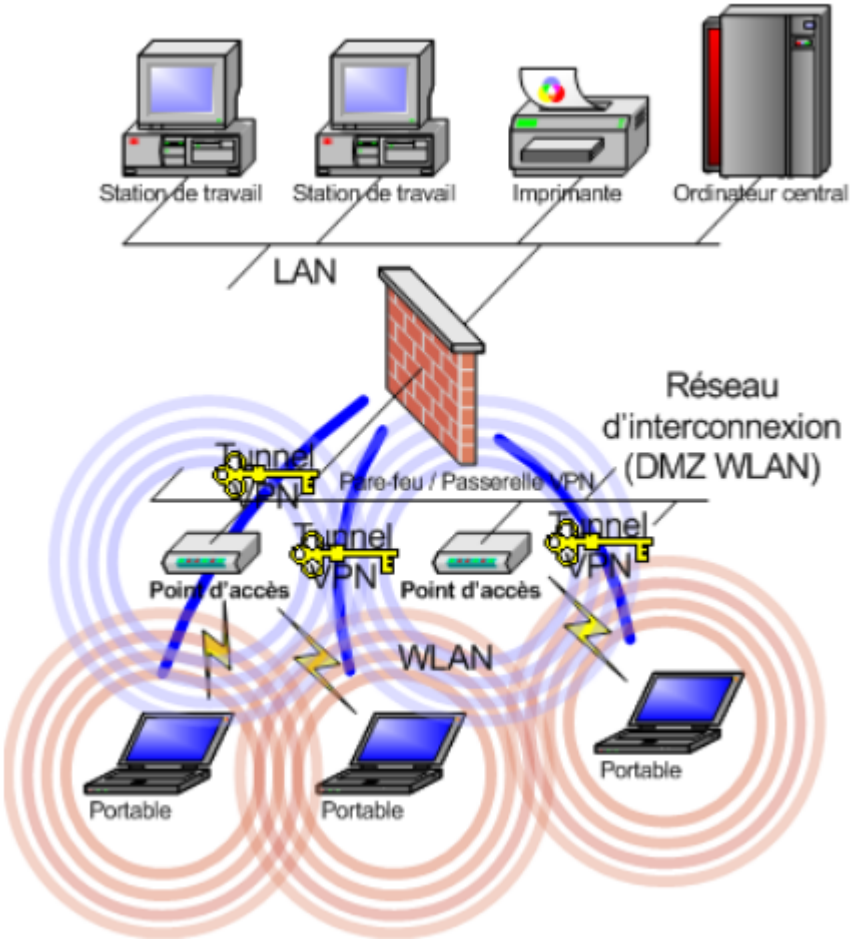


Figure 19 : Sécurité L3 pour WLAN

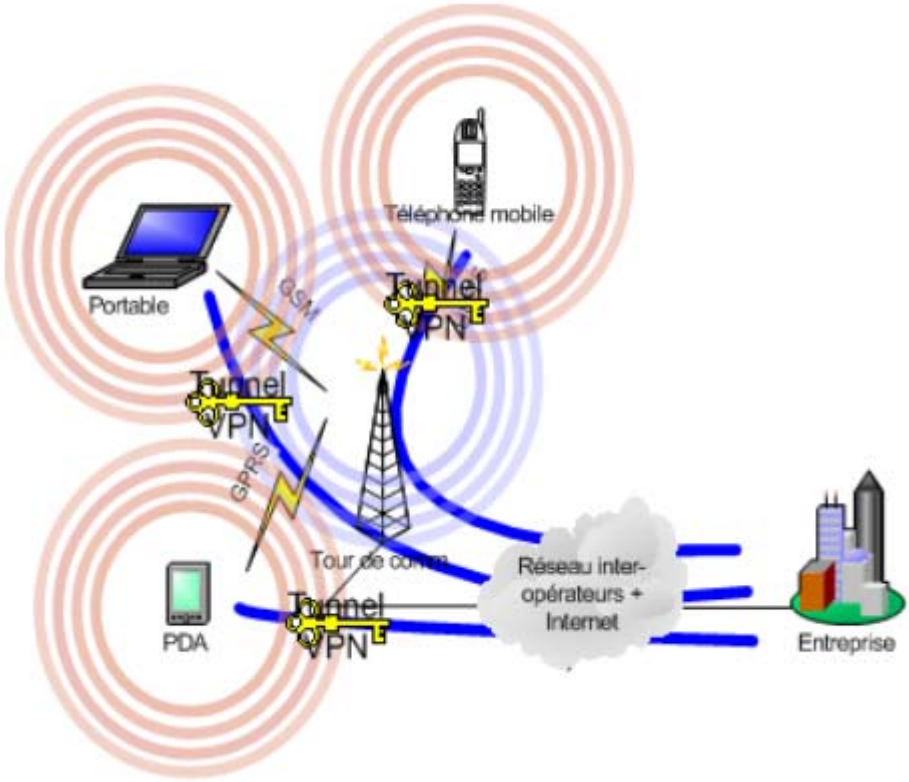


Figure 20 : Sécurité L3 pour WWAN

Cette solution nécessite de disposer d'un client VPN sur les terminaux mobiles. Cela peut être un client lourd ou, pour les hot-spot publics, une solution sans client utilisant SSL ou les fonctionnalités VPN disponibles sur les systèmes d'exploitation récents.

7.5. Maîtrise et surveillance de l'espace radio

Au vu des risques posés par les systèmes sans-fil, il devient nécessaire d'intégrer la surveillance de son espace radio dans sa stratégie de sécurité, qu'un déploiement de WLAN soit envisagé ou non.

Pour se faire, plusieurs actions peuvent être menées au sein de l'infrastructure WLAN.

7.5.1. Maîtrise de la topologie radio

Lors de la phase de conception d'une architecture WLAN, il est nécessaire de réaliser un premier audit de couverture sur le site cible dans le but de définir le nombre et le positionnement initial des équipements.

Des audits doivent être réitérés régulièrement dans le but de contrôler et d'optimiser l'infrastructure WLAN.

Ces études peuvent être réalisées à l'aide d'outils spécifiques indépendant de l'architecture WLAN, ou automatisé dans le cas de solutions de WLAN agrégé à l'aide d'outils de « site survey ». Le principal avantage des outils de site survey intégrés aux solutions de WLAN agrégé est de fournir des fonctionnalités avancées tels que la corrélation de données d'environnement (matériaux de construction, …) aux statistiques basiques de couverture, permettant ainsi d'affiner la cartographie d'un site.

7.5.2. Surveillance permanente de l'espace radio

Un audit de détection régulier est important pour toute entreprise disposant ou non d'un système sans-fil. Il va permettre d'inventorier les équipements radio non autorisés, actifs sur différentes plages du spectre radio dans le but de maîtriser la prolifération des points d'accès renégats et de dresser un état des lieux des systèmes sans-fil utilisés. Ce type d'audit réalisé le plus souvent manuellement à partir d'outil spécifique, est automatisable lors de la mise en place d'une solution de WLAN agrégé.

En complément d'audits de détection approfondis mais ponctuels, il est également intéressant d'implémenter des solutions de détection permanentes, proches dans l'esprit des systèmes de sondes de détection/prévention d'intrusion (IDS/IPS) utilisées sur les réseaux conventionnels. Ces systèmes sont constitués de sondes (points d'accès standard d'une architecture WLAN agrégé ou récepteurs radio spécialisés) reliées à un serveur d'analyse. Ils ont deux fonctions : détecter les équipements radio non autorisés et les attaques contre le WLAN de l'entreprise. Certains systèmes sont capables de combattre

activement les systèmes sans-fil renégats en empêchant la connexion des clients.

Il est également possible de compléter ces défenses radio permanentes par des systèmes de leurre (honeypot). Basiquement cela peut être des points d'accès volontairement peu sécurisés couplés à un système de détection/prévention d'intrusion, le tout ne donnant accès qu'à des ressources factices.

8. Conclusion

L'émergence des technologies sans-fil dans le monde des réseaux informatiques s'accompagne clairement de nouvelles problématiques sécurité. Ces dernières sont particulièrement graves et placent de nombreuses entreprises dans des situations d'insécurité critiques que des pirates n'hésitent pas à exploiter.

Il est important que les responsables informatiques intègrent au plus tôt ces technologies et les risques associés dans leur politique de sécurité globale puis prennent les mesures nécessaires pour protéger leur système d'informations. Cela doit être fait d'autant plus rapidement qu'il est devenu quasiment impossible de tenir complètement une entreprise à l'écart des systèmes sans-fil. Croire que cela est possible, c'est appliquer la « politique de l'autruche ». Il est de la sécurité des réseaux sans-fils comme de la sécurité en général : pour la gérer efficacement, il faut avant tout avoir conscience que l'insécurité existe mais qu'elle n'est en rien une fatalité.

Les solutions de sécurité relatives à ces nouveaux réseaux existent et sont simples à mettre en œuvre : elles sont en grande partie basées sur des principes et des systèmes de sécurité éprouvés issus de la sécurité Internet, un renforcement de la sécurité informatique interne de l'entreprise et la mise en place de moyens de contrôle de l'espace radio.

De part son expertise acquise depuis plus de 8 ans dans le domaine de la sécurité des systèmes d'information, CYBER NETWORKS apporte à ses clients les solutions performantes qu'ils attendent, tant sur le plan du conseil et de l'audit que des projets d'intégration et de développements applicatifs liés aux systèmes sans-fil et à la mobilité en général.

9. Glossaire

AES (Advance Encryption Standard) : standard de chiffrement récent et successeur du DES / 3DES. AES sera implémenté dans 802.11i pour chiffrer les communications sur les WLANs.

Bluetooth : norme radio IEEE 802.15 surtout utilisée pour les WPANs.

EAP (Extensible Authentication Protocol) : protocole servant de base au système d'authentification réseau pour l'accès à un WLAN. Il est utilisé conjointement au 802.1x et est indispensable à TKIP.

IEEE 802.1x : système de contrôle d'accès réseau par port utilisé avec EAP.

IEEE 802.11 : ensemble de normes très utilisées dans les WLANs. Les volets les plus connus sont le 802.11b et le 802.11a.

IEEE 802.11a : voir réseau Wi-Fi5.

IEEE 802.11b : voir réseau Wi-Fi.

IEEE 802.11i : volet sécurité de la norme 802.11.

IEEE 802.11g : norme compatible avec la 802.11b qui améliore les débits tout en restant dans la bande de fréquence des 2.4 GHz (donc autorisé en France)

IEEE 802.15 : nom de la norme Bluetooth.

IrDA : norme infrarouge.

Hot-spot : WLAN public destiné à offrir un service à des clients.

LAN (Local Area Network) : réseau local câblé traditionnel.

Réseau ad-hoc : autre terme désignant un WPAN.

TKIP (Temporal Key Integrity Protocol) : système améliorant la gestion et l'utilisation des clés de chiffrement RC4. TKIP est intégré dans certains systèmes propriétaires constructeur, WPA et 802.11i et nécessite un système d'authentification 802.1x/EAP.

WEP (Wired Equivalent Privacy) : système de sécurité natif 802.11 très faible.

Wi-Fi : norme radio WLAN basé sur la norme IEEE 802.11b (2,4 GHz - 11Mbps).

Wi-Fi5 : norme radio WLAN basé sur la norme IEEE 802.11a (5 GHz - 54Mbps).

Wireless : sans-fil en anglais.

WLAN (Wireless Local Area Network) : réseau sans-fil local à l'échelle d'un bâtiment ou d'un site : réseau d'entreprise, hot-spot public...

WLAN agrégé : WLAN basé sur une infrastructure de switchs ou d'appliances WLAN centralisant l'intelligence wireless et des points d'accès léger.

WLAN distribué : WLAN basé sur des points d'accès lourds embarquant chacun toute l'intelligence wireless nécessaire.

WMAN (Wireless Metropolitan Area Network) : réseau sans-fil à l'échelle d'une ville.

WPA (Wi-Fi Protected Access) : version allégée de 802.11i destinée à remplacer rapidement le WEP.

WPAN (Wireless Personnal Area Network) : réseau personnel temporaire et point à point entre deux ou plus équipements.

WWAN (Wireless Wide Area Network) : réseau sans-fil étendu sur de longues distances.

WWAN sur infrastructure publique : réseau sans-fil étendu basé sur une infrastructure non maîtrisée par l'entreprise, généralement une infrastructure télécom comme le réseau GSM ou GPRS.