Passeport pour des réseaux Wi-Fi hautement sécurisés et administrables

Wi-Fi sécurisé ou prévention d'intrusion ARUBA a créé les solutions

ARUBA Wireless Networks
France, Europe du Sud, Afrique:
120, avenue Charles de Gaulle
92522 Neuilly sur Seine Cedex, France
Tél : +33 (0) 1 72 92 05 56
Fax : +33 (0) 1 72 92 05 57
info-emea@arubanetworks.com
www.arubanetworks.com

"People Move. Networks must follow."

Table des Matières

1 Introduction

Le présent document a pour vocation de présenter, dans une première partie, la problématique associée aux réseaux Wi-Fi (Wireless Fidelity), puis dans une seconde partie les réponses qu'apportent la solution Aruba, tant au niveau technique, que logistique ou opérationnel.
Nous aborderons ainsi successivement la régulation, les problèmes de sécurité, la complexité de l'ingénierie, et les spécificités de la gestion inhérentes aux transmissions radio.
Mais nous profiterons aussi de ce récapitulatif pour décrire les produits évolués, leur architecture et les fonctionnalités avancées qu'ils offrent aujourd'hui pour constituer une solution complète, mature, fiable et sécurisée.

Enfin, en annexe, on retrouvera une liste de quelques livres et sites intéressants, un tableau récapitulatif, et les principaux acronymes à connaître (auxquels on peut aussi se référer au cours de la lecture).

1.1 Contexte

Le Wi-Fi, en tant que solution de transmission de donnée par voie hertzienne de type WLAN (Wireless Local Area Network), se trouve entouré par des technologies complémentaires, non concurrentes, et à peu près de même génération.

WPAN

Ainsi Bluetooth (IEEE 802.15.1) est la solution WPAN (Wireless Personal Area Network) la plus répandue, pour des besoins très courte portée (de l'ordre d'une dizaine de mètres) et bas débit, a priori entre les équipements voix et/ou données d'un même utilisateur (typiquement téléphone GSM <-> PDA ou PC ; téléphone GSM <-> écouteur sans-fil).

WMAN

A l'autre extrémité des besoins géographiques, on trouve la BLR (Boucle Locale Radio, WLL : Wireless Local Loop en anglais) qui répond aux besoins de type WMAN (Wireless Metropolitan Area Network), et apparaît comme technologie d'accès radio des opérateurs, pour une desserte sans fil, mais généralement fixe, offrant une portée de plusieurs kilomètres.
Plus récemment les spécifications en cours de WiMax (IEEE 802.16 et ETSI HiperMAN) cherchent à définir une technologie standard pour le monde de la BLR (ou BWA : Broadband Wireless Access) en topologie PMP (Point to MultiPoint), fonctionnant dans les bandes de fréquences de 2-11 et de 10-66 GHz, avec une meilleure efficacité spectrale.

1.1.1 Marchés

Le Wi-Fi, intermédiaire en terme de couverture, et plus élaboré par certains aspects que les WPAN et WMAN (support de la mobilité, voire du «roaming) a, quant à lui, la particularité d'adresser 3 typologies de marchés généralement indépendantes, comme nous allons le détailler ci-dessous.

Entreprise

En entreprise, le réseau Wi-Fi étant une extension du réseau LAN, il apporte un plus en terme de flexibilité (mobilité, rapidité de déploiement, installation temporaire, câblage difficile, etc.). Le Wi-Fi répond aussi à des besoins spécifiques, en tant que forme de connectivité sélective, par exemple dans les salles de réunions, permettant aux visiteurs d'avoir un accès aisé à l'Internet, et concurremment aux employés d'avoir accès à leur intranet. C'est aussi une solution duale qui permet à l'utilisateur d'un PC portable d'exploiter la même technologie (mais des réseaux distincts) pour se connecter à son VLAN dans son entreprise et à son réseau ADSL à domicile.

Domestique

La connectivité résidentielle, permettant aux clients d'une liaison Interne haut débit (ADSL, CableModem) de relier leurs différents ordinateurs au routeur Wi-Fi, lequel est connecté au modem. Les postes pouvant exploiter ce type de liaison sont aussi bien les PC (portables ou non),

quel que soit leur Système d'Exploitation (Windows, Mac, Unix) que les PDA, ou les périphériques (imprimantes, serveurs de fichiers, voire écrans). L'objectif est ici principalement de supprimer les inévitables câbles qui circulaient jusqu'alors d'une machine à l'autre à travers l'appartement.

Hot Spot

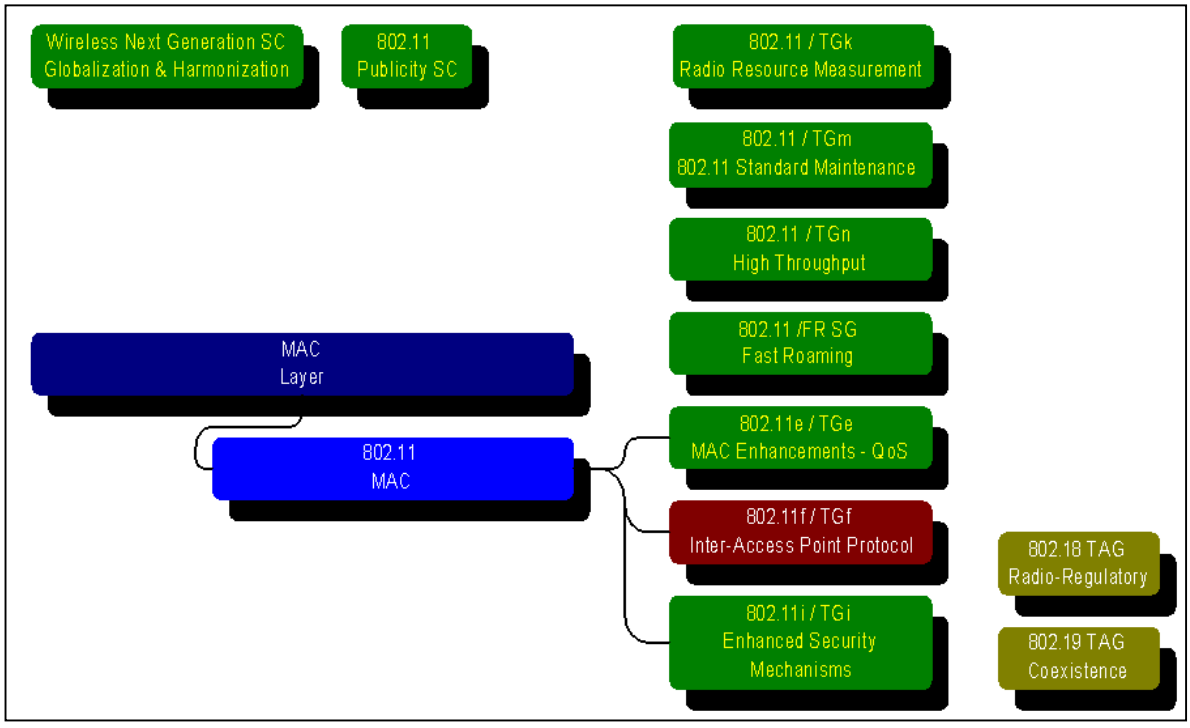
Les opérateurs, désireux de déployer des hot spot, lieux donnant accès à l'Internet, moyennant un abonnement préalable ou un mode de facturation en pré payé (comparable, voire en concurrence avec la connexion "data" en GSM et GPRS). Les zones équipées en hot spot étant typiquement des lieux de passage pour hommes d'affaires (hôtel, aéroport, salon d'exposition/de conférence). Il s'agit d'un mode de connectivité intrinsèquement nomade, et qui peut logiquement être combiné à un abonnement GSM.

Le Wi-Fi a cependant une histoire très particulière en terme de développement de marché. En effet, ses premières applications ont eu lieu dans le monde de l'entreprise dès la fin des années 90. Les standards et produits d'alors permettaient un débit de 1, 2 (voire 3) Mb/s nominal par cellule, sans beaucoup de sécurité, ni de moyens de gestion de la performance radio. Probablement dû à ses lacunes, le Wi-Fi n'a pas connu un développement aussi rapide que prévu, mais les prix ont cependant continué à baisser, permettant au marché résidentiel de prendre le relais.
Nous sommes aujourd'hui dans une phase où les 3 marchés cités ci-dessus sont en forte croissance, chacun avec sa propre dynamique, et son approche particulière.

En ce qui concerne l'entreprise, comme pour les opérateurs, c'est la maturité des solutions récentes riches et complètes, qui permet d'envisager aujourd'hui des installations professionnelles, sures et performantes.

1.2 Spécifications

Les premiers développements de technologies de transmission Radio pour de relativement courte portée (typiquement de l'ordre d'une centaine de mètres), fonctionnant dans la bande de fréquence ISM (Industry, Scientific, Medical) aux alentours de 2,4 GHz, datent des années 1990.



802.11 Activities - MAC & Others (source IEEE 802.11)

Quelques constructeurs innovants du monde radio et/ou data ayant abordé ce sujet avec diverses solutions propriétaires, l'IEEE (Institute of Eletrical and Eletronics Engineers) pris le premier la responsabilité de standardiser ce type de solutions avec le sous-comité 802.11, dont les premières spécifications furent publiées en 1997.

Les premières spécifications de l'IEEE 802.11, ciblèrent une méthode d'accès distribuée de type CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), qui correspond à une légère amélioration par rapport à la méthode CSMA/CD d'Ethernet.

La fonction de coordination est généralement de type distribuée (DCF), sachant que la coordination centralisée (PCF : Point Coordinated Function) est une capacité de QoS optionnelle, rarement implémentée aujourd'hui, qui sera significativement amélioré par le futur supplément 802.11 e, et permettra un meilleur support de la voix ou de la vidéo au niveau Méthode d'Accès Wi-Fi.

Ces spécifications, désirant prendre en considération les différentes études et travaux en cours des constructeurs, définissaient trois modes de transmission, un en infrarouge, un en radio avec un codage de type FHSS, et un dernier aussi en radio avec un codage de type DSSS. Ces trois modes offraient 1 ou 2 Mb/s de débit nominal à partager entre tous les utilisateurs présents dans la cellule (dite BSS : Basic Service Set).
Deux modes de communication ont été définit :

Ad Hoc

Une forme de point à point où chaque équipement terminal (STA, pour Station) peut communiquer directement avec un équipement voisin (IBSS : Independent BSS, dit couramment réseau Ad Hoc) moyennant une configuration préalable. Ce mode basique n'est utile que pour des configurations réduites, par exemple à la maison.

Infrastructure

Un mode dit Infrastructure, où les STA sont reliées entre elles par un équipement responsable d'"animer" une cellule (cette antenne "intelligente" est dite AP : Access Point). L'AP est au centre de la cellule est gère l'accès à la cellule, puis l'échange de tous les paquets. C'est le mode de fonctionnement le plus courant, qui évite aussi le problème du nœud caché (hidden node) dû à la non transitivité des communications avec des liaisons Ad Hoc.

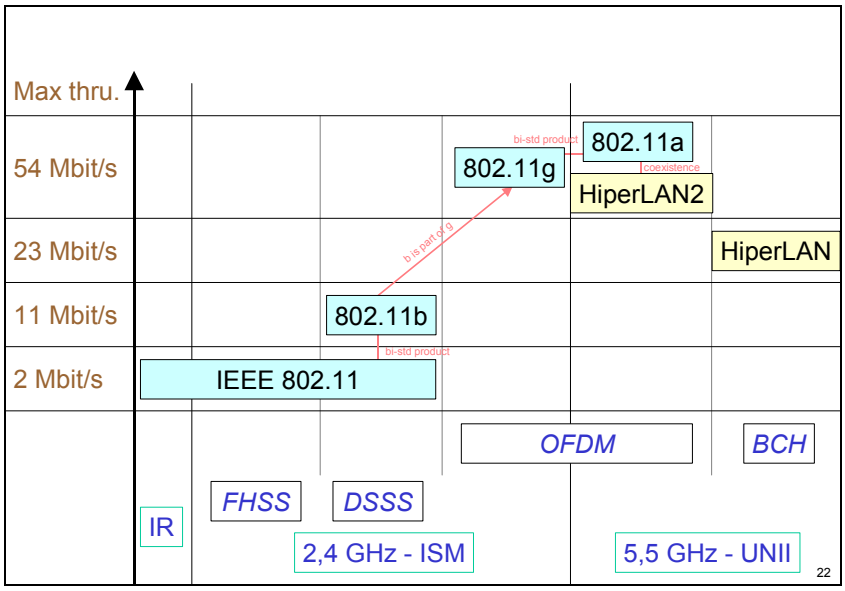
Quand plusieurs AP sont connectés ensemble au niveau 2 (MAC) par un LAN, les BSS correspondants sont ainsi réunis en un ESS (Extended Service Set).

Par la suite, l'IEEE améliora le débit avec le supplément b qui ne retint que le code DSSS, avec une modulation plus évoluée, et qui tout en étant compatible avec les précédents débits, pouvait aussi supporter 5,5 et 11 Mb/s (selon la distance ou la puissance du signal).

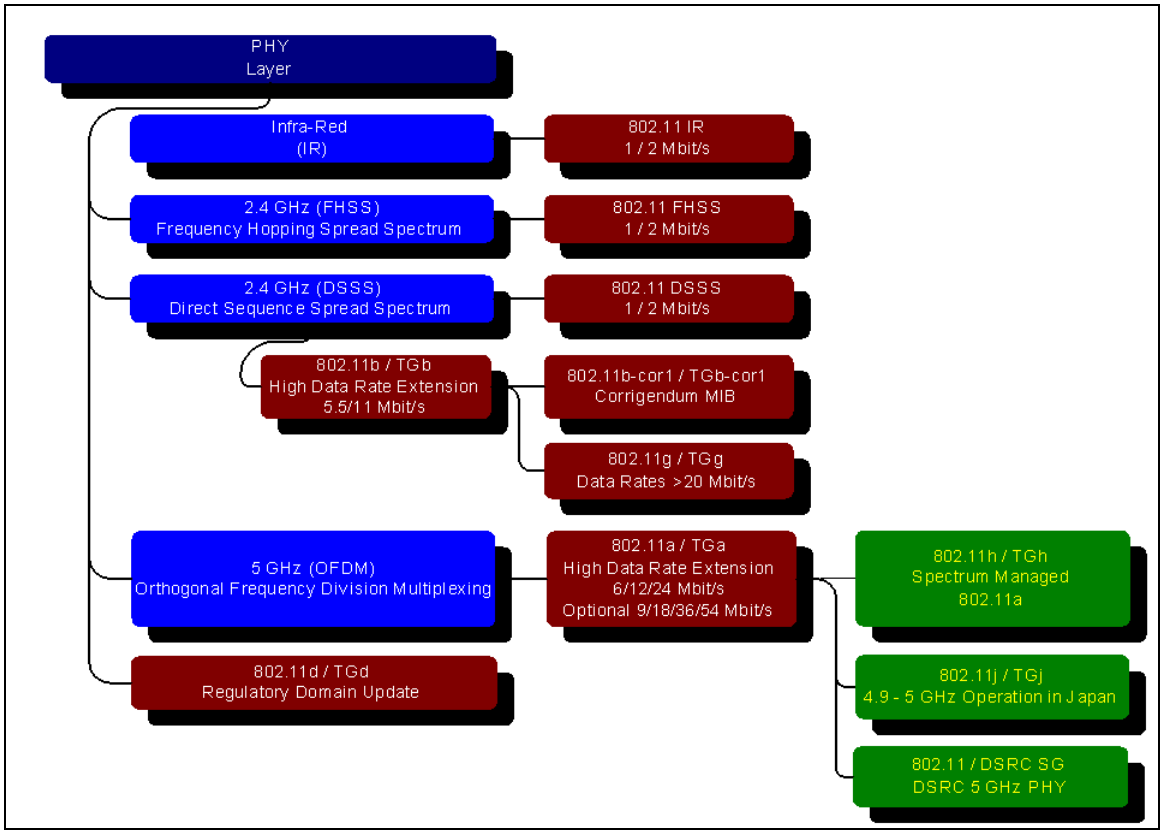
En 1999, l'IEEE 802.11 publia aussi le supplément a, qui décrit un fonctionnement dans la bande des 5 GHz, permet un débit nominal de 54 Mb/s, et autorise un plus grand nombre de bandes de fréquence (correspondant à autant de cellules potentiellement voisines). Ce supplément est couramment nommé Wi-Fi5.

Enfin, en terme de débit, en 2003, l'IEEE a ajouté le supplément g qui définit le fonctionnement à 54 Mb/s maximum (comme en a) mais toujours dans la bande des 2,4 GHz, et en compatibilité et continuité avec le supplément b.

La bande des 5 GHz a l'avantage de subir moins d'interférence ou de bruit que la bande 2,4 GHz. Les performances radio sont cependant légèrement moins bonnes dans la bande des 5 GHz que dans la bande des 2,4 GHz, la puissance radio autorisée étant identique. La couverture d'une cellule, à un débit donné, est cependant très comparable entre les suppléments a et g.



Notez aussi que les produits Wi-Fi multifréquences récents peuvent proposer une compatibilité avec les 3 suppléments a, b, et g. Les interfaces pour poste client choisissent le mode, et la fréquence de fonctionnement, soit automatiquement, soit grâce à une interaction avec l'utilisateur. Les AP évolués quant à eux peuvent avoir un fonctionnement double, à 2,4 et à 5 GHz, comme deux AP indépendants, travaillant sur un seul canal de fréquence dans chaque bande à un moment donné.



802.11 Activities - PHY (source IEEE 802.11)

Les équipements Wi-Fi modernes ayant des capacités de sécurité évoluées (WPA, VPN, etc.), et intégrant des fonctionnalités riches, ils font appel à des technologies complémentaires, tel le cryptage, ou la communication avec des serveurs d'authentifications.

Outre les standards de l'IEEE 802.11, ces équipements se conforment donc aux standards LAN connexes, et aux spécifications de l'IETF (VPN IPsec, EAP, Radius, LDAP) que nous ne rappellerons ici que très brièvement.
A titre indicatif, les équipements WLAN Aruba mettent en œuvre les protocoles et spécifications suivantes :
- Ethernet 10/100 & GigaEthernet (IEEE 802.3, i, u, z, ab), POE (IEEE 802.3af); Tagging VLAN (IEEE 802.1Q), Queues de priorité (IEEE 802.1p), Access Control (IEEE 802.1X)
- IP (RFC 791, 1812), SNMP (RFC 1155-58), Telnet (RFC 854), HTTP (RFC 2616), TFTP (RFC 1350), DHCP (RFC 2131); GRE (RFC 2784), PPTP (RFC 2637), L2TP (RFC 2661), IPsec (RFC 2401-2), SSH, SSL, TLS (RFC 2246), EAP-TLS (RFC 2716).
De plus, pour la gestion de l'authentification, les équipements doivent aussi savoir se mettre en relation avec un ou des serveurs AAA (Administration, Authorization & Authentication) en utilisant typiquement le protocole Radius (RFC 2865), ou LDAP (RFC 2251).

HiperLAN & IsWAN

On notera enfin qu'il existe des alternatives marginales aux spécifications de l'IEEE sur les réseaux locaux sans-fil.
D'une part, l'ETSI qui avait standardisé une première solution de WLAN : HiperLAN en 1996-98, a défini HiperLAN/2 plus récemment, en concurrence assez directe avec l'IEEE 802.11a. Mais à la différence des travaux de l'IEEE, ceux de l'ETSI ne sont cependant pas très suivis par les constructeurs d'équipements réseau.
D'autre part, au Japon, MMAC (Multimedia Mobile Access Communication systems) a standardisé l'IsWAN, une solution de transmission comparable à l'IEEE 802.11a, dont l'influence sur notre marché n'est pas très significative non plus actuellement.

	IEEE						ETSI	
unit	802.11			802.11b *Wi-Fi*	802.11g	802.11a *Wi-Fi5*	HiperLAN 2	1
Std Date	1997			1999	2003	1999		1996-8
Frequ range GHz	850-950 nm	2,4				5		
# channels	-	13 in Europe ; 11 aux USA				dizaines		
# non-overlapping		3				8 ou 12		
Coding	IR	FHSS	DSSS		DSSS/OFDM	OFDM		BCH
Modulation	4 PPM	2GFSK/ 4GFSK	DBPSK/ DQPSK	... + / DQPSK-CCK	... + OFDM/ OFDM-CCK	CCK	BPSK/ QPSK/ 16QAM/ 64QAM	FSK / GMSK
Baud Rate Mb/s	1 / 2			1... 5,5 / 11	1...48 / 54	6 / 9 /...54	54	1,47 / 23,53
MAC	CSMA/CA distribué						TDMA/ TDD centralisé	EY-NPMA

IEEE 802.1X

Un des standards complémentaires particulièrement important dans le monde Wi-Fi est l'IEEE 802.1X, qui définit une méthode d'authentification sécurisée de niveau 2 en environnement LAN. L'IEEE 802.1X spécifie comment le poste client (supplicant) requiert une connexion LAN au switch (authenticator) lequel va typiquement se référer à un serveur d'authentification externe en utilisant un protocole EAP (dérivé de PPP) sur le réseau câblé. En fait, l'authentification est mutuelle, permettant donc de se protéger contre les risques de type Man in the Middle.
Le serveur (Radius a priori) permettra ou non l'accès au réseau, et pourra aussi préciser le VLAN en retour. L'adresse IP qui est assignée au client suite à son authentification positive sera automatiquement sélectionnée dans le pool correspondant.

1.3 Régulation

Le Wi-Fi fonctionnant avec des émissions radio, sa mise en place n'est jamais totalement du domaine privé, et doit se conformer à certaines règles, édictées par les organismes nationaux de régulations de télécoms (en France, l'ART (Autorité de Régulation des Télécommunications) créée en 1997, gère depuis l'allocation des bandes de fréquences aux opérateurs).
Les spécificités de puissance par fréquence sont connues des équipements évolués, qui, une fois le paramètre "country" définit (France dans notre cas), gère automatiquement l'attribution des fréquences selon les plages autorisées.
En France, les conditions d'utilisation des bandes ISM du 2,4 et 5 GHz ont été modifiées puis publiées pour la dernière fois en juillet 2003 (voir ci-dessous les détails).

Fréquences en MHz	Intérieur	Extérieur
2400 2454	100 mW	100 mW
... 2483,5		10 mW

fréquences en MHz	Intérieur	Extérieur
5150 5250	200 mW	*impossible*
... 5350	200 mW avec DFS/TPC ou équivalent ou 100mW avec DFS uniquement	*impossible*
5470 5725	*impossible*	*impossible*

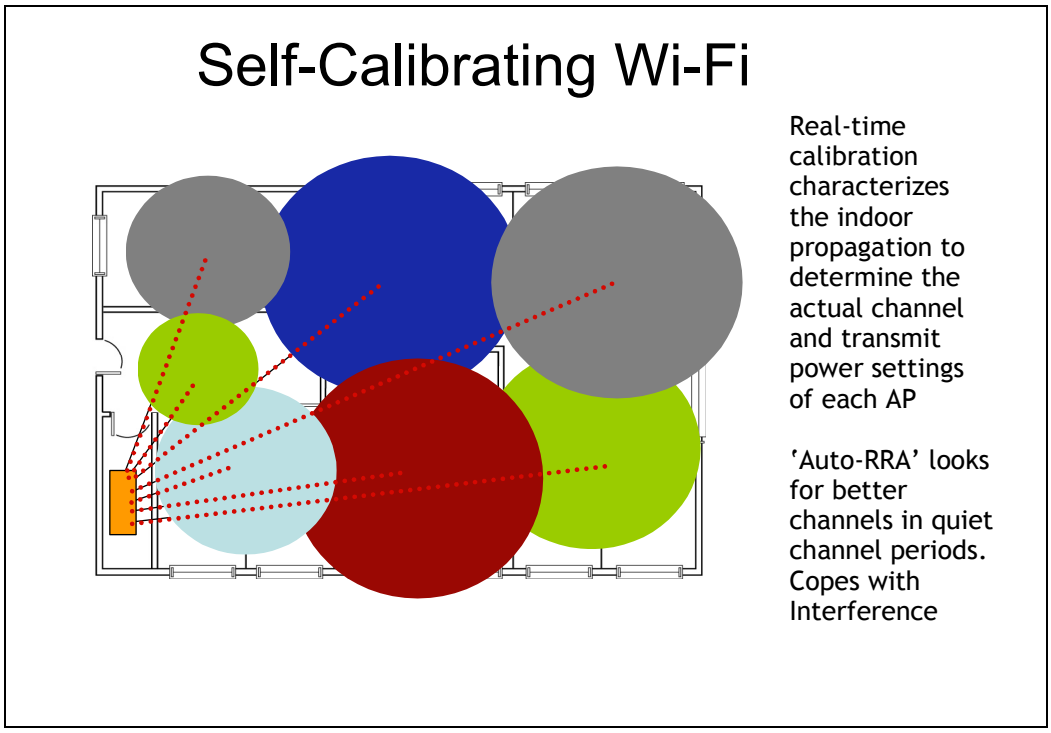
Puissances maximales autorisées pour la PIRE dans la bande 2,4 GHz & 5 GHz,
pour les départements métropolitains (source ART)

Chaque pays possède son propre organisme chargé d'édicter les règles précises qui définissent les fréquences ouvertes à l'utilisation en intérieur ou extérieur, avec les puissances maximales associées. A titre d'exemple, nous présentons ci-dessous la répartition des fréquences par pays, à la date de novembre 2001 (donc bien avant les dernières régulations, en ce qui concerne la France).
Le niveau de puissance par canal peut être différent pour chaque organisme de régulation.

Channel ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Frequ. (MHz)	2412	2417	2422	2427	2432	2437	2442	2447	2452	2457	2462	2467	2472	2484
FCC / IC	■	■	■	■	■	■	■	■	■	■	■			
ETSI	■	■	■	■	■	■	■	■	■	■	■	■	■	
France										■	■	■	■	
Espagne										■	■			
Japan														■
MPHPT	■	■	■	■	■	■	■	■	■	■	■	■	■	

High Rate PHY Frequency channel plan (IEEE 802.11b Cor 1 - 2001)

Le problème principal des outils d'aide à l'administration réseau consiste à définir les fréquences des différentes cellules de manière à ce que les cellules voisines travaillent sur des bandes suffisamment éloignées pour limiter au maximum les interférences. Ainsi, il est généralement conseillé de laisser 4 bandes inutilisées entre les fréquences de chaque cellule limitrophe pour qu'il n'y ait effectivement aucune interférence. Généralement on choisit les trois canaux 1, 6 et 11 pour composer le dallage des cellules qui constitueront la couverture Wi-Fi.



1.4 Futur

Des solutions propriétaires permettent dés à présent d'enrichir légèrement le fonctionnement des technologies Wi-Fi. Par exemple, le mode Turbo ou le mode Nitro permettent d'augmenter très significativement le débit nominal en b ou en g. Cette capacité étant liée à un ensemble de constructeurs (soit grâce au codage de modulation ou au chip qu'ils utilisent, Intersil / Prism en l'occurrence pour Nitro), elle n'est cependant pas supportée ou annoncée de manière générale par tous les constructeurs. Les débits standards étant toujours le plus grand dénominateur commun.

L'IEEE s'emploie actuellement à finaliser les standards relatifs aux compléments de sécurité des solutions Wi-Fi (802.11i), et à développer de nouvelles spécifications relatives à la mobilité, à de plus hauts débits, à une gestion de la qualité de service, tel que le tableau récapitulatif le présente en annexe 5.3.

Précisément, l'IEEE 802.11i, correspondant à WPA 2.0, et dont la ratification est attendue pour 2004, apportera un cryptage de type AES (plus puissant que 3DES), et la protection des trames d'administration (authentication, Association, Beacon, etc).

Tandis que la version interim WPA 1.0 (Wi-Fi Protected Access) offre pour le moment :
- l'authentification sécurisée et cryptée au niveau 2 avec 802.1X (propagation des informations vers le serveur avec EAP),
- clés TKIP (Temporal Key Integrity Protocol) gérant le cryptage au niveau 2 des données transmises,
- le contrôle de l'intégrité des données : MIC (Message Integrity Check).

Par ailleurs, il semble que la technologie Wi-Fi puisse aussi trouver prochainement des applications multiples et diversifiées, puisque l'on parle de téléphones Wi-Fi, qui pourraient à terme détrôner les téléphones DECT, que ce soit en entreprise ou sur le marché résidentiel (en prolongeant naturellement les développements de la voix sur IP (VoIP)).
De même, il est probable qu'à la maison les solutions de Media Center exploiteront intensivement ce mode de transmission performant, répandu et surtout très pratique (aspects Plug & Play très satisfaisants).

2 La problématique des réseaux Wi-Fi

Nous allons brièvement évoquer ci-dessous les spécificités des réseaux locaux sans-fil.

2.1 Complexité

Le premier problème auquel l'administrateur réseau est confronté est la diversité des compétences nécessaires à la mise en œuvre d'un réseau Wi-Fi. Il faut prendre en considération les problèmes de transmission radio, un éventuel audit du site, l'intégration de l'existant (réseau câblé, mais peut être aussi de quelques îlots Wi-Fi déjà en place), le respect de la régulation, le support effectif des standards actuels et à venir, l'administration de ce futur réseau, le monitoring du trafic, etc.

2.2 Sécurité

La sécurité est une préoccupation critique d'un administrateur réseau confronté au Wi-Fi, d'une part parce que les faiblesses des technologies ont été très largement traitées dans la presse, d'autre part parce qu'il s'agit d'une approche effectivement nouvelle du sujet, et qui présente une grande diversité.

2.2.1 Risques

Du fait des faiblesses des solutions standards, de nombreux risques existent en Wi-Fi, dont typiquement les Fake AP, Rogue AP, Honey Pot, Man in the Middle, dont on parle le plus souvent.

Fake AP

L'AP faux n'est pas un véritable AP. Des logiciels permettent de faire apparaître l'interface Wi-Fi d'un poste client (généralement sous Linux) comme un AP, et de configurer son ESSID et BSSID dans un objectif d'impersonation (voir ci-dessous 2.2.2).

Rogue AP

La faille de sécurité dite Rogue AP est la plus redoutée en entreprise (nous traduirons Rogue par indésirable ici). Elle survient quand un utilisateur du réseau, par commodité au niveau de ses bureaux par exemple, connecte un AP sur la prise Ethernet murale, lui permettant d'avoir une certaine mobilité avec son ordinateur à l'intérieur de la cellule ainsi créée. Ces installations pirates, pas nécessairement malveillantes, sont particulièrement dangereuses parce qu'elles ouvrent le réseau de l'entreprise au monde Wi-Fi, généralement avec un niveau de sécurité extrêmement minime (authentification réduite de type WEP avec une clé de 40 bits, pas de Firewall, pas d'IDS, pas de détection de tentative d'attaques, etc.). Au pire cas, l'ordinateur peut fonctionner comme un pont, créant un Wireless Bridge : un lien "ouvert" entre le réseau Wi-Fi et le réseau local câblé.

Honey Pot

Le pot de miel est un AP qui cherche à apparaître comme faisant partie intégrante du réseau de la société pour attirer les postes clients (utilisation du même ESSID), et les laisser se connecter (au niveau WLAN). De cette façon l'Honey Pot espère pouvoir espionner la phase de connexion, pour en déduire les paramètres utiles, quitte à effectivement reproduire simultanément la phase de connexion vers le réseau réel (cas du Man in the Middle).

2.2.2 Attaques & Intrusions

Les intrusions dans l'environnement sans-fil peuvent être classifiées selon 5 catégories :

Probing & Découverte réseau

Bien que la découverte du réseau soit une des fonctions initiales normales de Wi-Fi, c'est aussi une des premières étapes qu'un intrus doit accomplir, et au cours de laquelle on doit essayer de le détecter, même s'il est assez peu "bavard".
Aruba est capable de détecter l'emploi des applications de "war driving" les plus répandues : Netstumbler et Wellenreiter, grâce à leur "signature" spécifique, et d'envoyer un message

d'avertissement à l'administrateur. A ce stade aucune agression n'a encore été menée contre le réseau, mais il est indispensable de savoir qu'il est sous "observation" extérieure.

Attaque DoS

Les attaques DoS, qui ne sont pas propres au sans-fil, consistent à bloquer, par un trafic ou des connexions malveillantes en rafale (trames d'authentification/association), l'accès au réseau, en dégradant très significativement la qualité des communications, ou en générant une charge de traitement sur les équipements réseau ou client (requêtes de probe). Aruba détecte ce genre de flux, génère un avertissement, et aide l'administrateur à localiser la source de l'attaque. A noter que pour certaines attaques, comme la simple génération de fortes interférences radio (RF Jamming), il n'existe pas de moyen de s'en protéger, et l'administrateur est contraint de se déplacer et d'agir sur place, aidé des outils de localisation du système WLAN évolué.

Surveillance

La surveillance consiste à observer et décoder le trafic effectif du réseau. Comme évoqué précédemment, certains modes de cryptage possèdent des faiblesses intrinsèques qui autorisent de "craquer" le codage (le temps de traitement est inversement proportionnel à la quantité de trafic espionné). La principale protection étant l'emploi d'un cryptage fort (celui de WEP, basé sur RC4, n'est pas très robuste avec les clés de 40 ou 104 bits), donc plutôt WPA/TKIP au niveau 2, ou IPsec au niveau 3.
Un autre moyen plus pernicieux consiste à forcer la déconnexion abusive d'un client pour pouvoir déduire la clé de l'observation de la phase de reconnexion qui s'en suit (LEAP est typiquement vulnérable à ce genre d'attaque).

Impersonation

Ce type d'attaque consiste à prendre la place d'un client ou d'un AP valide en utilisant son adresse (BSSID (adresse MAC de l'AP) et ESSID (nom symbolique du WLAN) pour un AP), dans l'objectif d'accéder au réseau ou aux services. Dans le pire des cas, les éléments du réseau n'étant pas aisément localisables en transmission radio, un AP frauduleux peut inviter un client à se connecter au réseau par son accès, et en déduire les éléments d'authentification du client. Le mode de protection le plus efficace consiste à observer continuellement tout le trafic Wi-Fi, tout le trafic sur le réseau, et de pouvoir détecter tout client ou AP incohérent (il s'agit de détecter l'apparition d'un élément inconnu (Client ou AP), la "duplication" du client ou de l'AP, le "déplacement" d'un AP. Un moyen de surveillance est, par exemple, de vérifier que le trafic des Clients Wi-Fi connus et détectés passe bien par les LAN appropriés. Un autre consiste à associer une "signature" à chaque client, qui est dérivée de la puissance du signal émis. Si pour la même adresse MAC, deux signatures différentes sont perçues à un moment donné, les 2 Clients sont mis en quarantaine, et un avertissement est envoyé vers l'administrateur.
Les équipements Aruba qui gèrent/analysent continuellement les différents flux de communication, s'assurent que les communications provenant des AP ne parviennent pas directement au cœur du réseau (par un circuit illicite : Rogue AP typiquement), et à l'inverse, que ces communications radio sont effectivement visibles sur le réseau câblés après passage par le switch (et non pas détournées vers un réseau pirate via un Fake AP).

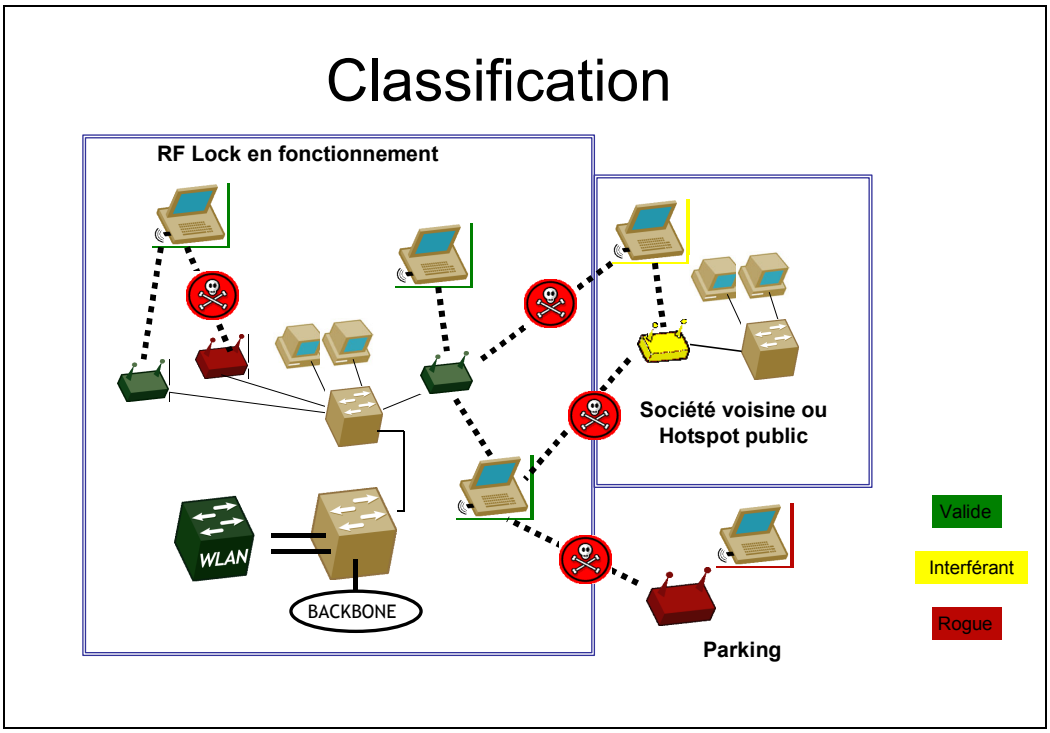
Un type de protection assez générique contre les AP frauduleuses (Fake AP), positionnées par exemple à l'extérieur du bâtiment (et donc avec une puissance radio faible), consiste à interdire aux Clients de se connecter avec un débit trop bas (1 ou 2 Mb/s), car inapproprié à la topologie de disposition des AP officiels.

Intrusion Client

Une attaque de ce genre consiste à exploiter une vulnérabilité du client pour accéder au réseau. Comme pour le monde des réseaux câblés, la meilleure protection étant la mise en place d'un Firewall, situé en l'occurrence au cœur du switch WLAN, entre la partie WLAN et le reste de l'infrastructure réseau. Idéalement, ce Firewall devra mettre en œuvre des protections de niveau 2 et 3, savoir gérer des filtres, ainsi que suivre les connexions dans le temps (capacité dite stateful), garantissant un niveau de sécurité au moins égal à celui de l'environnement câblé.

Intrusion Réseau

C'est une des attaques les plus critiques. Une intrusion réseau vise à prendre le contrôle des ressources réseau d'une entreprise. Les protections contre ce risque étant les systèmes IDS dédiés au Wi-Fi, qui vont chercher à corréler plusieurs évènements douteux pour déterminer si le réseau ou un système particulier est en train de subir une intrusion



La protection la plus courante consiste à forcer systématiquement le dé-attachement du client en cause (trame deauthenticate), ou de tous les clients connus qui se seraient attachés à un AP frauduleux. De cette façon le réseau Wi-Fi apparaît inaccessible à ces postes de travail qui ne parviennent pas à établir une connexion complète.
Cette capacité apporte une protection forte, elle nécessite cependant de régler définitivement le problème par une intervention physique, permettant, grâce aux fonctionnalités de localisation, de mettre la main sur le poste client ou l'AP à la source du danger.

2.3 Coûts

L'installation d'un réseau Wi-Fi en entreprise nécessite de compléter les équipements de transmission par des éléments d'optimisation des communications radio, des briques renforçant la sécurité sur les transmissions radio, ou aux points de connexion avec le réseau câblé, des appareils de mesures du trafic et de diagnostic spécifiques WLAN.
De même, une phase préalable d'audit du spectre radio et de mesure des paramètres de propagation du site, des phases optionnelles de mesures et de contrôles a posteriori, sont à prendre en considération.
Tout cela semble s'ajouter au coût de la solution matérielle.
On notera cependant que les systèmes évolués intègrent une majeure partie des besoins cités précédemment pour constituer une véritable solution complète, comme nous le verrons au paragraphe 3.5.

2.4 Mise en œuvre

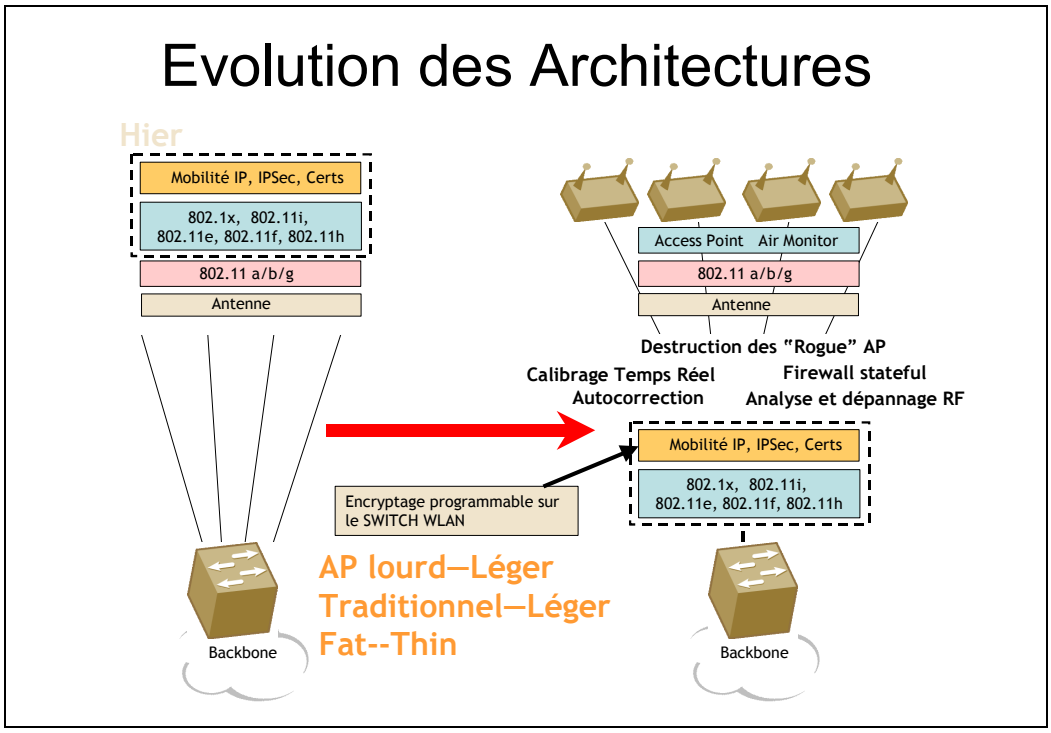
L'installation et la gestion d'un réseau Wi-Fi posent leurs défis particuliers, dont l'installation, l'alimentation et la mise à jour des AP en faux-plafond, le suivi des performances radio, le monitoring du trafic, le contrôle de la topologie des différentes cellules, etc. Bien heureusement, les solutions évoluées apportent une aide précieuse pour accomplir ces différentes taches.

3 La réponse et les solutions Aruba

Comme nous allons le voir ci-dessous, Aruba apporte aujourd'hui une réponse globale et intégrée à toutes les questions que se pose l'administrateur réseau devant gérer au mieux la mise en place d'un réseau Wi-Fi.

3.1 Architecture générale

Aruba Wireless Networks, constructeur spécialisé dans les technologies Wi-Fi a adopté une architecture stratifiée et centralisée qui découpe l'ensemble des fonctionnalités mises en œuvre entre les AP et un "concentrateur" spécialisé, dit switch ou commutateur WLAN (systèmes 800, 2400, 5000).
L'objectif est double, d'une part :
- l'AP devient plus simple, interchangeable (la majorité des paramètres sont stockés sur le switch, et récupérés au moment du boot de l'AP), facile d'installation (car focalisée sur la partie radio), tandis que le switch regroupe toutes les fonctions nécessitant une capacité de processing, conjointement à une redondance de ces fonctions. De plus en centralisant les échanges, le switch peut avoir une vue complète indispensable à ses fonctions de sécurité (authentification et cryptage), d'administration et de statistiques, et enfin de reconfiguration automatique
et d'autre part :
- les équipements sont d'autant plus flexibles, les AP, très spécialisées sur la partie radio, pouvant être upgradées pour supporter de nouvelles spécifications ou fonctionnalités par simple téléchargement. Le switch quant à lui possède une architecture interne (ASIC & FPGA) qui lui permet de mettre en œuvre de nouveaux algorithmes de cryptage sans impacter la fluidité des communications.
Cette stratification complémentaire qui correspond à une spécialisation de chaque type équipement est un élément révélateur de la maturité du domaine, et qui s'est déjà produit dans de nombreux secteurs techniques (spécialisation du type de mémoire des ordinateurs en fonction des contraintes de taille et de temps d'accès, dé corrélation des fonctions de routage/commutation de paquets, de celle de calcul de routes, pour les routeurs, etc.).
Les AP Aruba fonctionnent dans les bandes 2,4 GHz et 5 GHz simultanément, indépendamment. Chacune des 2 bandes correspondant à une AP quasi-autonome (Clients, débit, ESSID, cryptage, WLAN virtuels, etc.).



Noter enfin que dans la littérature anglo-saxonne, les AP simplifiées sont dénommées Thin-AP, à opposées aux Fat-AP plus anciennes, qui intègrent les capacités de sécurités (cryptage, authentification, etc.) localement.

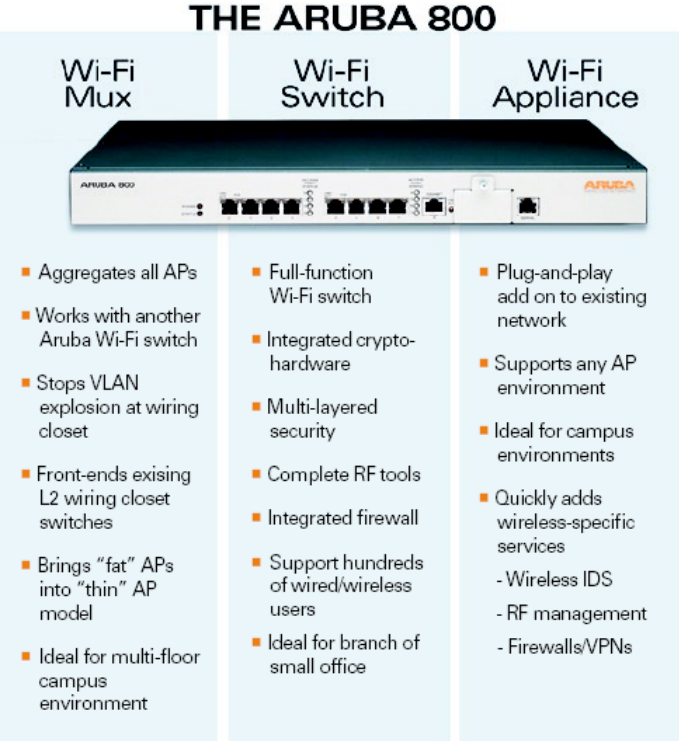
Dans le cas des équipements Aruba, l'ensemble du trafic perçu par les AP est dirigé vers le switch à l'intérieur d'un tunnel IP (en utilisant la technologie GRE). Ceci permet d'avoir une totale étanchéité entre les trafics Wi-Fi et LAN, les communications Wi-Fi devant passer par le commutateur et y subir les contrôles nécessaires (authentification, Firewall, IDS).
La seule contrainte sur l'architecture LAN éventuellement présente entre les AP et le switch, étant que celle-ci autorise le numéro de port TCP correspondant pour ne pas empêcher l'établissement du tunnel.

3.1.1 Commutateur WLAN

Les commutateurs Aruba 800, 2400 5000 contrôlent les AP, les alimentent, commutent le trafic (switch de niveau 2-MAC et 3-IP), mais ils sont aussi capables de terminer les VPN, de recopier le trafic en vue d'un décodage, d'être Firewal et IDS (donc de mettre en œuvre toutes les fonctions de protection : dé-attachement forcé de Clients à risque), et enfin d'administration nécessaires (configuration des AP, modification de leur mode de fonctionnement, calibrage, localisation des clients, etc).

Par ailleurs, il est aussi possible de créer une arborescence de switch ou certains sont locaux (connectés directement aux AP), et l'un, plus central, est maître (éventuellement secondé de son back-up). C'est le modèle dit Direct-Attach, à opposer au modèle dit Overlay, où les AP ne sont pas connectés directement au commutateur (voir illustration au paragraphe 3.4.4).
Les switch locaux font fonction de concentrateur, agrégeant le trafic de plusieurs AP sur un seul tunnel GRE vers le switch maître. Naturellement ces switch secondaires peuvent gérer l'alimentation électrique des AP, et décharger le commutateur central d'une partie du processing.
On retrouvera aussi le modèle Direct pour les réseaux comportant plusieurs sites, mais pour lesquels l'ensemble des réseaux Wi-Fi est géré par une administration unique et centrale.

Une problématique importante est aussi la prise en considération de l'existant, quand l'administrateur réseau a déjà déployé quelques AP d'une autre marque, et que l'on doit intégrer dans l'infrastructure Wi-Fi d'Aruba. Les commutateurs permettent de faire cela avec un mode dit Mux (de multiplexage, ou concentration) des AP, Aruba et autres, sur un tunnel GRE vers le switch maître.
Naturellement, il n'est pas possible de disposer de toutes les fonctionnalités proposées par les AP Aruba avec des AP hétérogènes, mais le réseau gagne cependant fortement en sécurité car le trafic de l'ensemble des AP est encapsulé et redirigé vers le commutateur central, pour un traitement identique (authentification, cryptage, Firewall, IDS).



Aruba propose une gamme de 3 commutateurs Wi-Fi, possédant un ensemble de fonctionnalités identiques, avec des puissances étagées, adressant donc des besoins différents, soit en taille de réseau, soit en position dans l'architecture. Ainsi le modèle 800 peut être positionné en central pour un réseau de taille moyenne (jusqu'à 256 clients sans-fil) ou bien encore en périphérie dans une architecture arborescente possédant un switch plus puissant en central (voir diagramme au paragraphe 3.4.4)

	5000	2400	800
Déploiement	Campus	Building	Filiale
Taille	3U	1U	1U
Access Points	128	48	16
Muxes	32	12	4
Utilisateurs	4096	512	256
Sans cryptage	4 Gb/s	2 Gb/s	1 Gb/s
Avec cryptage	2 Gb/s	400 Mb/s	100 Mb/s

3.1.2 Virtual WLAN

En permettant d'avoir plusieurs ESSID pour une même AP (mais obligatoirement un même canal par bande de fréquences), Aruba transpose la notion de réseaux virtuels à l'intérieur de chaque cellule. Ces VLAN Wi-Fi pouvant tout naturellement être mis en correspondance avec leurs équivalents en LAN en utilisant le tagging IEE 802.1Q.
Par ailleurs, chaque ESSID peut aussi être associé à une méthode d'authentification et de cryptage différente, correspondant à divers niveaux de sécurité.
Outre la différentiation des utilisateurs en plusieurs ensembles ou catégories, cette fonctionnalité apporte aussi un plus en terme de déploiement en permettant de migrer progressivement les utilisateurs (au fil des upgrade des postes de travail) vers des ESSID nécessitant une mode de sécurité plus évolué et plus exigeant, que leur NIC ou leur OS ne supportait pas à l'instant *t*.

3.2 Sécurité

Le mode de fonctionnement du Wi-Fi reposant sur une transmission radio, généralement omnidirectionnelle, il correspond à une communication broadcast, (diffusion générale) où tout le monde peut écouter toutes les communications, voire transmettre des paquets en prétendant être un autre équipement (*impersonation* en Anglais).
En effet, à la différence des réseaux locaux de ces dernières années (avec le remplacement du câble Ethernet par une arborescence de commutateurs), le WLAN est implicitement ouvert, et par-là, présente une forme de vulnérabilité spécifique.
Les constructeurs et organismes de standardisation se sont donc évertués à développer des méthodes de protection capables de fournir un niveau de sécurité comparables aux réseaux «câblés», voire dans certains cas, supérieures.
En effet, pour un administrateur réseau, le développement d'un réseau Wi-Fi en extension de son LAN, ne peut être envisagé s'il présente une vulnérabilité supérieure à l'architecture déjà en place, ou bien si le réseau Wi-Fi apparaît comme un maillon faible, mettant en péril l'ensemble de l'infrastructure (tel un cheval de Troie).
La connexion d'un poste client en entreprise au réseau Wi-Fi est considérée comme la connexion par le RTC au travers d'une infrastructure non sûre. On applique donc des procédés très comparables : authentification de la connexion (avec un protocole dérivé de PPP, propagation de la requête sur l'identité de l'utilisateur vers un serveur Radius et/ou LDAP), cryptage éventuel des communications par un tunnel VPN (L2 ou L3).
Un certain nombre de compléments fondamentaux sont apportés par la solution Aruba, comme les filtres (ACL au niveau IP ou MAC), un Firewall stateful, un IDS, parallèlement à la détection de tout évènement pouvant être la prémisse d'une attaque Wi-Fi.

Les procédures de sécurisation des équipements Aruba reposent sur leur capacité à suivre tous les équipements actifs "visibles", tant AP que clients, et à les classer selon le degré de risque qu'ils peuvent présenter (par exemple : Valid, Interfering, Rogue pour les AP). Ainsi un poste client qui s'est déjà authentifié dans le passé, est, lors d'une nouvelle connexion, considéré différemment d'un poste nouvellement découvert. La classification permet au système complet de pouvoir déceler tout évènement alarmant et de réagir au mieux.

Dans ce paragraphe nous allons aborder ces fonctionnalités sous deux angles, l'étape ou la fonction correspondant au complément de sécurité, puis nous les résumerons par niveau du protocole de sécurité dans la pile IP.

3.2.1 Attachement

Plusieurs mécanismes permettent d'améliorer significativement la sécurité de la phase de connexion.
Un premier niveau de protection consiste à ne pas diffuser le nom du réseau (SSID). Dans ce cas c'est au poste client de connaître ce nom pour s'attacher. Une autre technique similaire consiste à ne pas répondre aux broadcast demandant quelles sont les ESSID disponibles ou visibles (Probe Request Frame de la procédure DCF). Il s'agit cependant, d'une part, de protections très limitées, car les ESSID peuvent être découverts via les communications des autres STA observées, et d'autre part parce qu'elles peuvent bloquer l'attachement de certains NIC dont les implémentations ont besoin de ces étapes dans leur processus de connexion.

3.2.2 Authentification utilisateur

Pour l'authentification, plusieurs modes sont possibles. Le premier consiste à ne rien demander au niveau Wi-Fi (pas de clé), c'est le mode utilisé en hot spot par exemple, puisque l'utilisateur lors de sa connexion n'a aucune connaissance du réseau, et réciproquement. L'authentification se fera alors sur un portail web.
Le mécanisme de sécurité le plus courant pour l'attachement et le WEP (Wired Equivalent Privacy) qui possède par défaut une clé de 40 bits (plus un vecteur d'initialisation de 24 bits). Mais des programmes existent maintenant dans le public pour casser ces clés. Des implémentations à 128 (24+104) et 256 bits sont courantes, et plus robustes. Un autre moyen d'améliorer le WEP et de le rendre dynamique en forçant une modification périodique de la clé, et d'en allouer une par client (Dynamic WEP).
Quoi qu'il en soit le WPA 1.0, en attendant la ratification du IEEE802.11i a apporté un plus très significatif. Il fait usage du standard IEEE 802.1X pour faire référence à un serveur d'authentification, ce qui correspond à considérer le switch WLAN comme un concentrateur de modem (RAS ou BAS) dans une architecture de collecte traditionnelle.
Le protocole utilisé entre le switch Aruba (authenticator) et le serveur pouvant être une des variantes d'EAP (Extensible Authentication Protocol) : EAP-TLS, EAP-TTLS, PEAP, LEAP .
WPA fait aussi usage de TPKI pour le cryptage des données (niveau 2 puisqu'il s'agit encore de Wi-Fi) qui remplace avantageusement WEP.

Comme évoqué ci-dessus, le dernier mode d'authentification par un serveur Web "forcé" à la connexion, répond au besoin de type hot spot pour les opérateurs, et est donc positionné au niveau 7.
Il correspond à effectuer l'authentification de l'utilisateur sur une page Web (le serveur Web tournant dans le switch WLAN) par un ID + Password. La liaison entre le Client et le switch est sécurisée grâce à SSL (https) et l'authentification peut être réalisée, comme précédemment, grâce à une base locale, ou en se référant à un serveur AAA avec le protocole Radius ou LDAP.
En retour l'utilisateur est assigné à une catégorie (rôle/profil) définissant son VLAN, ses droits, etc. Par exemple si l'utilisateur est connu mais qu'il n'a plus de crédit, il peut être redirigé vers un VLAN aboutissant à une page particulière lui demandant de renouveler son abonnement.
Le serveur Web ne gérant que la partie authentification, dans certains cas on demandera ensuite au Client de télécharger un Dialer VPN (Client VPN) pour pouvoir crypter les communications qui s'en suivent.

3.2.3 Communication

Une fois l'utilisateur authentifié, et autorisé, et donc associé à une catégorie, ou rôle, tous les échanges qu'il va avoir à travers le switch WLAN seront encore soumis à un niveau élevé de contrôle et de surveillance.
Il s'agit d'une part de se protéger contre les observations indélicates (eavesdropping), mais aussi potentiellement des attaques véhiculées par le trafic lui-même.
La protection contre le premier risque consiste à crypter les communications, celle contre le second à vérifier son contenu à l'aide d'un Firewall et/ou d'un IDS (Intrusion Detection System) orienté wireless.

3.2.3.1 Cryptage

L'utilisation de réseau virtuel privé (VPN) gère la liaison entre le client et le switch (partie radio et tunnel) comme une liaison RTC (liaison téléphonique commutée, via modem). En effet, en partant du principe que cette partie de la connexion est jugée non fiable, on emploie un VPN pour le cryptage (et l'authentification), protégeant tous les trafics de l'ordinateur client, jusqu'au concentrateur de VPN (un commutateur Wi-Fi dans l'architecture Aruba). Ce dernier a la charge de terminer les VPN de tous les clients (sans impact sur les performances), et de livrer un trafic "sain" au réseau LAN auquel il est connecté. Implicitement, ceci signifie que l'architecture matérielle du switch lui permet d'effectuer la terminaison de grandes quantités de VPN (jusqu'à quelques milliers de clients dans la pratique).

Avec les équipements Aruba, différents types de VPN sont supportés :
- L2TP
- L2TP over IPsec
- XAUTH
- PPTP

Les types de VPN : IPsec, Policy sub-mode, Dynamic Map sub-mode, L2TP, PPTP
Les protocoles d'authentification : PAP, CHAP, MSCHAP, MSCHAPv2, CacheSecureIDToken.
Les cryptages IKE : DES, 3DES (AES très bientôt)
Les algorithmes de Hash IKE : SHA ou MD5
L'authentification IKE : Signature RSA ou Preshared Key Password

Encryption Protocol	Key Size	Encryption Method	Vulnerabilities
WEP	40, 128 bit	RC-4	No message integrity code makes it open to packet injection and replay attacks, weak initialization vectors
Dynamic WEP	40, 128 bit	RC-4	Open to packet injection, weak initialization vector
TKIP - WPA 1.0	128 bit	RC-4	Weak message integrity code, packet injection
IPsec	128, 168, 192 or 256 bit	3DES, AES	
AES-CCMP - IEEE 802.1i	128, 192 or 256 bit	AES	Message integrity code and encryption keys are identical

IPsec étant beaucoup plus robuste que PPTP, la combinaison la plus répandue est généralement une authentification WEP associée à un VPN de type L2TP/IPsec.

3.2.3.2 Firewall

Le Firewall intégré au switch Aruba est un switch hardware complet :
- stateful : il maintient une connaissance de l'état des sessions / connexions
- dynamique : les informations concernant les adresses IP peuvent changer quand la règle est appliquée aux utilisateurs

- bidirectionnel, à la différence de la plupart des ACL qui ne s'appliquent qu'au trafic entrant ou bien sortant sur une interface
Il possède des ACL (cisco-like), par défaut associées à une interface physique, qui peuvent aussi être configurées pour avoir des plages horaires de mise en œuvre.
Ces filtres peuvent être définis au niveau :
- Ethertype
- MAC
- Standard (adresse IP source)
- Extended (adresse IP source ou destination, port source ou destination, protocole IP)
Les actions possibles sont l'autorisation (permit), l'interdiction (deny), le choix de la queue de priorité, ou le log. Notons effectivement que les switch possèdent plusieurs queues (dont 2 sont utilisables actuellement), permettant d'envisager la gestion de flux avec QoS (typiquement la VoIP à partir d'un ordinateur, et bientôt avec des téléphones Wi-Fi : VoWLAN).

Des capacités NAT sont aussi accessibles avec le Firewall, pour la modification de l'adresse IP destination, ou de l'adresse IP source.

3.2.3.3 IDS

Les capacités de l'IDS wireless intégrées au switch Aruba consistent à surveiller continuellement les échanges et les flux Wi-Fi pour détecter au plus tôt tout risque ou évènement anormal, informer immédiatement l'administrateur et réagir en temps réel.
Comme nous l'avons vu précédemment, les équipements Aruba savent repérer les clés Wep faibles, Rogue AP, les ponts wireless (WBS), localiser les équipements responsables d'un DoS, détecter une impersonation ou une attaque ASLEAP. Ces capacités reposent sur la base de connaissance (WMS Wireless Management System) que possède le switch central, et qu'il enrichit au fil de l'eau lors de toute connexion, authentification, tout échange, tout déplacement ou toute modification des caractéristiques d'un équipement.

3.2.4 Layer 2 - Layer 3

En reprenant les éléments cités jusqu'ici, nous allons brièvement récapituler les différents mécanismes de sécurité qui sont offerts par la solution ARUBA, en les classant par niveau d'opération : 2 - MAC, 3 - IP, et 7 - Web (nous conservons la numérotation du modèle ISO, mais appliquée à la pile TCP/IP).

Au niveau 2
- WEP (statique,dynamique)
- WPA-PSK
- WPA (802.11i interim : 802.1X, TKIP)

Au niveau 3
- VPN IPsec
- VPN PPTP

Au niveau 7
- Portail captif

Application Layer Stateful Firewalls
Encryption Layer WEP, Dynamic WEP, TKIP; AES, IPsec
Authentication Layer IEEE 802.1X, IPsec, https
RF / Physical Layer Wireless IDS, Rogue AP Protection

Concernant le support du VPN, pour simplifier au plus l'utilisation de ce mode de sécurité sur le poste Client, le switch Aruba propose sur la page Web d'authentification le téléchargement d'un Dialer VPN permettant à tout PC d'être doté des mêmes capacités de cryptage, indépendamment de sa configuration antérieure ou de ses drivers précédents. C'est une réponse complète et sûre, qui garanti une gestion et une administration professionnelle du parc d'ordinateurs clients.

3.3 Monitoring

Le mode de fonctionnement de Wi-Fi veut que dès qu'un AP est associé à une fréquence (pour chaque bande de fréquence 2,4 et 5 GHz), il ne fonctionne que sur cette fréquence, et même si celui-ci est capable, tout en gérant les transmissions de surveiller aussi tout autre trafic dans cette bande fréquence, il n'a plus la possibilité de basculer sur les autres canaux pour surveiller ce qui s'y passe. C'est donc tout naturellement le rôle d'AP particuliers, dits AM (M pour Monitoring) dédiés à l'écoute, donc passifs, qui eux vont continuellement balayer les différents canaux (en 2,4 GHz et en 5 GHz simultanément) pour surveiller les flux des différentes cellules qu'ils reçoivent, mais aussi vérifier le bon fonctionnement des autres AP voisins.
Noter que les AP et les AM Aruba sont les mêmes équipements, et que le switch peut commander dynamiquement le basculement d'un mode de fonctionnement à l'autre.
Tout le trafic de ces AM étant remonté vers le switch, celui-ci pourra de cette façon enrichir sa base de connaissance, non seulement du trafic qu'il gère effectivement par ses propres AP, mais s'assurer qu'aucun de ses clients connus ne se connecte à un AP "non référencé".
Il est ainsi fortement recommandé de faire arriver tous les VLAN du réseau sur le switch WLAN, même ceux qui ne feront transiter aucun trafic par le switch. Cela permet au switch, grâce à l'écoute des requêtes DHCP en broadcast, de localiser tous les équipements, et de détecter la présence anormale d'un flux ou d'un client sur un segment où il ne devrait pas figurer.
Les AM étant passifs, en mode d'écoute ils peuvent détecter et suivre des signaux relativement faibles, provenant d'équipements assez éloignés. Par conséquent, leur couverture est beaucoup plus large que celle des AP. En considérant qu'un AM peut couvrir une superficie estimée grossièrement à 5 ou 6 fois celle d'un AP, l'on déduit une règle d'ingénierie.
Cependant ce travail est grandement simplifié grâce aux outils logiciels d'Aruba qui permettent de travailler sur le plan des bâtiments et la position des AP et AM pour déterminer de manière théorique les emplacements optimums.

Enfin, concernant les capacités de monitoring, il est intéressant de noter qu'un administrateur réseau peut envisager de se doter d'un système Wi-Fi, non pas dans le but d'étendre son réseau en Wi-Fi, mais dans le but premier de surveiller qu'aucune installation pirate (Rogue AP) n'a effectivement été installée et connectée au réseau, mettant en péril l'ensemble de l'infrastructure pas son manque de sécurité. Ainsi, un switch WLAN uniquement équipé d'AM permet de surveiller quotidiennement l'apparition de transmissions Wi-Fi, et ce, avant même qu'une installation officielle ne soit déployée.

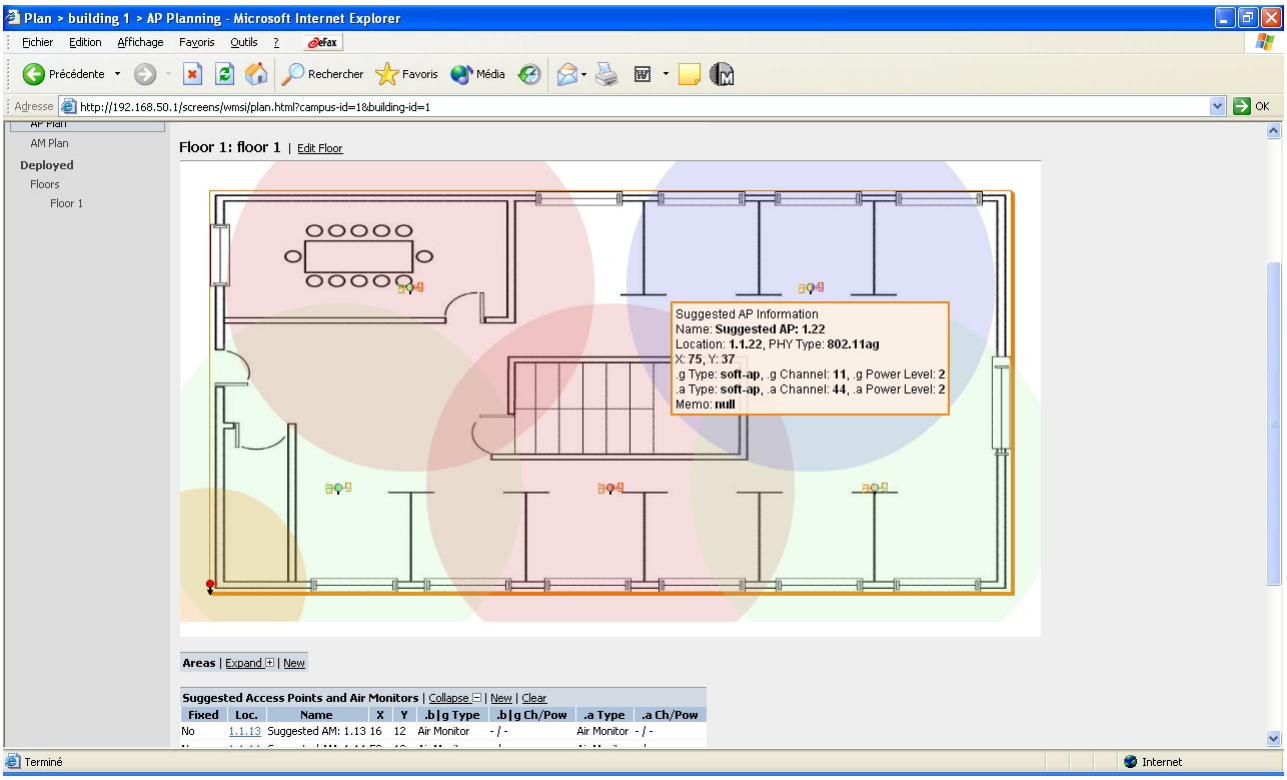
3.4 Mise en œuvre et maintenance

La génération moderne d'équipements Wi-Fi comme ARUBA a pris en considération les problématiques des administrateurs et des équipes de maintenance pour optimiser leur phase de conception, simplifier les phases d'installation et de maintenance, et enfin pour enrichir au maximum la connaissance du réseau et son suivi.
On a vu que le premier critère correspondant à cette approche consiste à regrouper un maximum de fonctionnalités dans le commutateur, rendant l'AP aisément interchangeable, et garantissant les performances.

3.4.1 Ingénierie

La mise en place d'un réseau Wi-Fi, assez simple en apparence, et ce d'autant plus que certains utilisateurs l'ont déjà expérimenté chez eux avant d'en aborder la problématique en entreprise, fait appel à un type de compétence rarement présent dans les équipes réseaux. En effet, le "lego" Ethernet est beaucoup plus facile à maîtriser, qu'une compétence globale en Wi-Fi. Et ceci parce que Wi-Fi ne fait pas appel qu'à des compétences "data" (connectique, méthode d'accès, cryptage, échange de clés) mais aussi à une compréhension des phénomènes de propagation hertzienne, et si possible à la capacité de mesurer et contrôler les transmissions radio, leur couverture, leur atténuation, leurs interférences, leur réflexion, etc.
L'installation d'un réseau Wi-Fi en entreprise nécessite donc une étude de site, mesure et définition de l'emplacement des AP, calibrage des niveaux de puissance.

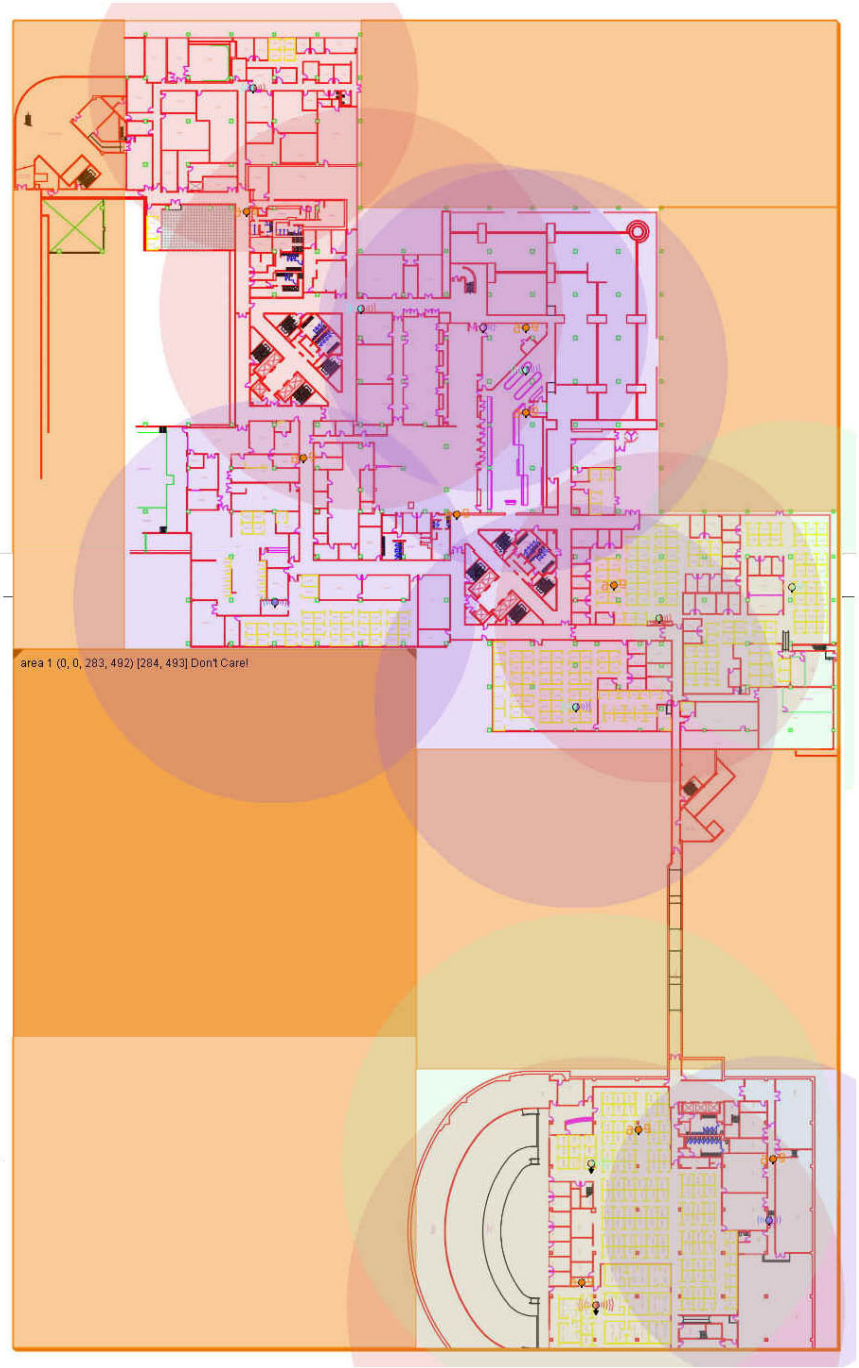
Les propriétés de propagation du milieu, l'air en l'occurrence, sont non seulement complexes, mais de plus, évolutives.
En effet, à 2,4 GHz, les rayonnements sont très fortement atténués par l'eau (comme pour les micro-ondes) et le métal. A 5 GHz, le ciment, les briques, le bois et le métal sont aussi des matériaux bloquants.
Ce qui veut dire que l'ouverture d'une porte, le déplacement d'une armoire, voire d'un individu dans le trajet des ondes peut modifier sensiblement leur propagation ou leur réflexion.
A noter que les AP Aruba possèdent deux antennes, principalement pour créer un minimum de diversité dans les trajets des ondes radios entre l'AP et chaque client, ce qui évite ou limite très significativement les problèmes d'interférences destructives qui peuvent survenir entre des rayonnements cohérents en opposition de phase (après réflexion).



RFPlan simple

Nous déduisons de ce qui précède qu'il n'est pas réaliste de réaliser une mesure des conditions de propagation trop fine. Il est plutôt recommandé de se focaliser sur des mesures plus globales, sachant que l'installation devra offrir une certaine marge de fonctionnement pour palier aux micro-changements, nécessairement imprévisibles.
Les fonctions logicielles intégrées à la solution Aruba proposent ainsi d'accompagner l'administrateur dans le positionnement des AP, pas seulement en fonction des aires à couvrir, mais en intégrant aussi des critères comme le nombre maximum de clients que l'on désire voir se connecter à un AP, ou encore le niveau de redondance AP-AM que l'on souhaite. Cet outil est généralement très suffisant pour déterminer la disposition des AP et la couverture qui s'en déduira (voir figure ci-dessus).

Suite à la phase de conception, une fois les AP (et AM) installés, le switch Aruba les télé contrôle pendant une phase de calibrage automatique, durant laquelle le canal de fonctionnement et le niveau de puissance de chaque AP est déterminé grâce aux mesures menées par chaque AP. L'objectif de cette phase étant de minimiser les interférences entre cellules (on a vu précédemment qu'il était préférable de laisser 4 canaux inutilisés entre chaque cellules voisines), mais aussi d'optimiser le niveau de puissance de manière à ne pas laisser de trou, tout en conservant une marge de manœuvre en cas de défaillance d'un AP.



Areas | Expand | New

Suggested Access Points and Air Monitors | Collapse | New | Clear

Fixed	Loc.	Name	X	Y	.b|g Type	.b|g Ch/Pow	.a Type	.a Ch/Pow
No	1.1.1	Suggested AP: 1.1	532	90	Aruba AP	11 / 2	Aruba AP	149 / 2
No	1.1.4	Suggested AP: 1.4	396	451	Aruba AP	11 / 3	Aruba AP	56 / 3
No	1.1.5	Suggested AP: 1.5	455	514	Aruba AP	1 / 2	Aruba AP	48 / 2
No	1.1.6	Suggested AP: 1.6	548	536	Aruba AP	6 / 2	Aruba AP	40 / 2
No	1.1.7	Suggested AM: 1.7	204	626	Air Monitor	- / -	Air Monitor	- / -
No	1.1.8	Suggested AP: 1.8	361	688	Aruba AP	11 / 3	Aruba AP	56 / 3
No	1.1.9	Suggested AP: 1.9	245	731	Aruba AP	1 / 3	Aruba AP	60 / 3
No	1.1.10	Suggested AP: 1.10	331	718	Aruba AP	11 / 2	Aruba AP	161 / 2
No	1.1.11	Suggested AP: 1.11	169	887	Aruba AP	1 / 2	Aruba AP	60 / 2
No	1.1.12	Suggested AM: 1.12	400	46	Air Monitor	- / -	Air Monitor	- / -
No	1.1.13	Suggested AM: 1.13	440	154	Air Monitor	- / -	Air Monitor	- / -
No	1.1.14	Suggested AM: 1.14	535	133	Air Monitor	- / -	Air Monitor	- / -
No	1.1.15	Suggested AM: 1.15	423	537	Air Monitor	- / -	Air Monitor	- / -
No	1.1.16	Suggested AP: 1.16	184	525	Aruba AP	11 / 3	Aruba AP	149 / 3
No	1.1.17	Suggested AM: 1.17	312	586	Air Monitor	- / -	Air Monitor	- / -
No	1.1.18	Suggested AM: 1.18	361	718	Air Monitor	- / -	Air Monitor	- / -
No	1.1.19	Suggested AM: 1.19	164	800	Air Monitor	- / -	Air Monitor	- / -
No	1.1.20	Suggested AM: 1.20	361	658	Air Monitor	- / -	Air Monitor	- / -

Deployed Access Points and Air Monitors | Collapse

Loc.	Name	X	Y	.b|g Type/Ch/Pow	.b|g Bssid	.a Type/Ch/Pow	.a Bssid
1.1.2	Suggested AP: 1.2	410	30	Aruba AP / 1 / 4	00:0b:86:80:2d:10	Aruba AP / 36 / 4	00:0b:86:80:2d:18
1.1.3	Suggested AP: 1.3	407	130	Aruba AP / 6 / 4	00:0b:86:80:44:10	Aruba AP / 40 / 4	00:0b:86:80:44:18

3.4.1.1 Interférences

La bande de fréquence des 2,4 GHz est relativement sujette aux interférences, avec d'autres réseaux Wi-Fi proches, avec le Bluetooth, mais aussi aux micro-onde, ou au DECT dans certains pays.
Même si le codage et la diversité des canaux permettent théoriquement de palier à ce type de difficulté, il est important de mesurer ou de surveiller le spectre radio sur le site.
Un haut niveau d'interférence pourra dégrader significativement les performances, voire empêcher le fonctionnement de certaines cellules.
La bande des 5 GHz est légèrement moins perturbée, mais la propagation y est légèrement moins performante aussi.

3.4.2 Installation

Une technologie répandue qui permet de simplifier l'installation des AP consiste à utiliser l'alimentation par le câble Ethernet. En effet l'IEEE 802.3af définit un mode d'alimentation en 48 Volt qui utilise le câblage Ethernet standard (POE Power Over Ethernet), et permet typiquement d'alimenter des AP qui, couramment situés dans les faux plafonds, ne sont pas nécessairement proches d'une source de courant ou d'une prise électrique.
A noter que les AP Aruba peuvent aussi avoir recours à une source d'alimentation standard par un connecteur dédié.
Le mode de fonctionnement POE nécessite cependant une connexion directe entre le switch et l'AP (modèle Direct, diagramme du paragraphe 3.4.4), ou alors l'emploi de switch ou de concentrateurs intermédiaires supportant aussi le POE.
En reprenant ce principe, Aruba permet aussi de se connecter aux AP en mode série par le câble Ethernet (à condition que celui-ci ait 4 paires), comme par un port série DB9.
A noter que le switch est un concentrateur de terminaux, et que les ports RJ-45 du switch intègrent l'équivalent d'un petit "splitter" Ethernet + Série. Comme pour le POE, cette capacité nécessite que les AP soient connectés en direct sur le switch Aruba.

Ces deux facilités sont particulièrement intéressantes en terme de déploiement, puisque le câblage nécessaire à la mise en place d'un AP n'est que d'un seul câble, tout en conservant les 3 fonctions : alimentation électrique, trafic utile sur Ethernet, port série pour la console, et donc en conservant tous les moyens de contrôle de l'équipement une fois le faux-plafond refermé.
On notera qu'il est possible de ne donner à l'AP que son identificateur de position (# de site, # de bâtiment, # d'emplacement) pour lui permettre de s'auto configurer via le switch central, donc quasiment en Plug & Play.

Un dernier point important concernant l'installation des AP ARUBA en faux plafond, donc hors des locaux techniques, est que la configuration locale de l'AP ne possède aucun paramètre critique pouvant être utilisé pour perpétrer une attaque sur l'infrastructure Wi-Fi. En effet, les AP sont plus vulnérables à des actes malveillants que les autres éléments réseau, puisque qu'ils peuvent être soumis à des risques physiques supplémentaires : Déconnexion, destruction, etc. Cependant, à l'extrême, le fait de voler un AP ne donne au malfaiteur accès à aucun code, clé, paramétrage radio ou autre, toutes les informations vitales étant stockées sur le switch. Seule la position "logique" de l'AP, et éventuellement quelques adresses IP sont sauvegardées sur la mémoire locale.
Naturellement, le remplacement de l'élément dérobé est par conséquent très aisé, puisqu'il suffit de remplacer l'AP par un autre, configuré avec le même # de position, pour permettre sa réintégration immédiate au réseau.

3.4.3 Performance

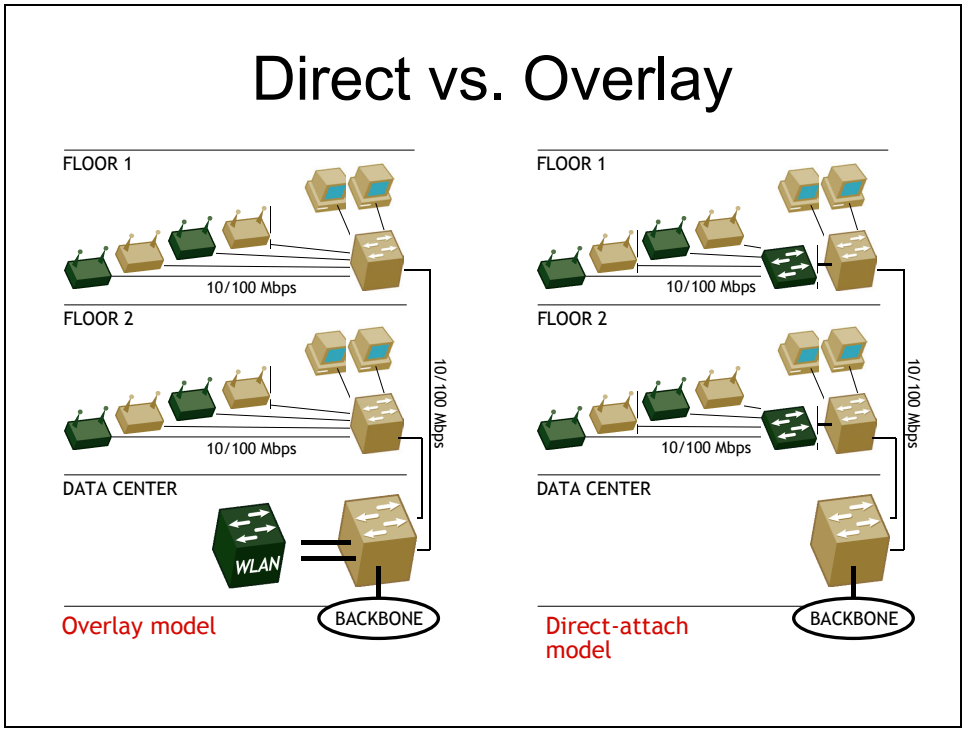
Les réseaux Wi-Fi nous rappellent aussi une façon de considérer la performance, que nous avions oublié depuis que nous sommes habitués à l'Ethernet 10/100 Mb/s commuté, avec lequel la bande passante est dédiée par port. En effet, une cellule propose un débit nominal de 11 ou 54 Mb/s partagé entre tous les clients attachés, et entre tous les WLAN virtuels gérés par l'AP (et bien sûr implicitement en half-duplex). Ce qui plus est, ce débit est réellement nominal (de par la méthode

d'accès CSMA/CA, et les délais consacrés aux IFS Inter Frame Space, Backoff et Contention Windows, Network Allocation Vector, Ack), la limite effective étant très sensiblement inférieure (selon les cas, de 30 à 50 %).
Noter au passage que la mise en œuvre simultanée d'émission/réception en technologie b et g (donc dans la bande 2,4 GHz), réduit aussi légèrement la performance des transmissions.
Ceci veut dire que, d'une part, il n'est pas raisonnable d'avoir plusieurs dizaines d'utilisateurs actifs par cellule, et que d'autre part, il faut aussi en bannir les machines exagérément exigeantes (serveur, station de traitement graphique, unité de stockage, etc.), pour lesquelles les technologies WLAN ne sont pas adaptées aujourd'hui.
Par contre, une cellule comportant au plus une vingtaine d'utilisateurs leur offrira un potentiel de confort tout à fait satisfaisant pour une utilisation bureautique générique. On peut effectivement considérer qu'un utilisateur standard a généralement besoin de moins d'1 Mb/s en moyenne.
Aruba propose cependant certains fonctionnalités permettant d'améliorer la situation, en surveillant précisant le nombre de stations connectées à chaque AP, et dans chaque WLAN virtuel, et en basculant éventuellement un utilisateur d'un AP encombré vers un autre automatiquement.
Cette fonction nommée Load Balancing permet d'optimiser le trafic global au bénéfice de chaque utilisateur, sans nécessairement faire intervenir l'administrateur systématiquement.

3.4.4 Intégration

La plupart des installations de réseaux Wi-Fi se fait en excroissance d'un réseau préexistant. Pour l'administrateur réseau, cette installation doit donc être pensée pour s'intégrer d'une manière aussi aisée que possible.
Pour cela les WLAN reconnaissent les VLAN existants sur le réseau (grâce au Tagging 802.1Q), et peuvent les prolonger sans difficulté sur la partie sans-fil, tout en conservant, grâce à leurs différents mécanismes de sécurité un niveau de confidentialité identique, voire supérieur.

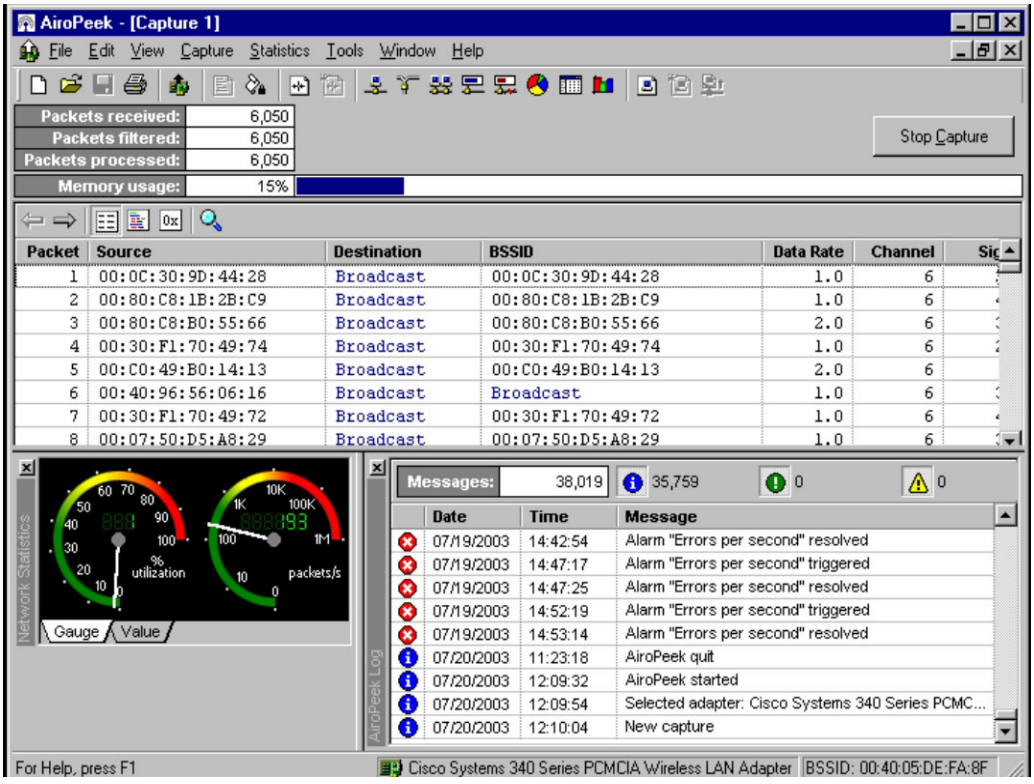
Mais la question devient plus compliquée quand il s'agit de déployer un réseau Wi-Fi global sur une infrastructure qui comporte déjà quelques îlots sans-fil. La reprise de l'existant est cependant tout à fait possible, en sachant que les AP d'autres marques peuvent être reliés aux switch Aruba (typiquement en mode local) pour rapatrier l'ensemble du trafic Wi-Fi sur le commutateur central par un tunnel GRE.
Cette agrégation est indispensable pour garantir la sécurité en n'ayant qu'un seul point de passage et de contrôle entre le WLAN et le "Wired".



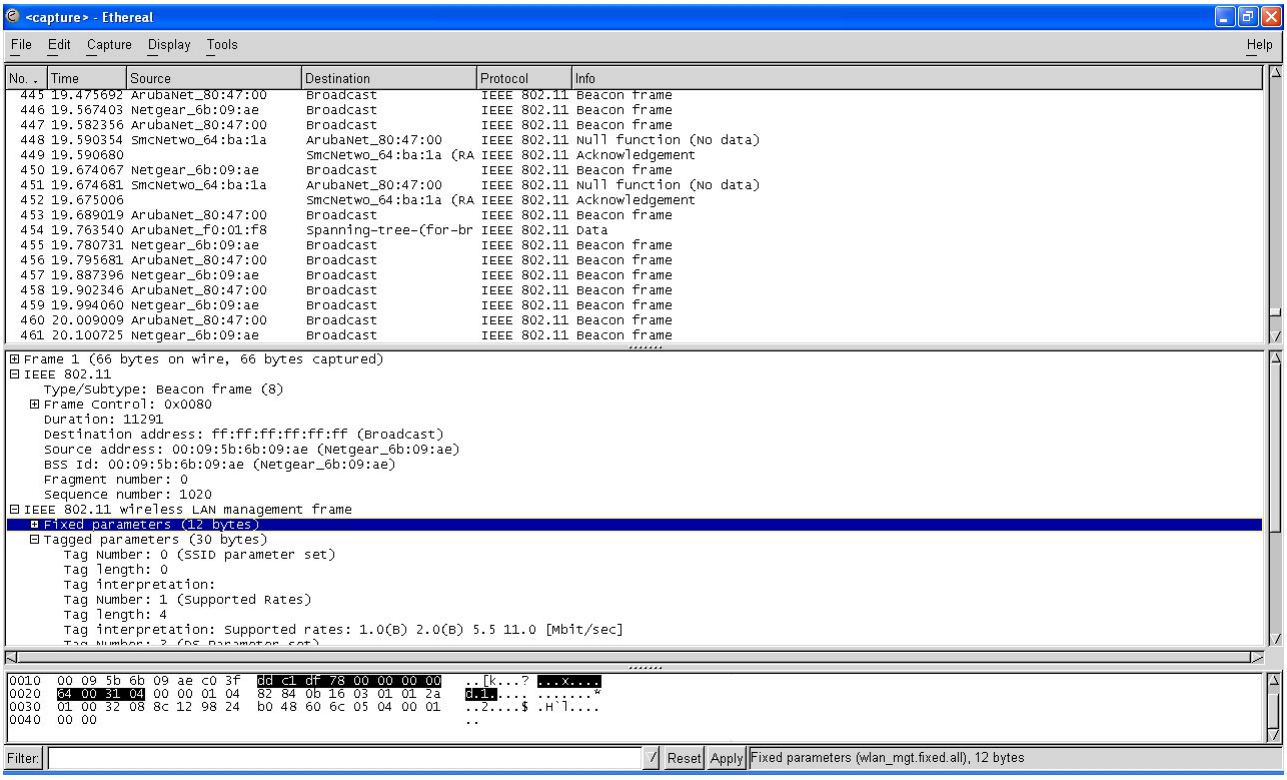
Cependant, les AP autres, n'ayant pas toutes les fonctionnalités des AP Aruba, certaines fonctions ne seront pas disponibles (WLAN virtuel, réglage de la puissance, auto calibrage).
A noter que les interventions de l'IDS (trame deauthenticate) en cas de danger, sont de la responsabilité des AM, les AP autres sont aussi protégées par ce mécanisme Aruba.

3.4.5 Exploitation

Pour l'administrateur réseau, le Wi-Fi correspond à une approche renouvelée de la problématique de maintenance et d'exploitation. En effet, d'une part les équipements réseau ne sont pas tous dans les locaux techniques, d'autre part, il s'agit d'un domaine encore très dynamique, dans lequel de nouvelles fonctionnalités viennent périodiquement compléter les technologies en place.
L'architecture qui consiste à concentrer l'intelligence du réseau Wi-Fi dans le switch WLAN, permet de simplifier au plus l'AP (Thin-AP), et de centraliser le traitement, et donc de limiter au strict minimum le nombre des équipements qu'il faut upgrader pour ajouter de nouvelles fonctionnalités et l'évolution des standards. De même, tout le trafic circulant par le switch WLAN, il est possible de surveiller en un point central l'ensemble des communications. Ce qui est un avantage décisif, que ce soit pour le monitoring et les statistiques, ou pour la détection de toute intrusion ou anomalie dans le cheminement des paquets (par exemple pour la détection des AP Rogues).
Ce qui plus est, l'architecture matérielle des switch WLAN Aruba est suffisamment flexible pour permettre de rajouter d'éventuels futurs mécanismes de cryptage ou d'authentification sans impacter les performances, et avec une mise à jour centralisée, et donc unique.
Comme vu précédemment, cette architecture permet une coopération intelligente entre les AP, que ce soit pour le choix du canal de fréquence, pour le niveau de puissance optimum pour minimiser les interférences, et éviter les "trous", ou pour la répartition du nombre de clients par AP.
Enfin, cette gestion centralisée permet aussi au parc d'AP d'offrir un certain niveau de Self-healing, par exemple, en augmentant automatiquement la couverture des AP voisines, lors de la détection d'une défaillance sur un AP.
Dans le même esprit, la possibilité de demander aux AM de remonter un trafic particulier en vue d'un décodage détaillé permet de réaliser des manipulations de mesure et en évitant tout déplacement, et toute installation physique d'un analyseur ou autre sonde.



Analyse Remote AiroPeek



Décodage avec Ethereal

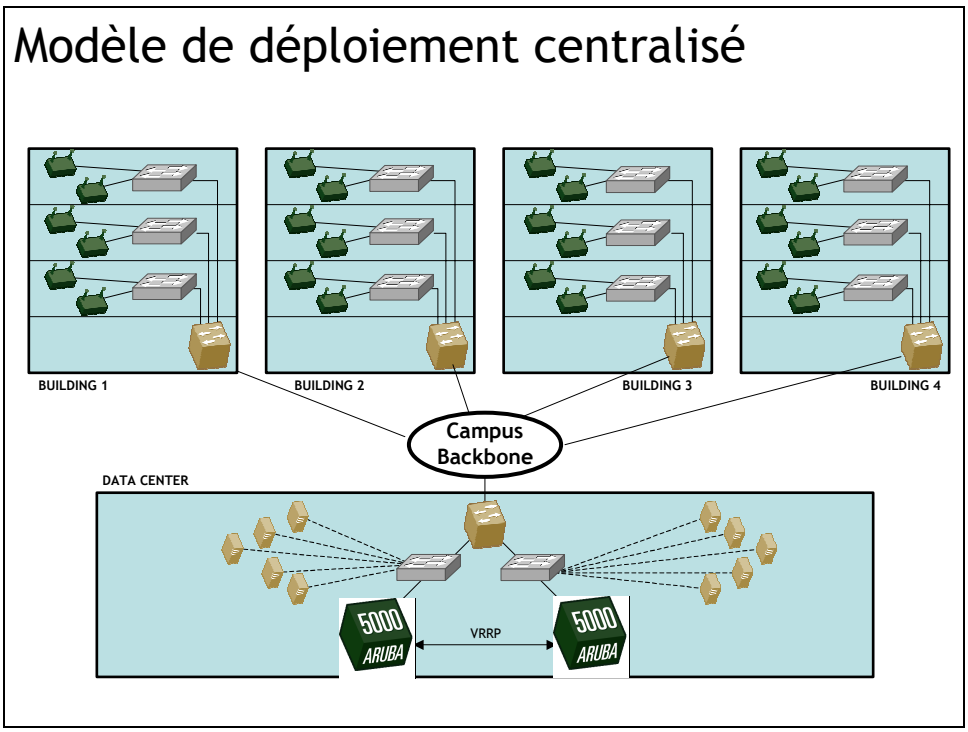
3.5 ROI & TCO

La solution Aruba est composée de commutateurs Wi-Fi associés à de multiples Thin-AP.
Mais le switch héberge aussi un grand nombre de fonctionnalités complémentaires :
- un concentrateur POE
- un concentrateur de terminaux série
- un terminateur de VPN extrêmement performant
- un Firewall hardware stateful
- un IDS (Intrusion Detection System) wireless
- une base de données des utilisateurs, de leurs paramètres et historique d'authentification
- une capacité de capture de trafic globale, comparable à un analyseur distribué
- une capacité de monitoring radio sur tout le site, permettant la localisation

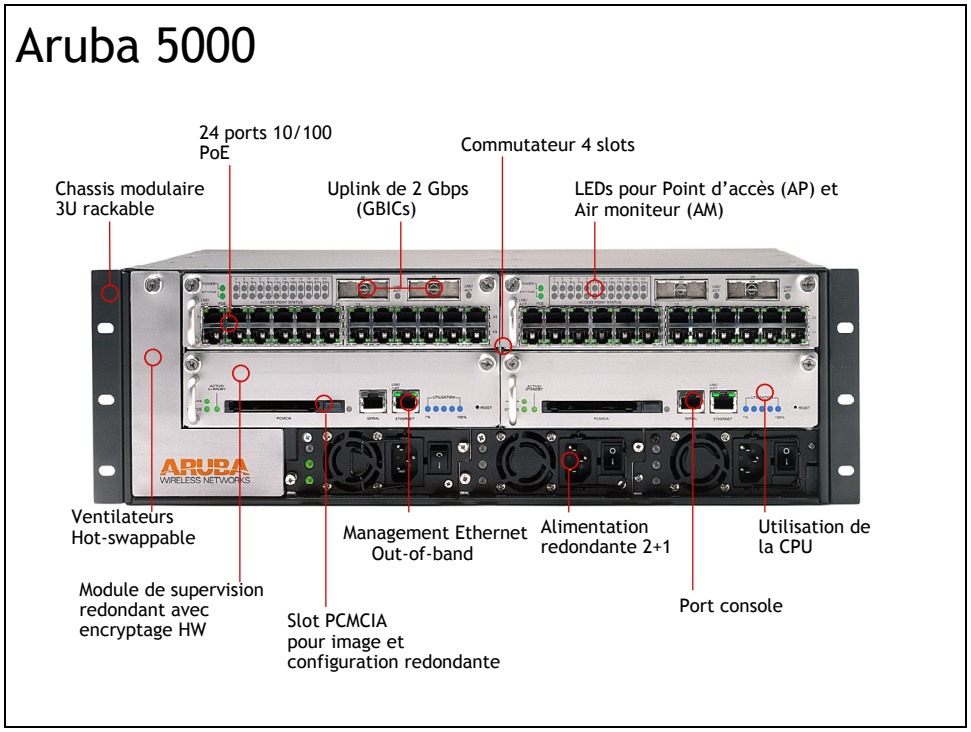
A travers la richesse de l'offre, elle apporte une solution complète et autonome, et évite l'achat éventuel d'équipements complémentaires, tout en offrant une administration centralisée et unifiée de ces différentes briques. La solution intégrée étant indiscutablement plus sûre, plus performante et très significativement moins chère.
Enfin, la gestion des extensions du parc de postes clients d'un réseau sans-fil ne nécessitant aucune intervention physique sur le réseau, une économie d'échelle très significative peut être réalisée de cette manière (pas de modification du câblage, pas de jarretière défectueuse, etc.).

3.6 Résilience

La solution WLAN faisant dorénavant partie intégrante du réseau de l'entreprise, elle doit répondre aux même exigences concernant les niveaux de disponibilité, ou les caractéristiques de redondance.



Les solutions Aruba répondent aisément à ce cadre avec une approche duale : d'une part des équipements centraux entièrement redondants, et d'autre part une architecture de déploiement qui sécurise chaque élément.
Le commutateur Aruba 5000 possède une structure qui offre la redondance des modules de connectique, des alimentations (2+1), des ventilateurs, des ports up-link (GigaEthernet), et du module CPU : Traitement, sécurité et supervision (administration, authentification, cryptage, statistiques). Les modules de connectiques 10/100 et de supervision (CPU) sont aussi hot-swappables, permettant des interventions de maintenance en minimisant l'impact opérationnel.



Châssis Aruba 5000 , 2 modules CPU (actif+redondant) & 2 modules de 24 ports 10/100 Mb/s (48 ports physiques, mais gère jusqu'à 128 AP)

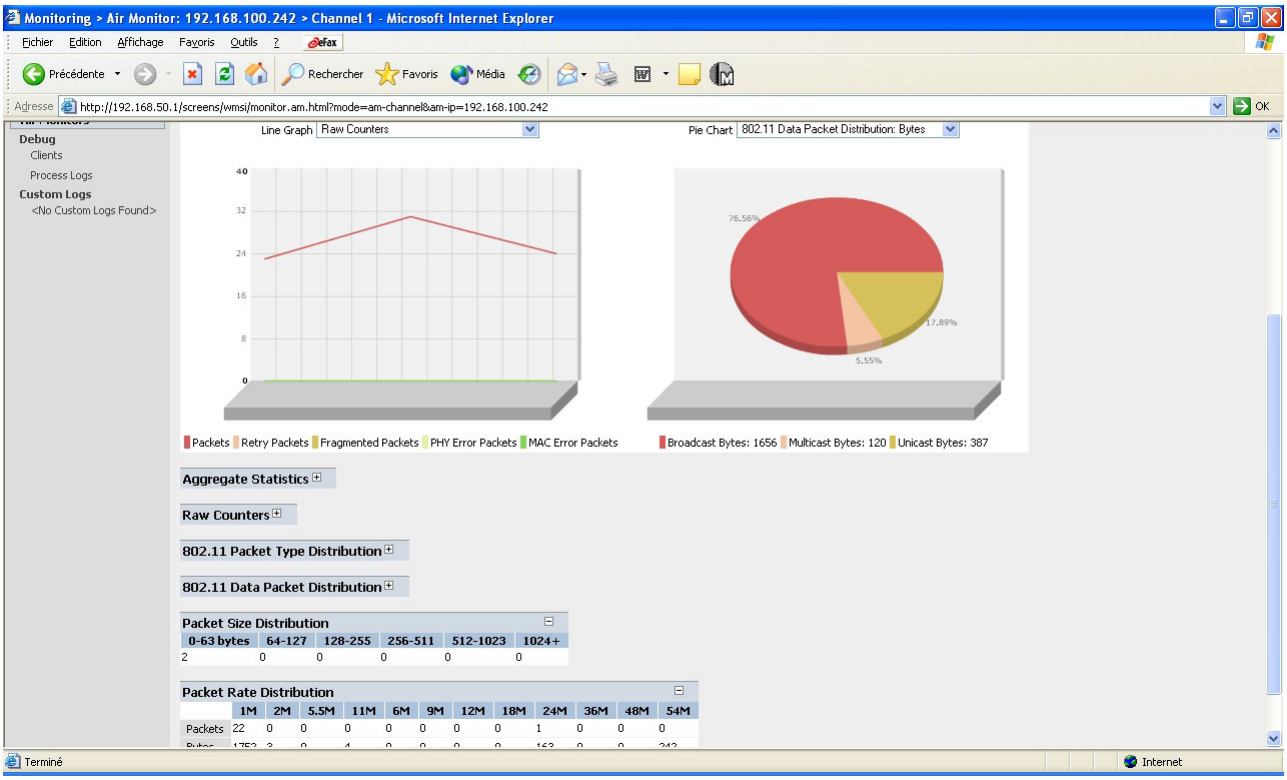
Par ailleurs le déploiement de 2 switch WLAN centraux en redondance actif/passif permet d'ajouter encore un niveau supérieur de garantie de disponibilité, parfaitement compatible avec les exigences élevées des administrateurs réseau, et totalement transparent grâce au protocole VRRP.

Enfin, en ce qui concerne les AP, deux mécanismes peuvent être employés.
D'une part la phase de calibrage paramètre les AP de manière a ce qu'ils ne fonctionnent pas à pleine puissance en situation normale (toujours selon le niveau autorisé par la régulation, 100 mW typiquement), laissant une marge qui servira à augmenter la taille de la cellule si un des AP voisins venait à tomber en panne. Le Switch pouvant commander automatiquement d'augmenter la puissance du signal pour couvrir le trou laissé par l'équipement défaillant.
D'autre par le déploiement d'AM (par exemple avec un ratio de 1 AM pour 5 AP) permet aussi de subvenir immédiatement et automatiquement au trou éventuel que pourrait provoquer la défaillance d'une AP, en attendant le remplacement de l'élément en panne.

Le service de connexion Wi-Fi étant par conséquent sécurisé par ces 2 formes de redondance dites aussi self-healing, au niveau des AP.

3.7 Supervision

Les outils centraux de supervision de la solution Aruba (RFDirector) offrent une vue complète et unifiée à l'administrateur réseau.
Celui-ci dispose de statistiques centralisées et riches, au format RMON, des logs de toutes les évènements au niveau Wi-Fi, comme au niveau du Firewall ou de l'IDS.



Statistiques RMON

La fonction de port mirroring est reproduite au niveau de chaque AP, puisque l'on peut, sans impacter le fonctionnement, configurer la recopie du trafic d'un AP, ou d'un poste client en

particulier, et le rediriger vers un ordinateur équipé d'un logiciel de décodage AiroPeek ou Ethereal par exemple.
L'administrateur bénéficie de plus d'un outil de localisation qui permet de situer tout équipement WLAN sur la topologie des cellules, ce qui est indispensable pour pouvoir trouver efficacement l'équipement physique dans les locaux en un temps limité.
Enfin, le commutateur propose des logs extrêmement complets de l'activité, permettant à l'administrateur de retracer l'historique des évènements, leur enchaînement, et/ou les modifications ayant eu lieu.

4 Conclusion

Nous avons vu dans ce document comment les technologies s'étaient enrichies au cours du temps pour répondre au besoin de plus en plus important de la connexion data nomade, au bureau, dans la rue ou chez soi.
Et nous avons identifié aussi les réponses des solutions modernes qui adressent tous les aspects critiques de l'administrateur réseau, qu'il s'agisse des phases d'ingénierie, d'installation, de gestion, de supervision et de maintenance, ou des approches critiques concernant la sécurité, la fiabilité et le niveau de disponibilité.
Enfin, nous avons aussi évoqué comment ces équipements évolués, intelligents sont dores et déjà prêts pour les évolutions prévues à court et long terme, qu'il s'agisse de compléments de sécurité,standards ou de qualité de service pour le support de nouveaux flux et de nouvelles applications.

5 Annexes

5.1 Livres

802.11 Wireless Networks: The Definitive Guide, Creating and Administrering Wireless Networks
Matthew Gast - O'Reilly - ISBN: 0-596-00183-5

Wireless Communications, Principles and Practice (2nd Edition)
Theodore S. Rappaport - Prentice Hall - ISBN: 0-13-042232-0

5.2 Sites web

Aruba : http://www.arubanetworks.com

ART http://www.art-telecom.fr/

WECA : http://www.weca.net/OpenSection/index.asp

WLANA : http://www.wlana.org/index.html

IEEE 802.11 : http://grouper.ieee.org/groups/802/11/

Wi-Fi Planet : http://www.wi-fiplanet.com/

Wi-Fi Networking News : http://wifinetnews.com/

UnStrung : http://www.unstrung.com/

Microsoft Technology Center :
http://www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx

O'Reilly - comparaison technique de TTLS et PEAP
http://www.oreillynet.com/pub/a/wireless/2002/10/17/peap.html

IEC - Tutoriel EAP pour 802.1X
http://www.iec.org/online/tutorials/acrobat/eap_methods.pdf

5.3 Tableau des Suppléments

Work Group, Task Groupe et Study Group de l'IEEE 802.11.
http://grouper.ieee.org/groups/802/11/ puis WG info, puis 802.11 QuickGuide

WG		
MAC/PHY	Common MAC for WLANs applications, 3 PHY's for WLANs applications, using IR, 2.4 GHz FHSS, and 2.4 GHz DSSS	Published as IEEE Std. 802.11-1997 (8802-11: 1999)
TG a	Develop a PHY to operate in the newly allocated UNII band (54 Mb/s in 5 GHz band, with OFDM)	Published as IEEE Std. 802.11a-1999
TG b	Higher rate PHY in the 2.4GHz band (11 Mb/s, with DSSS)	Published as IEEE Std. 802.11b-1999
TG c	Support of the Internal Sub-Layer Service by specific MAC Procedures to cover bridge operation with IEEE 802.11 MAC	Part of the ISO/IEC 10038 (IEEE 802.1D) Standard
TG d	Physical layer requirements (channelization, hopping patterns, new values for current MIB attributes, and other requirements to extend the operation of 802.11 WLANs to new regulatory domains (countries)	Published as IEEE Std. 802.11d 2001
TG e	Enhance MAC to improve and manage QoS, provide CoS, and enhanced security and authentication mechanisms. Consider efficiency enhancements in the areas of the Distributed Coordination Function (DCF) and Point Coordination Function (PCF)	On going
TG f	Develop recommended practices for an Inter-Access Point Protocol (IAPP) which provides the necessary capabilities to achieve multi-vendor Access Point interoperability across a Distribution System supporting IEEE P802.11 Wireless LAN Links. This IAPP will be developed for the following environment(s): 1) A Distribution System consisting of IEEE 802 LAN components supporting an IETF IP environment. 2) Others as deemed appropriate This Recommended Practices Document shall support the IEEE P802.11standard revision(s)	Approved, and part of Std
TG g	Higher speed(s) PHY extension to the 802.11b standard. Compatible with the 802.11 MAC. Max PHY data rate targeted by this project > 20 Mbit/s. New extension shall implement all mandatory portions of 802.11b PHY standard (54 Mb/s in 2.4 GHz, with OFDM).	Approved June 2003
TG h	Enhance MAC standard and 802.11a High Speed PHY in the 5 GHz Band supplement to the standard; to add indoor and outdoor channel selection for 5 GHz license exempt bands in Europe; and to enhance channel energy measurement and reporting mechanisms to improve spectrum and transmit power management (per CEPT and subsequent EU committee or body ruling incorporating CEPT Recommendation ERC 99/23)	On going
TG i	Enhance MAC to enhance security and authentication mechanisms	On going
TG j	Enhance the 802.11 standard and amendments, to add channel selection for 4.9 GHz and 5 GHz in Japan to additionally conform to the Japanese rules for radio operation	On going
TG k	define Radio Resource Measurement enhancements to provide interfaces to higher layers for radio and network measurements	
TG m	Maintenance of the IEEE 802.11-1999 (reaff. 2003) standard	
SG		
5GSG	Investigated the globalization and harmonization of the 5GHz band jointly with ETSI-BRAN, and MMAC	Closed
HT SG	Investigating the possibility of improvements to the 802.11 standard to provide high throughput (380 Mb/s ?)	

5.4 Acronymes

AP	Access Point
BLR	Boucle Locale Radio
BPSK	Binary Phase Shift Keying
BSS	Basic Service Set
CCK	Complementary Code Keying
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
ETSI	European Telecommunications Standard Institute
FHSS	Frequency Hopping Spread Spectrum
IBSS	Independent BSS
IDS	Intrusion Detection System
IEEE	Institute of Electrical & Electronic Engineers
IKE	Internet Key Exchange
LAN	Local Area Network
LEAP	Lightweight EAP
L2TP	Layer 2 Tunneling Protocol
OFDM	Orthogonal Frequency Division Multiplexing
PAN	Personnal Area Network
PEAP	Protected EAP
PIRE	Puissance Isotrope Rayonnée Equivalente
PPTP	Point-to-Point Tunneling Protocol
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial-In User Service
RLAN	Radio LAN
SSID	Service Set Identification
STA	Station
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled TLS
VPN	Virtual Private Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WISP	Wireless ISP
WLAN	Wireless LAN
WLL	Wireless Local Loop
WMAN	Wireless MAN
VoWLAN	Voice over WLAN
WPA	Wi-Fi Protected Access
WPAN	Wireless PAN

ARUBA Wireless Networks
France, Europe du Sud, Afrique:
120, avenue Charles de Gaulle
92522 Neuilly sur Seine Cedex, France
Tél : +33 (0) 1 72 92 05 56
Fax : +33 (0) 1 72 92 05 57
info-emea@arubanetworks.com
www.arubanetworks.com

"People Move. Networks must follow."