Sécurité et architecture des réseaux WiFi

11 mars 2010

Pierre ANSEL – Orange Labs
pierre.ansel AT orange-ftgroup.com

Wireless LAN ?

- **Un Wireless LAN est un système de communication flexible, qui a pour but de fournir une extension de LAN filaire**

- **Les réseaux Wireless LANs utilisent les mécanismes de transmission radio pour transmettre et recevoir des informations à travers l'air**

- **Avantages :**
  - Sans fil, bien sûr !!! Ergonomie d'utilisation !
  - Coût faible par rapport à un câblage
  - Spectre de fréquence non utilisé (micro-ondes…)

- **Un démarrage un peu trop rapide ?**

Plan

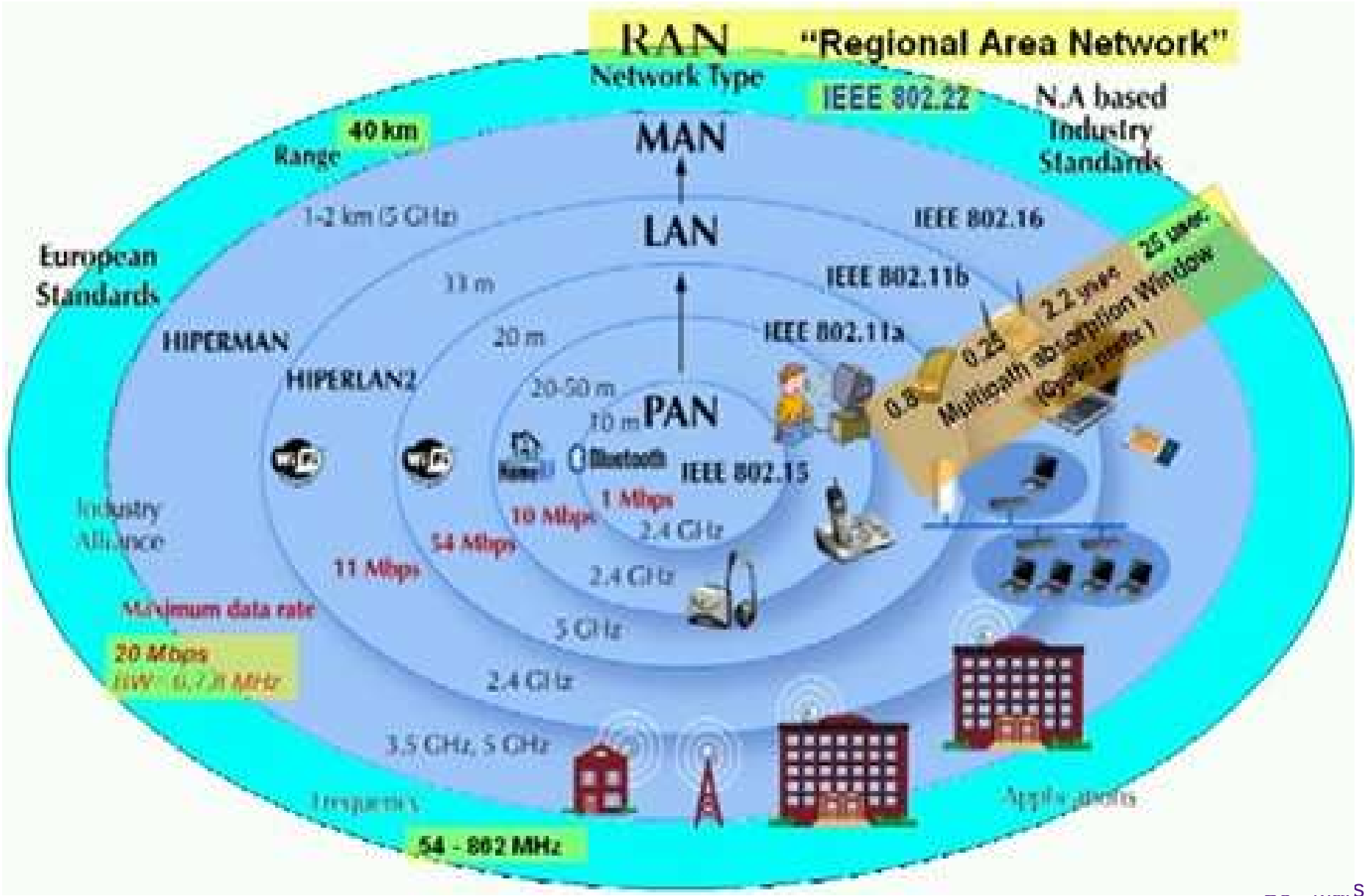
- **Le 802.11 : écosystème et fonctionnement**
  - Positionnement technologique et évolution du marché
  - Les différents acteurs (IEEE, IETF, WiFi-Alliance)
  - Quelques mots sur la législation française
  - La norme 802.11
  - Modes de fonctionnement
- **Les premiers mécanismes de sécurité : failles et attaques**
  - Premiers mécanismes de sécurité
  - Failles conceptuelles dans IEEE 802.11
  - Attaques sur IEEE 802.11
- **Les nouveaux mécanismes de sécurité**
  - Réutilisation de briques de sécurité éprouvées (802.1X, EAP, AES …)
  - Une solution à court-terme, le WPA
  - Recherche de failles d'implémentation dans les drivers WiFi
- **Architecture des réseaux WiFi**
  - Contexte résidentiel
  - Contexte hot spot
  - Contexte entreprise
  - Surveillance des intrusions WiFi

Plan

- **Le 802.11 : écosystème et fonctionnement**
  - Positionnement technologique et évolution du marché
  - Les différents acteurs (IEEE, IETF, WiFi-Alliance)
  - Quelques mots sur la législation française
  - La norme 802.11
  - Modes de fonctionnement
- Les premiers mécanismes de sécurité : failles et attaques
- Les nouveaux mécanismes de sécurité
- Architecture des réseaux WiFi

Plan

- **Le 802.11 : écosystème et fonctionnement**
  - Positionnement technologique et évolution du marché
  - Les différents acteurs (IEEE, IETF, WiFi-Alliance)
  - Quelques mots sur la législation française
  - La norme 802.11
  - Modes de fonctionnement
- **Les premiers mécanismes de sécurité : failles et attaques**
- **Les nouveaux mécanismes de sécurité**
- **Architecture des réseaux WiFi**


RAN
"Regional Area Network"
Network Type
IEEE 802.22
N.A based
Industry
Standards
40 km
Range
MAN
1-2 km (5 GHz)
LAN
IEEE 802.16
European
Standards
11 m
IEEE 802.11b
20 m
IEEE 802.11a
HIPERMAN
HIPERLAN2
20-50 m
10 m
PAN
Bluetooth
IEEE 802.15
1 Mbps
10 Mbps
2.4 GHz
54 Mbps
11 Mbps
2.4 GHz
5 GHz
2.4 GHz
3.5 GHz, 5 GHz
54 - 862 MHz

Évolutions du Wireless LAN ? (1/3)

- **Engouement depuis 2002/2003**
- **Forte progression aux États-Unis; l'Europe a suivi ensuite…**

hotspots Wi-Fi en Europe (sources IDC-Gartner, février 2003)

Wi-Fi : évolution du parc de hotspots			
Période	**Nombre de hotspots**	**Dont Amérique du Nord**	**Dont Europe**
2001	269	--	--
2002	6 000	3 420	840
2003	20 000	10 000	5 000

Le marché mondial du Wi-Fi (Sources Wi-Fi Alliance, In-Stat/MDR - 2002)

Evolution du marché mondial Wi-Fi		
Période	Marché (en milliards de dollars)	**Parc** (en millions d'unités)
2001	1,0	--
2002	2,0	6
2005	6,0	33

Le nombre de "hot spots" publics par pays (Source HotSpots.com - octobre 2002)

Classement des pays selon le nombre de "hot spots" Wi-Fi publics	
Pays	**Nombre de hot spots**
Etats-Unis	1 800
Autriche	110
Royaume-Uni	90
Allemagne	65
Australie	43
Canada	28

Évolutions du Wireless LAN ? (2/3)

- http://www.jiwire.com/search-hotspot-locations.htm
- **Avril 2005**

Top 10 Countries		Top 10 Cities		Top 10 Location Types	
United States	25,384	London	1,219	Hotel/Resort	17,534
United Kingdom	9,858	Tokyo	1,015	Restaurant	10,850
Germany	5,880	New York	863	Cafe	9,910
France	3,352	Paris	795	Store / Shopping Mall	6,991
Japan	2,484	Singapore	613	Pub	5,084
Switzerland	1,331	Hong Kong	475	Other	2,553
Italy	1,275	Sao Paulo	463	Gas station	1,099
Canada	1,073	Chicago	418	Airport	990
Spain	1,007	Berlin	415	Bar	778
Australia	914	San Francisco	368	Library	708

- **Septembre 2006**

Top 10 Countries		Top 10 Cities		Top 10 Location Types	
United States	40,866	Seoul	2,056	Hotel / Resort	31,839
United Kingdom	14,900	London	1,913	Restaurant	25,441
Germany	12,424	Tokyo	1,844	Cafe	15,808
South Korea	9,415	Taipei	1,786	Store / Shopping Mall	14,835
Japan	6,259	Paris	1,203	Other	7,844
France	5,326	Berlin	818	Pub	5,348
Taiwan	2,899	San Francisco	805	Office Building	2,383
Italy	2,547	Daegu	787	Gas Station	1,735
Netherlands	2,515	Singapore	671	Airport	1,581
Australia	2,337	New York	669	Library	1,400
more ▸		more ▸		more ▸	

Évolutions du Wireless LAN ? (3/3)

More than 120 Million Wi-Fi® Chipsets Shipped in 2005

Wi-Fi is expanding into consumer electronics and phones, building on success in the PC market

Austin, TX, November 28, 2005 – Wi-Fi technology has seen its annual unit sales grow to more than 100 million chipsets in six years, according to new data released by In-Stat and the Wi-Fi Alliance, and it's now a staple of computer networking and a powerful presence in millions of homes and businesses. The 100 million chipset milestone was quickly passed and the explosive 64% average yearly growth rate reflects the transforming nature of Wi-Fi and the value of interoperable, standards-based technology.

Worldwide Wi-Fi Hotspots Hits the 100,000 Mark

Industry milestone reinforces the rapid adoption of public wireless access.

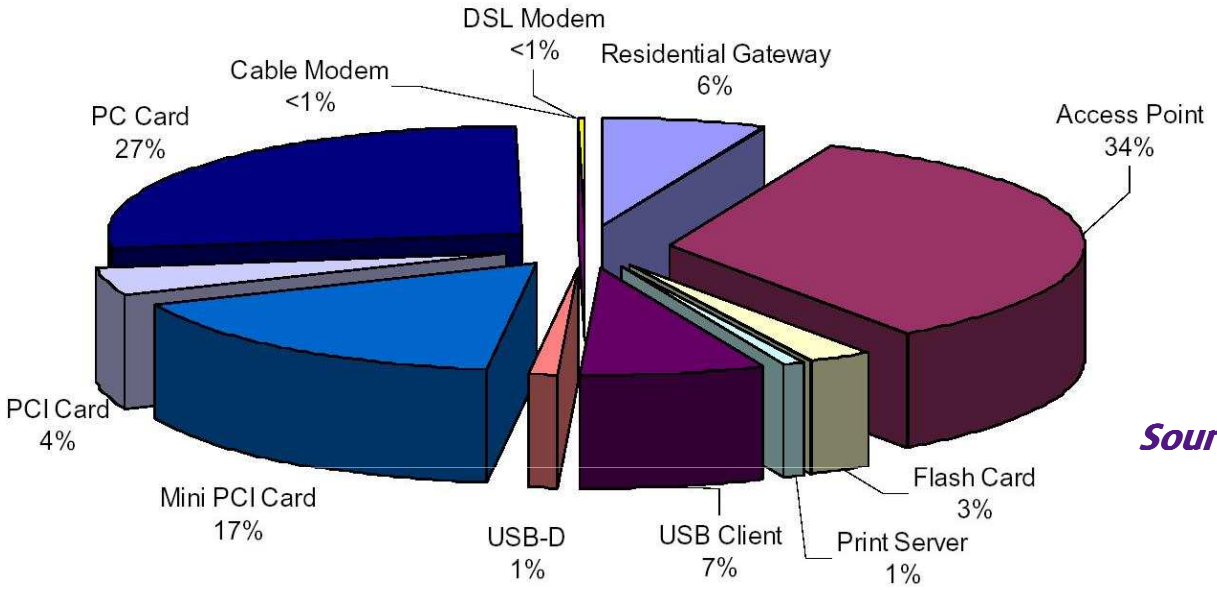
Seoul, Tokyo and London top JiWire's international Wi-Fi Cities list. San Francisco, New York and Chicago top JiWire's domestic Wi-Fi Cities list.

San Francisco, Calif. – January 24, 2006 -The number of worldwide Wi-Fi hotspots has surpassed the 100,000 milestone according to recent numbers released by JiWire, the leading provider of Wi-Fi hotspot information and services (www.jiwire.com). A hotspot is a physical address where people can connect to a public wireless network, such as a cafe, hotel or airport.

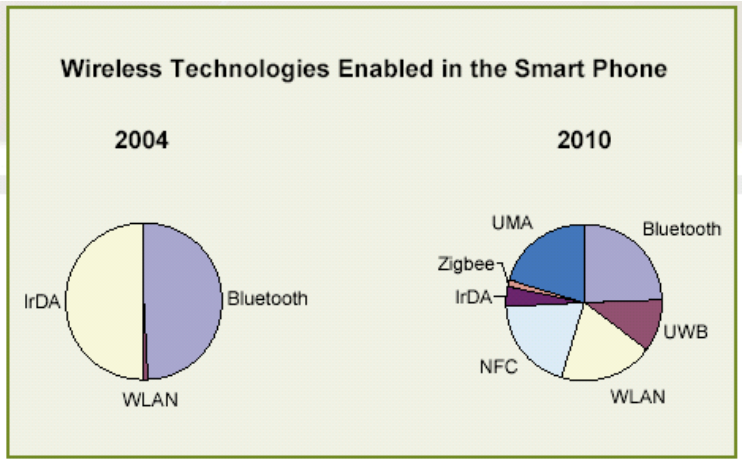
Key growth milestones from January 2005 to January 2006:

- The number of worldwide hotspots grew 87%, from 53,779 in 93 countries to 100,355 hotspots in 115 countries.
- The top three Wi-Fi cities in January 2005 were London, New York and Paris, whereas in 2006 the top three cities are Seoul, Tokyo and London.
- The top three Wi-Fi countries in January 2005 were the United States, the United Kingdom and Germany, whereas in January 2006 the top three countries are the United States, the United Kingdom and South Korea.

Diversité du matériel Wi-Fi



Source : Wi-Fi Alliance



Source : IMS

Plan

- **Le 802.11 : écosystème et fonctionnement**
  - Positionnement technologique et évolution du marché
  - Les différents acteurs (IEEE, IETF, WiFi-Alliance)
  - Quelques mots sur la législation française
  - La norme 802.11
  - Modes de fonctionnement
- **Les premiers mécanismes de sécurité : failles et attaques**
- **Les nouveaux mécanismes de sécurité**
- **Architecture des réseaux WiFi**

Institute of Electrical and Electronics Engineers

- **Association à but non lucratif, 370000 membres répartis dans 150 pays**

- **IEEE 802 LAN/MAN Standards Committee**
  - Développe des standards pour les réseaux locaux et métropolitains (LAN/MAN)
  - Ex : Ethernet, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs
  - En particulier sur les 2 premiers niveaux du modèle de référence de l'OSI

- **Quelques groupes de IEEE 802**
  - 802.11 Wireless LAN (WLAN) Working Group
  - 802.15 Wireless Personal Area Network (WPAN) Working Group
  - 802.16 Broadband Wireless Access (BBWA) Working Group
  - 802.20 Mobile Wireless Access Working Group
  - 802.21 Media Independent Handover Services

Groupes de l'IEEE 802 (1/2)

802.15 : Working Group for Wireless Personal Area Networks

- Spécifier des standards possédant les propriétés suivantes :
  - Faible complexité – donc faible coût
  - Faible consommation – donc durée d'utilisation importante

- 802.15.1 - 1Mb/s WPAN/Bluetooth v1.x derivative work

- 802.15.3 - 20+ Mb/s High Rate WPAN for Multimedia and Digital Imaging (aka UWB)

- 802.15.3a - 110+ Mb/s Higher Rate Alternative PHY for 802.15.3

- 802.15.4 - 200 kb/s max for interactive toys, sensor and automation needs

Groupes de l'IEEE 802 (2/2)

- **802.16 : Working Group on Broadband Wireless Access Standards**
  - Pour la boucle locale ("first-mile/last-mile") dans les réseaux métropolitains
  - 802.16-2004 : 134 Mb/s, pas de mobilité
  - 802.16d : 75 Mb/s, pas de mobilité
  - 802.16e : 15 Mb/s, ajout de mobilité à des vitesses "véhiculaires"
- **802.20 : Mobile Broadband Wireless Access (MBWA) Working Group**
  - Bandes de fréquences en dessous de 3.5 GHz
  - Vitesses de 250 km/h

IEEE 802.11

- **802.11 Working Group for Wireless Local Area Networks**
- **But : Spécifier une interface « sans-fil » entre un client et un point d'accès ou un autre client**
- **Les spécifications IEEE 802.11 précisent les aspects :**
  - Physical (PHY)
  - Medium Access Control (MAC)
- **Similaire au standard IEEE 802.3 (Ethernet pour les réseaux filaires)**

IEEE 802.11

- **IEEE 802.11 est la norme de réseaux radio locaux sans-fil la plus utilisée**
  - 802.11-1997 : ratification
  - 802.11-1999 : corrections apportées à la norme ratifiée en 1997
- **IEEE 802.11a – High Speed Physical Layer in the 5 GHz band**
  - Bande de fréquence 5 GHz – 54 Mbps
  - Ratifiée en 1999
- **IEEE 802.11b – Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band**
  - Bande de fréquence 2,4 GHz – 14 canaux (2,421 à 2,484 GHz) – 11 Mbps
  - Ratifiée en 1999, révision en 2001
- **IEEE 802.11g – Standard for Higher Rate**
  - Bande de fréquence 2.4GHz (jusqu'à 54 Mbps)

Travaux en cours à IEEE 802.11

- 802.11e : Medium Access Control (MAC) Quality of Service Enhancements
- 802.11k : Radio Ressource Measurement of Wireless LANs
- 802.11n : High Throughput
- 802.11p : Wireless Access for the Vehicular Environment
- 802.11r : Fast Roaming
- 802.11s : ESS Mesh Networking
- 802.11t : Wireless Performance
- 802.11u : Interworking with External Networks
- 802.11v : Wireless Network Management
- 802.11w : Protected Management Frames
- État des normes : http://standards.ieee.org/cgi-bin/status?wireless

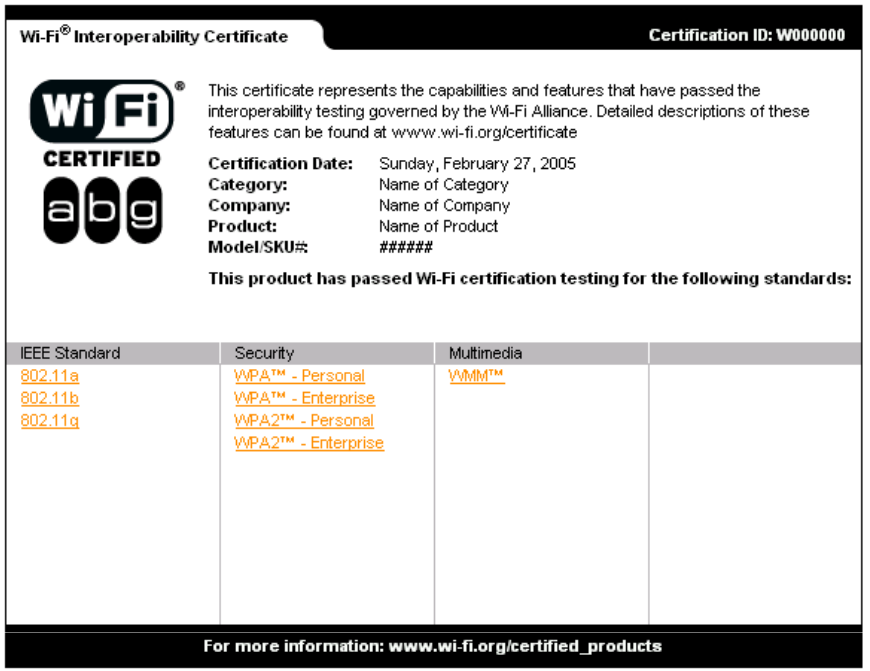
Wi-Fi Alliance

- **Wi-Fi Alliance – Wireless Fidelity Alliance (anciennement WECA – Wireless Ethernet Compatibility Alliance)**

- **Association internationale à but non lucratif crée en 1999, qui a pour but de certifier l'interopérabilité des produits basés sur la spécification IEEE 802.11. Composée de 182 constructeurs, 698 produits ont reçu la certification Wi-Fi depuis son démarrage en mars 2002.**

- **MISSION**
  The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability

Certification Wi-Fi



Wi-Fi – Wireless Fidelity

Wi Fi CERTIFIED a b g

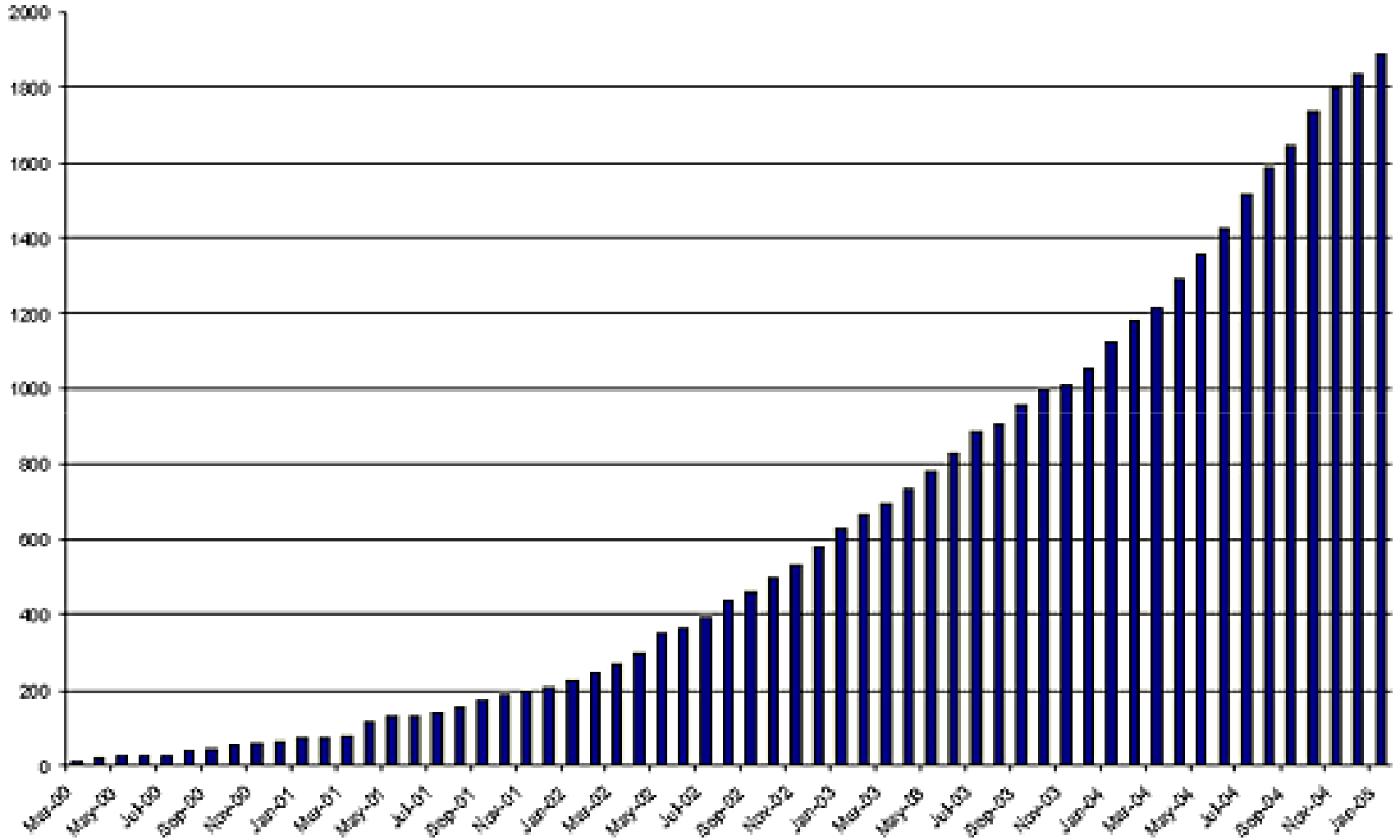
Wi Fi CERTIFIED a b g

But : assurer l'interopérabilité des produits

Permet de limiter :

- Fonctionnalités propriétaires dans les produits des constructeurs
- Mauvaise interprétation de la norme
- Erreurs d'implémentations de la norme dans les produits
- Tests de validation en laboratoire

Historique certification Wi-Fi



Wi-Fi Product Certifications Since March 2000

Source : Wi-Fi Alliance

Plan

- **Le 802.11 : écosystème et fonctionnement**
  - Positionnement technologique et évolution du marché
  - Les différents acteurs (IEEE, IETF, WiFi-Alliance)
  - Quelques mots sur la législation française
  - La norme 802.11
  - Modes de fonctionnement
- **Les premiers mécanismes de sécurité : failles et attaques**
- **Les nouveaux mécanismes de sécurité**
- **Architecture des réseaux WiFi**

Législation française (1/4)

- **Régie par l'ARCEP** L'AUTORITÉ de RÉGULATION des COMMUNICATIONS ÉLECTRONIQUES et des POSTES — RÉPUBLIQUE FRANÇAISE

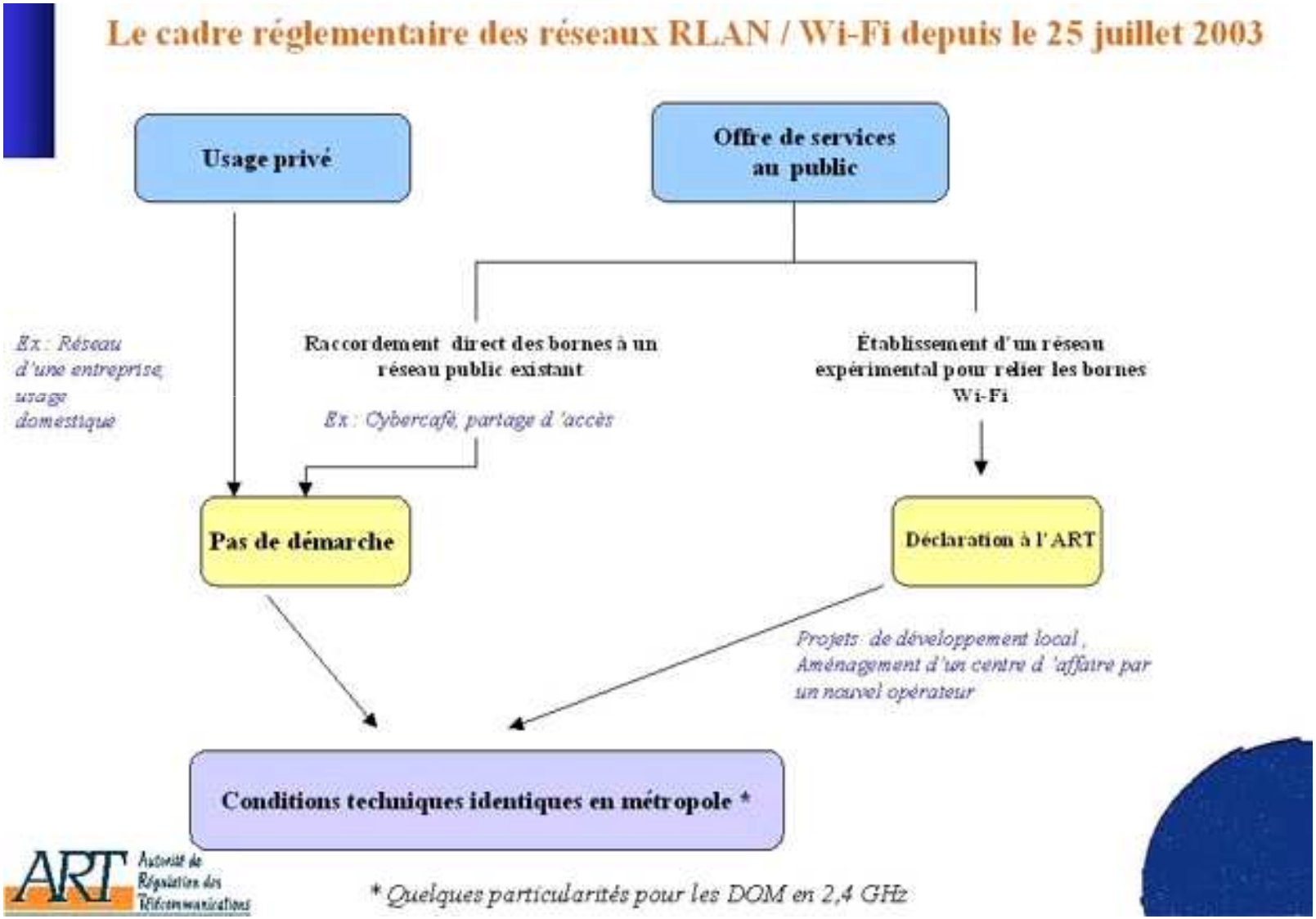
- **Le 7 novembre 2002, l'Autorité adopte les textes permettant l'utilisation des réseaux locaux radioélectriques (RLAN)**
  - http://www.art-telecom.fr/communiques/communiques/2002/index-07-11-2002.htm

- **Evolution du régime d'autorisation pour les RLAN à compter du 25 juillet 2003**
  - http://www.art-telecom.fr/publications/lignedir/ld-rlan250703.htm

- **Les décisions permettant l'installation de bornes d'accès sans fil dans les lieux de passage du public (" *hotspots* " : gares, aéroports, centres d'affaires, …)**
  - Ainsi les fournisseurs de services et les opérateurs autorisés vont pouvoir installer **sans autorisation** des bornes d'accès utilisant les technologies de la bande 2,4 GHz, dans le respect de certaines conditions

Source : ART

Législation française (2/4)



Législation française (3/4)

Conditions d'utilisation des RLAN dans les *hotspots* :

- La bande 2400-2454 MHz est utilisable à l'intérieur comme à l'extérieur des bâtiments avec une puissance inférieure à 100 milliwatts (mW)
- La bande 2454-2483,5 MHz est utilisable à l'intérieur des bâtiments avec une puissance inférieure à 100 mW et à l'extérieur des bâtiments avec une puissance inférieure à 10 mW. Sur les propriétés privées, cette puissance peut atteindre 100 mW à l'extérieur avec une autorisation du ministère de la Défense

	Intérieur	Extérieur
2400 – 2454	100 mW	100 mW
2454 – 2483,5		10 mW

Source : ART

Législation française (4/4)

- **Tableau récapitulatif sur les puissances autorisées pour les réseaux locaux radioélectriques dans la bande 5 GHz**

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*

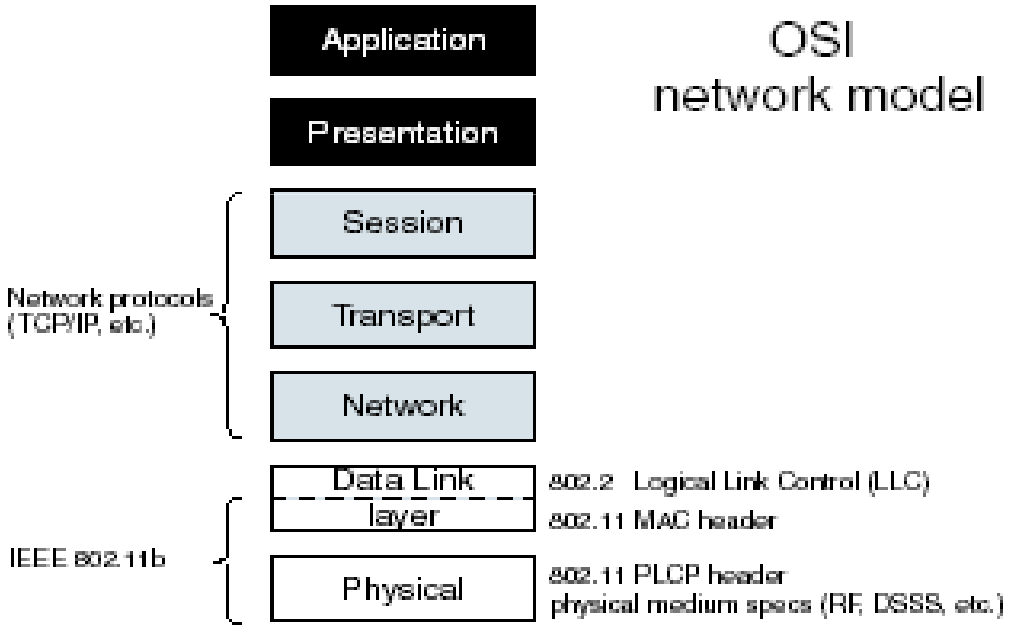
- **Assouplissement à prévoir dans peu de temps…**

Source : ART

Plan

- Le 802.11 : écosystème et fonctionnement
  - Positionnement technologique et évolution du marché
  - Les différents acteurs (IEEE, IETF, WiFi-Alliance)
  - Quelques mots sur la législation française
  - La norme 802.11
  - Modes de fonctionnement
- Les premiers mécanismes de sécurité : failles et attaques
- Les nouveaux mécanismes de sécurité
- Architecture des réseaux WiFi

Couches de l'OSI – IEEE 802.11



Mode infrastructure

- **BSS : Basic Service Set**
- **ESS : Extended Service Set, ensemble de deux (ou plus) BSS**
- **Minimum un AP connecté au réseau filaire, auquel les clients se connectent**

Mode ad-hoc

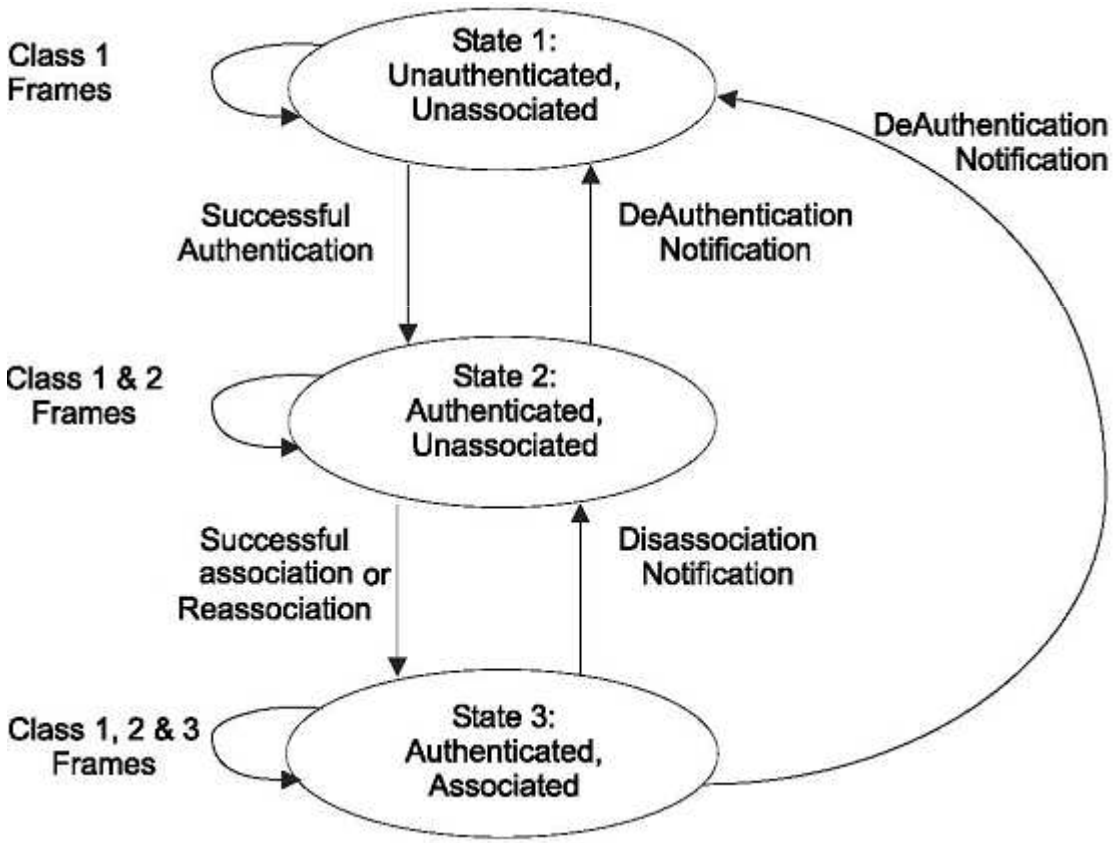
- **IBSS : Independent Basic Service Set**
- **Ensemble de deux (ou plus) stations communiquant entre elles sans infrastructure**

Plan

- Le 802.11 : écosystème et fonctionnement
  - Positionnement technologique et évolution du marché
  - Les différents acteurs (IEEE, IETF, WiFi-Alliance)
  - Quelques mots sur la législation française
  - La norme 802.11
  - Modes de fonctionnement
- Les premiers mécanismes de sécurité : failles et attaques
- Les nouveaux mécanismes de sécurité
- Architecture des réseaux WiFi

Machine à état IEEE 802.11

- **Trois phases :**
  - Découverte
  - Authentification
  - Association



Source : IEEE

Processus de découverte réseaux Wi-Fi

- **La station doit découvrir les APs dans sa zone géographique avec lesquels elle peut s'associer**
  - Réalisé par la fonction « scan » de la couche MAC
    - Écoute des messages de Beacon (envoyés par les APs périodiquement) : possibilité de créer une liste ordonnée d'APs en fonction de la puissance du signal reçue
- **Deux types de « scan » sont définis dans le standard**
  - Actif : la station envoie des requêtes Probe Request sur tous les canaux afin de découvrir les APs sur un nom de réseau spécifique (SSID) de 32 octets
  - Passif
- **Dégradation du signal, et du rapport signal à bruit entre une station et un AP**
  - Perte de connectivité, et initiation d'un « handoff »

Plan

- Le 802.11 : écosystème et fonctionnement
- **Les premiers mécanismes de sécurité : failles et attaques**
  - Premiers mécanismes de sécurité
  - Failles conceptuelles dans IEEE 802.11
  - Attaques sur IEEE 802.11
- Les nouveaux mécanismes de sécurité
- Architecture des réseaux WiFi

Mécanismes de sécurité originels dans 802.11

- **Autorisation**
  - Medium Access Control (MAC)
- **Authentification**
  - Shared Key : Secret partagé
  - Open System : Ouvert
- **Confidentialité / Intégrité**
  - Wired Equivalent Privacy (WEP)

MAC Access Control List

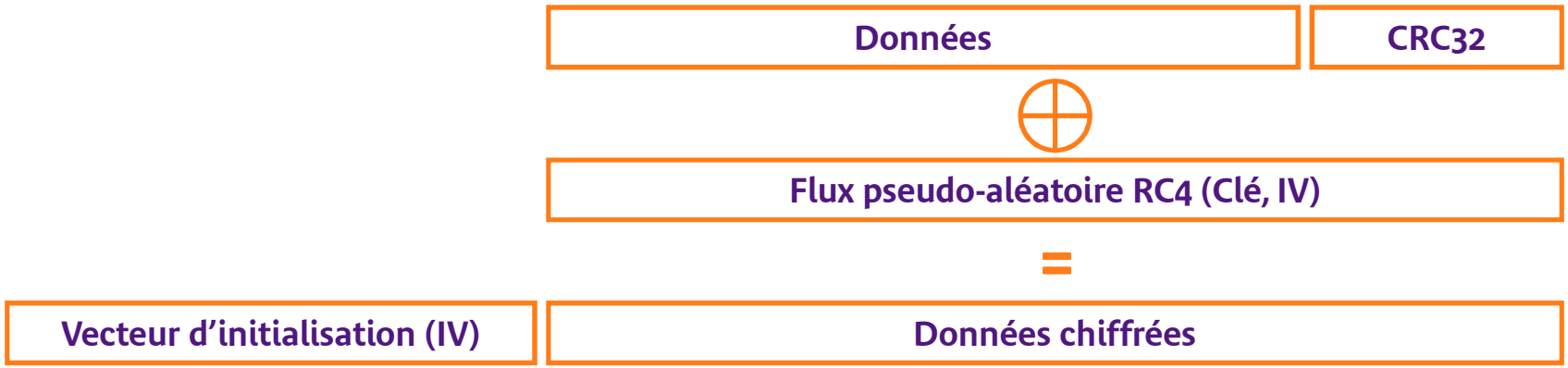
- **La configuration d'une liste blanche d'adresses MAC sur le point d'accès permet un contrôle d'accès**
- **Permet d'éviter les erreurs de configuration**
- **Ne peut pas être considéré comme un mécanisme de contrôle d'accès**
  - Basé sur un élément public !
    - « ifconfig wlan0 hw ether xx:xx:xx:xx:xx:xx »
  - C'est un identifiant, pas un authentifiant !
- **Certains constructeurs offrent la possibilité d'avoir une base centrale hébergeant la liste blanche d'adresses MAC**
  - Répartition centralisée grâce à un serveur AAA (Authentication, Authorization, Accounting) tel que RADIUS (Remote Access Dial-In User Service)

WEP : Wired Equivalent Privacy

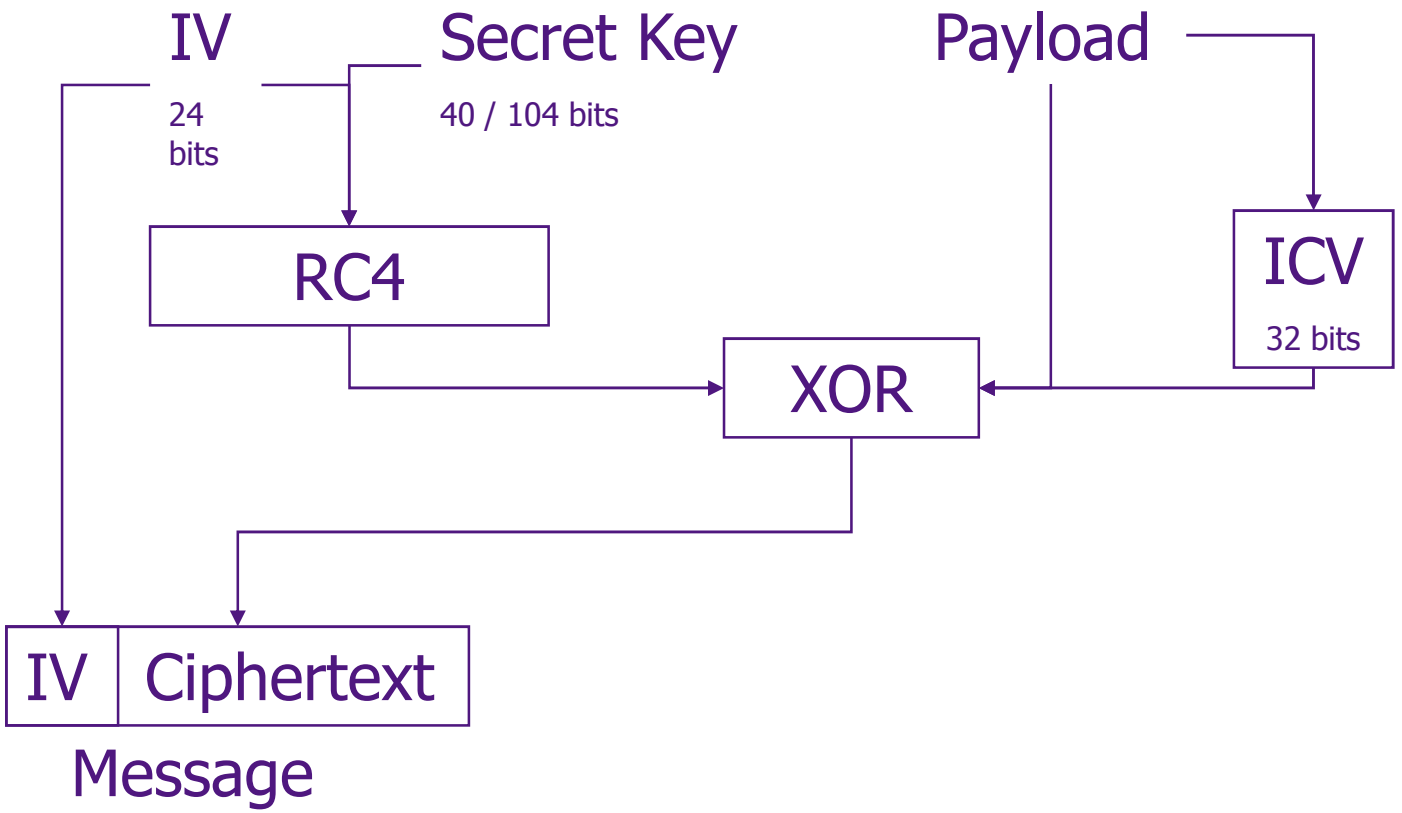
- **But : Atteindre la sécurité des réseaux filaires…**
- **Utilise l'algorithme RC4 pour la confidentialité**
  - Clé = secret partagé (40 ou 104 bits) suivi du vecteur d'initialisation (24 bits) : chiffrement 64 bits ou 128 bits.
  - Clé : {K,IV}
  - 2^{24} IV différents

Trame WEP

- **Trame constituée de l'IV en clair et du chiffrement des données et du CRC32 (ICV)**
  - **CRC32 indépendant de la clé**
- **Chiffrement avec une clé différente par paquet car IV différent à chaque paquet**



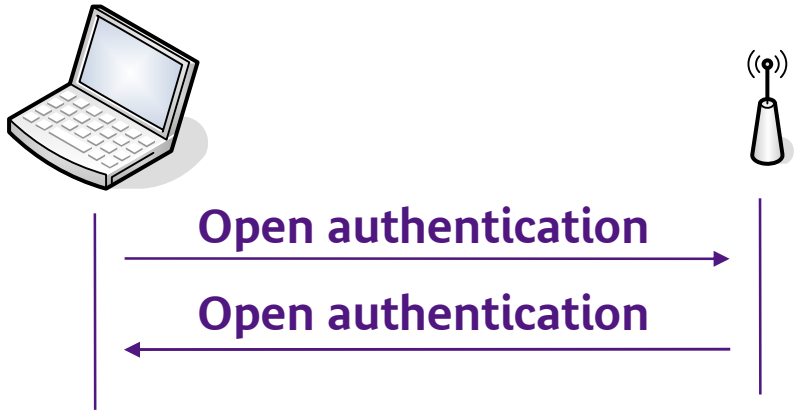
Chiffrement WEP



Authentification

Authentification ouverte

- Par connaissance du SSID



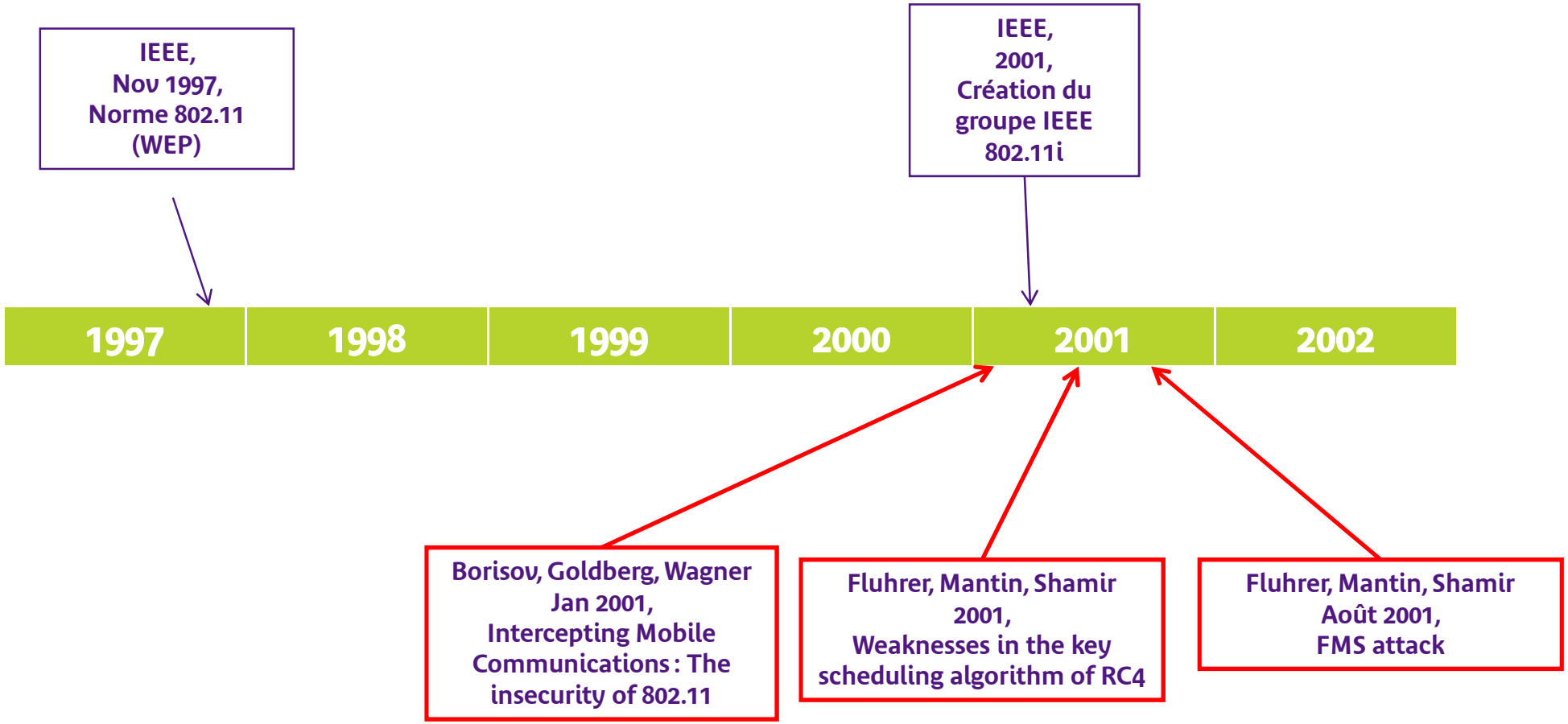
Par clé partagée (défi-réponse)

- Demande d'authentification sur l'AP
- L'AP envoie un aléa a de 128 bits
- Le client retourne [IV, $c_k(a)$, crc32(IV, $c_k(a)$)]
- L'AP vérifie $c_k(a)$, la somme de contrôle et valide ou non l'authentification

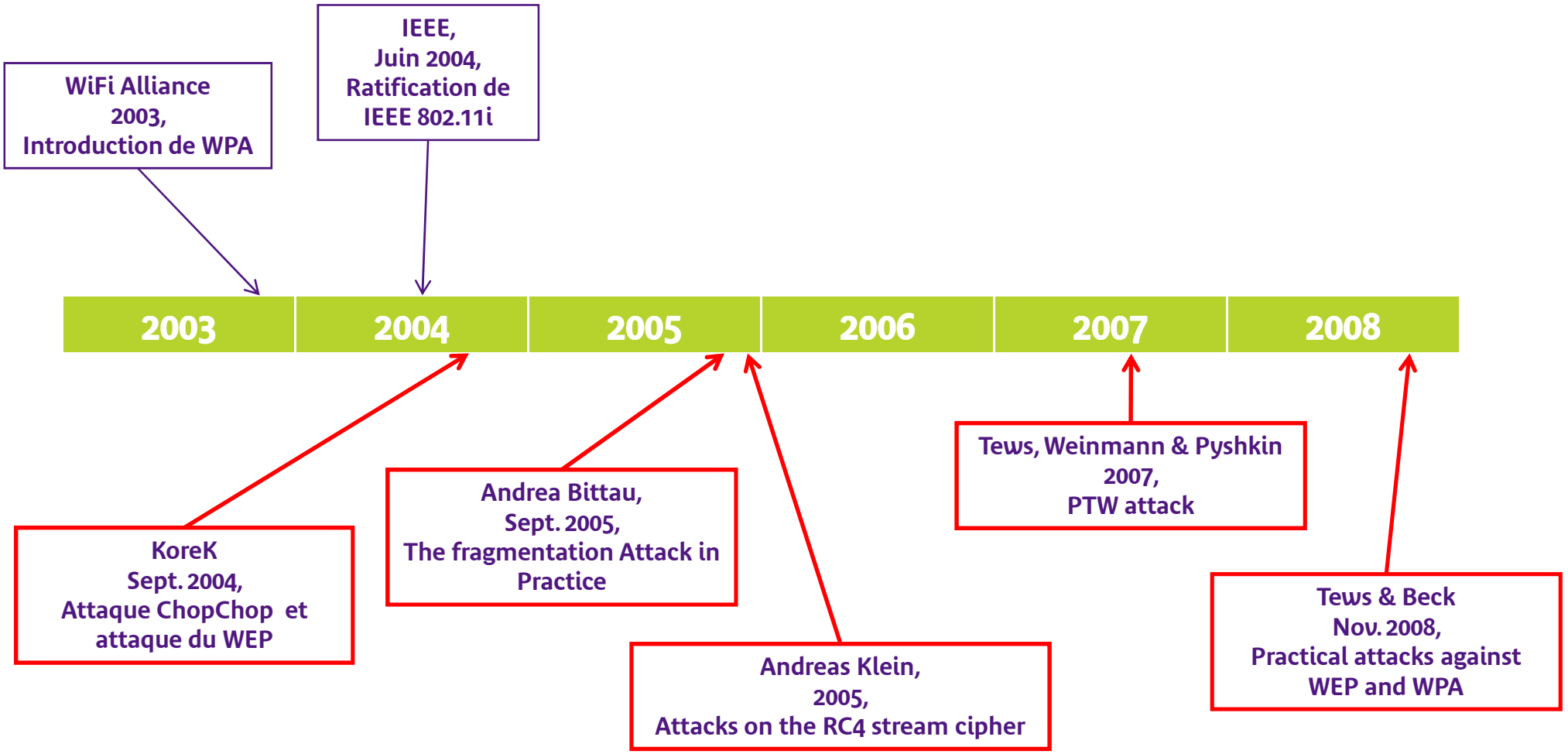
Plan

- Le 802.11 : écosystème et fonctionnement
- **Les premiers mécanismes de sécurité : failles et attaques**
  - Premiers mécanismes de sécurité
  - Failles conceptuelles dans IEEE 802.11
  - Attaques sur IEEE 802.11
- Les nouveaux mécanismes de sécurité
- Architecture des réseaux WiFi

Historique des publications



Historique des publications



Faille conceptuelle : collision des IVs

- **Un IV est codé sur 24 bits**
- **Si tirage aléatoire dans 2^{24}, alors on a 50% de chance d'avoir une collision sur 4823 paquets**
  - Paradoxe des anniversaires

$$p_k = \left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right)\dots\left(1 - \frac{k-1}{365}\right)$$

- **Permet une attaque statistique sur les chiffrés avec un même IV**
  - P : Plaintext; C : Ciphertext; B = Key stream
  - C1 = P1 XOR B
  - C2 = P2 XOR B
  - Donc C1 XOR C2 = P1 XOR P2
- **En pratique, ne constitue pas une attaque (extrèmement) critique**

Faille concepturelle : intégrité faible

- **Le contrôle d'intégrité est basé sur un CRC32**
- **Possibilité de**
  - Modifier un bit du payload data en ayant un impact que sur un seul bit du CRC32
  - modifier plusieurs bits du payload data sans changer la valeur du CRC32
- **Attaques réalisables**
  - Modification de paquet avec le même contrôle d'intégrité
  - Injection de paquets
  - Récupération du plaintext (attaque ChopChop)

Faille conceptuelle : pas d'anti-rejeu

- **Aucune protection contre le rejeu**
  - Les IVs sont aléatoires, pas de test possible sur leur valeur
- **Permet de faire facilement de l'injection de paquet !**
- **Extrêmement critique !**
  - Beaucoup d'attaques exploitent cette faille

Faille conceptuelle : partage du secret

- **Partage d'un secret entre n entités : ce n'est plus un secret !**
  - Toutes les stations
  - Tous les APs
- **Pas de mécanisme de distribution du secret**
  - Configuration « à la main » dans les stations et APs
- **Secret de longueur 40 bits ou 104 bits**
  - Souvent dérivé d'un mot de passe
  - Il peut être trivial à deviner : l'entropie n'est pas forcement élevée
    - Mot de 5 caractères ou 13 caractères
    - Fait partie d'un dictionnaire
    - Force brute réalisable sur 40 bits

Faille conceptuelle : authentification

Processus :

- Envoi du challenge
- Calcul du Encrypted Challenge = {Challenge} XOR {RC4 Key Stream}
- Vérification avec : {Challenge} XOR {RC4 Key Stream}

L'attaquant connaît donc :

- Le challenge
- La réponse au challenge : challenge chiffré
- Il peut en déduire le {RC4 Key Stream}
  - L'attaquant peut donc s'authentifier
    - *Mieux vaut ne pas utiliser l'authentification !*
  - L'attaquant ne peut toutefois pas déchiffrer les paquets reçus
    - *Il ne connaît pas le secret partagé*
  - Mais il peut injecter des paquets chiffrés valides

Faille conceptuelle : clés RC4 faibles

- **Cryptanalyse proposée par Fluhrer, Mantin, Shamir**
- **Existence de clés faibles pour certains IV**
  - Ils entraînent une corrélation entre le premier octet du flot en sortie de RC4 et un octet du secret partagé
  - 9000 IV sur 2^{24} faibles
- **Premier octet de la trame 802.11 à envoyer connu (en-tête LLC/SNAP) !**
  - Chiffré = Clair XOR KeyStream
  - On en déduit donc le premier octet du keystream et donc des bits de clé !
- **FMS recommandent un changement du secret partagé toutes les 15 minutes !**

Améliorations de l'attaque FMS

- **Des optimisations ont été successivement publiées en 2002 (h1kari), 2004 (Korek) et 2007 (Université de Darmstadt)**
- **Réduisent considérablement le nombre de paquets requis pour casser WEP à 128 bits**
  - Avec FMS : 4 millions de paquets
  - FMS Optimisé : 1 à 2 millions de paquets
  - 2004 : 500k paquets, voire moins, suivant l'AP (200k pour une WEP à 64bits…)
  - 2007 (PTW) : 50k (50% de chances) à 90k paquets (85% de chances)
    - "Breaking 104 bit WEP in less than 60 seconds"
- **Attaque statistique → les résultats peuvent (beaucoup) varier…**

Résumé des failles conceptuelles

- **Partage du secret entre n entités !**
  - Authentification de groupe
  - Pas de mécanisme de distribution de secret de manière dynamique
    - Distribution des clés « à la main »
- **Vérificateur d'intégrité faible**
- **Pas d'anti-rejeu → injection de trames**
- **Faiblesses de certaines clés RC4 qui compromettent le secret partagé**

Outils d'attaques

- **WEPCrack – sourceforge.net/projects/wepcrack**
- **Airsnort – www.shmoo.org**
- **BSD-Airtools – www.dachb0den.com/projects/bsdairtools.html**
- **Aircrack – www.cr0.net:8040/code/network/ (Google)**
- **Aircrack-ng – www.aircrack-ng.org**

Plan

- Le 802.11 : écosystème et fonctionnement
- Les premiers mécanismes de sécurité : failles et attaques
  - Premiers mécanismes de sécurité
  - Failles conceptuelles dans IEEE 802.11
  - Attaques sur IEEE 802.11
- Les nouveaux mécanismes de sécurité
- Architecture des réseaux WiFi

Presse…

Le Canard enchaîné

09/10/2002

Rubrique :

Pge : 4

1/2

Comment espionner depuis un banc public

Nouvel eldorado pour les pirates, les réseaux informatiques sans fil peuvent être captés dans les rues.

AU moment de fignoler la restructuration du capital d'une société de haute technologie, un dirigeant du groupe Dassault s'interroge : faudra-t-il *« opérer une offre publique d'achat »* ? Quelles seront les incidences finales de l'opération ? Doit-on utiliser tel ou tel *« moyen de pression »* pour se trouver en meilleure position ? Et il rédige une petite note intitulée « Aide-mémoire sur la situation du dossier X », sans se douter que son partenaire, des concurrents, ou quelque malveillant puissent y avoir accès.

C'est pourtant ce qui s'est produit voilà quelques semaines. Heureusement, seul « Le Canard » a eu connaissance de ce document, par l'intermédiaire d'un informaticien qui traque, à temps perdu, les failles dans la sécurité des réseaux. Cette fois, ce n'est pas une faille qu'il a pu explorer, c'est une brèche, un trou béant qui menace des milliers d'entreprises et de particuliers.

Espion fantôme

Une campagne de « sensibilisation » est en cours pour inciter les industriels à plus de vigilance. D'autant que cette technique d'espionnage a une particularité amusante. Contrairement à un pirate passant par Internet, qui laisse toujours une trace, et, au bout du fil, une piste même ténue, une intrusion par réseau Wi Fi ne se signale par

C'est un calendrier très serré et extrêmement ambitieux.

LISTE (NON EXHAUSTIVE) DES SUJETS A TRAITER

- Conditions juridiques de l'opération : peut-on se satisfaire d'une majorité aux 2/3 ou faut-il l'unanimité des associés (ce qui aurait bien sûr la faveur des autorités accordant les dérogations). J'ai accepté de considérer que c'était une question un peu pour mémoire, puisque nous n'avons pas l'intention de nous opposer au projet mais c'est un moyen de pression.

Extrait d'une note interne de la maison Dassault sur une négociation financière. Ce document a été capté depuis le rond-point des Champs-Elysées, sans aucune manœuvre de piratage.

Presse…

ZDNet Where Technology Means Business

HOME | NEWS | TECH UPDATE | WHITE PAPERS | DOWNLOADS | REVI

Page One | Hardware | Software | Security | Commentary | Headline Archives

News sub_default

Many wireless networks open to attack

By Lee Gomes
The Wall Street Journal Online
April 26, 2001, 5:00 PM PT

It is a Friday afternoon, and Peter Shipley and Matt Peterson are sitting in a late-model Saturn in a Silicon Valley parking lot, balancing notebook computers on their laps, checking out e-mail and looking after files.

Not their own e-mail and files, but those of Sun Microsystems Inc., in whose lot the two are sitting and on whose corporate network they are, in effect, spying.

"Look, there's someone transferring a file," says Peterson, looking down at his computer. Shipley sees even more: "There – someone just turned on an NT machine and is getting mail."

Despite outward appearances, Shipley and Peterson aren't malevolent hackers. To the contrary, their aim is utterly benign: to expose one of the newest and potentially most dangerous security holes in U.S. business, in the form of wireless computer networks.

These are the increasingly popular systems that connect computers in offices or homes to other computers, or to printers, by using radio signals, much as cellphones do. These networks are remarkably convenient; they not only dispense with cables but also allow someone to roam around an office with a laptop computer while staying connected to the Internet.

Monday, 19 August, 2002, 11:27 GMT 12:27 UK

Wireless hackers take to the air

Perth has been buzzed by wireless net seekers

Australian hackers have taken the practice of looking for open wireless networks to new heights.

Before now many curious hackers have taken to cars and bicycles to look for wireless network nodes that are free for everyone to use or are inadequately protected.

But the Australians have them all beaten by using a light aircraft to fly over the city of Perth and look for the wireless nodes from 460 metres (1500 feet) up.

During their flight the group found up to 95 wireless nodes.

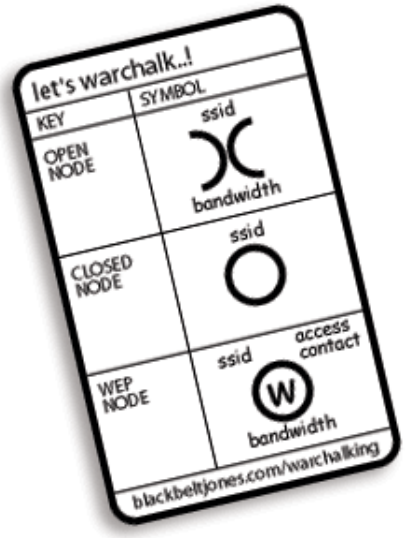
Wardriving

Wardriving ?

- Terme issu de « WarDialing » : Procédé de découverte des modems RTC par appels téléphoniques
- Procédé de découverte des réseaux Wi-Fi (en voiture !)

Et des variantes…

➔WarDriving



➔WarChalking

➔WarFlying

➔WarParking

➔BlueJacking (bluetooth)

'I like your pink stripy top'

Wardriving contest Defcon 11

Final Results

Place	Team	AP	WEP	SSID	Unique	Total
1	Lords of Wireless	2119	612	748	1264	7883
2	Team WirelessCon	1983	625	604	737	6048
3	Team 5	1311	393	422	380	3659
4	WarDriving Miss Daisy	809	234	262	486	2997
5	Team 12	668	199	211	331	2270
6	Fear & Loathing	721	153	211	191	1891

)(WARDRIVER

Plusieurs types d'attaques

- **Déni de service**
- **Brute-force de la clé**
- **Réutilisation de keystreams et injection de paquets**
  - Keystream lié à l'authentification
  - Keystreams quelconques
    - Récupération d'un keystream de taille donnée
    - Expansion du keystream et récupération d'un keystream de 1500 octets
    - Injection de paquets et construction d'un dictionnaire d'IVs – keystreams
- **Cassage des clés WEP à partir d'IVs faibles**
  - Récupération des IVs et des cipher-texts correspondants
  - Déduction de la clé
  - Accélération de l'attaque par injection de trames (ARP par exemple) et récupération de paquets chiffrés

Exemple d'attaque : Bittau

- **Récupération des 8 premiers octets du keystream (en-tête LLC/SNAP)**
- **Utilisation des possibilités de fragmentation (en 16 trames)**
  - Injection de 16 fragments de 4 octets (+4 octets de CRC)
  - Récupération d'un message de 64 octets (+4 octets de CRC) avec un nouvel IV
    - Informe des 68 premiers octets du keystream
  - Recherche séquentielle des octets suivants du keystream
    - Obtention d'un keystream de 1500 octets

Déni de service

- **Attaques extrêmement faciles à réaliser**
- **Accès complètement interrompu**
- **Void11:**
  - Flood deauth
  - Flood auth
  - http://www.wlsec.net/downloads/
- **Scapy**
  - Drivers Airjack, Prism54, HostAP, madwifi…
  - Création des paquets Deassociation et Deauthentication

Plan

- Le 802.11 : écosystème et fonctionnement
- Les premiers mécanismes de sécurité : failles et attaques
- **Les nouveaux mécanismes de sécurité**
  - Réutilisation de briques de sécurité éprouvées (802.1X, EAP, AES …)
  - Une solution à court-terme, le WPA
  - Recherche de failles d'implémentation dans les drivers WiFi
- Architecture des réseaux WiFi

Plan

- Le 802.11 : écosystème et fonctionnement
- Les premiers mécanismes de sécurité : failles et attaques
- **Les nouveaux mécanismes de sécurité**
  - Réutilisation de briques de sécurité éprouvées (802.1X, EAP, AES …)
  - Une solution à court-terme, le WPA
  - Recherche de failles d'implémentation dans les drivers WiFi
- Architecture des réseaux WiFi

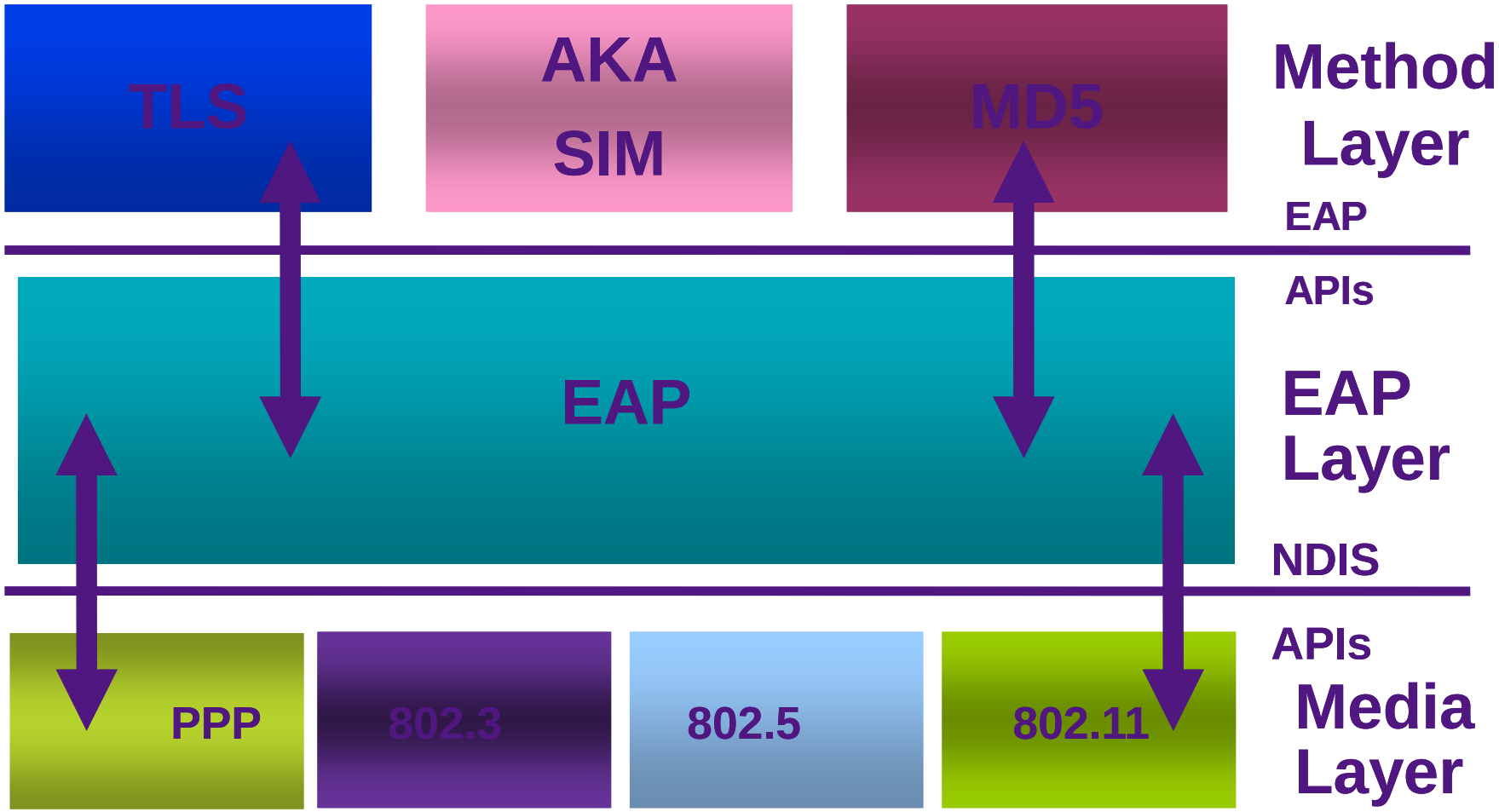
IEEE 802.11 TGi
Présentation

- **Task Group i : Specification for Robust Security**
- **But : Améliorer les mécanismes de sécurité des réseaux IEEE 802.11**
- **Axes de travail :**
  - Définition de mécanismes d'authentification et de contrôle d'accès
    - Basés sur IEEE 802.1X : « Port-based Network Access Control »
      - *Basé sur EAP : Extensible Authentication Protocol*
  - Définition de nouveaux mécanismes de confidentialité et d'intégrité
    - TKIP : Temporal Key Integrity Protocol
    - CCMP : Counter-Mode/CBC-MAC Protocol
  - Définition de mécanismes de distribution de clés
    - Basés sur IEEE 802.1X
  - Pré-authentification durant du roaming

Authentification / Contrôle accès
IEEE 802.1X – Définition

- **Contrôle d'accès sur les technologies LAN (IEEE 802.3)**
- **Assure le transport de l'authentification grâce à EAP (RFC 2284) – Extensible Authentication Protocol**
  - Structure modulaire
  - Nombreuses méthodes d'authentification
    - TLS : Certificats (server-side, client-side)
    - MD5 : Username / Password
    - SIM/AKA : Cartes SIM/USIM
    - Constante évolution en fonction des besoins…
- **Principe de « Port de contrôle »**
  - Un port « non contrôlé » permet le passage de l'authentification (trames EAP)
  - Un port « contrôlé » permet le passage des données selon le résultat de l'authentification

Authentification / Contrôle accès
Structure EAP



Source : IEEE

Authentification / Contrôle accès
Méthodes EAP

- **Protection cryptographique d'EAP**
  - But : Protéger les méthodes d'authentification plus « sensibles »
    - Protection de l'identité
    - Authentification mutuelle et dérivation de clé
    - Modulaire dans le choix de l'authentification client
- **Protected EAP (PEAP) : Internet Draft (draft 10)**
  - Internet Draft de Microsoft / Cisco
  - Tunnel TLS entre le client et le serveur PEAP
    - Authentification du réseau par certificat
  - Méthodes d'authentification encapsulées
    - Par exemple, MS-CHAP-v2 dans le cas d'une architecture complète Microsoft
    - Autres possibilités…
- **Tunneled TLS (TTLS) : Internet Draft (draft 5)**
  - Internet Draft de Funk Software
  - Même principe que PEAP

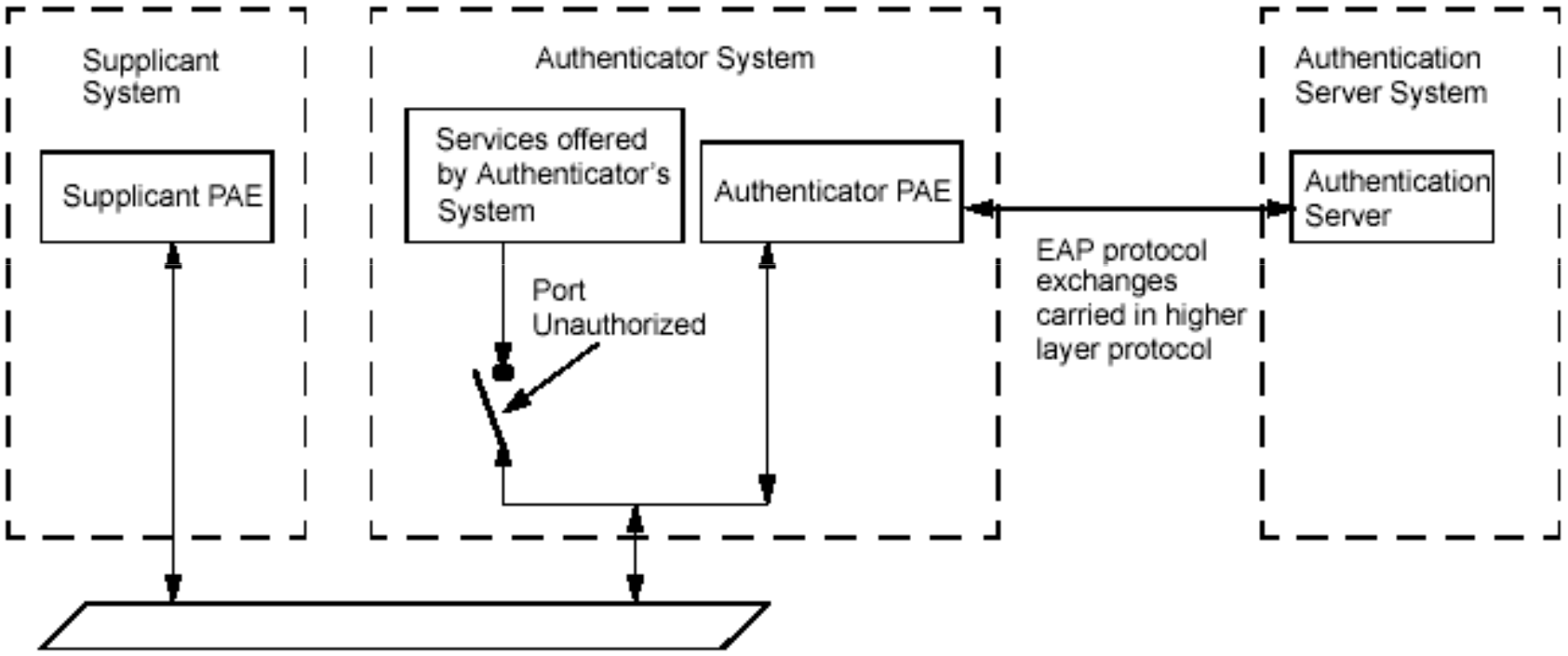
Authentification / Contrôle accès
Méthodes EAP

- **EAP-MD5 : obligatoire dans RFC 2284 – Mars 1998**
  - Authentification du client par couple username / password
    - MD5 [Identity + Challenge + Secret]
  - Pas d'authentification du réseau
  - Pas de dérivation de clé

- **EAP-TLS : RFC 2716 – Octobre 1999**
  - Authentification du client et/ou réseau par certificats
    - En pratique, authentification mutuelle forte par certificats
  - Dérivation de clé basée sur les fonctions internes de TLS

- **EAP-{SIM/AKA} : RFC 4186/4187 – Janvier 2006**
  - Authentification du client et réseau basée sur l'authentification GSM/UMTS
  - Dérivation de clé
    - Besoins internes d'EAP-{SIM/AKA} : protection de l'identité, authentification du réseau
    - Chiffrement et intégrité du lien radio

Authentification / Contrôle accès
IEEE 802.1X – Entités

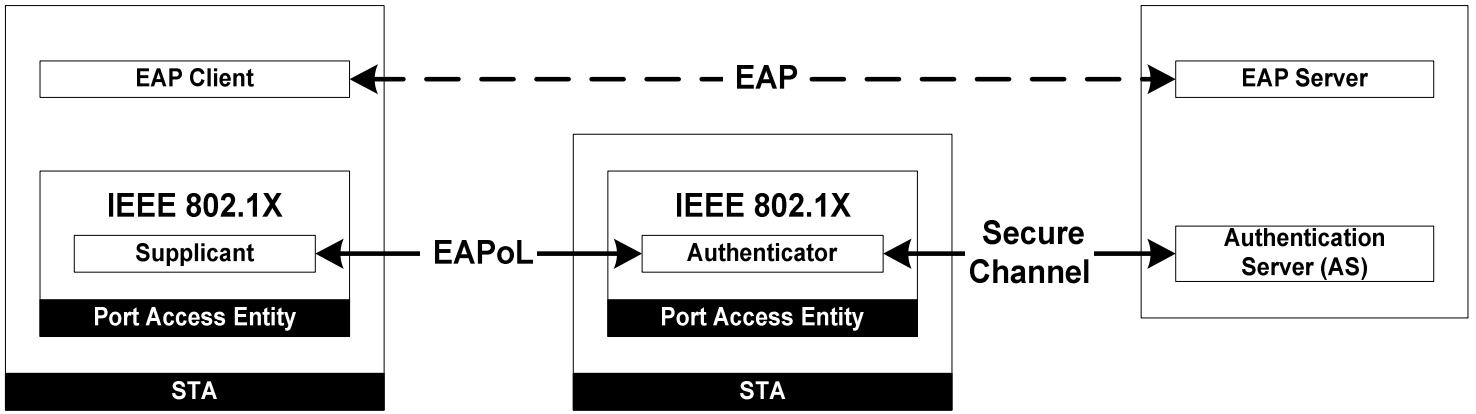


Authenticator, Supplicant, and Authentication Server roles

Source : IEEE

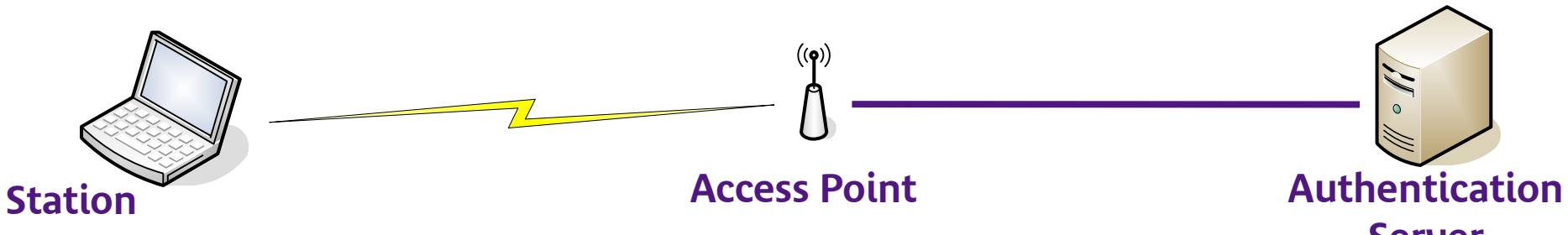
Authentification / Contrôle accès
IEEE 802.1X – Entités

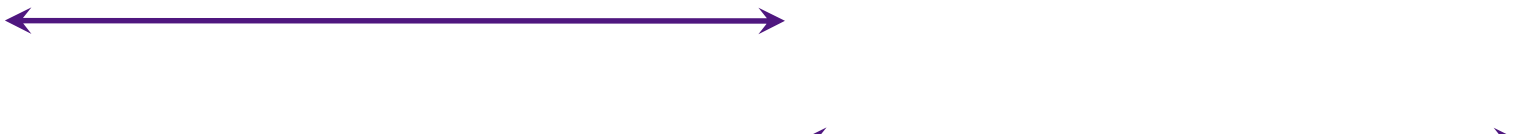
- Supplicant
- Authenticator
- Authentication Server



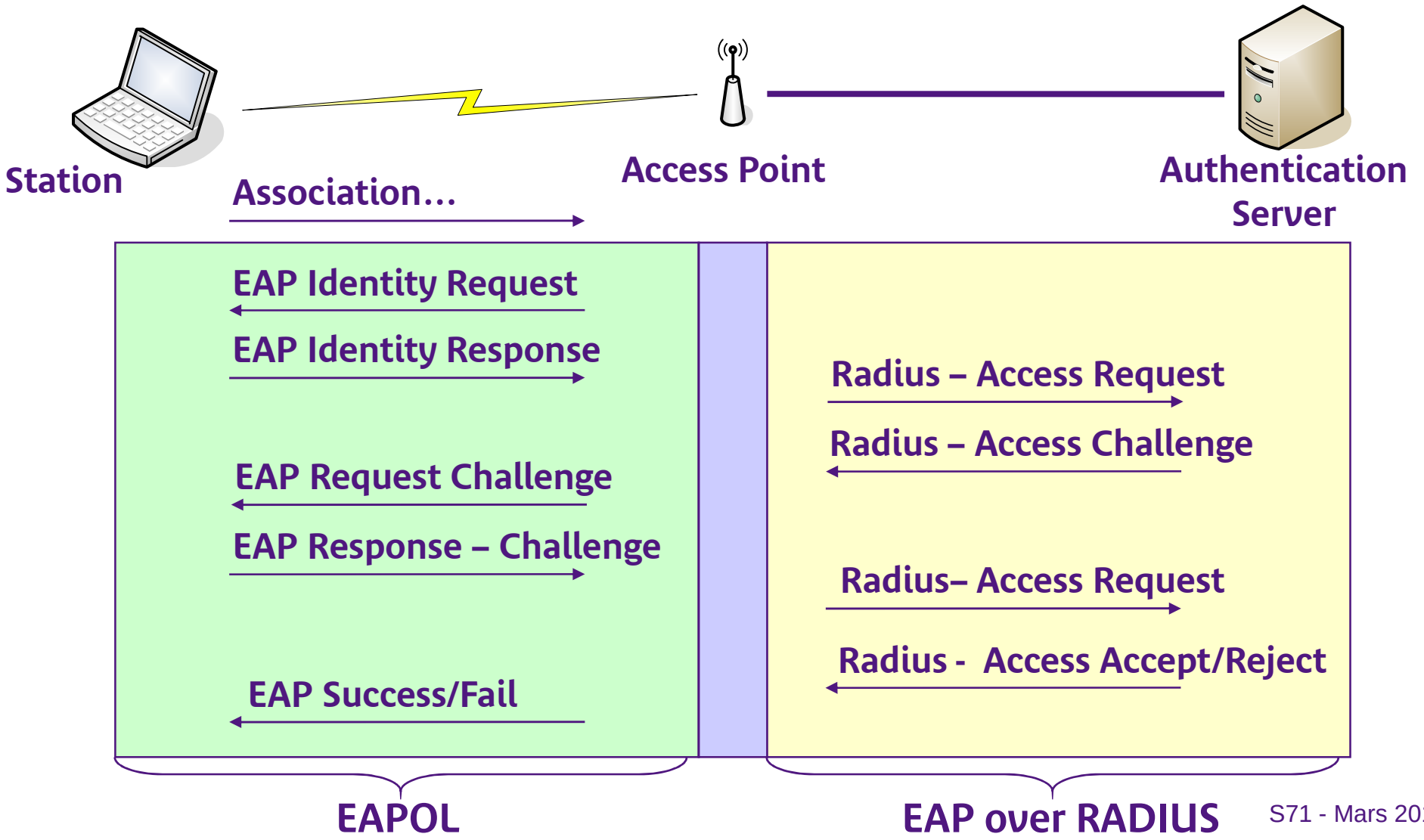
Source : IEEE

Encapsulation des échanges EAP

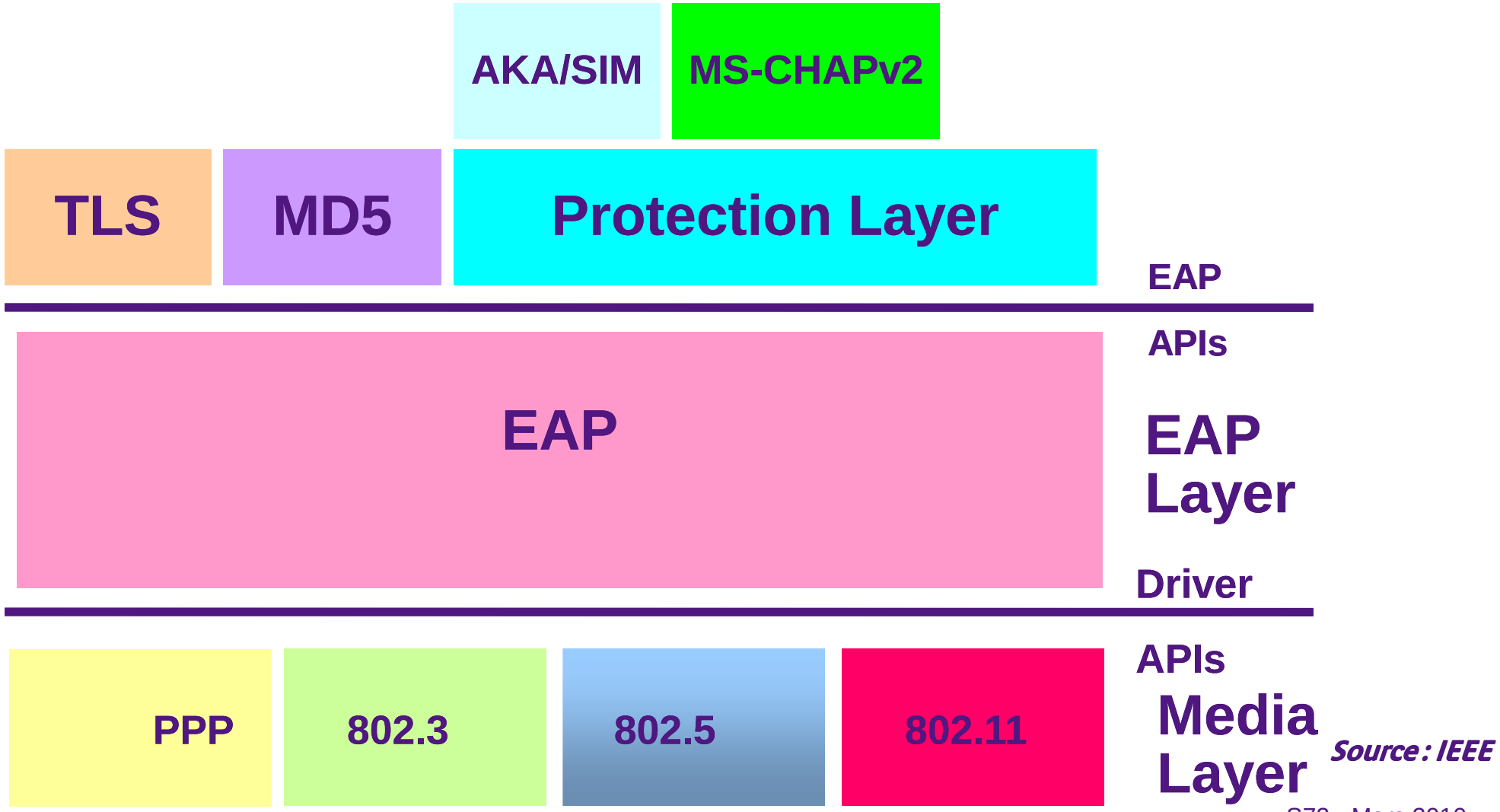




Authentification EAPoL/Radius



Authentification / Contrôle accès
Protection d'EAP

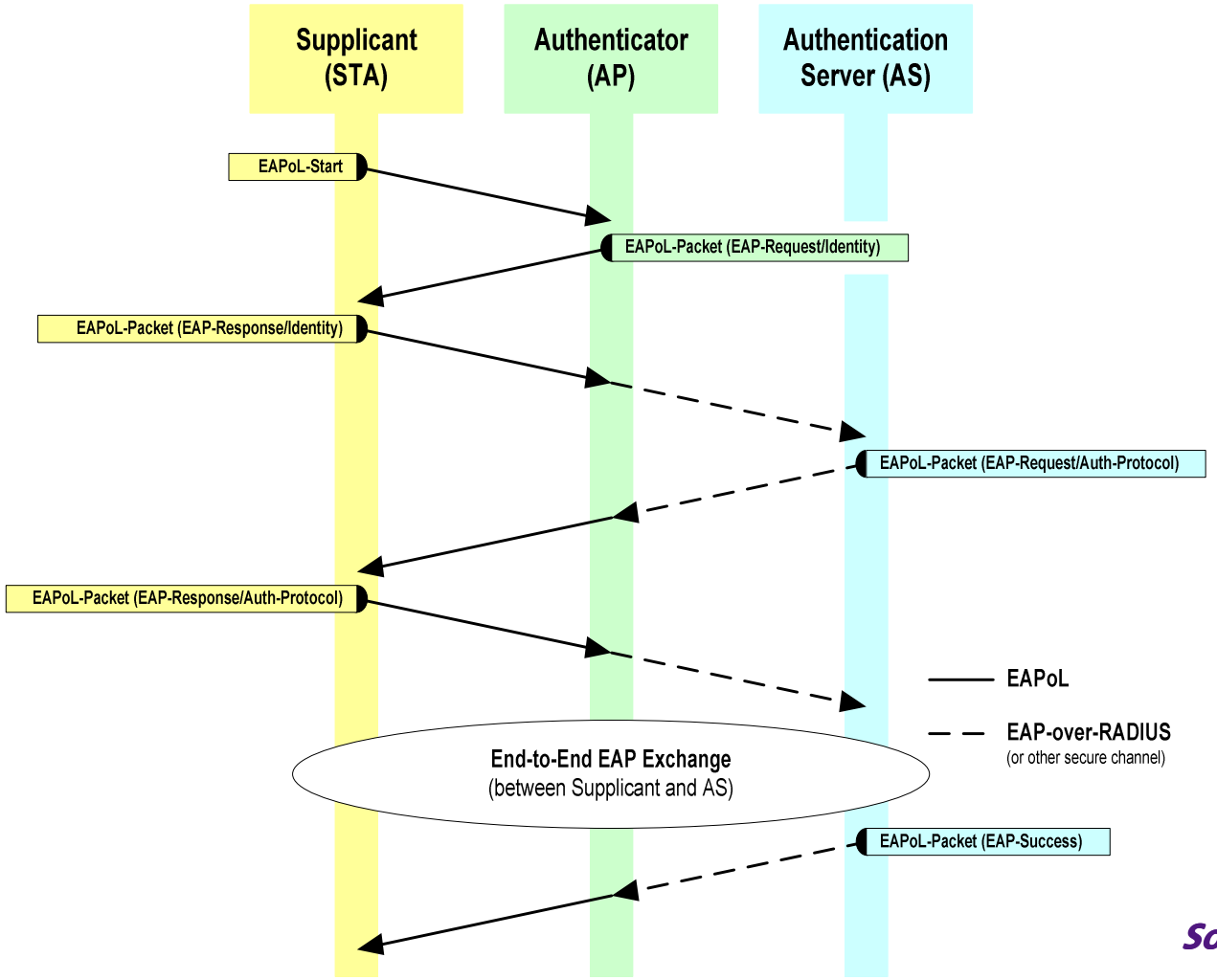


Source : IEEE

Authentification / Contrôle accès
Résumé méthodes EAP

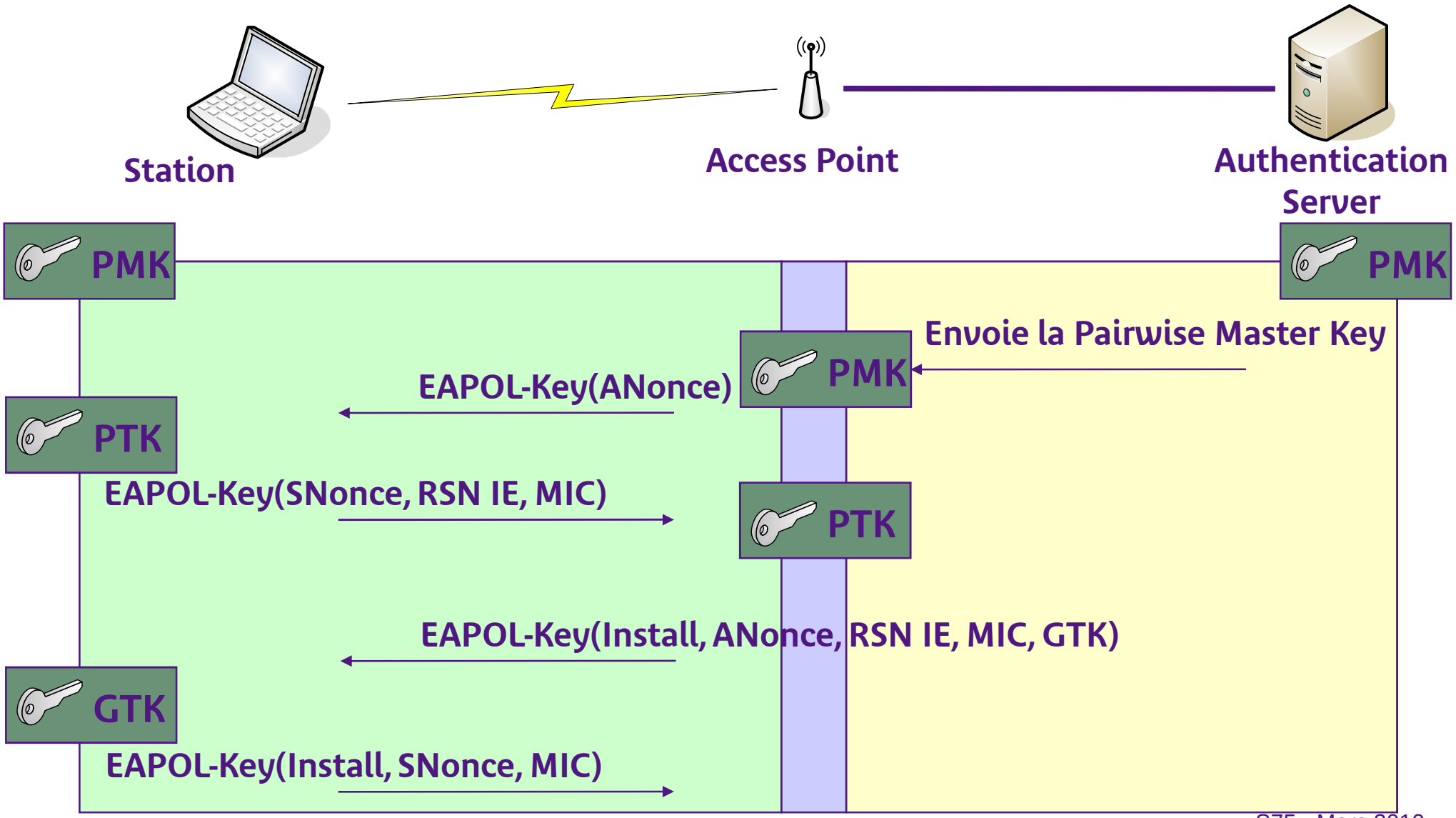
EAP Method	Identity-privacy	Key generation	Authentication type	Tokens needed	Deployment constraints
MD5	No	No	Client authentication (one-way)	Username / Password	Low
OTP	No	No	One Time Password client authentication (one-way)	One Time Password on client side	Low
TLS	No	Yes	Certificate-based mutual authentication (mutual)	Certificates on both client and server side	High
TTLS + MS-CHAPv2	Optional	Yes	Certificate-based on server side Username / Password on client side (mutual)	Certificate on server side Username / Password on client side	Average
PEAP + MS-CHAPv2	Optional	Yes	Certificate-based on server side Username / Password on client side (mutual)	Certificate on server side Username / Password on client side	Average
SIM	Optional, limited	Yes	GSM-based authentication (mutual)	SIM-based authentication tokens on both client and network side	Low-Average
AKA	Optional, limited	Yes	(GSM or UMTS)-based authentication (mutual)	(SIM or USIM)-based authentication tokens on both client and network side	Low-Average

Authentification / Contrôle accès
Échanges radio / filaire

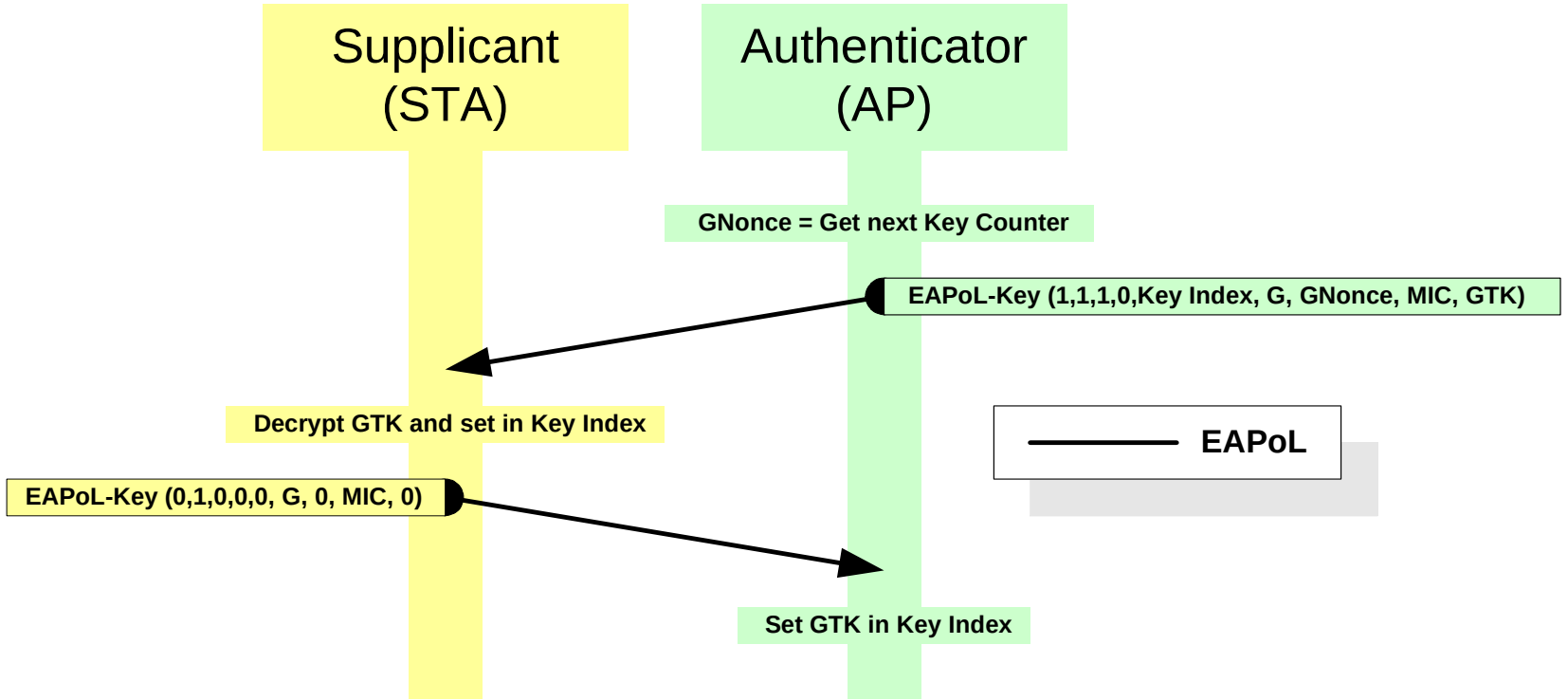


Source : IEEE

Dérivation des clés : 4-way handshake



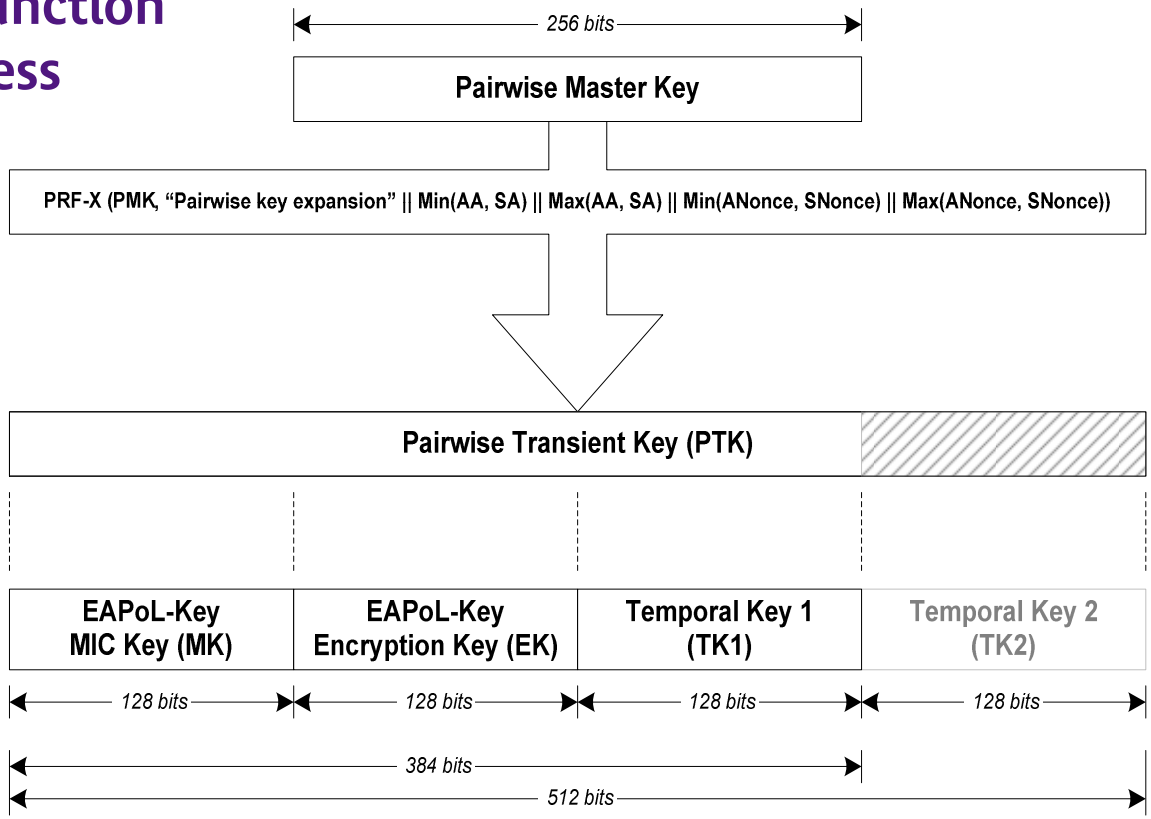
Distributions des clés
Group Key Handshake



Source : IEEE

Hiérarchie des clés
Clés individuelles

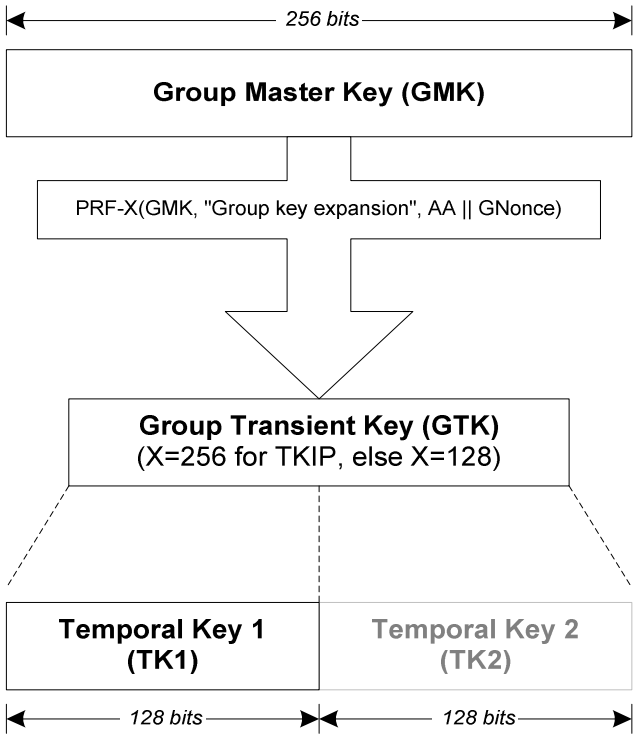
- Snonce : Graine générée par la station
- ANonce : Graine générée par l'AP
- PRF : Pseudo Random Function
- AA : Authenticator Address
- SA : Station Address



Source : IEEE

Hiérarchie des clés
Clés de groupe

- AA : Authenticator Address
- GNonce : Graine générée par l'AP

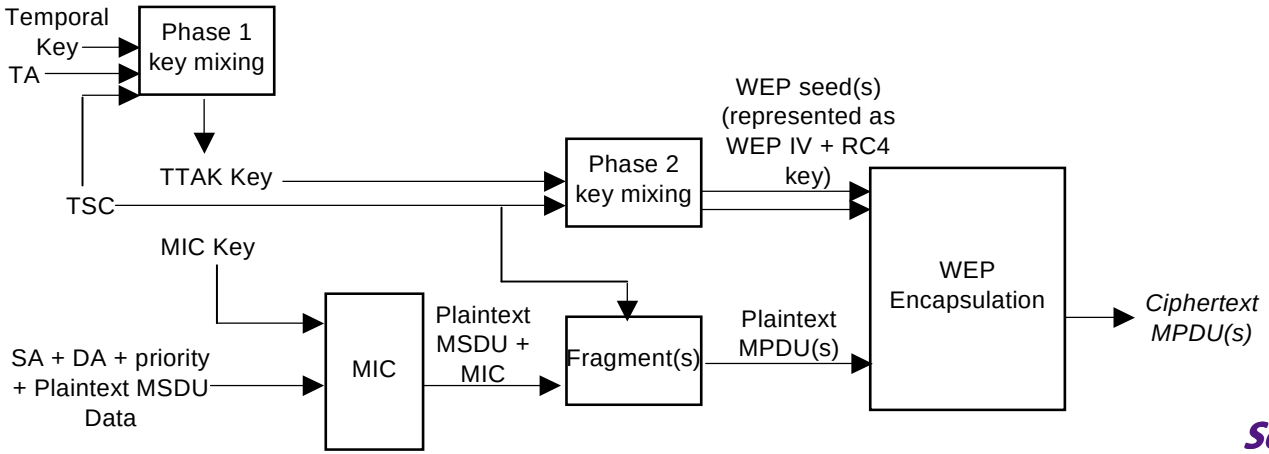


Source : IEEE

Confidentialité / Intégrité TGi
TKIP

Temporal Key Integrity Protocol

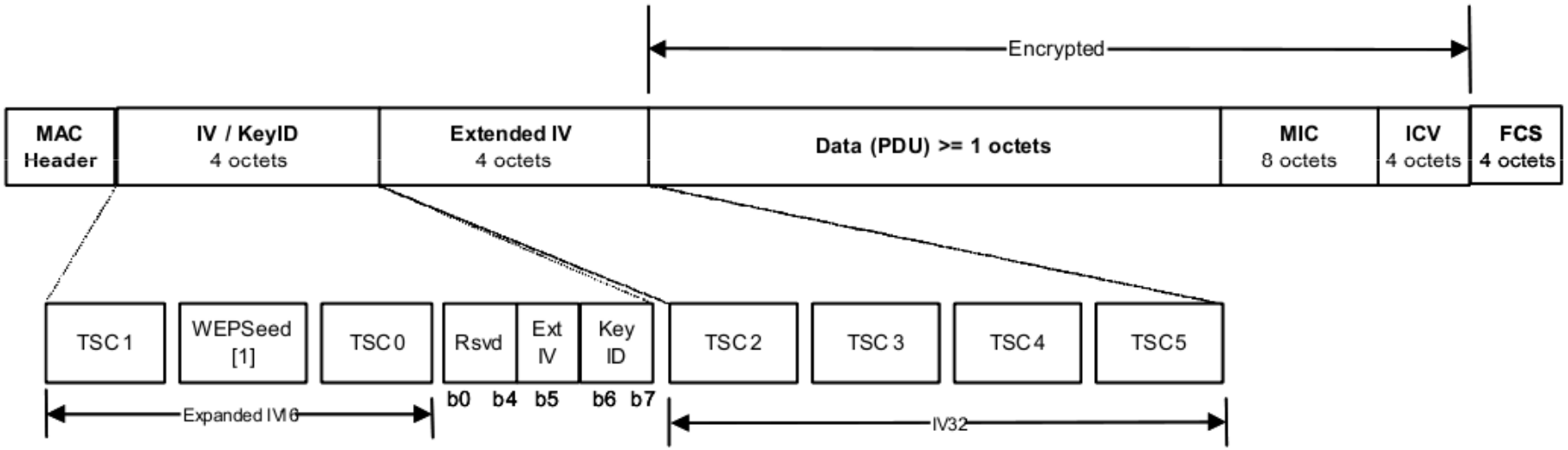
- Basé sur RC4 pour compatibilité avec le matériel existant
- Amélioration du protocole WEP
  - Message Integrity Check de 8 octets (en plus de l'ICV original de WEP)
    - Obtenu à partir de l'algorithme cryptographique Michaël
  - Contre-mesures (en particulier sur le MIC à cause de sa faiblesse)
  - TKIP sequence counter (TSC) : numéro de séquence
  - Fonction de mixage en amont pour apporter une clé "par paquet".



Source : IEEE

Confidentialité / Intégrité TGi
TKIP

MPDU TKIP

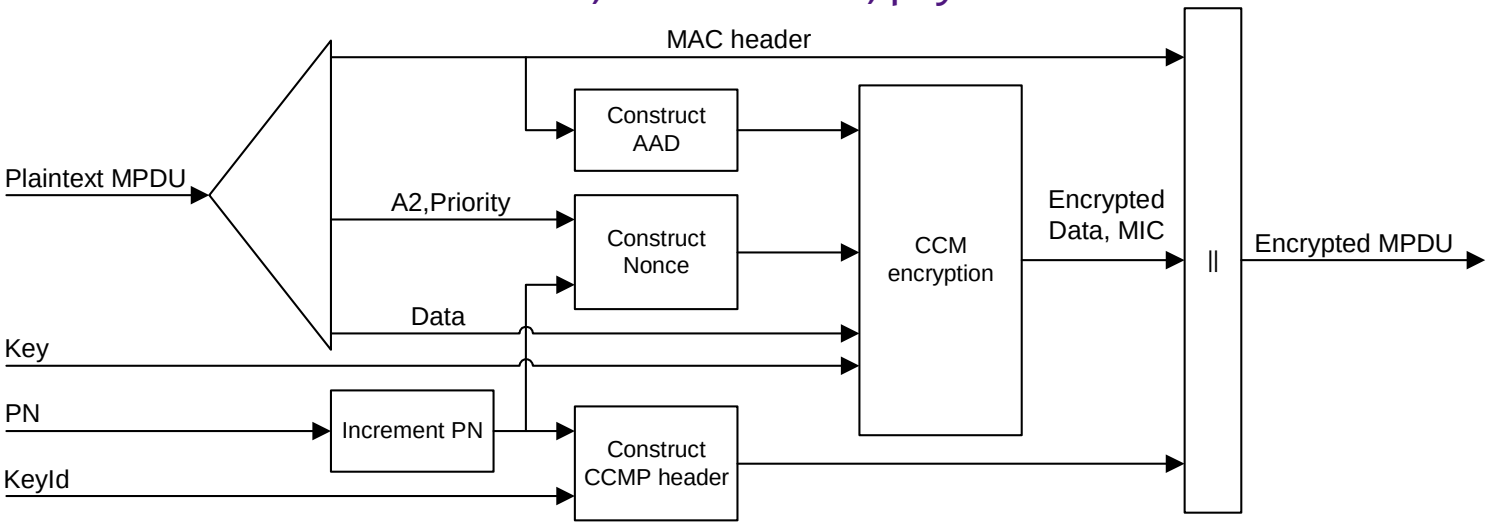


Source : IEEE

Confidentialité / Intégrité TGi CCMP

Counter-Mode/CBC-MAC Protocol

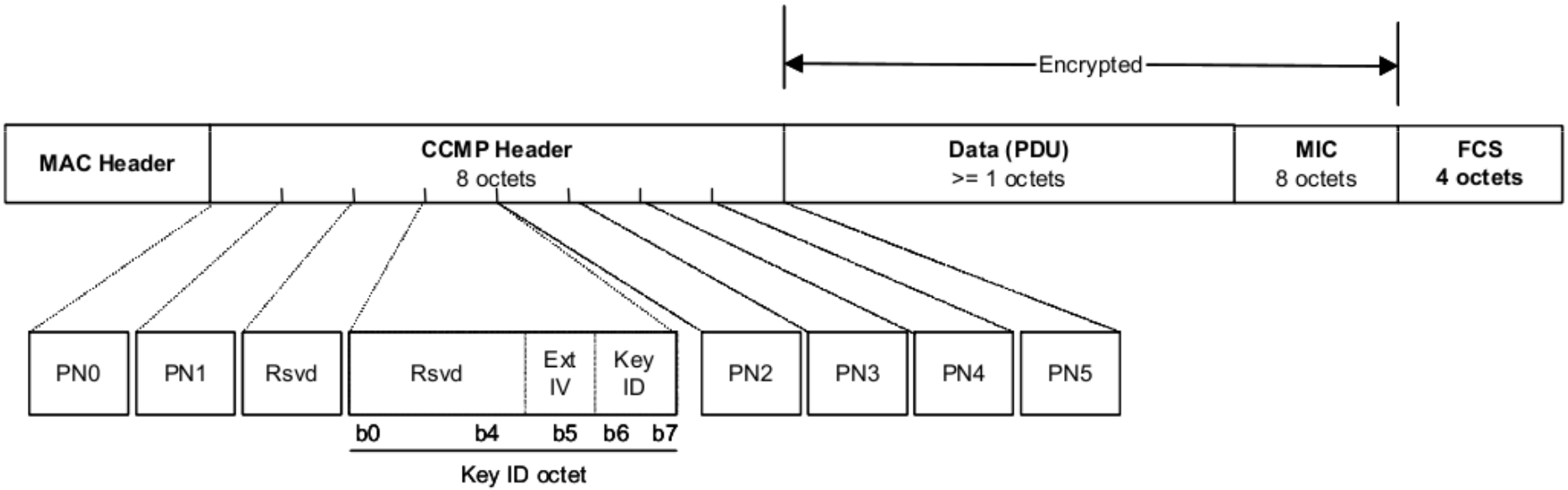
- Basé sur AES
  - Counter Mode (CTR) pour la confidentialité
  - Cipher Block Chaining Message Authentication Code (CBC-MAC) pour l'authentification et l'intégrité
- Packet Number (PN) : numéro de séquence de 48 bits
- MIC calculé sur en-tête MAC, en-tête CCMP, payload



Source : IEEE

Confidentialité / Intégrité TGi
CCMP

MPDU CCMP

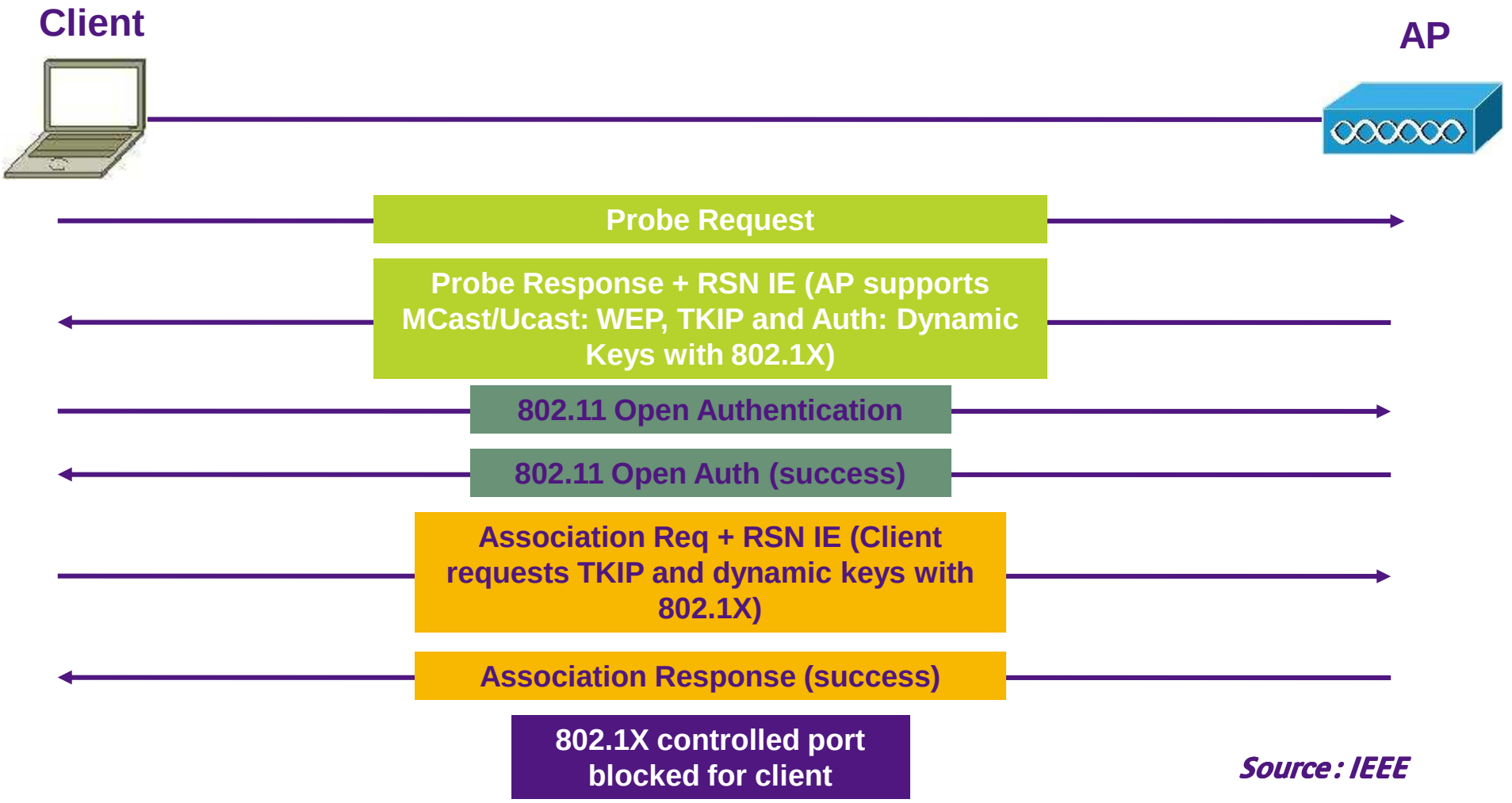


Source : IEEE

Comparaison

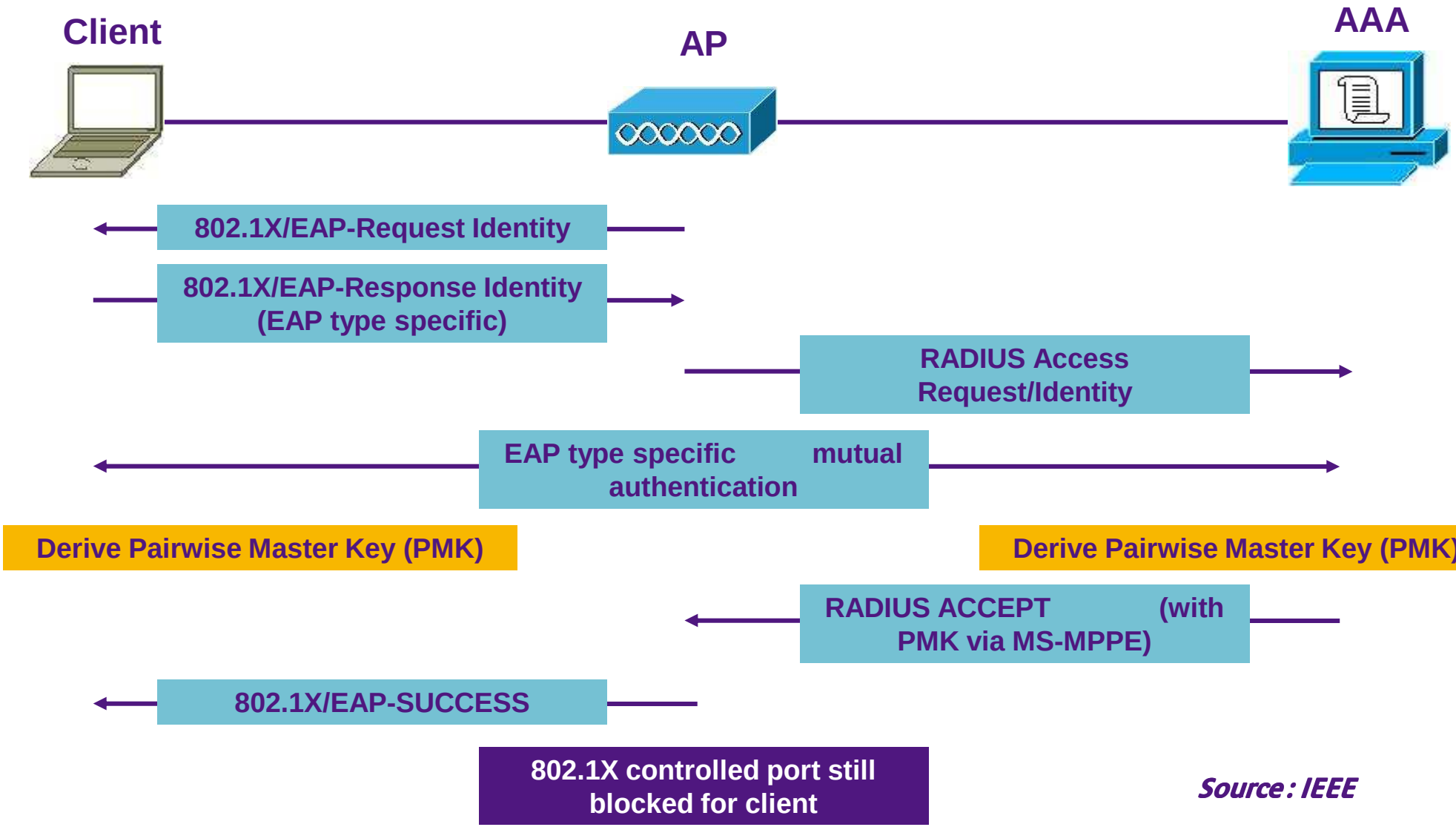
	WEP	TKIP	CCMP
Chiffrement	RC4	RC4	AES
Taille des clés	40 ou 104 bits	128 bits pour chiffrer 64 bits pour authenticité	128 bits
Durée de vie	IV de 24 bits	IV de 48 bits	IV de 48 bits
Clé par paquet	Concaténation IV / clé	Mixing Function	Pas de clé par paquet
Intégrité des données	CRC32	Michael	CCM
Intégrité du header	Aucun	Michael	CCM
Rejeu	Aucun	IV croissant	IV croissant
Gestion des clés	Aucune	802.11i 4-way handshake	802.11i 4-way handshake
Contraintes par rapport au matériel existant	Aucune	Aucune : simple upgrade logiciel	Besoin de nouveaux équipements

Connexion : découverte et association



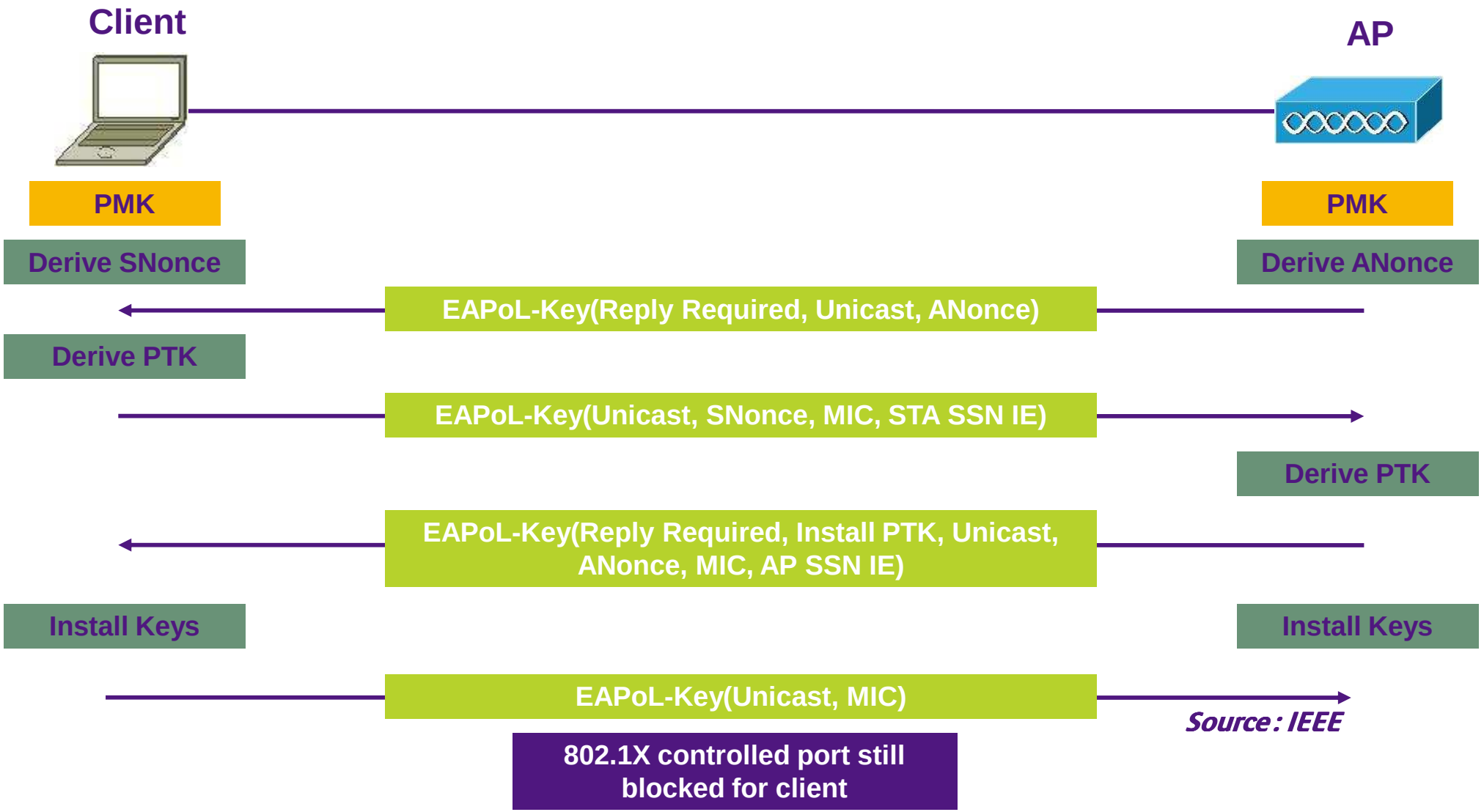
Source : IEEE

Connexion : authentification de l'utilisateur



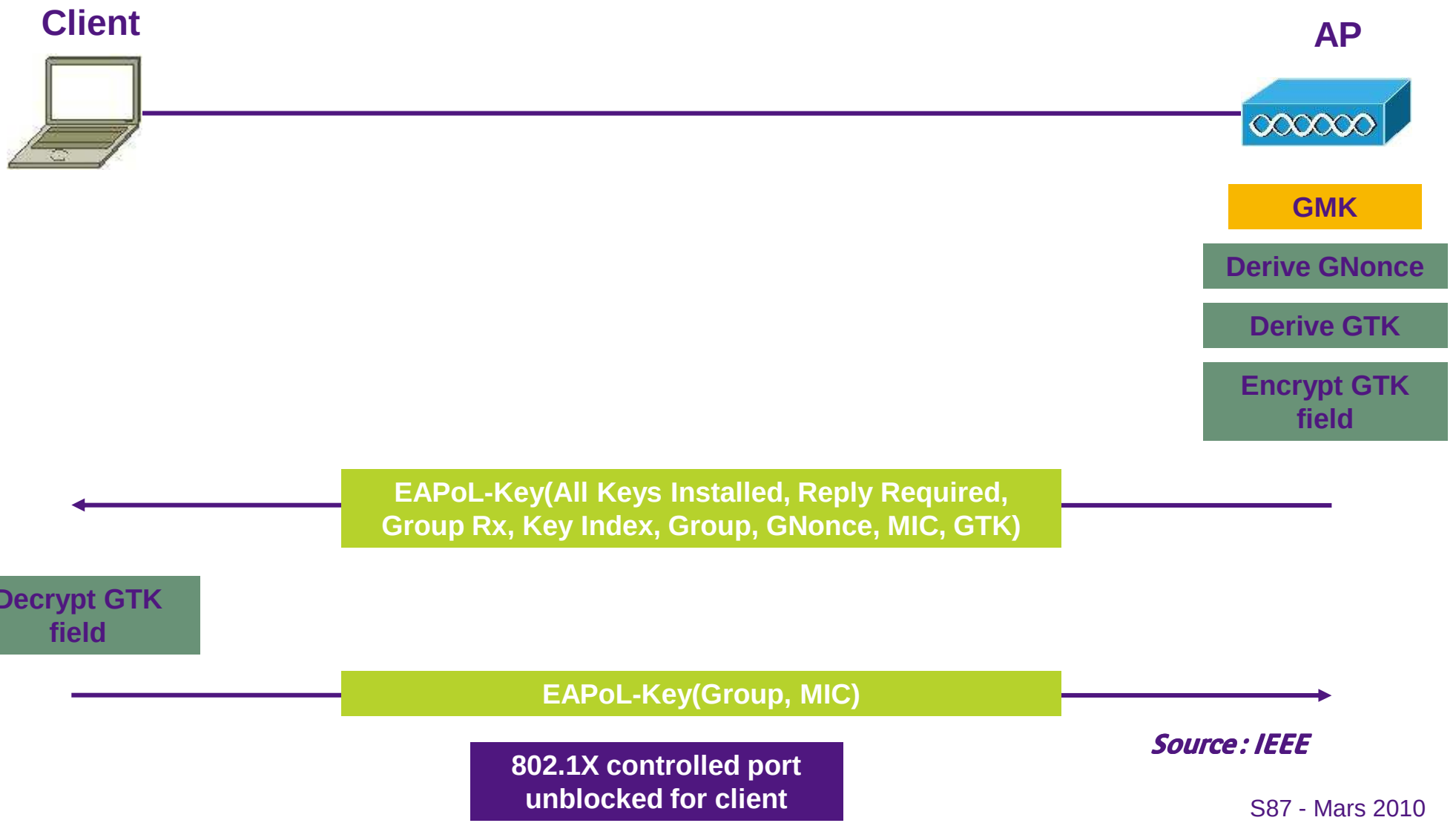
Source : IEEE

Connexion : 4-Way Handshake



Source : IEEE

Connexion : group key update



Source : IEEE

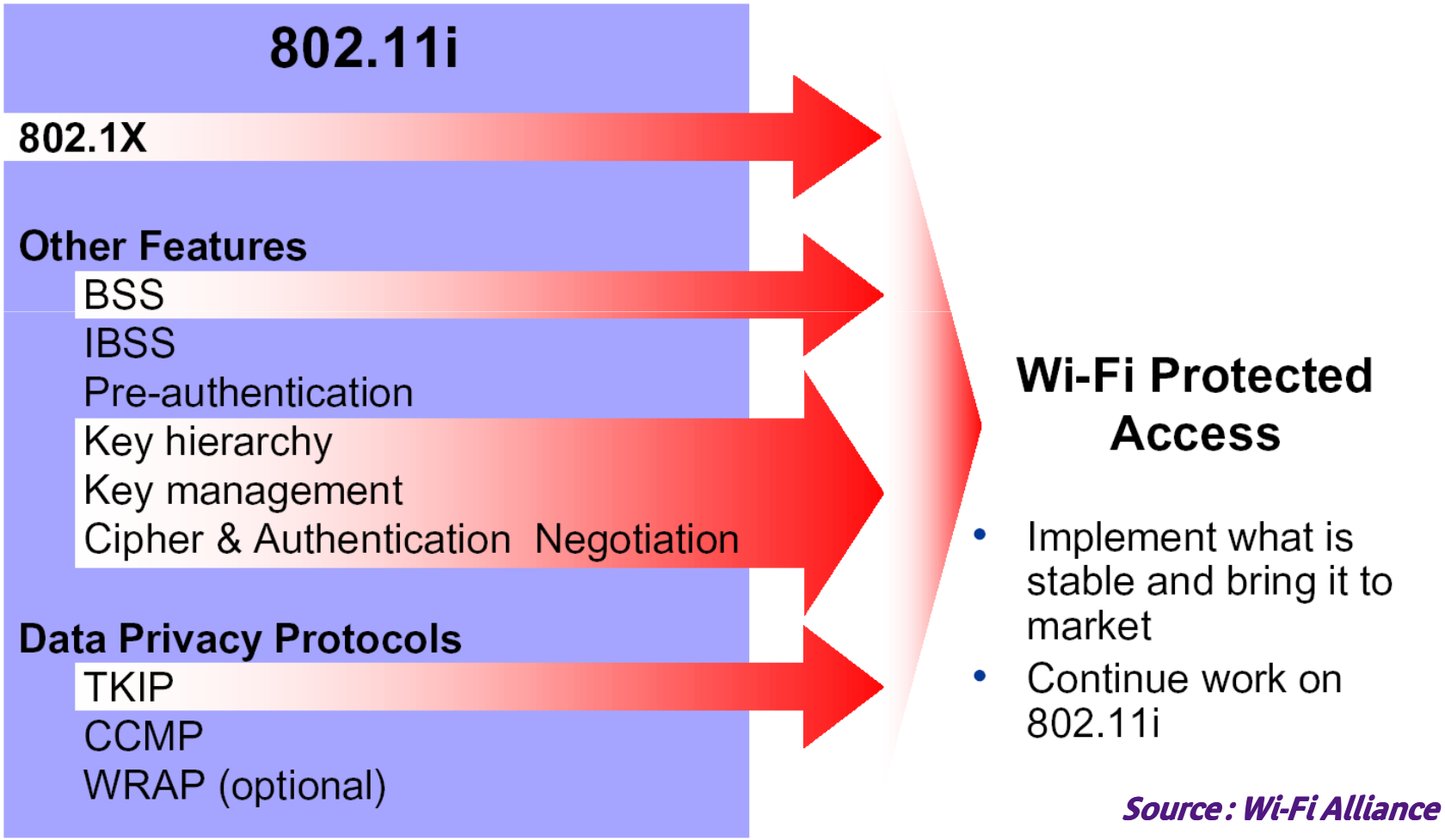
Plan

- Le 802.11 : écosystème et fonctionnement
- Les premiers mécanismes de sécurité : failles et attaques
- **Les nouveaux mécanismes de sécurité**
  - Réutilisation de briques de sécurité éprouvées (802.1X, EAP, AES …)
  - Une solution à court-terme, le WPA
  - Recherche de failles d'implémentation dans les drivers WiFi
- Architecture des réseaux WiFi

WPA (1/2)
Définition

- **WPA** Wi-Fi Protected Access™
- **Norme définie par la Wi-Fi Alliance en octobre 2002**
  - Sous-ensemble du draft 3.0 du TGi de 802.11
  - Dernière révision, version 1.2 décembre 2002
- **Buts :**
  - Apporter les évolutions en sécurité considérées comme stables
  - Volonté d'apporter ces évolutions le plus rapidement possible
  - Doit être « backward-compatible », et supporter un mode « mixte »
  - Répondre aux contextes entreprise, résidentiel et hot spot
  - Apporter la certification Wi-Fi WPA dès fin août 2003

WPA (2/2)
Résumé



WPA2
Définition et description

- **WPA** WPA2™ Wi-Fi Protected Access 2
- **Norme définie par la Wi-Fi Alliance à la suite de la ratification de IEEE 802.11i**
- **Buts :**
  - Certifier les nouveaux mécanismes ratifiés dans IEEE 802.11i
  - Le nouveau protocole de confidentialité CCMP est recommandé
- **Les premiers produits certifiés WPA2 sont disponibles**
- **Approbation par le NIST en mai 2004**

Plan

- Le 802.11 : écosystème et fonctionnement
- Les premiers mécanismes de sécurité : failles et attaques
- Les nouveaux mécanismes de sécurité
  - Réutilisation de briques de sécurité éprouvées (802.1X, EAP, AES …)
  - Une solution à court-terme, le WPA
  - Recherche de failles d'implémentation dans les drivers WiFi
- Architecture des réseaux WiFi

Ce que l'on savait…

- **Le Wi-Fi rend difficile la protection périmétrique de l'entreprise**
  - Infrastructures réseau Wi-Fi friables (WEP, WPA mal utilisé)
  - Infrastructures réseau avec point d'accès illégitimes ou mal configurés
- **Mais aussi la sécurité du poste client**
  - Les points d'accès illégitimes dans les zones publiques (conférences, hot spots…)
  - Les faux points d'accès attaquant les clients [KARMA]
  - L'injection de trafic dans les communications clients [WIFITAP, AIRPWN]
- **Et tout ca, bien entendu difficilement détectable…**

Ce dont on se doutait…

- **Erreurs de programmation dans les drivers 802.11**
  - Code développé en C/C++
  - Nombreux constructeurs de chipsets ⇨ Nombreux développeurs ⇨ Hétérogénéité de la qualité des développements
    - Intégrateurs ⇨ Packages de drivers obsolètes
- **Erreurs de programmation intéressantes à exploiter**
  - Exécution de code arbitraire en mode ring0 (kernel)
    - Contournement des fonctions de sécurité de type PFW, HIPS, AV…
  - Accessibles à distance par la voie radioélectrique
    - Sans (forcément) avoir besoin d'être associé à un point d'accès malveillant
- **Plutôt intéressant, non ?!?**

Ce qui arriva…

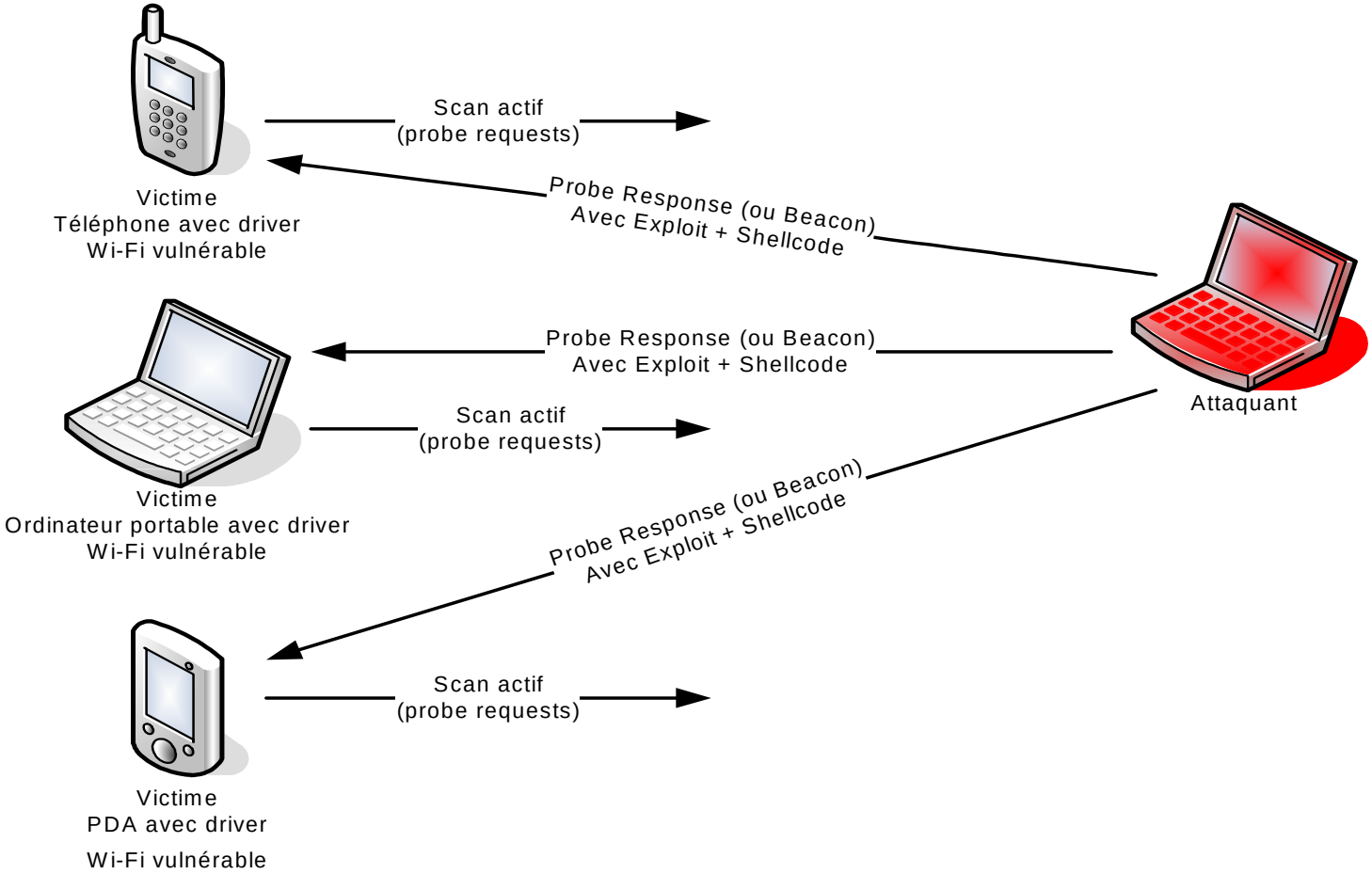
- **Premières publications à BlackHat US 2006 par Johnny Cache et David Maynor [CACHE-MAYNOR]**

- **Month of Kernel Bugs de novembre 2006 [MOKB]**
  - Apple Airport 802.11 Probe Response Kernel Memory Corruption (OS X)
  - Broadcom Wireless Driver Probe Response SSID Overflow (Windows)
  - D-Link DWL-G132 Wireless Driver Beacon Rates Overflow (Windows)
  - NetGear WG111v2 Wireless Driver Long Beacon Overflow (Windows)
  - NetGear MA521 Wireless Driver Long Rates Overflow (Windows) (*)
  - NetGear WG311v1 Wireless Driver Long SSID Overflow (Windows) (*)
  - Apple Airport Extreme Beacon Frame Denial of Service (OS X)

- **Mais aussi sous Linux…**
  - Madwifi stack-based overflow (*)
    - Potentiellement toutes les distributions Linux non patchées avec chipset Atheros

(*) failles découvertes par notre fuzzer

Schéma d'une attaque



- **802.11 exploits a.k.a. 0wn3d par une trame 802.11 ! ;-)**

Fuzzing 802.11

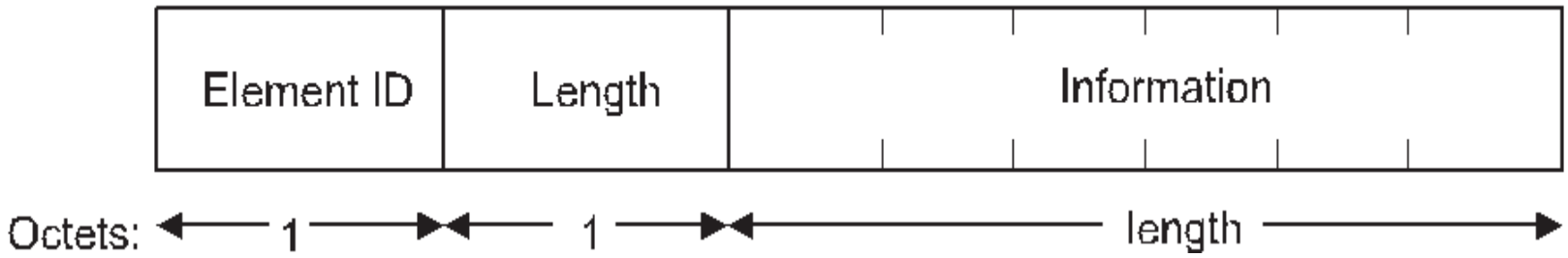
- **La norme 802.11 est « riche »**
  - Plusieurs types de trames (management, data, control)
  - Transport de nombreuses informations de « signalisation »
    - Débits, canal, nom de réseau, capacités cryptographiques, capacités propriétaires…
- **Ses extensions le sont (seront) aussi**
  - 802.11i pour la sécurité, 802.11e pour la QoS…
  - 802.11w, 802.11r, 802.11k…
- **Complexité ++ ⇨ Lignes de code ++ ⇨ Erreurs ++**

Aperçu de trames 802.11

Beacon / Probe Response format

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set information element is present within Beacon frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	The DS Parameter Set information element is present within Beacon frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	The CF Parameter Set information element is only present within Beacon frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set information element is only present within Beacon frames generated by STAs in an IBSS.
10	TIM	The TIM information element is only present within Beacon frames generated by APs.

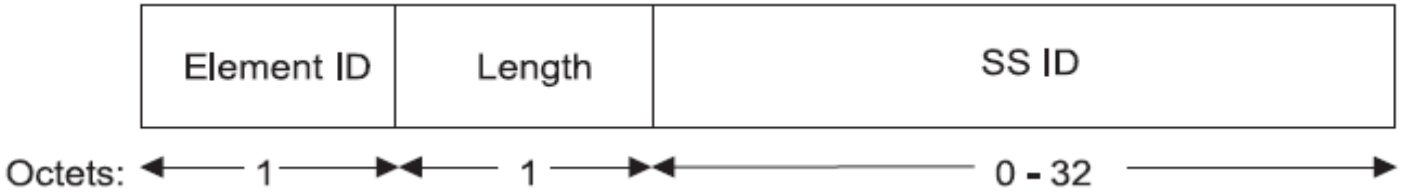
Aperçu de trames 802.11

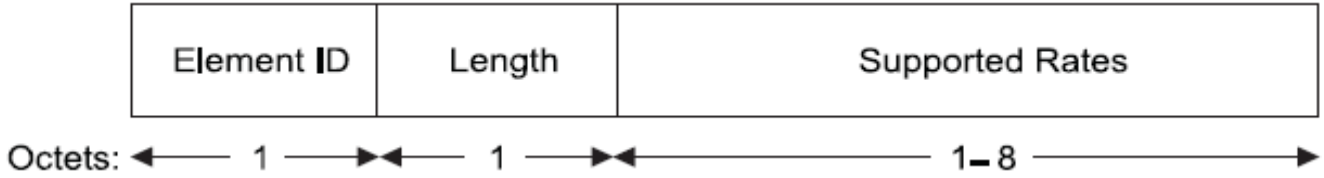


Information element	Element ID
SSID	0
Supported rates	1
FH Parameter Set	2
DS Parameter Set	3
CF Parameter Set	4
TIM	5
IBSS Parameter Set	6
Reserved	7–15
Challenge text	16
Reserved for challenge text extension	17–31
Reserved	32–255

Aperçu de trames 802.11

Some Information Elements

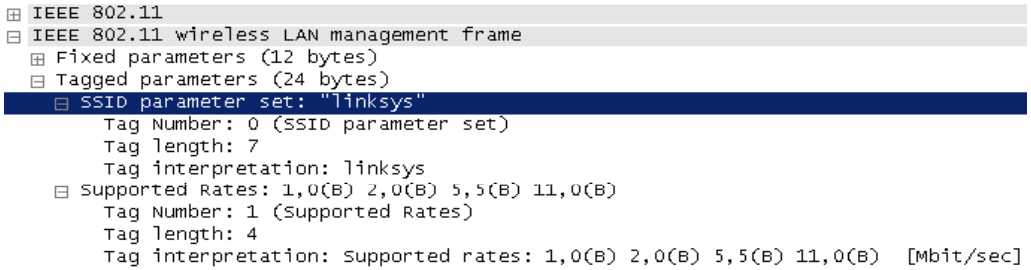




Fuzzer l'Information Element

Information Element

- Champ optionnel des trames de management
- De la forme : Type, Length, Value



On sent alors tout l'intérêt de fuzzer l'Information Element !

- Certains IE sont souvent de longueur fixe ou maximale
- On imagine bien alors les erreurs de programmation
  - On attribue un buffer statique d'une longueur fixe prédéfinie (en fonction de ce qui est décrit dans la norme ou de façon arbitraire)
  - On lit sur la trame 802.11 le champ « length »
  - Puis on copie le contenu de « value » dans le buffer statique
  - On déborde alors sur la pile ou le tas

Plan

- Le 802.11 : écosystème et fonctionnement
- Les premiers mécanismes de sécurité : failles et attaques
- Les nouveaux mécanismes de sécurité
- **Architecture des réseaux WiFi**
  - Contexte résidentiel
  - Contexte hot spot
  - Contexte entreprise
  - Surveillance des intrusions WiFi

Plan

- Le 802.11 : écosystème et fonctionnement
- Les premiers mécanismes de sécurité : failles et attaques
- Les nouveaux mécanismes de sécurité
- **Architecture des réseaux WiFi**
  - Contexte résidentiel
  - Contexte hot spot
  - Contexte entreprise
  - Surveillance des intrusions WiFi

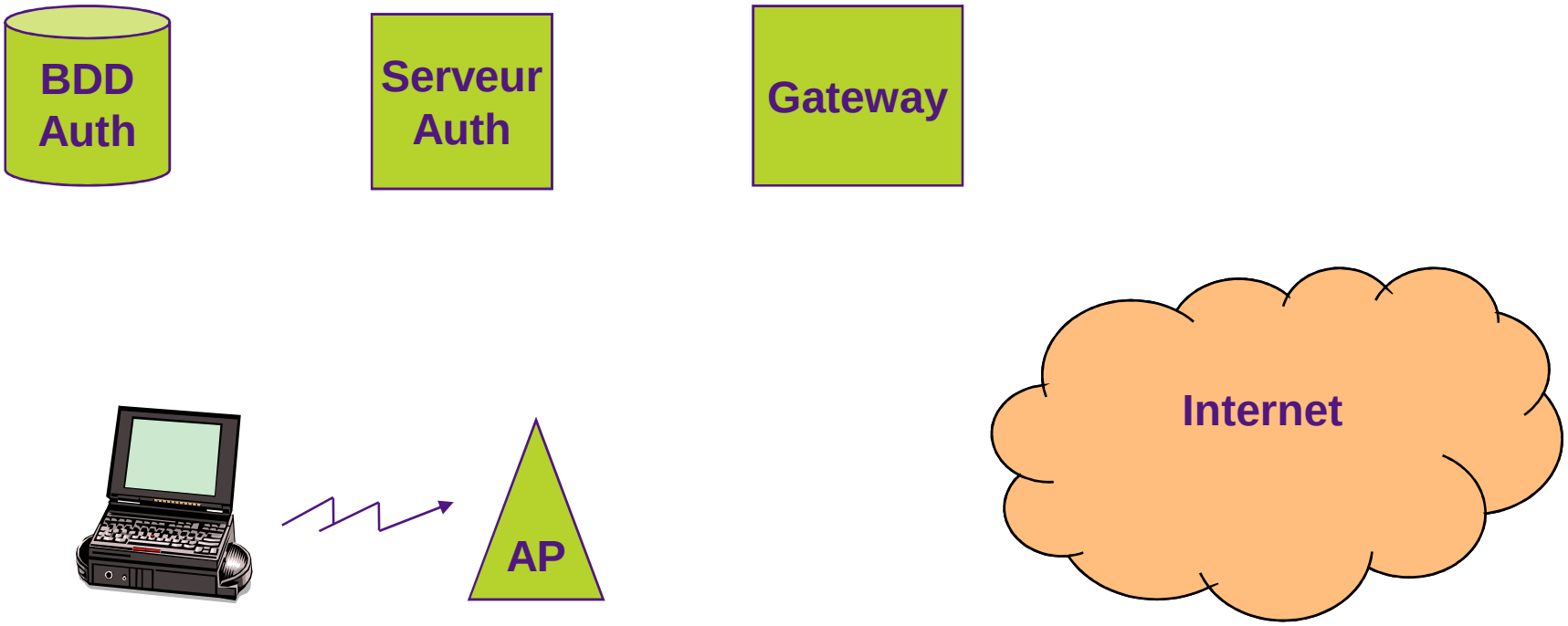
Contexte résidentiel
Solution actuelle

- **Utiliser les nouveaux mécanismes de sécurité développés dans les produits**
  - A base de WPA/WPA2 avec une PSK
  - Utilisation de TKIP ou AES-CCMP obligatoire !!!
- **Bien entendu, il faut choisir une passphrase robuste**
  - 20 caractères variants est le minimum recommandé
- **Attention certains ont eu des soucis**
  - SHA1(SSID) = PSK !

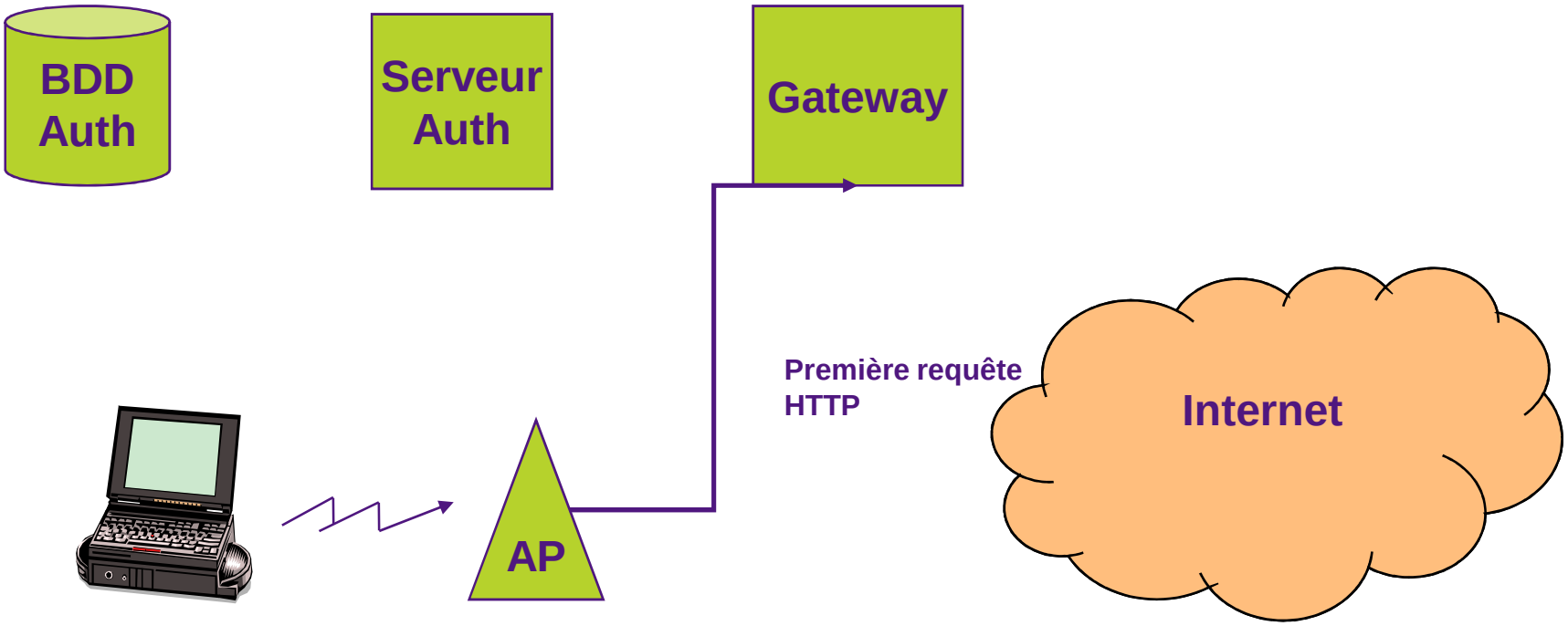
Plan

- Le 802.11 : écosystème et fonctionnement
- Les premiers mécanismes de sécurité : failles et attaques
- Les nouveaux mécanismes de sécurité
- **Architecture des réseaux WiFi**
  - Contexte résidentiel
  - Contexte hot spot
  - Contexte entreprise
  - Surveillance des intrusions WiFi

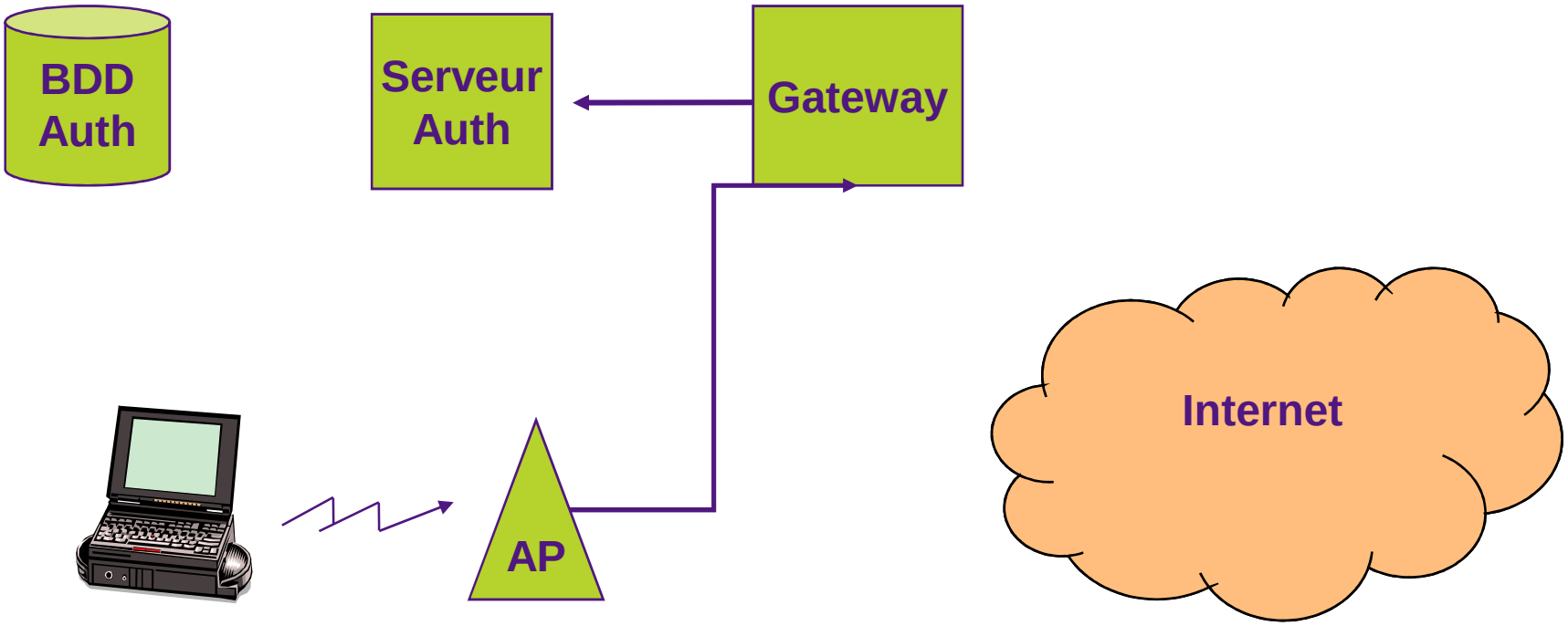
Contexte hot spot
Portail captif (1/6)



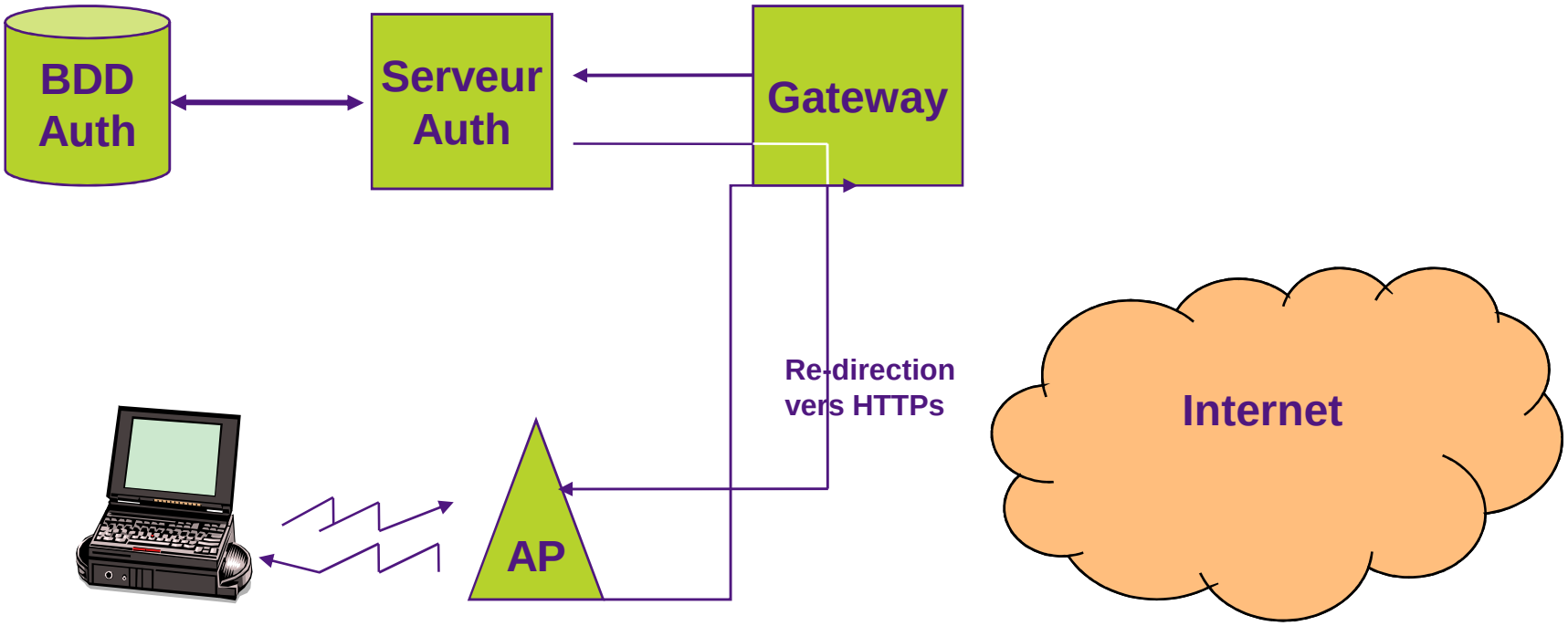
Contexte hot spot
Portail captif (2/6)



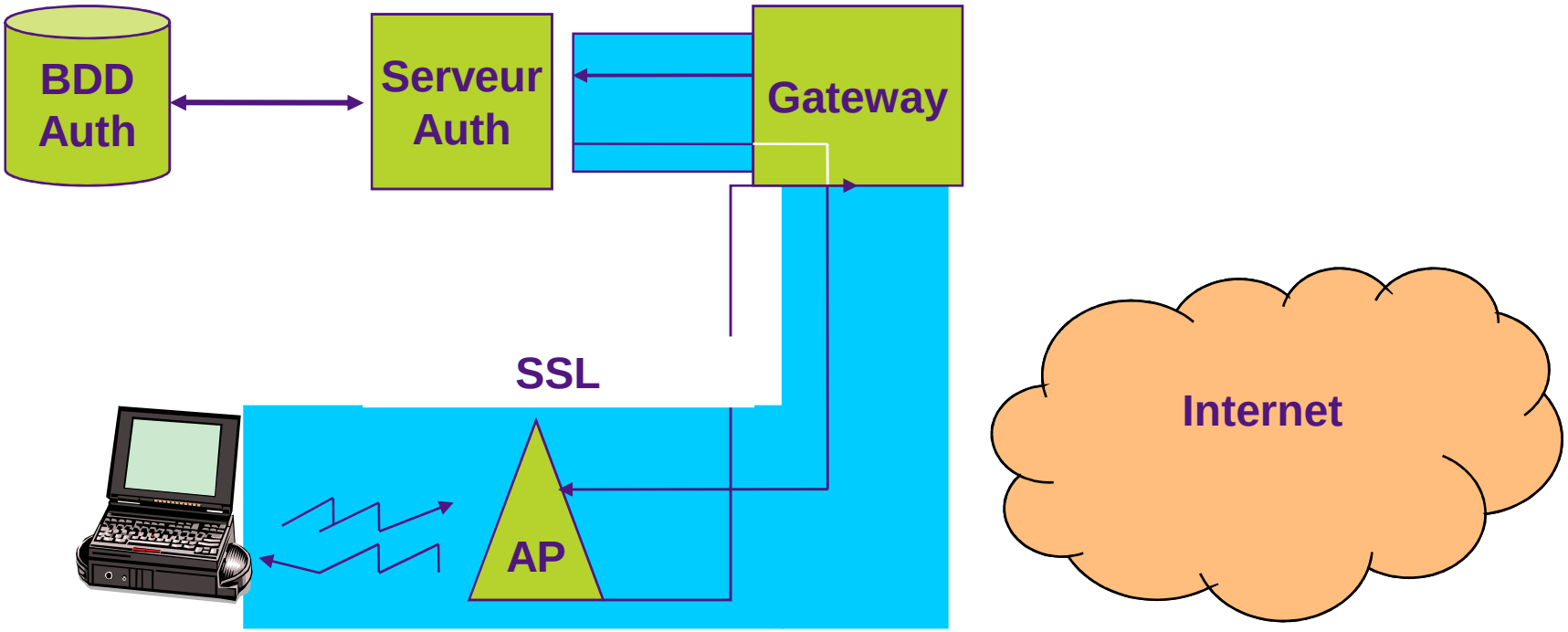
Contexte hot spot
Portail captif (3/6)



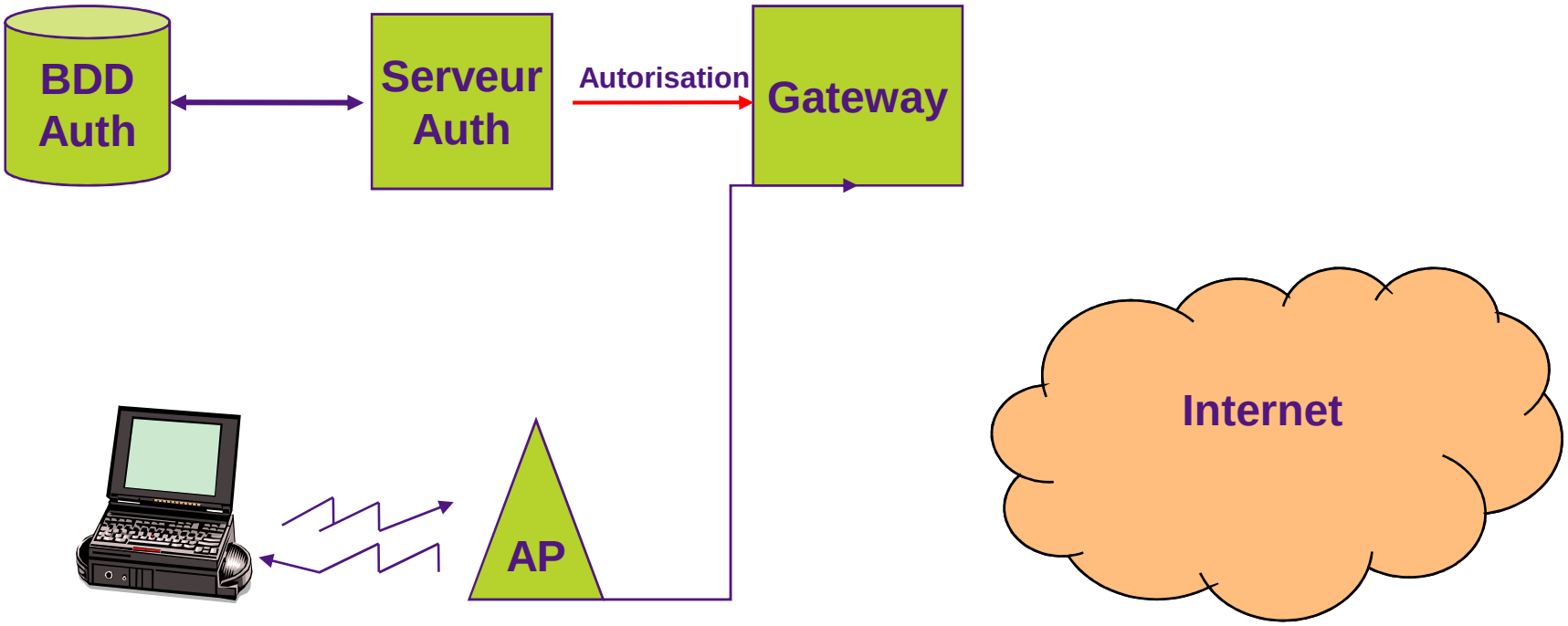
Contexte hot spot
Portail captif (4/6)



Contexte hot spot
Portail captif (5/6)



Contexte hot spot
Portail captif (6/6)



Plan

- Le 802.11 : écosystème et fonctionnement
- Les premiers mécanismes de sécurité : failles et attaques
- Les nouveaux mécanismes de sécurité
- **Architecture des réseaux WiFi**
  - Contexte résidentiel
  - Contexte hot spot
  - Contexte entreprise
  - Surveillance des intrusions WiFi

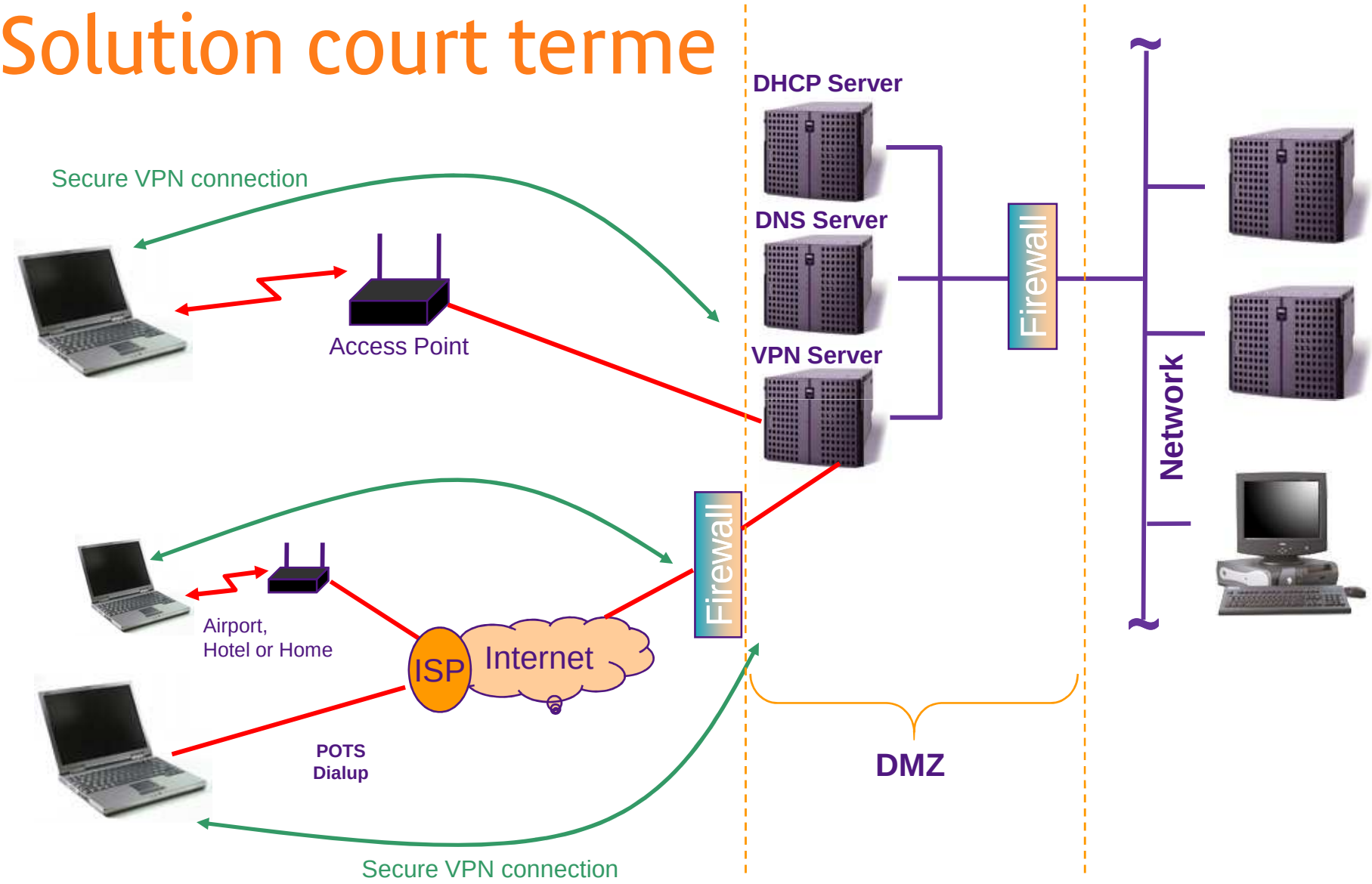
Contexte entreprise
Solution court terme

- **Utiliser les mécanismes de sécurité des couches supérieures (IPsec, SSH, TLS…)**

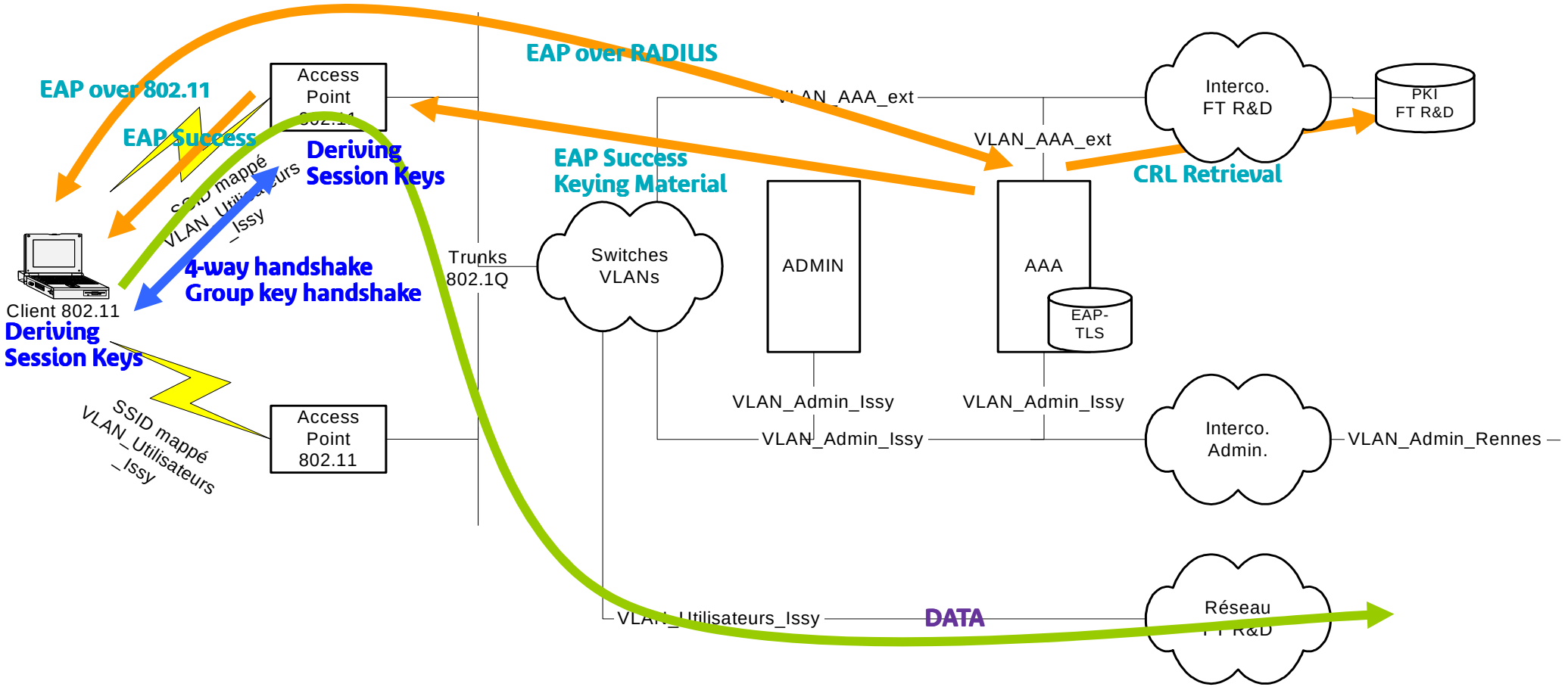
- **Impératifs :**
  - Utiliser les mécanismes de sécurité des couches supérieures (confidentialité, intégrité et authentification)
  - Contrôle d'accès avec authentification forte
  - Isolation du trafic des réseaux radio locaux IEEE 802.11 (point d'accès)

- **Déploiement à FTR&D**
  - Tunnels IPsec avec authentification forte avec certificats sur carte à puce
    - Le concentrateur VPN : Point de passage obligé des utilisateurs

Contexte entreprise
Solution court terme



Déploiement expérimental FT R&D – architecture



Contexte entreprise
Résumé

- **Court terme :**
  - Intégration des solutions existantes de sécurité au niveau 3 : IPsec
- **Moyen terme :**
  - Intégration des solutions à base de WPA et 802.1X
    - Authentification utilisateur par plusieurs modes possibles (TLS, PEAP)
    - Distribution de clés dynamiquement et par utilisateur
  - Intégration du mécanisme de confidentialité (TKIP)
- **Moyen – Long terme :**
  - Intégration des solutions à base de 802.11i
    - Authentification utilisateur par plusieurs modes possibles (TLS, PEAP)
    - Distribution de clés dynamiquement et par utilisateur
  - Intégration des nouveaux mécanismes de confidentialité (CCMP)

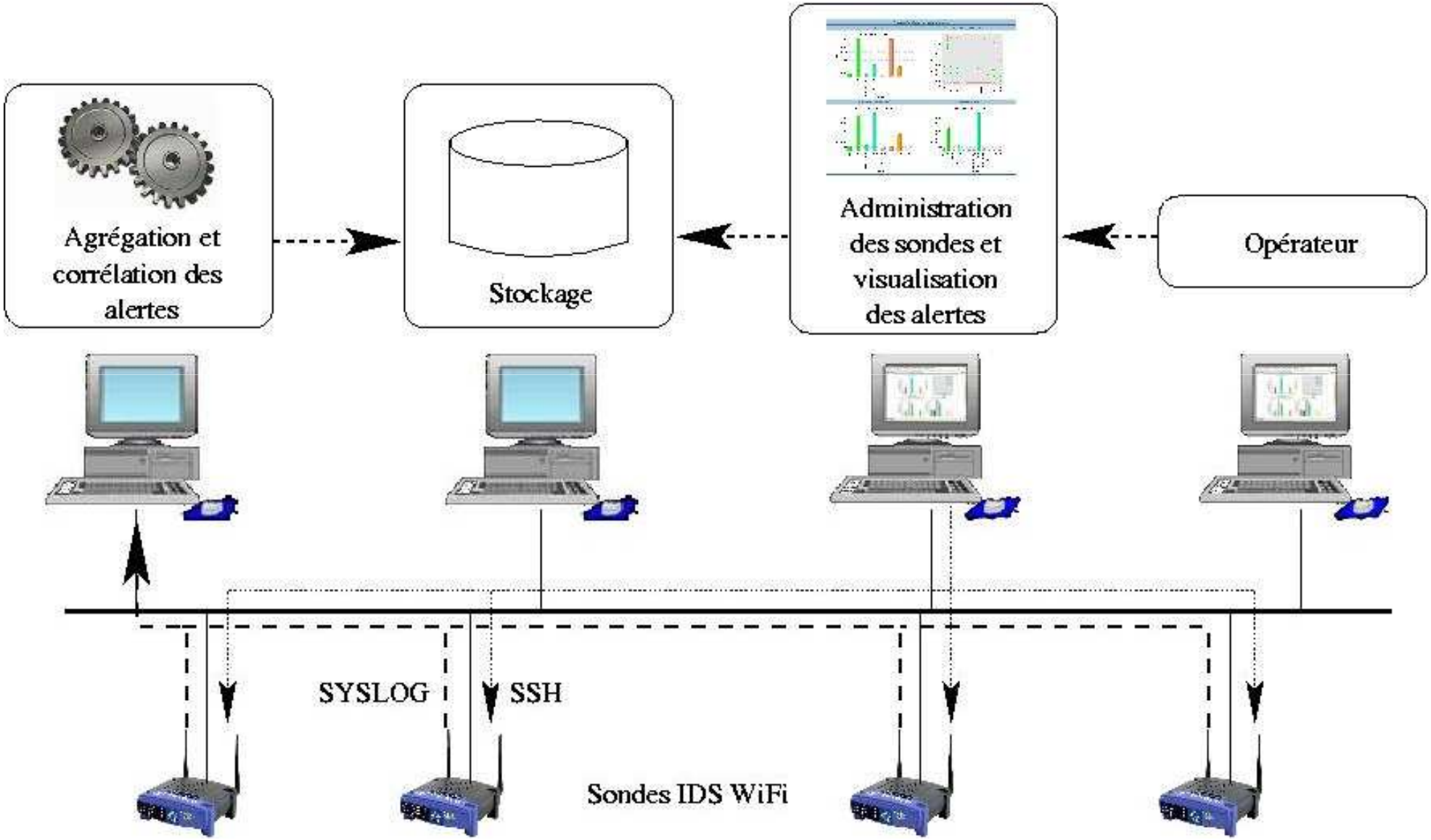
Plan

- Le 802.11 : écosystème et fonctionnement
- Les premiers mécanismes de sécurité : failles et attaques
- Les nouveaux mécanismes de sécurité
- **Architecture des réseaux WiFi**
  - Contexte résidentiel
  - Contexte hot spot
  - Contexte entreprise
  - Surveillance des intrusions WiFi

Besoins

- **Besoin d'une architecture complète de sécurité WiFi**
  - Sondes dans le réseau
  - Traitement des alertes
  - Visualisation et présentation à l'administrateur

Architecture globale



Sondes

Utilisation des APs Cisco-Linksys WRT54G

Remplacement du firmware d'origine par le firmware minimal OpenWRT

- Possibilités de rajouter des packages comme « apt-get » sous Debian,
- Utilisation du package airinvaders (IDS Wifi)

Airinvaders utilise un jeu de règles

- Analyse chaque trame
- Compare avec les précédentes (détection de spoofing)
- Selon les règles, génère des alertes SYSLOG

Alertes remontées

Format des alertes remontées

```
<@ MAC source>|<@ MAC destination>|<classification>|<sévérité>|<signature>|<champs additionnels>|
```

Exemples d'alertes :

- AP interférent

```
00:0E:D6:43:6B:AA|FF:FF:FF:FF:FF:FF|Unauthorized AP|2|RogueAP|rssi=-85|ssid=maison|channel=0A|
```

- Spoofing

```
00:0E:D6:43:6B:AA|FF:FF:FF:FF:FF:FF|Spoofing|2|AP MAC Spoofing|rssi=-70|spoofing_type=Timestamp Difference|
```

- Scans

```
00:0B:43:36:47:D4|FF:FF:FF:FF:FF:FF|Info|1|STA Searching AP|rssi=-78|ssid_searched=I2E_TELBUS_PETIT|
```

- Scan Netstumbler

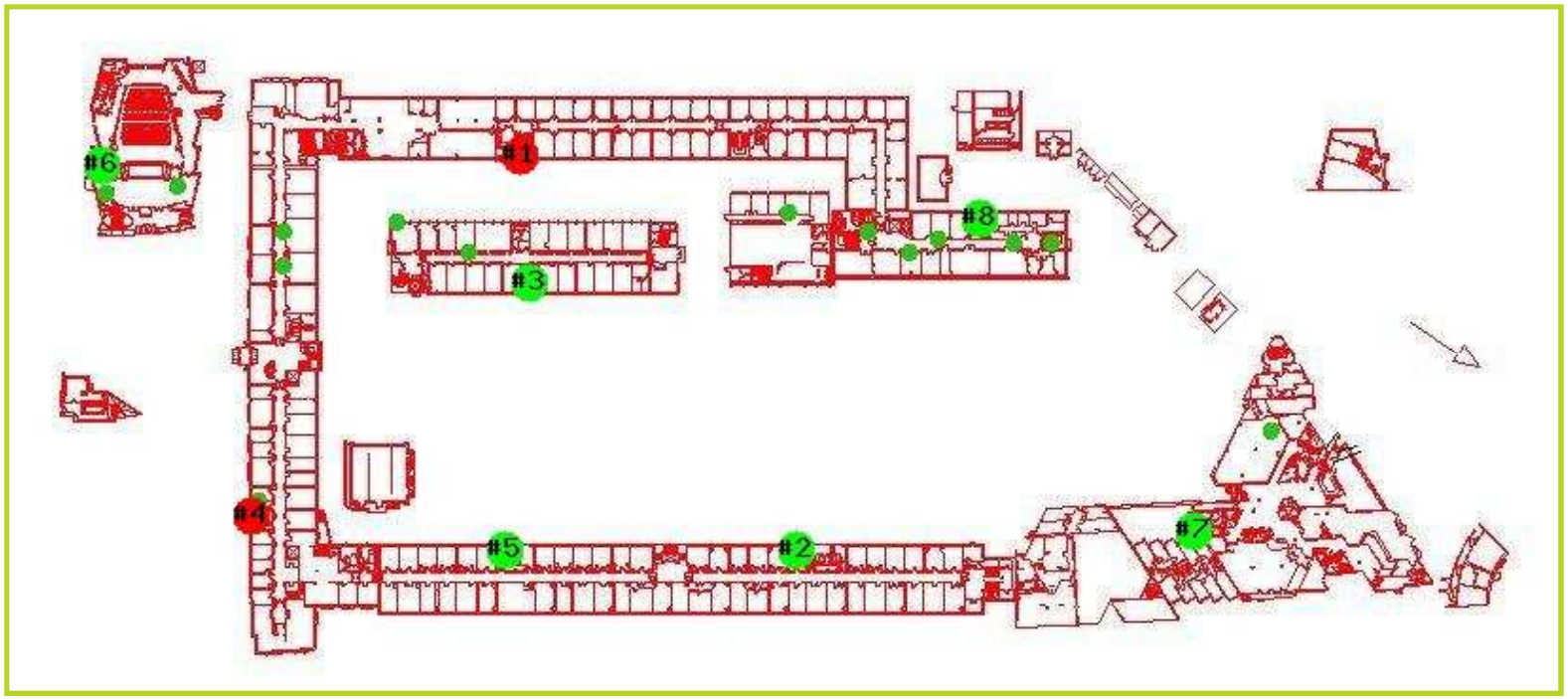
```
00:0B:43:36:47:D4|FF:FF:FF:FF:FF:FF|Scan|2|Scanner Signature|rssi=-93|scan_type=Netstumbler 0.4.0|
```

- Broadcasted SSID

```
00:03:4B:12:A3:B7|FF:FF:FF:FF:FF:FF|Info|1|Broadcasted SSID|rssi=-68|ssid=WifiFT|channel=01|
```

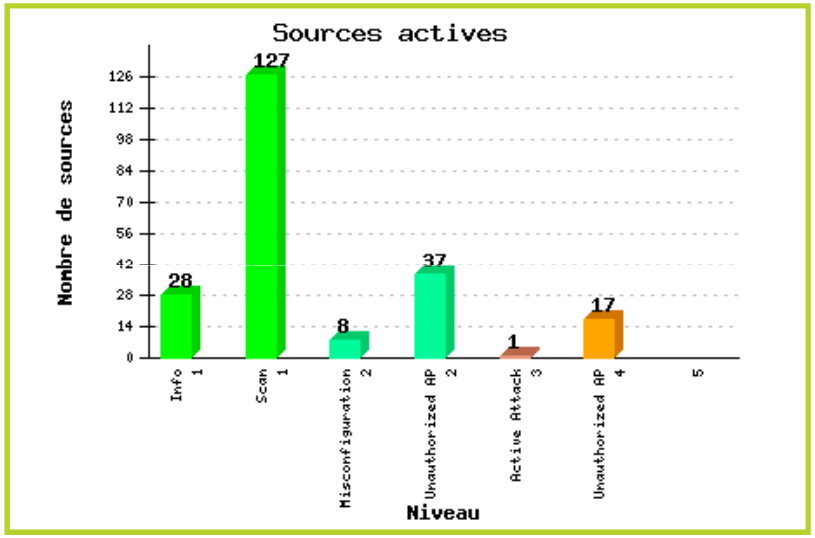
- … + de 70 types d'alertes différents

Localisation des sondes



Visualisation des alertes

Répartition des alertes par niveau de sévérité, par classification



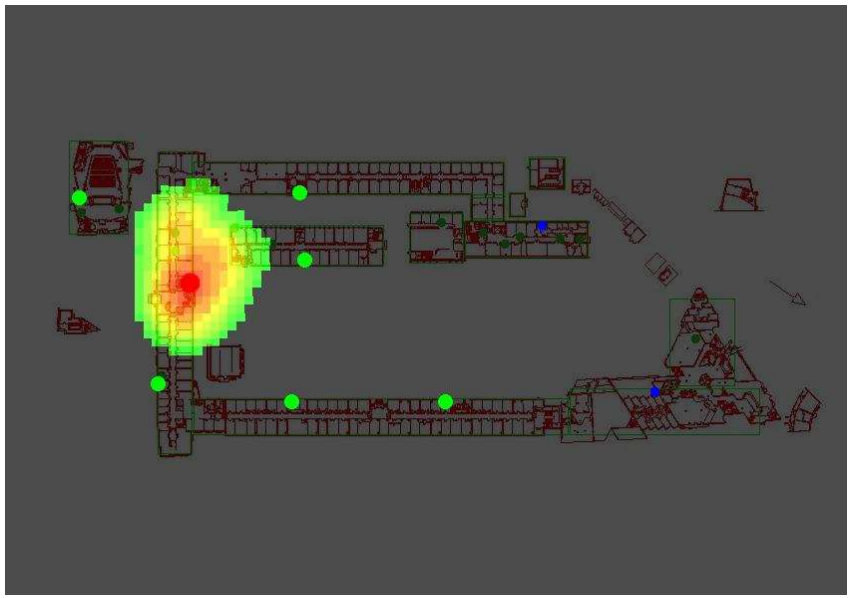
Aperçu des points d'accès

- Illégitimes
- Interférents (voisins)
- Autorisés

Résumé des attaques de type Spoofing

Module de géolocalisation

- **Utiliser les RSSI (Received Signal Strength Indicator) remontés par les sondes pour géolocaliser un équipement**



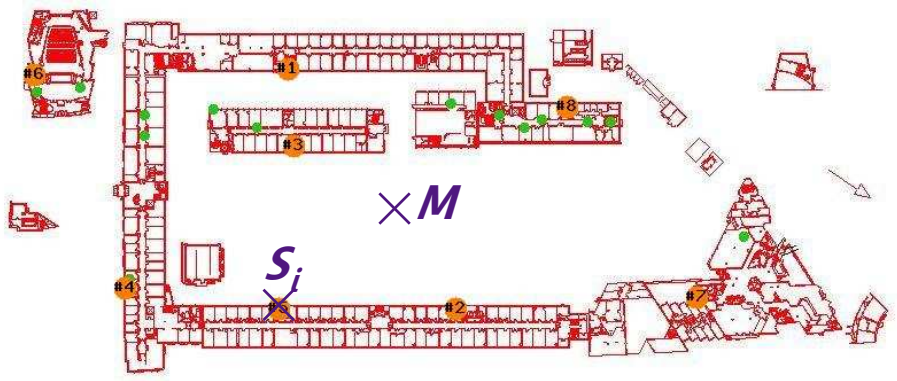
- **Contrainte : pas de cartographie préalable de la zone (fastidieux !!!)**
  - Nécessité d'utiliser des modèles de propagation

Système à résoudre

- **Même si positions fixes de la sonde et de l'émetteur, fortes variations de la puissance de signal reçu (RSSI).**
  - Utilisation du maximum de puissance reçue sur une certaine plage temporelle

- **Une équation par sonde ayant capté le signal:**

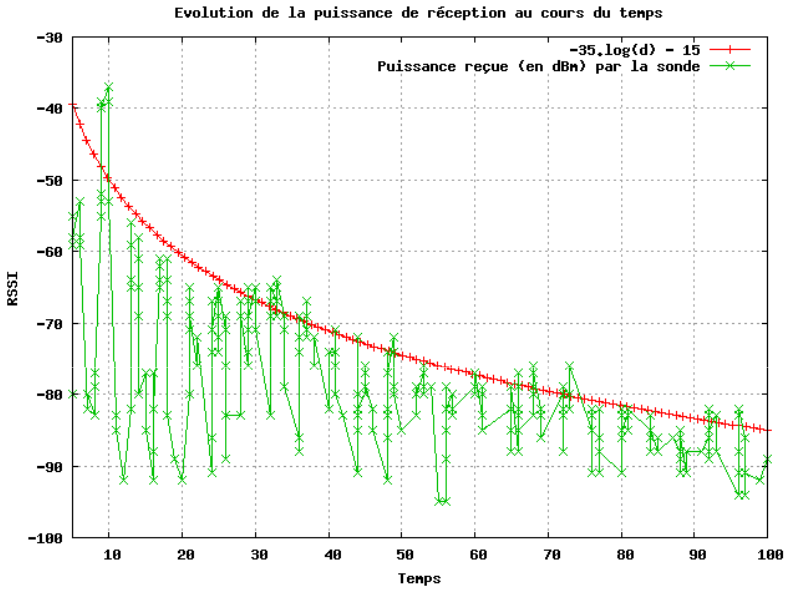
$$(S)\begin{cases} RSSI(S_1) = P_e + C - A(S_1 \leftrightarrow M) \\ RSSI(S_2) = P_e + C - A(S_2 \leftrightarrow M) \\ \dots \\ RSSI(S_i) = P_e + C - A(S_i \leftrightarrow M) \\ \dots \\ RSSI(S_n) = P_e + C - A(S_n \leftrightarrow M) \end{cases}$$



- P_e : puissance d'émission
- C : constante
- $A(S \leftrightarrow M)$: atténuation de la puissance de l'onde sur son parcours entre S et M

Quel modèle de propagation ? (1)

Espace ouvert



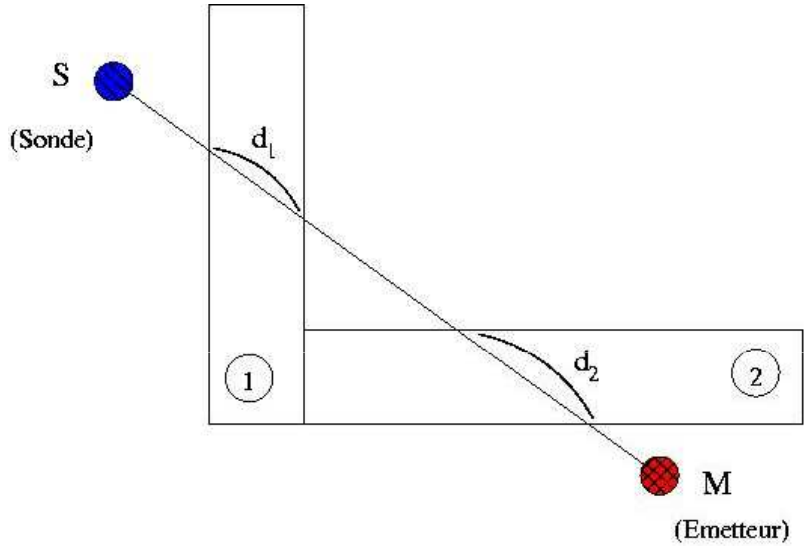
$$A(S \leftrightarrow M) = 10\eta log(d_S(M))$$

- $d_S(M)$: distance entre le point M et la sonde

On trouve η=3,5

Quel modèle de propagation ? (2)

Prise en compte des bâtiments (modélisation par des rectangles)

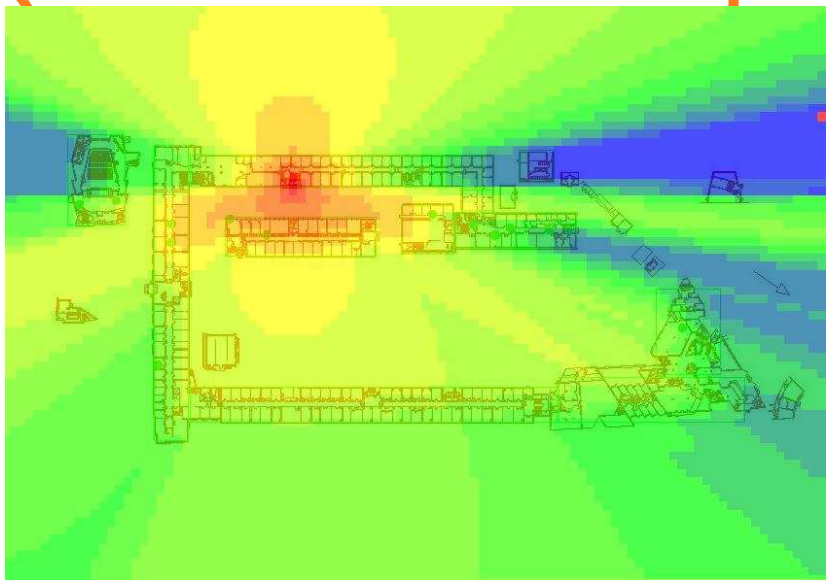


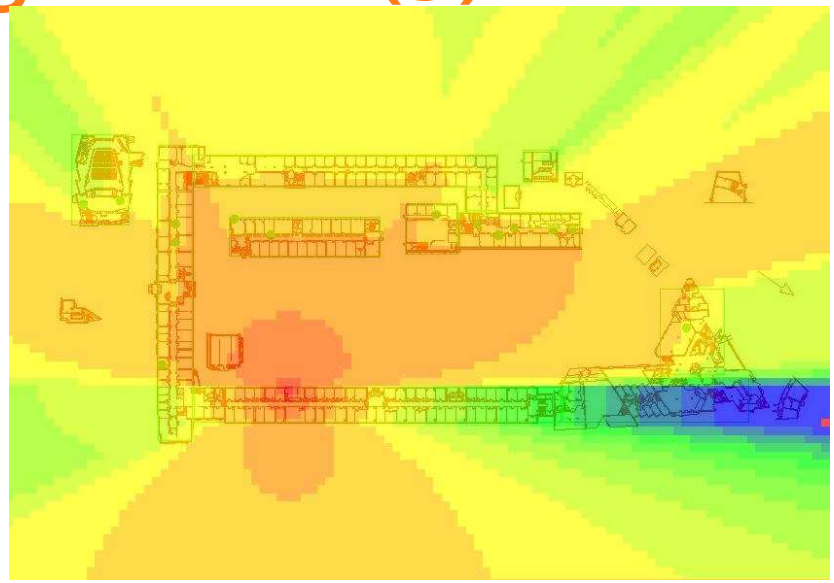
$$A(S \leftrightarrow M) = 35log(d) + \mu A_{mur}(\sum_{i=1}^{N} d_i)$$

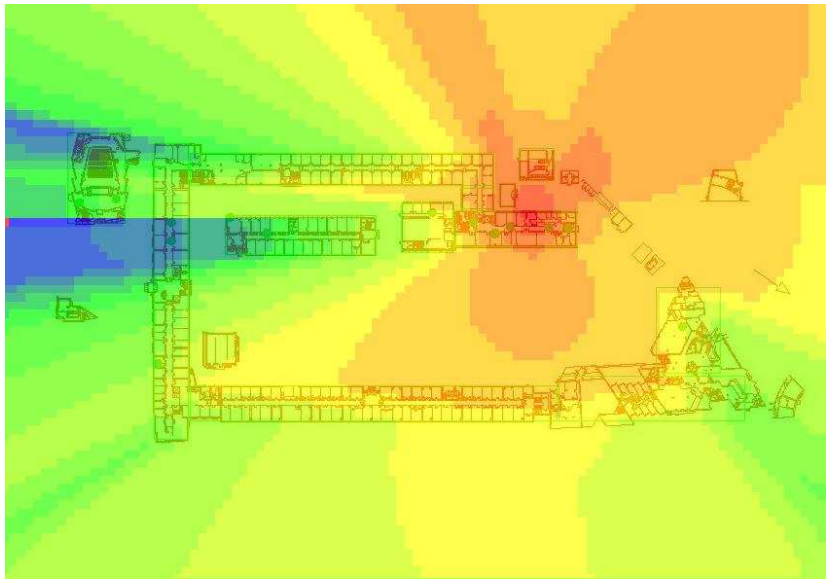
$$\mu = 0.12, A_{mur} = 13dB.$$

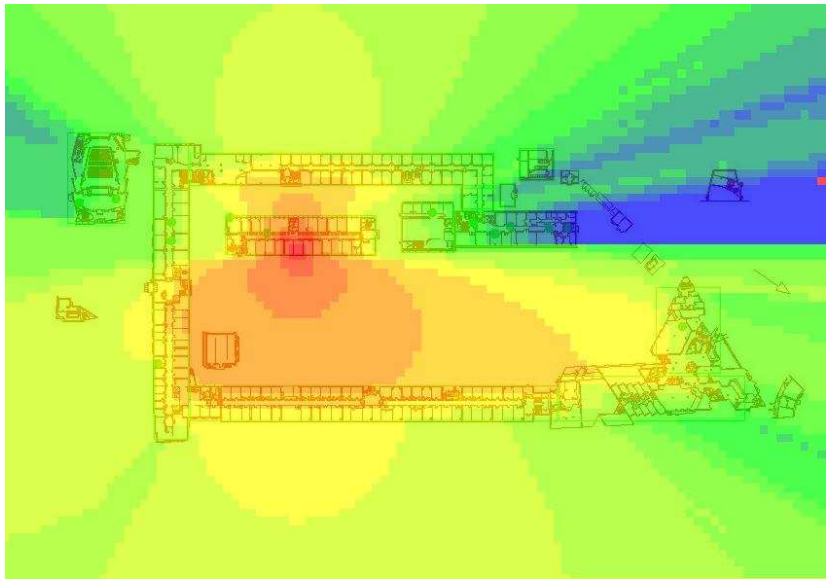
- μ : densité linéïque de murs dans les bâtiments (nombre de murs traversés par u. de distance)
- A_{mur} : atténuation due à la traversée d'un mur.

Quel modèle de propagation ? (3)









Quelle méthode de résolution ? (1)

- **Résolution numérique (« point par point ») du système**

$$(S)\begin{cases} RSSI(S_1) = P_e + C - A(S_1 \leftrightarrow M) \\ RSSI(S_2) = P_e + C - A(S_2 \leftrightarrow M) \\ \dots \\ RSSI(S_i) = P_e + C - A(S_i \leftrightarrow M) \\ \dots \\ RSSI(S_n) = P_e + C - A(S_n \leftrightarrow M) \end{cases}$$

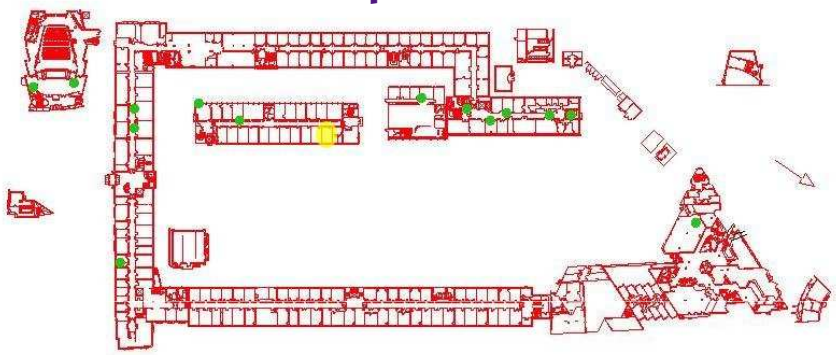
- **Méthode 1 : différence 2 à 2 des équations et évaluation de la fonction *f(M)* en chaque point M de la carte :**

$$f(M) = exp(-\sum_{i=1}^{n-1}(RSSI(S_{i+1}) - RSSI(S_i) + (A(S_{i+1} \leftrightarrow M) - A(S_i \leftrightarrow M)))^2.$$

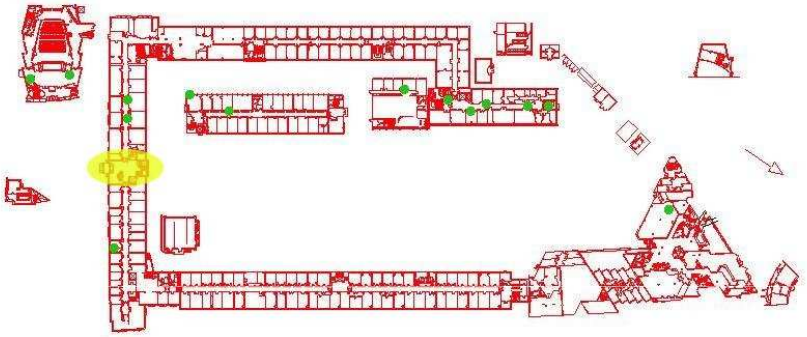
Quelle méthode de résolution ? (2)

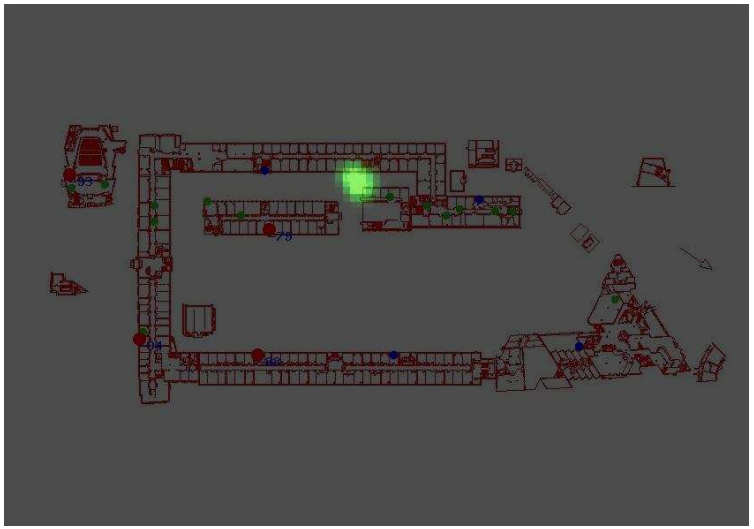
Modèle « espace ouvert » avec la première méthode de résolution :

Expérience 1



Expérience 2

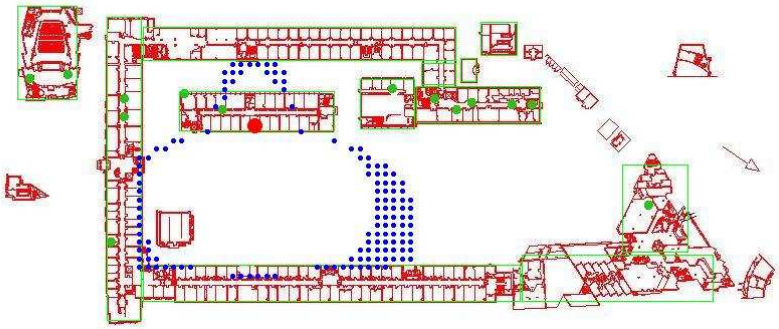




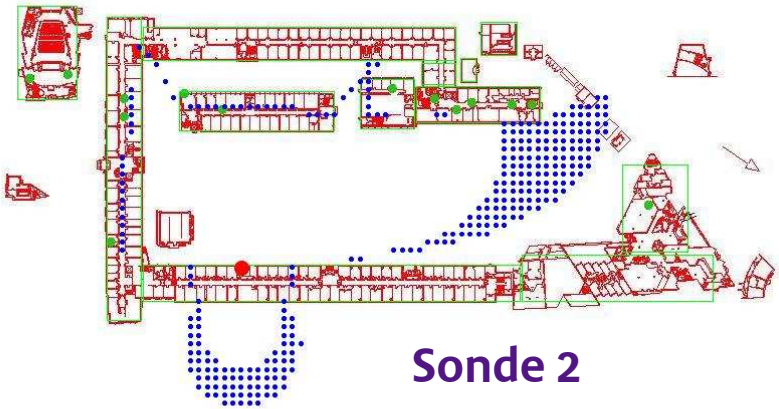
Quelle méthode de résolution ? (3)

Résolution de chaque équation (à 3% près)

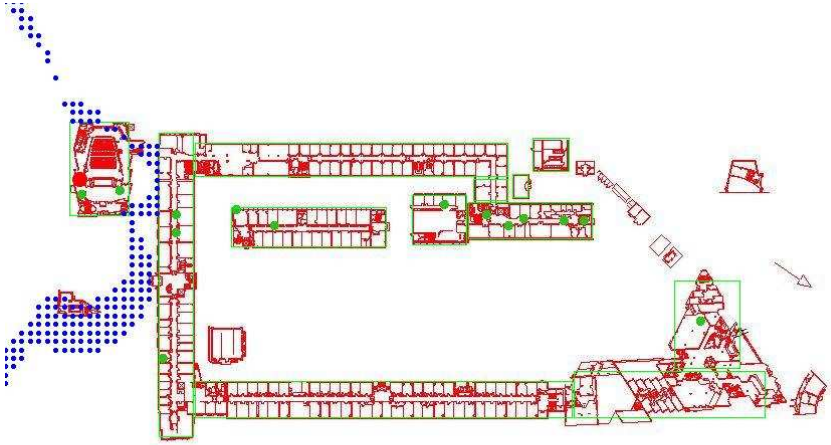
$$RSSI(S_i) = P_e + C - A(S_i \leftrightarrow M)$$



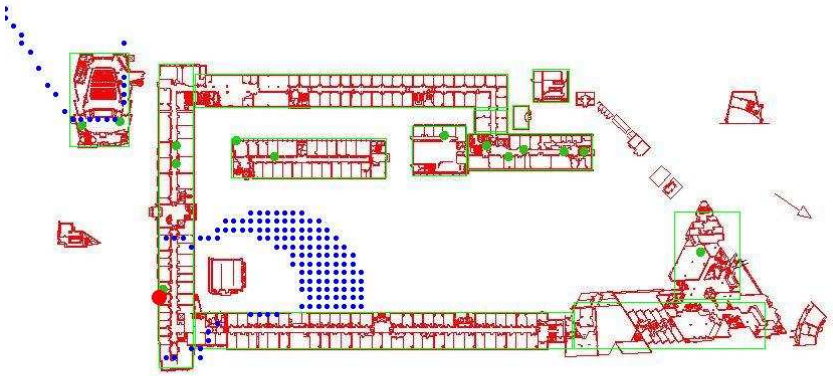
Sonde 1



Sonde 2



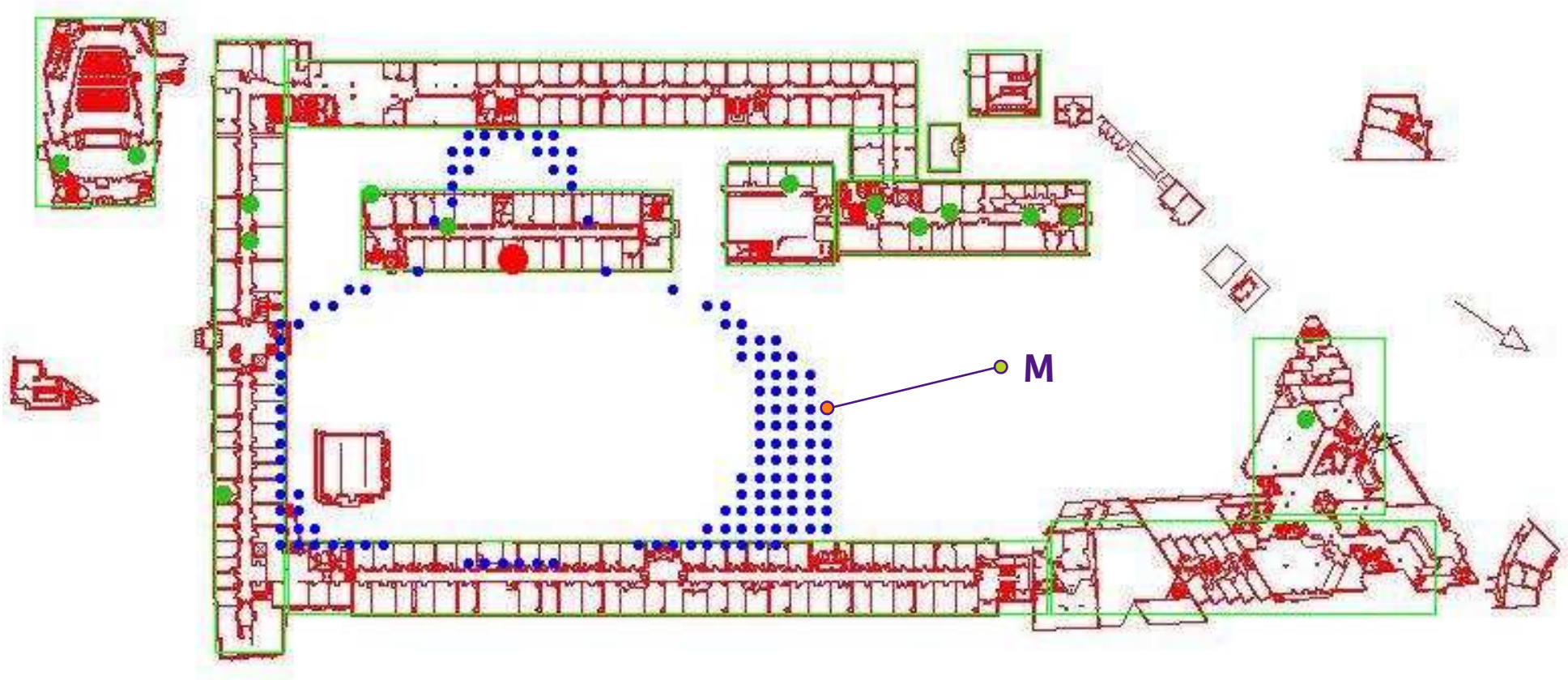
Sonde 3



Sonde 4

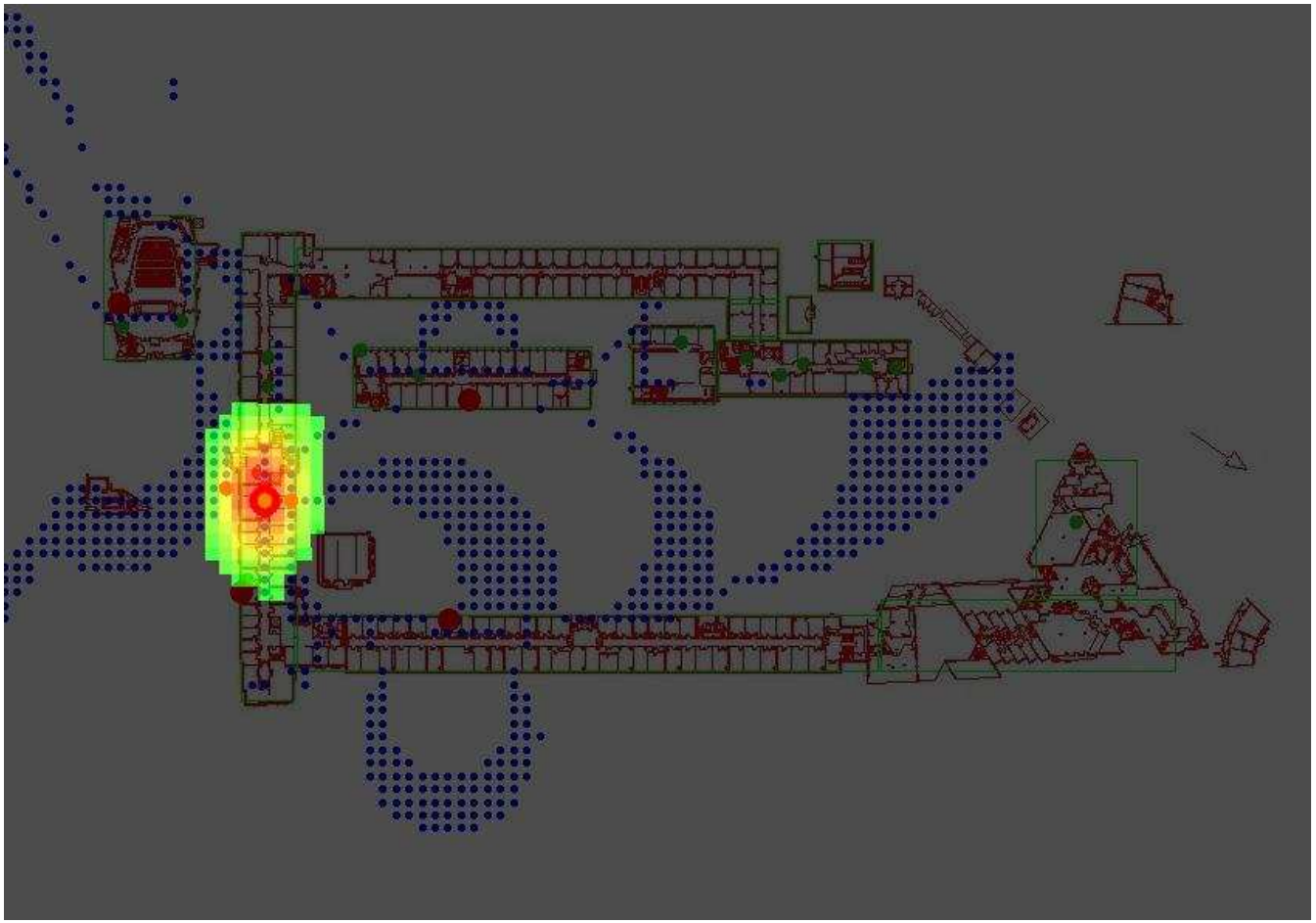
Quelle méthode de résolution ? (4)

- **Distance d'un point M à un ensemble de solutions**



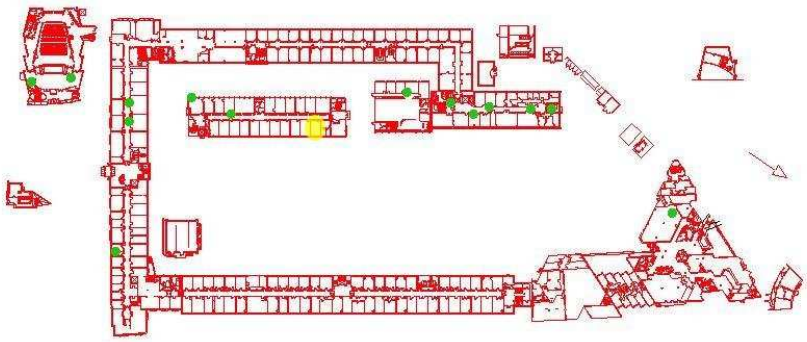
Quelle méthode de résolution ? (5)

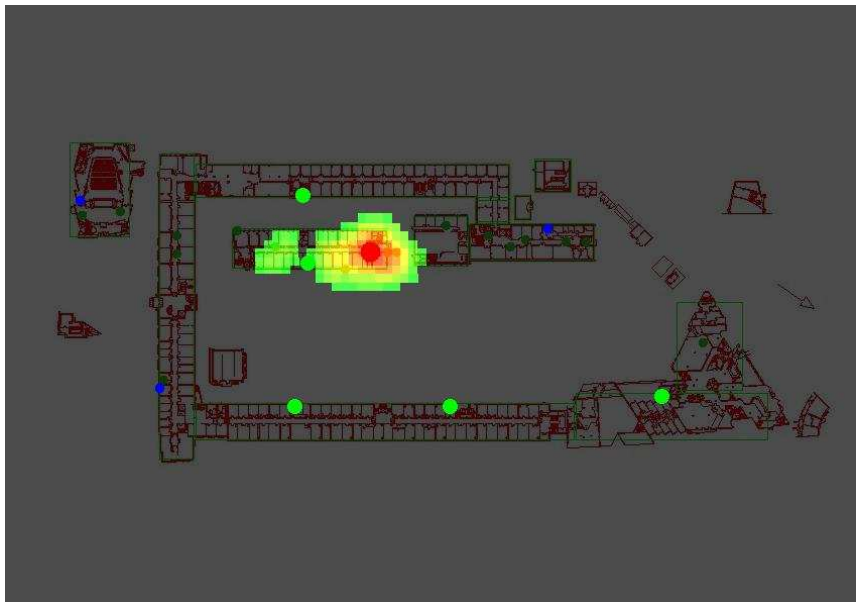
- **Ensemble des points qui minimisent la somme des distances (à une marge près)**



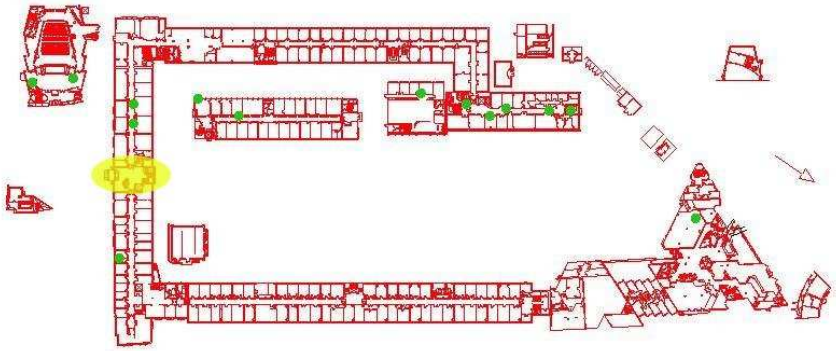
Quelle méthode de résolution ? (6)

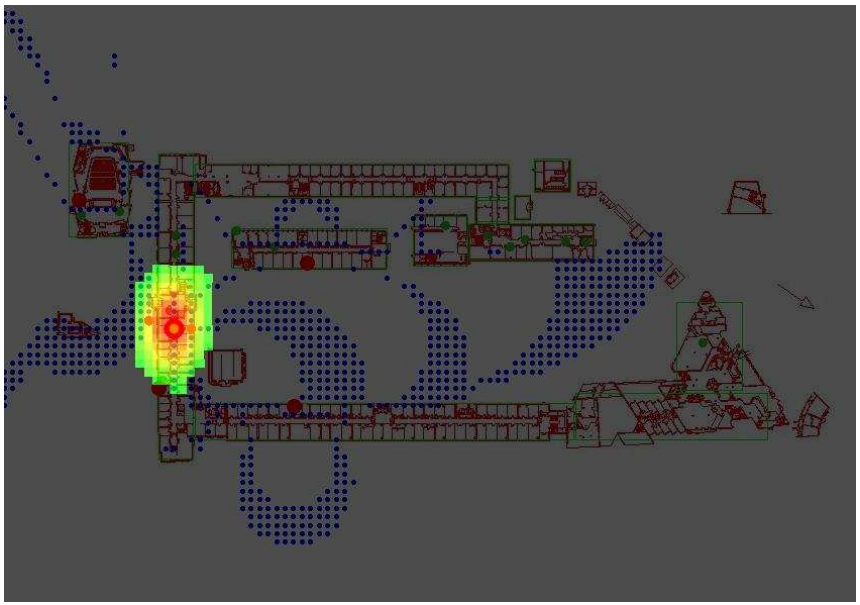
Expérience 1





Expérience 2





Fin !

- **Merci pour votre attention !**

- **Des questions ?**