Technologies WiFi

Frédéric Weis
Frederic.Weis@univ-rennes1.fr

Université Rennes 1 - IUT Saint-Malo
Département Réseaux et Télécommunications

-

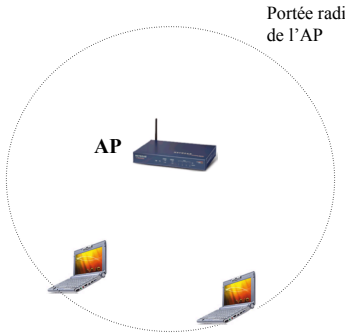
Octobre 2018

Les aspects clés

➢**Mode « réseau local sans fil » (WLAN)**
Wifi ou 802.11 ?
Sécurité WiFi
Qualité de service
Gestion de la mobilité
AP lourd ou AP léger ?

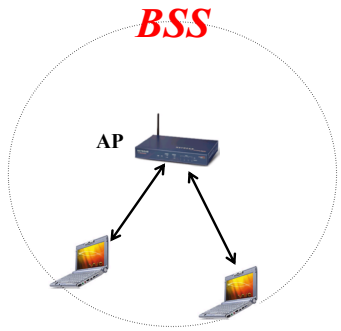
Mode « WLAN sans fil »

- Deux éléments
  - AP (*Access Point*)
  - Station mobile, équipée d'une carte de communication sans fil



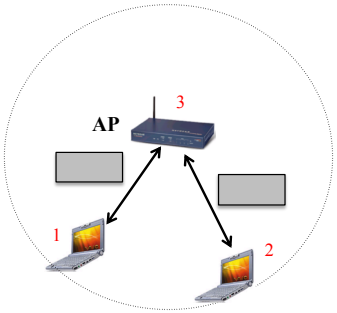
Mode « WLAN sans fil »

- Deux éléments
  - AP (*Access Point*)
  - Station mobile, équipée d'une carte de communication sans fil
- Toutes les communications au sein d'une cellule (**BSS** – *Basic Service Set*) passent par l'AP



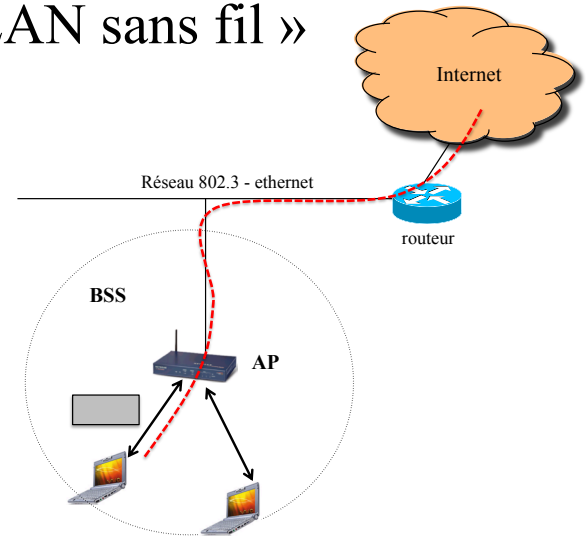
Mode « WLAN sans fil »

- Deux éléments
  - AP (*Access Point*)
  - Station mobile, équipée d'une carte de communication sans fil
- Toutes les communications au sein d'une cellule (**BSS** – *Basic Service Set*) passent par l'AP
- Une trame 802.11 comporte trois adresses MAC
  - 1- source, 2 - destination, 3 - BSSID (adresse de l'AP)



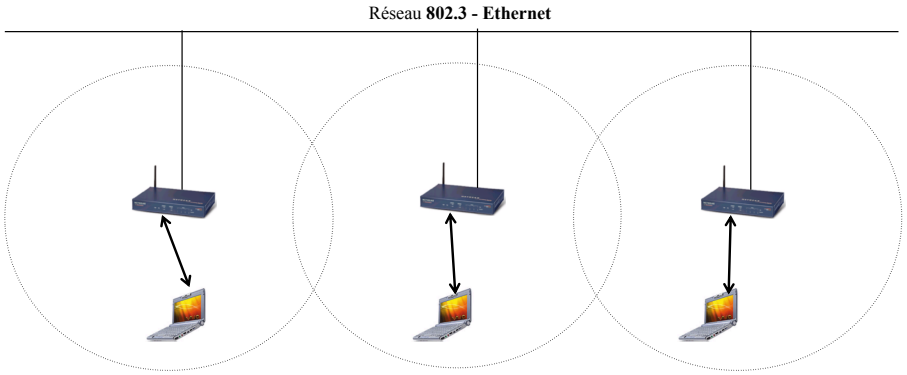
Mode « WLAN sans fil »

- Un AP dispose d'une interface de connexion Ethernet
- Un AP « assure » le passage automatique (sans configuration) et transparent du BSS 802.11 vers le réseau Ethernet auquel il est connecté



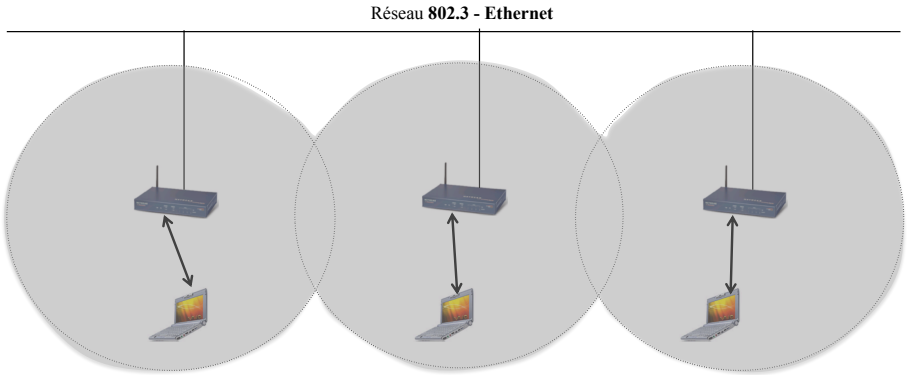
Mode « WLAN sans fil »

Mode **infrastructure** = connexion de plusieurs APs sur le réseau Ethernet



Mode « WLAN sans fil »

Intérêt : couverture WiFi étendue
Problématique : exploitation propre des différents canaux WiFi



Mode « WLAN sans fil »

Réseau d'entreprise

 **APs** + Réseau de « distribution » (**802.3 - Ethernet**) +  routeur

Mode « WLAN sans fil »

Réseau d'entreprise

 **APs** + Réseau de « distribution » (**802.3 - Ethernet**) +  routeur

WiFi (mono AP)
Commutateur Ethernet
Accès IP (ADSL, FTTH)

Box opérateur
réseau « personnel »

Les aspects clés

Mode « réseau local sans fil » (WLAN)
- **Wifi ou 802.11 ?**

Sécurité WiFi
Qualité de service
Gestion de la mobilité
AP lourd ou AP léger ?

802.11 ou WiFi ?

- 802.11
  - IEEE 802.11 = une famille de normes IEEE pour les réseaux locaux sans fil
  - 802.11 (norme d'origine), 802.11b – 802.11 g – 802.11a – 802.11n – 802.11 ac (normes radio), 802.11i (sécurité), 802.11e (qualité de service) etc.

802.11 ou WiFi ?

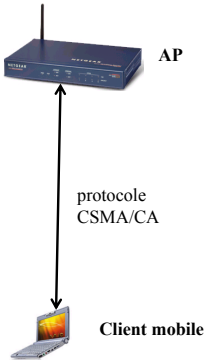
- 802.11
  - IEEE 802.11 = une famille de normes IEEE pour les réseaux locaux sans fil
  - 802.11 (norme d'origine), 802.11b – 802.11 g – 802.11a – 802.11n – 802.11 ac (normes radio), 802.11i (sécurité), 802.11e (qualité de service) etc.
- WiFi
  - Une programme de certification garantissant le respect de **certaines** des normes 802.11
  - Ex. : label WPA2 sur un produit WiFi = respect de la norme 802.11i (sécurité WiFi)
- Dans la suite du cours, nous utilisons indifféremment les termes 802.11 et WiFi

Les aspects clés

Mode « réseau local sans fil » (WLAN)
Wifi ou 802.11 ?
➢ **Sécurité WiFi**
Qualité de service
Gestion de la mobilité
AP lourd ou AP léger ?

Que vise la sécurité WiFi ?

*Protection du lien radio entre l'AP et le client mobile, via **deux mécanismes***



Que vise la sécurité WiFi ?

Mécanisme 1

***Contrôle d'accès au réseau WiFi** = authentification de la station mobile à son entrée dans le réseau*

Que vise la sécurité WiFi ?

Mécanisme 1

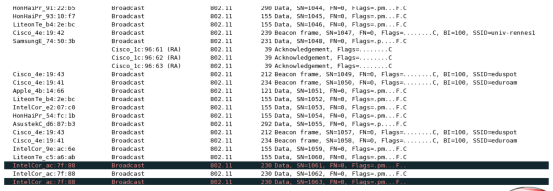
Contrôle d'accès au réseau WiFi = *authentification de la station mobile à son entrée dans le réseau*

AP -> validation de l'identité du client mobile

Données d'authentification (*login* + *mdp* ou *mdp* ou *certificat électronique*)

Entrée du client mobile de la réseau WiFi

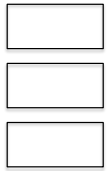
Que vise la sécurité WiFi ?



Capture des trames 802.11 par écoute passive du canal WiFi exploité par l'AP

AP

Trames 802.11



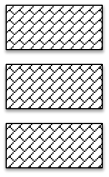
Client mobile

Que vise la sécurité WiFi ?

Mécanisme 2

Chiffrement des trames 802.11 entre l'AP et le client mobile = protection contre les écoutes

AP



Trames 802.11 **chiffrées**

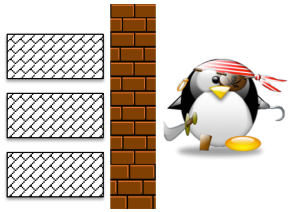
Client mobile

Que vise la sécurité WiFi ?

Mécanisme 2

Chiffrement des trames 802.11 entre l'AP et le client mobile = protection contre les écoutes

AP

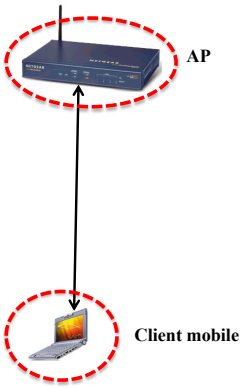


Client mobile

Qui implémente la sécurité WiFi ?

L'authentification et le chiffrement sont configurés au niveau du client mobile et de l'AP

Spécifications WiFi = WPA et WPA2
WPA = WiFi *Protected Access*



Les aspects clés

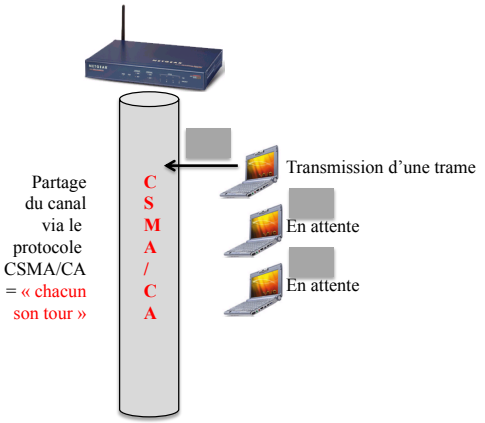
Mode « réseau local sans fil » (WLAN)
Wifi ou 802.11 ?
Sécurité WiFi
➢ **Qualité de service**
Gestion de la mobilité
AP lourd ou AP léger ?

Limites du lien radio

Canal radio configuré au niveau de l'AP

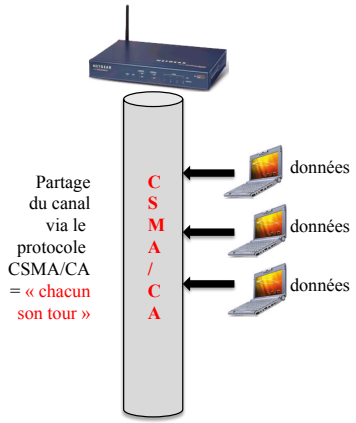
Par ex. canal 6 dans la bande à 2,4 GHz

Limites du lien radio



Partage du canal via le protocole CSMA/CA = « chacun son tour »

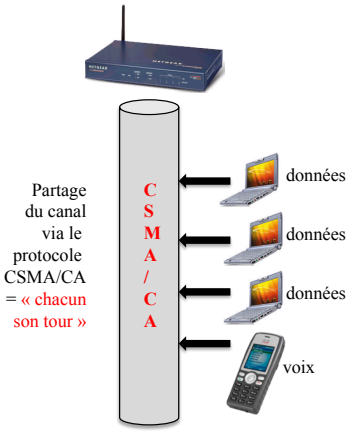
Limites du lien radio



CSMA/CA :
Probabilité d'accès
au canal identique
pour toutes les stations

Limites du lien radio

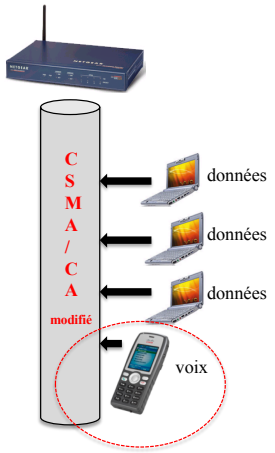
La voix ne doit pas être transmise de la même manière que les données



CSMA/CA :
Probabilité d'accès
au canal identique
pour toutes les stations

Limites du lien radio

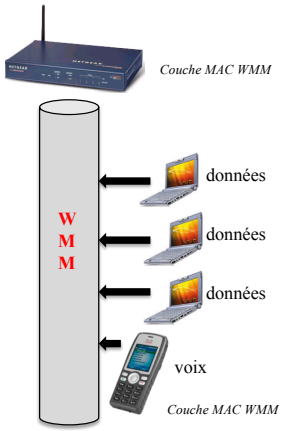
Modification du protocole CSMA/CA pour rendre « plus » prioritaire le trafic voix dans l'accès au canal radio



Limites du lien radio

spécification WMM (WiFi multimedia)

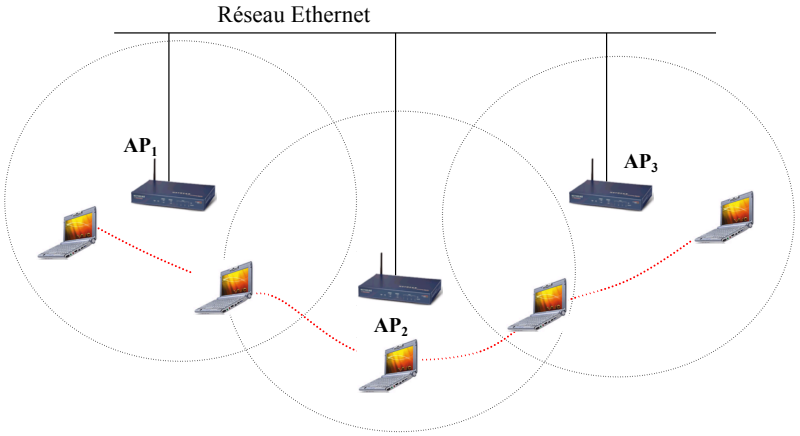
Temps d'accès
au canal fonction de
la nature des données
transmises



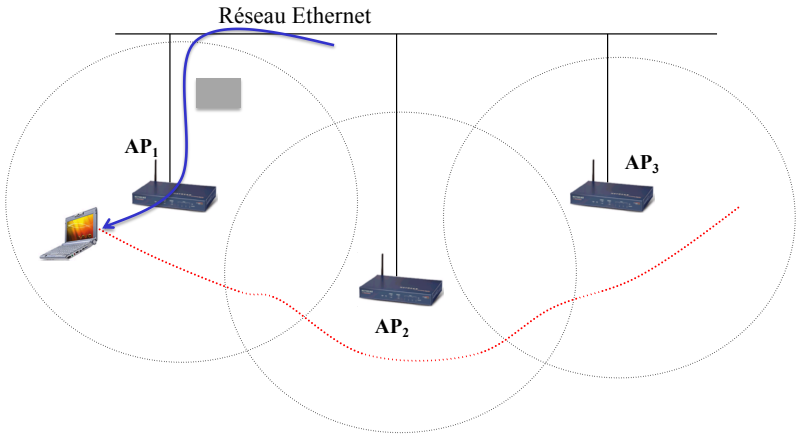
Les aspects clés

Mode « réseau local sans fil » (WLAN)
Wifi ou 802.11 ?
Sécurité WiFi
Qualité de service
➢ **Gestion de la mobilité**
AP lourd ou AP léger ?

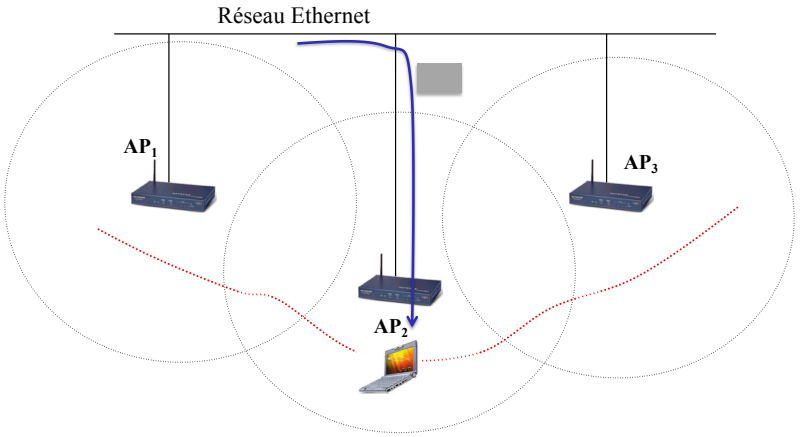
Réseau WiFi étendu



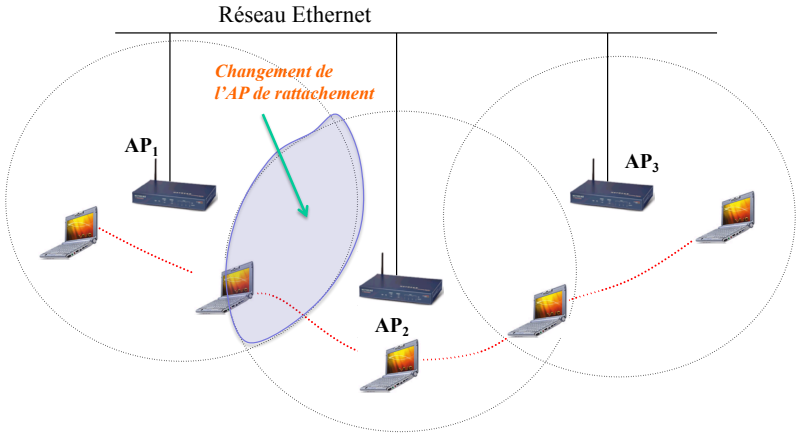
Réseau WiFi étendu



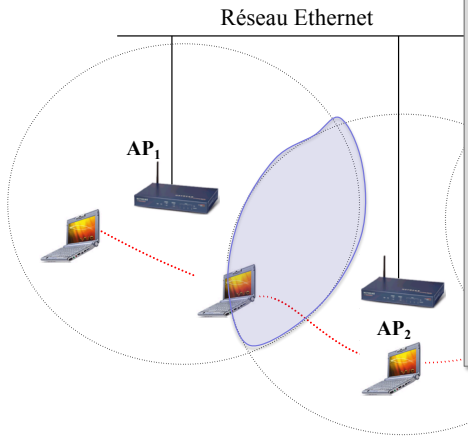
Réseau WiFi étendu



Gestion de la mobilité



Gestion de la mobilité = *handover*



Détachement de
AP_1 puis rattachement
à AP_2

Pour un service voix :
Doit être inférieur à
100 ms

Normes IEEE 802.11r/k
Certification WiFi
« voice enterprise »

Les aspects clés

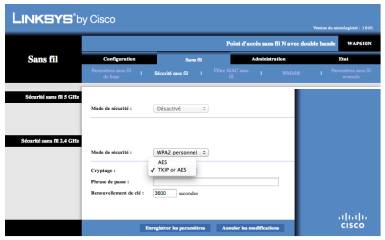
Mode « réseau local sans fil » (WLAN)
Wifi ou 802.11 ?
Sécurité WiFi
Qualité de service
Gestion de la mobilité
➢ **AP lourd ou AP léger ?**

Configuration d'un AP

AP

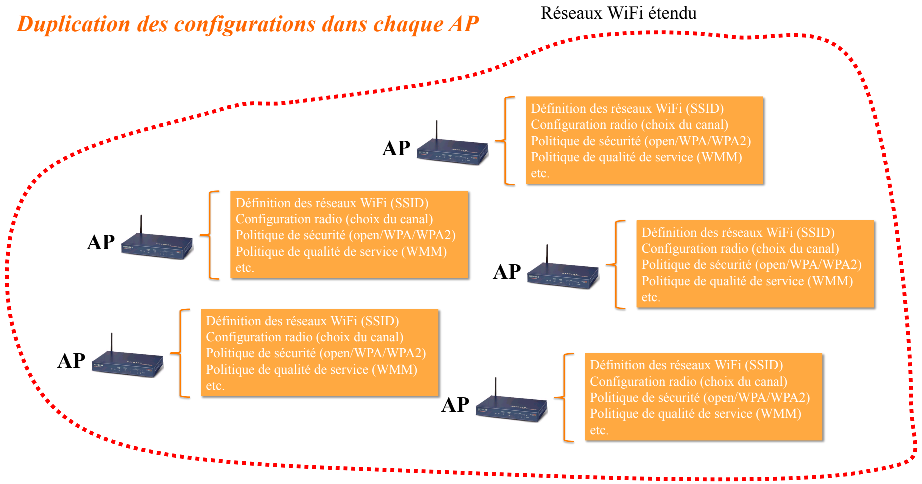
Configuration locale

Définition des réseaux WiFi (SSID)
Configuration radio (choix du canal)
Politique de sécurité (open/WPA/WPA2)
Politique de qualité de service (WMM)
etc.



Configuration des plusieurs APs

Duplication des configurations dans chaque AP



Principe d'un AP *léger*

- L'AP est piloté par un équipement spécifique connecté au réseau Ethernet
  - Un contrôleur
- Le contrôleur a la capacité de piloter plusieurs APs simultanément
- AP léger = AP déchargé d'une partie de ces fonctions vers le contrôleur
  - Les mécanismes WiFi / 802.11 sont assurés par le couple contrôleur / AP léger
  - Transparent pour le client mobile, pas de modification des standards 802.11

Plate-forme d'APs légers

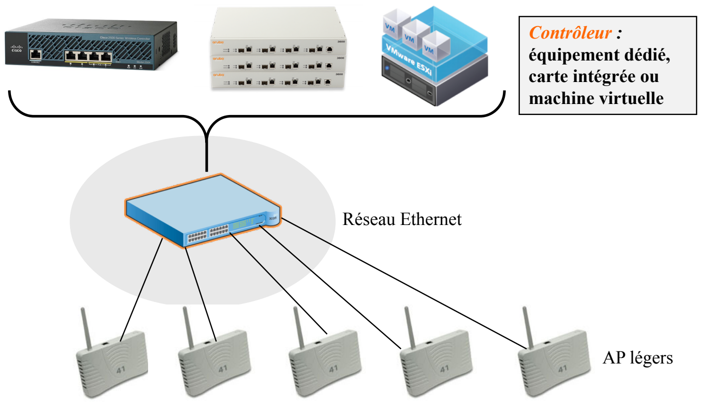
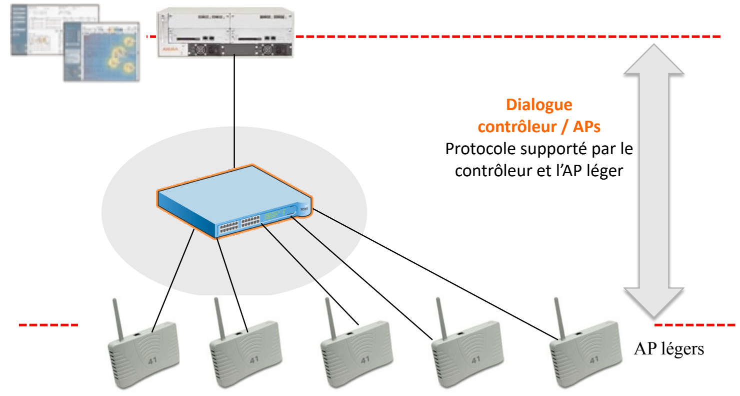
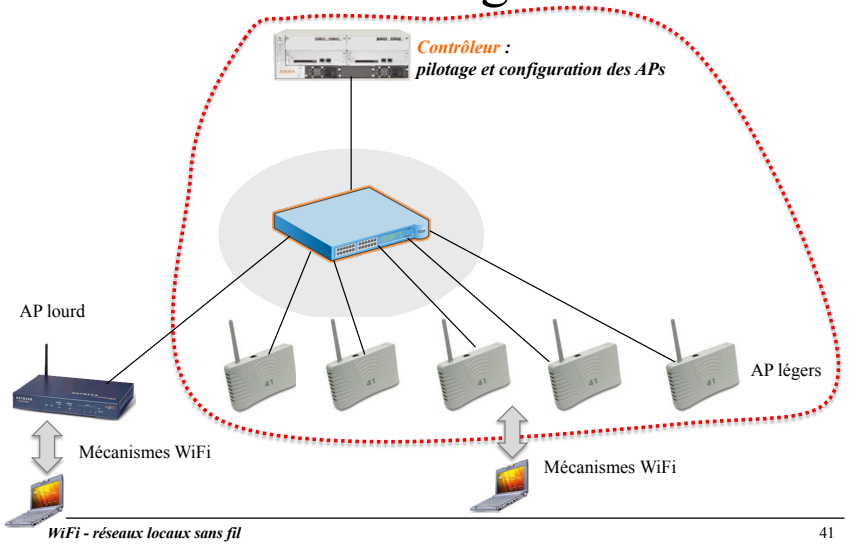


Plate-forme d'APs légers



Coexistence AP légers – AP lourds

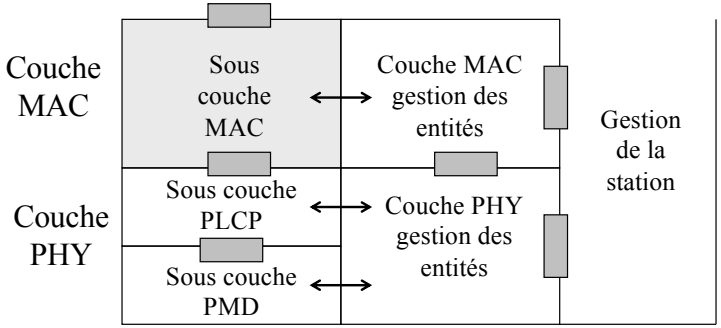


AP lourd / AP léger

- AP lourd
  - Destiné à des petites configurations
  - Ex. : réseau WiFi intégré à une *box* opérateur
- AP léger
  - Fonctionne en coordination avec un contrôleur
  - Réseau WiFi étendu, évolutif, avec des fonctions avancées pour l'administration et la sécurisation

Mécanisme d'accès CSMA/CA

Couche MAC



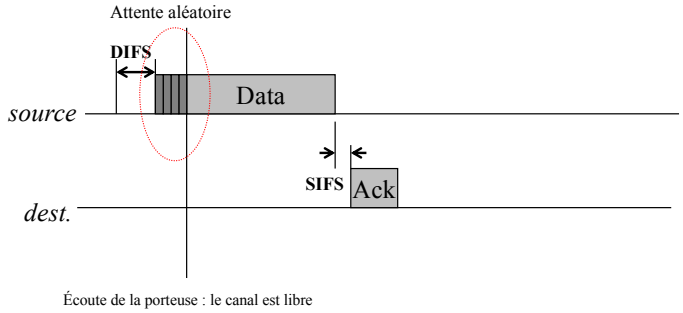
Mécanisme d'accès

- Méthode d'accès de base : DCF (*Distributed Coordination Function*)
  - S'appuie sur le CSMA/CA (*Collision Avoidance*)
- CSMA
  - Une station qui veut transmettre écoute le support
  - S'il est libre, la station transmet
  - Sinon, elle attend

Problème des collisions

- CA plutôt que CD (*Collision Detection*)
  - En transmission sans fil, on ne peut pas être certain que toutes les stations s'entendent entre-elles, les collisions sont difficiles à détecter
- Principe de l'esquive des collisions
  - Au moment où une station veut transmettre, attente **systématique** d'un silence pendant un temps **DIFS** (*Distributed Inter Frame Space*) égal à 50µs
  - Tirage d'un temps d'attente aléatoire inférieur à **CW** (Collision Window) -> algorithme de *backoff*
  - Si le support est libre à la fin de l'attente, la station transmet sa trame
  - Retour d'un ACK positif = le paquet a été reçu
  - L'ACK est désactivé lorsqu'on utilise une adresse de *multicast* ou de *broadcast*

Vue d'ensemble du CSMA/CA

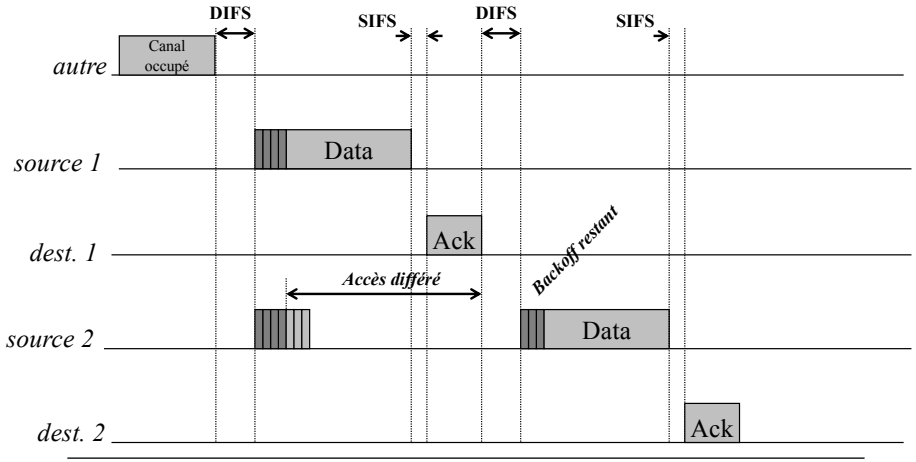


SIFS (*Short Inter Frame Space*) : utilisé pour séparer les transmissions appartenant au même dialogue, égal à 10µs

Algorithme du *backoff* exponentiel

- Une station choisit un nombre **a** aléatoire
  - Compris entre 0 et CW
  - Attend a « *slots time* » (un slot = 20µs) avant de chercher à accéder au support
  - Suspend son attente si le support est occupé, et reporte son crédit de *backoff* « non consommé »
- « *Backoff* exponentiel »
  - CW est doublé à chaque fois en cas d'échec
    - Non réception de l'ACK
    - Support occupé après l'attente de a slot time
    - CW vaut successivement 15, 31, 63, 127, 256, 511, 1023
    - Abandon au bout de 7 tentatives de transmission (report de l'erreur à la couche supérieure)

Report du crédit de *backoff*



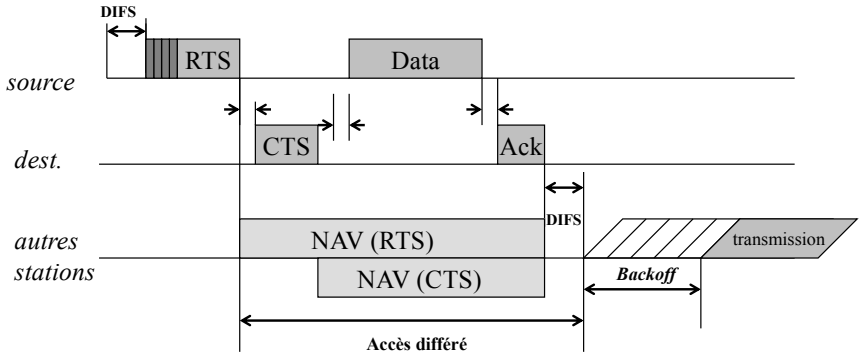
Problème des nœuds cachés

- L'écoute de la porteuse au niveau physique ne permet pas d'éviter toutes les collisions
  - Lors d'un échange (data + ack), une station peut voir le récepteur, et pas l'émetteur
- Définition du *virtual carrier sense* (« sensation virtuelle » de porteuse)
  - Envoi d'un petit paquet RTS (*Request To Send*)
  - Réponse par CTS (*Clear To Send*)

Mécanisme RTS/CTS (1)

- La station émettrice indique dans le RTS un temps de transaction (data + ack)
- Toutes les stations qui reçoivent le RTS ou le CTS déclenchent leur NAV (*Network Allocation Vector*)
  - NAV = porteuse virtuelle = un compteur
  - Déclenché pour un certain temps, pendant lequel l'émetteur est protégé des collisions
  - Deux zones couvertes : celle du RTS, et celle du CTS

Mécanisme RTS/CTS (2)



Mécanisme RTS/CTS (3)

- Utilisation du paramètre *RTS Threshold*
  - Fixe la taille des trames à partir de laquelle le mécanisme RTS / CTS est utilisé
- Il peut être intéressant d'augmenter la valeur de ce paramètre, si le réseau est faiblement chargé
  - Dans ce cas, peu de stations sont susceptibles de transmettre en même temps

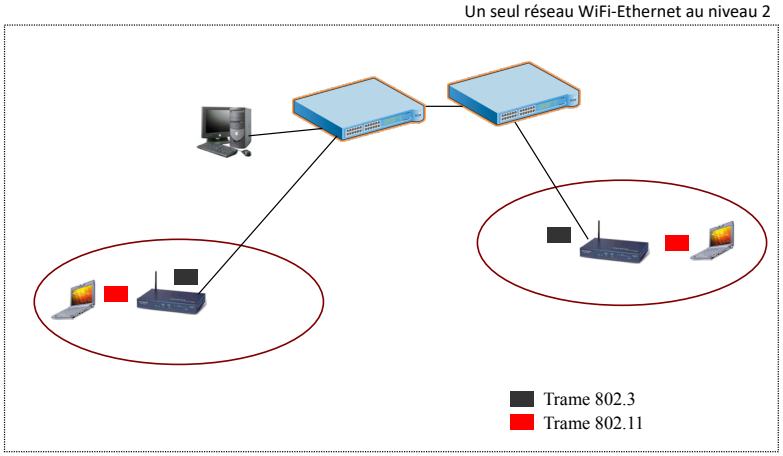
Mise en œuvre de la sécurité dans les réseaux 802.11

➢**Rappel de la problématique générale**
Présentation des mécanismes intégrés aux produits WiFi
Déploiement d'un réseau multi SSID

« Compatibilité » 802.3 | 802.11

- Adressage MAC 802.11 = adressage MAC 802.3
  - Une adresse MAC = 6 octets codés en hexa
    WiFi = `3c:07:54:75:b0:61`
    Ethernet = `68:a8:6d:4f:90:32`
- Un AP permet le passage de manière transparente de la « bulle radio » 802.11 au réseau commuté 802.3
  - AP = pont 802.11 <-> 802.3
  - Pas de configuration de l'AP spécifique pour rendre Ethernet « visible »

« Compatibilité » 802.3 | 802.11



Que vise-t-on ?

- Réseau 802.3 (Ethernet) – 802.11 (WiFi)
  - Un seul réseau logique de niveau 2, toutes les ressources sont accessibles au niveau MAC
  - Pas le même niveau de sécurité que pour un réseau filaire
    - Pas de protection des points d'accès au niveau physique, contrairement à un Ethernet filaire
    - Propagation radio difficile à maitriser = les prises « physiques d'un réseau WiFi peuvent sortir sans contrôle du bâtiment »
- Sécurité d'un réseau WiFi = **mécanismes de sécurité intégrés à la certification WiFi**
  - Il ne s'agit pas d'une sécurité de « bout en bout », cette sécurité ne s'applique qu'à la partie sans fil entre la station et l'AP
  - Mécanismes de sécurité configurés au niveau de l'AP et imposés à la station qui entre dans le réseau WiFi

Un peu de vocabulaire

- Authentification
  - Assurance qu'une station est bien authentifiée quand elle entre sur le réseau WiFi
- Confidentialité
  - Protection contre les écoutes sur la partie radio, entre la station et l'AP
- Intégrité
  - Garantie que les données n'ont pas été modifiée entre la station et l'AP

Un peu de vocabulaire …

- Chiffrer : utiliser une clé pour coder un message afin de le rendre illisible
- Déchiffrer : utiliser une clé pour décoder un message chiffré
- Message en clair : version non chiffrée d'une trame 802.11
- Décrypter : décoder un message chiffré sans recourir à la clé
- Casser un code : élaborer une méthode permettant de décrypter les messages chiffrés à l'aide d'un code

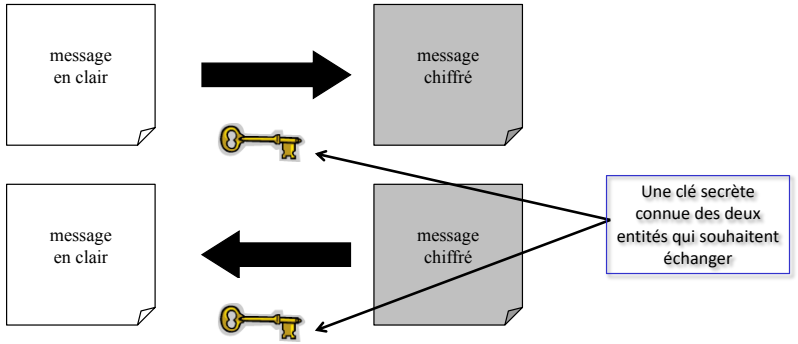
La cryptographie …

- Clé de chiffrement = 1 nombre (mot de passe)
- Clé de déchiffrement = 1 nombre (mot de passe)
- Algorithme de chiffrement = 1 opération mathématique
- Algorithme de déchiffrement = 1 opération mathématique

Chiffrement symétrique

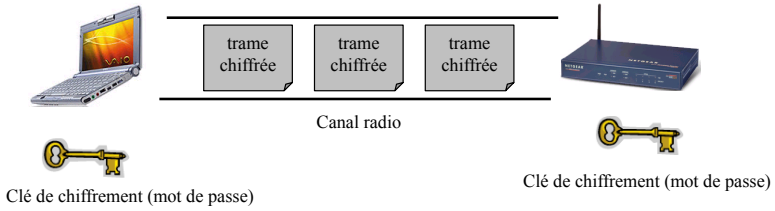
- La clé est unique
  - Elle permet de chiffrer et déchiffrer un message
  - Le message codé n'est déchiffrable qu'avec cette clé
  - La clé doit rester confidentielle
    - Une clé « secrète »
- Problème
  - Il faut réussir à transmettre cette clé secrète au destinataire via un moyen sûr
  - Il faut *a priori* une clé différente pour chaque destinataire

Chiffrement symétrique



À comparer à un clé qui ouvre et et qui ferme une porte … Cela fonctionne à condition de ne pas la perdre, où d'en laisser traîner des copies ….

Chiffrement symétrique dans WiFi



Algorithme de chiffrement symétrique

Algorithme	Longueur de la clé
DES	56 bits
Triple DES	128, 156 bits
RC4 (WEP*, TKIP*)	Variable
AES*	128, 192, 256 bits

* Utilisé dans la sécurité WiFi

WiFi : les deux aspects à traiter

- Chiffrement de la **trame** sur le lien sans fil
  - Protocoles **WEP, TKIP, AES**
- Authentification de la **station mobile** sur le réseau
  - Authentification tournée vers les **réseaux d'entreprises**
    - « Beaucoup d'utilisateurs »
    - Spécification **802.1x,** exploitant le protocole EAP et un serveur d'authentification Radius
  - Authentification tournée vers les réseaux **personnels** / SoHo (*Small Office Home Office*)
    - « Peu d'utilisateurs »
    - Authentification **PSK** (*Pre Shared-Key*), exploitant un mot de passe configuré à l'identique dans l'AP et la station

WiFi : les deux aspects à traiter

- Ces deux aspects sont traités dans l'ordre suivant
  1. Mécanismes d'**authentification** de l'équipement juste après l'établissement de l'association ou de la ré-association (en cas de *handover*)
  2. Si l'authentification réussit, **chiffrement** de données échangées entre la station et l'AP
- A chaque réseau WiFi, on attache donc (côté AP et client)
  - Une politique d'authentification de l'équipement (optionnelle)
  - Une politique de chiffrement (optionnelle)
- En pratique, deux choix
  - Authentification + chiffrement (réseau WiFi protégé)
  - Pas d'authentification et pas de chiffrement (réseau WiFi **ouvert**)

Repères

- Le passé (normalisé avec 802.11b) : le protocole WEP
  - Chiffrement WEP et authentification partagée uniquement (PSK) WEP
- Le présent (normalisé avec 802.11i) : les recommandations WPA (*WiFi Protected Access*) et WPA2
  - WPA = chiffrement **TKIP** + authentification partagée (PSK) ou 802.1x (*enterprise*)
  - WPA2 = chiffrement **AES** + authentification partagée (PSK) ou 802.1x (*enterprise*)

Mise en œuvre de la sécurité dans les réseaux 802.11

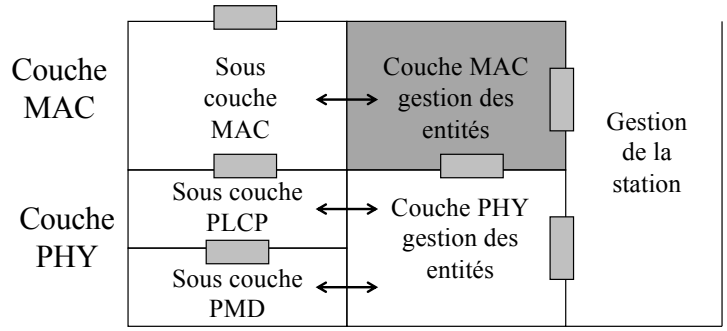
Rappel de la problématique générale

➢ **Présentation des mécanismes intégrés aux produits WiFi**

- Mécanismes d'entrée dans un réseau WiFi
- Mécanismes de chiffrement WEP, TKIP, AES
- Mécanismes d'authentification 802.1x
- Spécifications WPA et WPA2, norme 802.11i

Déploiement d'un réseau multi SSID

Gestion de la synchronisation dans une pile WiFi



Synchronisation dans 802.11 (1)

- Les stations d'une même cellule doivent rester synchroniser sur l'horloge de l'AP
  - Même gestion des périodes d'émission/réception entre l'AP et la station mobile
- L'AP transmet périodiquement (100 ms par défaut) des trames balise (*beacon*) sur sa bande de fréquence
  - Contient l'horloge de l'AP au moment de la transmission (= accès au support)

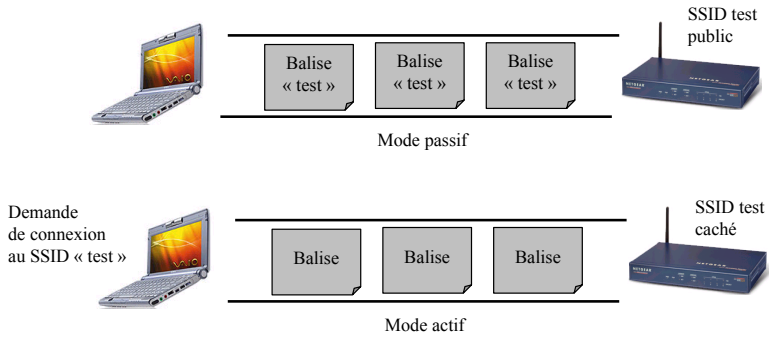
Synchronisation dans 802.11 (2)

- Les stations mobiles réceptrices vérifient la valeur de l'horloge au moment de la réception
  - Correction éventuelle pour calibrer l'horloge locale avec l'horloge de l'AP
  - Evite les dérives d'horloge
- La trame *beacon* contient également des informations utiles à la gestion de l'énergie, aux mécanismes d'**entrée dans une cellule**, aux mécanismes de gestion de la mobilité

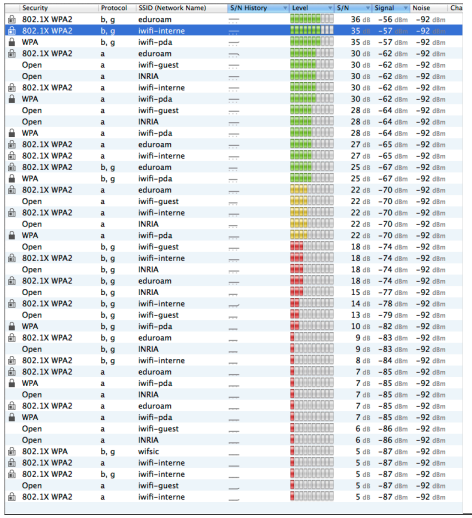
Entrée dans une cellule

- Vue de l'utilisateur, chaque réseau sans fil est caractérisé par un **SSID** (*Service Set IDentity*)
  - SSID = une chaîne de caractères
  - Un SSID est configuré au niveau de l'AP
  - SSID = 1 ESS (un ensemble de cellules) ou 1 BSS indépendant (une cellule unique)
- Deux modes pour se rattacher à un SSID
  - Mode **passif** = SSID diffusé dans les trames balise = SSID « public » ou SSID *guest*
  - Mode **actif** ou ***scanning*** = SSID non diffusé dans les trames balises = SSID « caché »

Entrée dans une cellule

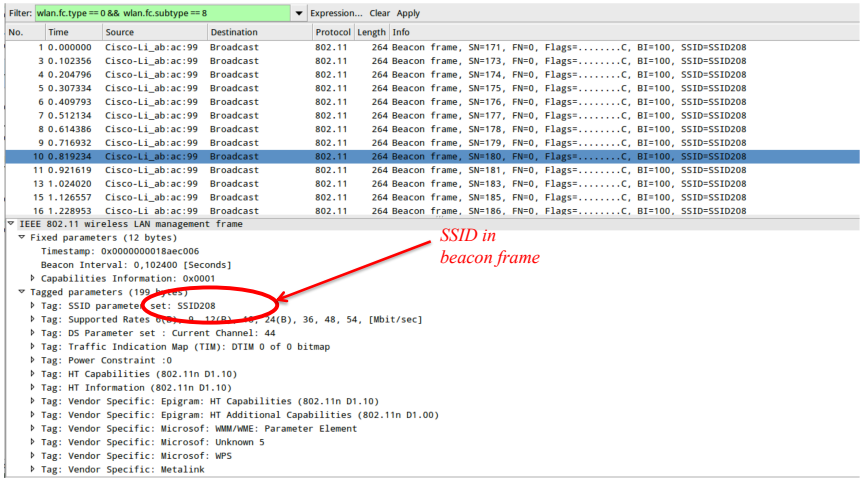


Exemple de voisinage radio



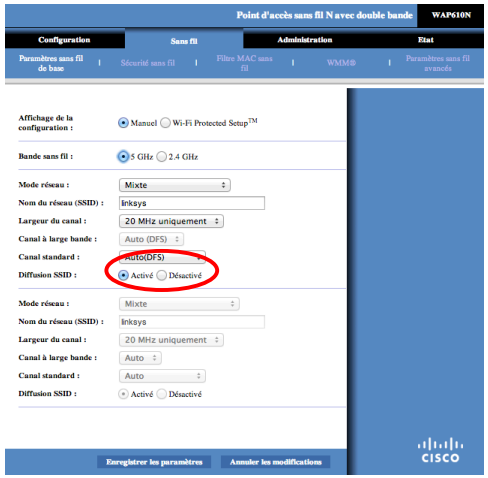
Ensemble de SSID diffusés via les *beacon* 802.11 (capture via l'outil netstumbler)

Exemple de *beacon*



Entrée dans une cellule

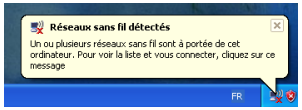
Mode passif

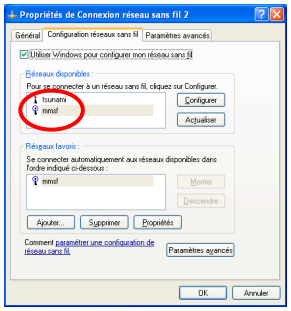


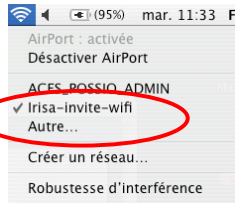
Entrée dans une cellule

Mode passif

- La station attend de recevoir une trame *beacon,* et l'utilise pour se synchroniser avec l'AP
  - Le nom du SSID apparaît automatiquement au niveau de la station mobiles dans la liste des réseaux accessibles





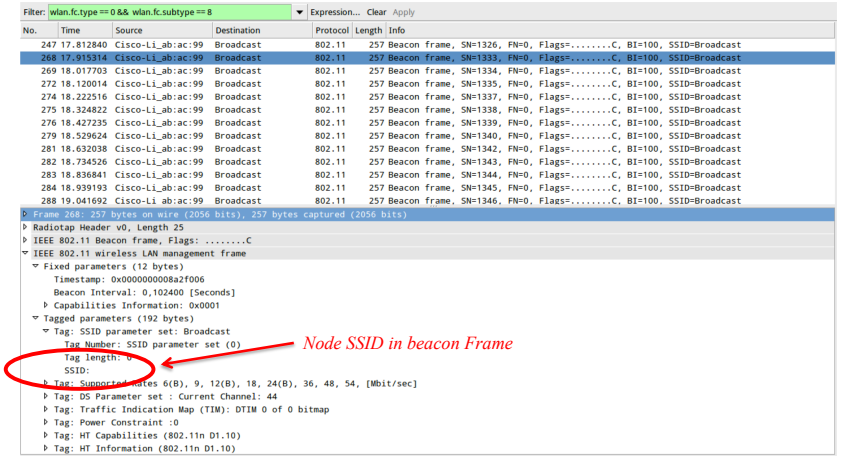


Entrée dans une cellule

Mode actif

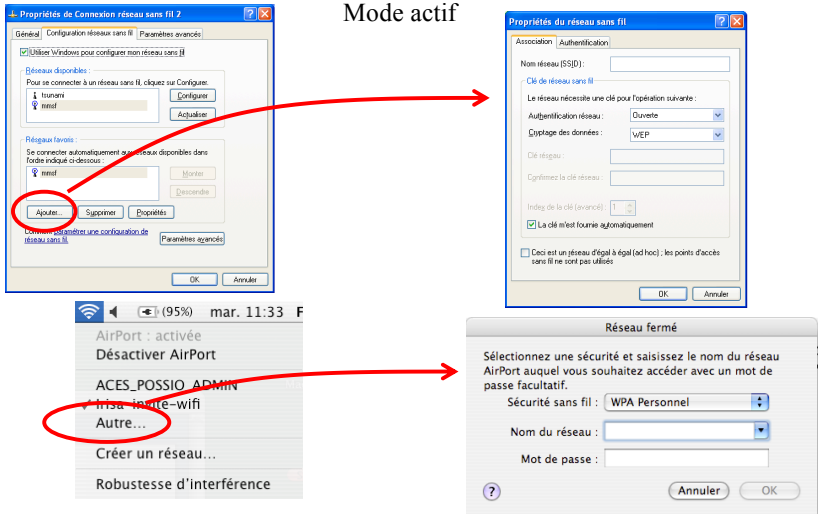
- Mode actif ou *scanning*
  - Mise en œuvre d'une association « explicite » vers un SSID « caché »
- C'est le client mobile qui doit définir à la première association le SSID qu'il souhaite rejoindre
  - Généralement, le SSID est ensuite sauvegardé par le client parmi les « *réseaux WiFi favoris* »
  - Le réseau est alors automatiquement recherché pour les associations suivantes

Exemple de trame *beacon*

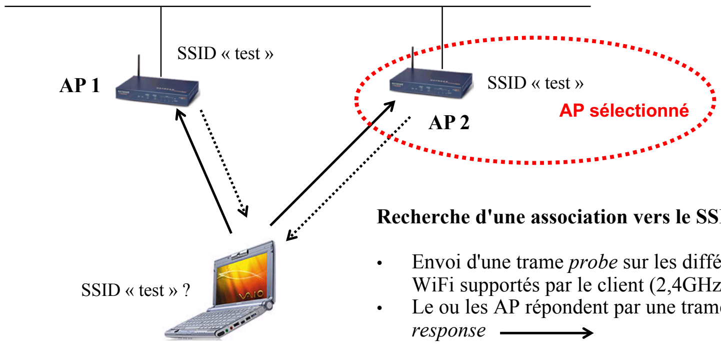


Entrée dans une cellule

Mode actif



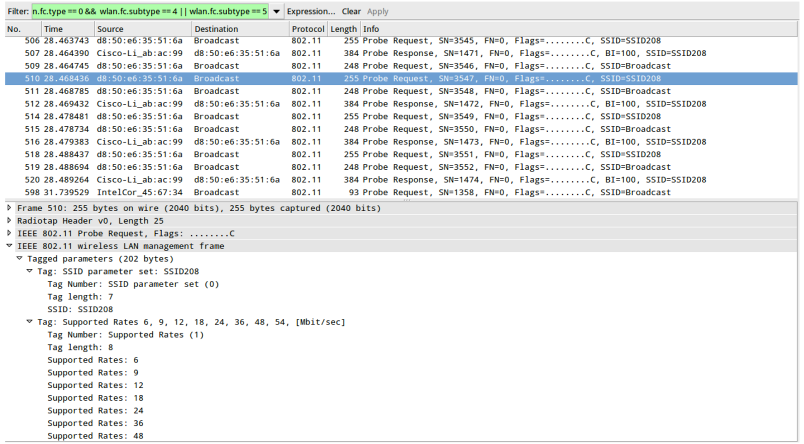
Exemple de connexion via un *scan*



Recherche d'une association vers le SSID « test »

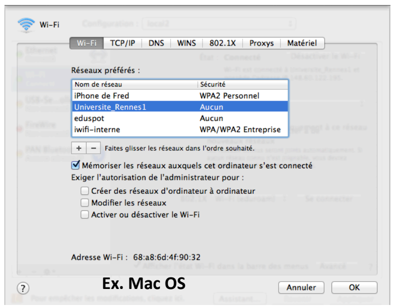
- Envoi d'une trame *probe* sur les différents canaux WiFi supportés par le client (2,4GHz et/ou 5GHz)
- Le ou les AP répondent par une trame *probe response* ⟶
- La station sélectionne le « meilleur AP » (pour un SSID donné), et se retrouve synchronisé avec cet AP ⋯⋯⋯>

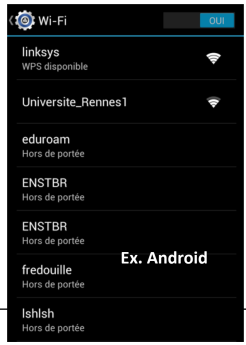
Exemple de connexion via un *scan*



Liste de réseaux favoris

- ❑ Les caractéristiques d'un SSID accroché dans le passé (nom, paramètres de sécurité) sont conservées par la station
- ❑ Ces réseaux favoris sont automatiquement recherché dès lors que la carte WiFi est de la section est activée





Rattachement effectif

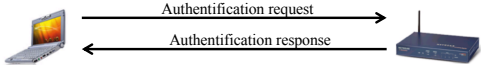
« joining »

- ❑ Suite à une réception de trame *beacon* (mode passif) ou un *scan* (mode actif), la station est synchronisée avec l'AP
  - La cellule de rattachement est identifié, ainsi que le canal WiFi utilisé par l'AP
  - Station et AP ont la même période d'envoi des trames *beacon*
- ❑ Rattachement en deux étapes
  1. Authentification
  2. Association

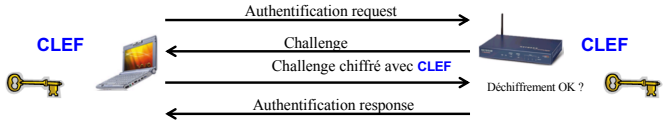
Phase 1 : authentification

Deux modes possibles

Open = pas d'authentification

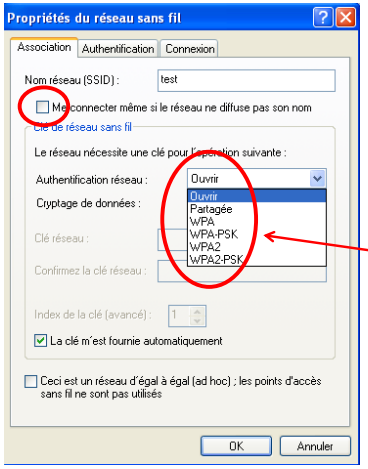


Pre Shared-Key (PSK) = s'appuie sur le partage d'une clef de chiffrement configurée hors échange réseau sur l'AP et la station



Configuration d'un client

Exemple sous OS Windows



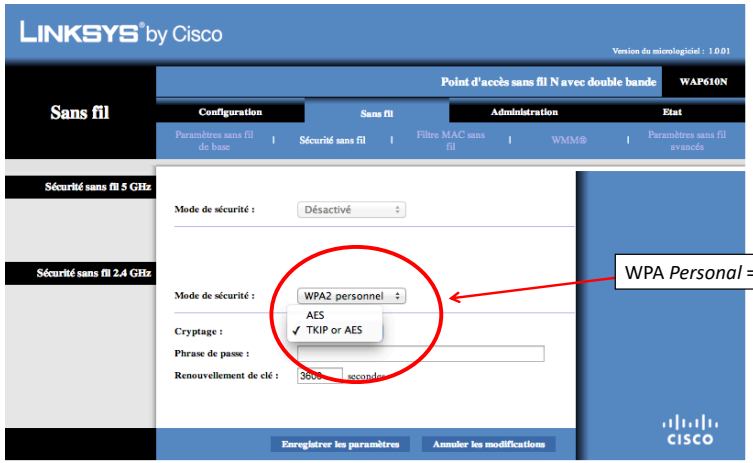
Choix du type d'authentification

Ouvrir = pas de sécurité
OU
Partagée = PSK mot de passe WEP
WPA PSK = PSK mot de passe TKIP
WPA2 PSK = PSK mot de passe AES

WPA / WPA2 = authentification EAP (suite du cours)

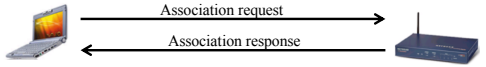
Configuration d'un AP

Exemple d'un AP lourd



WPA *Personal* = WPA2 PSK

Phase 2 : association



Juste après la phase d'authentification …

- Envoi d'une trame *association request*
- L'AP répond par un *association response*
- L'AP et la station peuvent commencer à s'échanger des données

Au final …

- Deux modes configurables dans un AP pour un SSID
  - SSID annoncé dans les trames balises = SSID public
  - SSID non annoncé dans les trames balises = SSID caché
- Un SSID « caché » peut être vu comme un élément de sécurité
  - Le client doit le connaître pour s'y accrocher
  - Mais …
    - Des outils simples d'accès existent pour trouver ce type de SSID
    - C'est une source de problèmes (paramétrage des postes client) pour les équipes systèmes
  - Donc …
    - Privilégier les SSID publics dans les réseau WiFi d'entreprise ou publics (grande population d'utilisateurs), et s'appuyer sur des mécanismes de contrôle d'accès efficaces

Mise en œuvre de la sécurité dans les réseaux 802.11

Rappel de la problématique générale

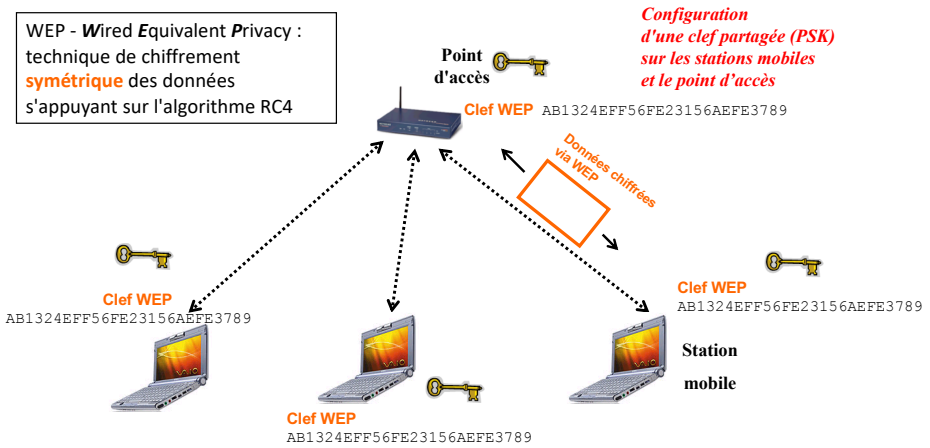
➢ **Présentation des mécanismes intégrés aux produits WiFi**

- Mécanismes d'entrée dans un réseau WiFi
- Mécanismes de chiffrement WEP, TKIP, AES
- Mécanismes d'authentification 802.1x
- Spécifications WPA et WPA2, norme 802.11i

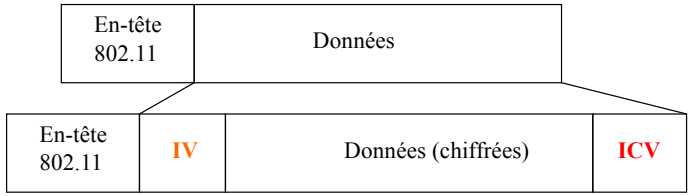
Déploiement d'un réseau multi SSID

A l'origine : le protocole WEP

WEP - ***W****ired* ***E****quivalent* ***P****rivacy* : technique de chiffrement **symétrique** des données s'appuyant sur l'algorithme RC4



Encapsulation WEP



- Algorithme de chiffrement utilisé par WEP = algorithme RC4
- Clef de chiffrement utilisée pour chaque paquet transmis = vecteur d'initialisation **IV** sur 24 bits (nombre pseudo aléatoire), **combiné** avec la clef définie au niveau de la station et de l'AP (PSK)
- L'intégrité des données est assurée par un code CRC de 32 bits, calculée sur la base des données non chiffrées (**ICV**)

Principe d'un algorithme RC4

Clef de chiffrement ***K***

Clé saisie par l'utilisateur dans l'AP et la station

AB1324EFF56FE23156AEFE3789

L'algorithme est exécuté à l'identique par une station et le point d'accès

Principe d'un algorithme RC4

Clef de chiffrement ***K***

Clé saisie par l'utilisateur dans l'AP et la station

AB1324EFF56FE23156AEFE3789

Générateur de nombre pseudo aléatoire

Ajout du vecteur d'initialisation (IV)

Principe d'un algorithme RC4

Clef de chiffrement ***K***

Clé saisie par l'utilisateur dans l'AP et la station

AB1324EFF56FE23156AEFE3789

Générateur de nombre pseudo aléatoire

Ajout du vecteur d'initialisation (IV)

Nombre aléatoire ***b***

= clé WEP

Principe d'un algorithme RC4

Clef de chiffrement ***K***

Clé saisie par l'utilisateur dans l'AP et la station

AB1324EFF56FE23156AEFE3789

Générateur de nombre pseudo aléatoire

Ajout du vecteur d'initialisation (IV)

Nombre aléatoire ***b***

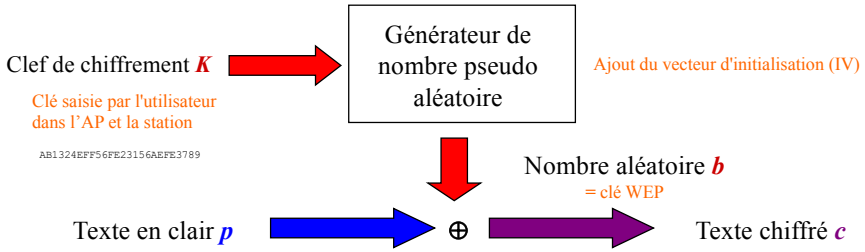
= clé WEP

Texte en clair ***p***

⊕

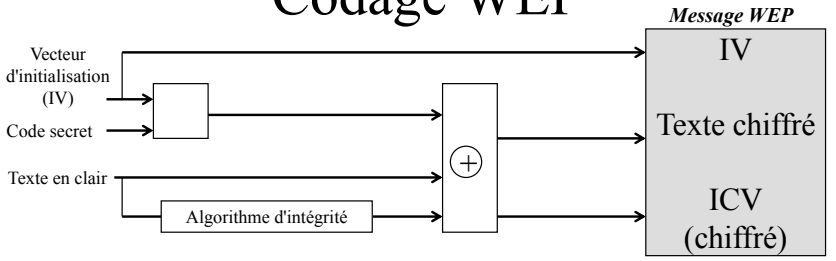
Texte chiffré ***c***

Principe d'un algorithme RC4



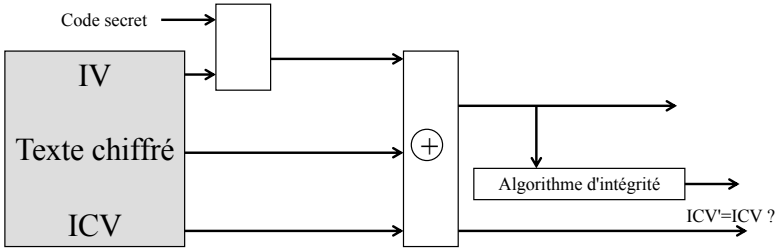
Le déchiffrement fonctionne de la même façon : $p = c \oplus b$

Codage WEP



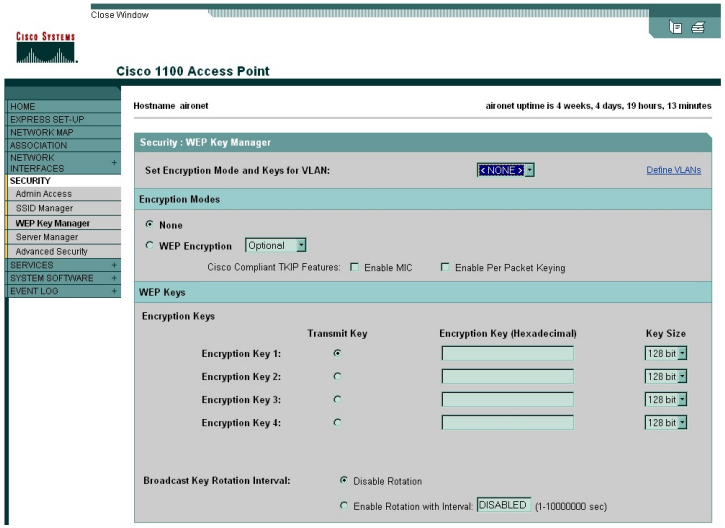
- Le code secret (= la clef) et l'IV sont concaténés pour former la clef de chiffrement WEP
- Le texte est chiffré en réalisant un **ou exclusif** entre la clef de chiffrement et le texte en clair
- L'IV et l'ICV sont dans le message chiffré

Le décodage WEP

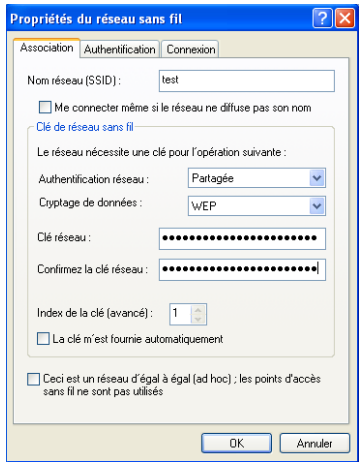


- La clef de déchiffrement est formée de l'IV reçu et de la clef partagée
- On compare le code d'intégrité reçu au code d'intégrité recalculé

Concrètement …côté AP



Concrètement …côté terminal



- Taille de la clef WEP utilisée = taille de la clef saisie + taille du vecteur d'IV (24 bits)
- Pour une clef WEP de 128 bits, on saisit 104 bits, soit 26 caractères hexa
- Méthode d'administration très contraignante

Propriété « intéressante » d'un algorithme RC4

Que se passe-t-il quand p_1 et p_2 sont chiffrés avec la même clef b (produite avec l'IV et la clef "partagée") ?

$$c_1 = p_1 \oplus b \qquad c_2 = p_2 \oplus b$$

Alors

$$c_1 \oplus c_2 = (p_1 \oplus b) \oplus (p_2 \oplus b) = p_1 \oplus p_2$$

Donc ce peut être dangereux lorsqu'on chiffre deux messages quelconques avec la même clef produite par un algorithme RC4. Si on connaît p_1, on peut en déduire p_2. On peut également utiliser des méthodes d'analyse statistique pour trouver p_1 et p_2

C'est ce qu'on appelle une collision, les deux paquets produits partagent le même IV

C'est encore plus facile si on a trois paquets utilisant le même IV

Attaque par écoute passive (1)

- On utilise les collisions
  - On récupère par écoute passive deux paquets issus d'un même IV (qui circulent en clair dans le paquet), et on commence à déchiffrer …
- Sur un AP « chargé », il y a une collision toutes les 4s !

Attaque par écoute passive (2)

- Pour accélérer l'attaque, l'intrus provoque l'envoi de message dont il connaît le contenu
- Quand on a déchiffré 2^{24} textes en clair correspondants aux 2^{24} valeur d'IV, on peut déchiffrer tous les paquets

WEP : un protocole sans état

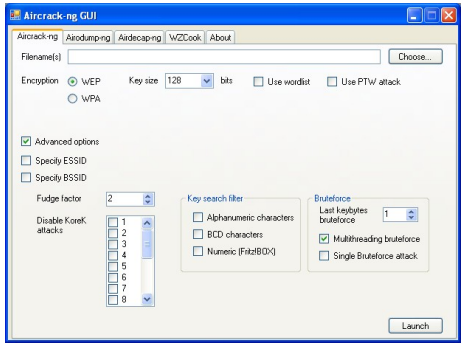
- Les stations mobiles et les APs ne gardent pas de trace des échanges passés
- Conséquence importante : un intrus peut « rejouer » du trafic capturé
  - *A priori*, la duplication n'est pas un problème trop grave (cf. protocole IP)
- Mais on peut aller plus loin en « rejouant » du trafic modifié

La fin de WEP …

- "Weaknesses in the Key Scheduling Algorithm of RC4", rapport de Scott Fluhrer, Itsik Mantin et Adi Shamir
  - Décrit les faiblesses des algorithmes RC4 en général, et propose un schéma d'attaque passive
  - Article largement diffusé
- WEP est un protocole qui devient très vulnérable
- L'article propose une approche entièrement nouvelle
  - Pas une extension des articles précédents
  - Apparition de programmes sur Internet (*WEPCrack, AirSnort*)
  - Mise en défaut d'une clef WEP en moins d'une heure

Les faiblesses de WEP (1)

- Attaque par écoute passive
  - Sur un AP chargé, récupération d'une clef WEP 128 bits en moins d'une heure
  - De nombreux outils à disposition
- Possibilité de « rejouer » du trafic modifié



De WEP à TKIP

- Administration très contraignante
  - Gestion de clés sur 128 bits (104 bits saisis + 24 bits de vecteur d'IV) configurées en hexa
  - Les clés doivent normalement être changées régulièrement par l'administrateur
- L'approche retenue … conserver WEP en …
  - Provoquant un changement régulier de la clé de chiffrement
  - Simplifiant l'administration des clés
  - ➢ **Protocole TKIP** = surcouche de WEP

Notion d'empreinte numérique (1)

- Résumé (de taille fixe) d'un document électronique
- Deux documents différents (même légèrement) ont des empreintes différentes
- Algorithme ou « *fonction de hashage* » permettant de calculer une empreinte
  - = opération mathématique
  - **MD5, SHA1**
  - Non réversible, on ne peut pas retrouver le document d'origine à partir de son empreinte

Notion d'empreinte numérique (2)

TKIP

Temporal Key Integrity Protocol

- Compatible avec le protocole WEP, la méthode de chiffrement ne change pas
  - Peut être vu comme une « surcouche » du WEP
- S'appuie sur une clef « maître » (PMK : *Primary Master Key*) configurée au niveau de la station et de l'AP
  - L'utilisateur saisit une *passphrase* de 8 à 63 caractères dérivé automatiquement en une clé PMK sur 256 bits via une fonction de hashage
  - Dérive ensuite un ensemble de clefs, en partant de cette clef maître PMK, dont la clef de chiffrement WEP
  - ➢ **Chaque association calcule une clef WEP différente**
  - Cette clef change de manière régulière, suivant une périodicité configurable au niveau de l'AP (par ex. toutes les 10000 trames échangées)
  - Attaque beaucoup plus difficile que pour le WEP statique

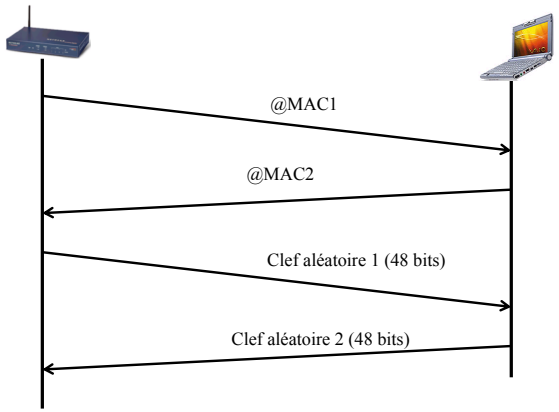
TKIP

Temporal Key Integrity Protocol

- Vecteur d'initialisation étendu sur 48 bits (24 bits pour le WEP)
- Utilisation d'un nouveau code d'intégrité : MIC (*Message Integrity Code*) ou Michael
  - WEP utilise un ICV sur 4 octets linéaire
  - TKIP rajoute un MIC sur 8 octets non linaire

TKIP

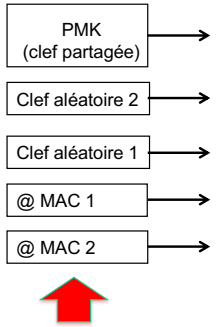
Echange automatique *4-Way Handshake* juste après l'association



Données échangées dans des trames EAPOL (*EAP Over Lan*) – voir partie EAP du cours
Ces échanges n'existent pas dans WEP statique

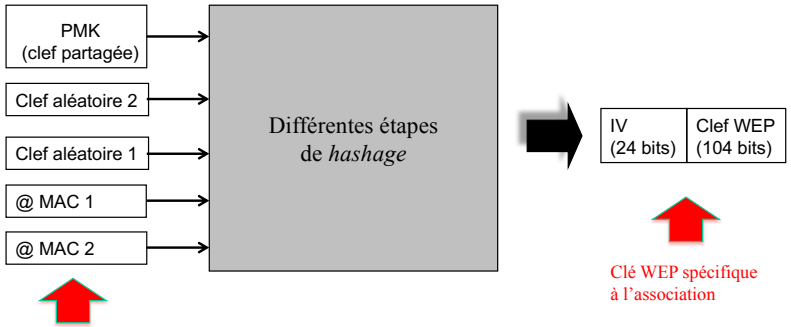
TKIP

Génération de la clé WEP



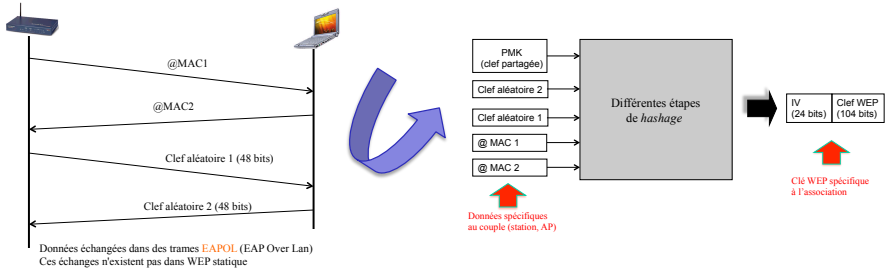
TKIP

Génération de la clé WEP



Rotation des clés TKIP

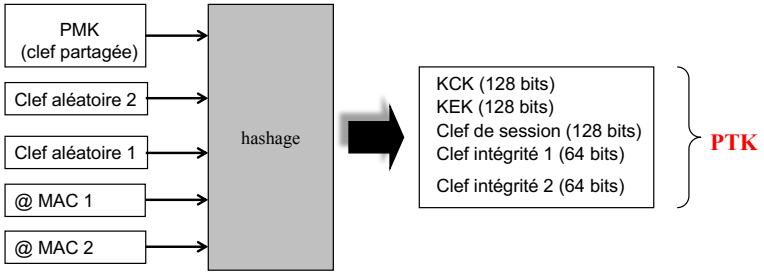
Calcul de la clé TKIP par la station et l'AP



Rotation des clés TKIP

TKIP plus en détails

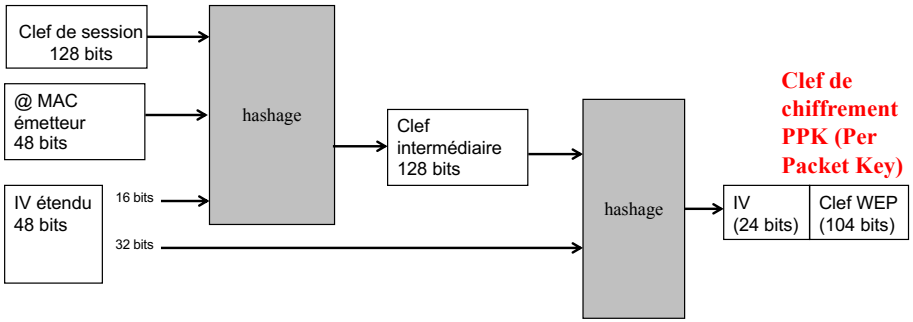
L'AP et la station génère le PTK



- KCK (*Key Confirmation Key*) : utilisée pour la phase d'authentification, si **l'authentification 802.11** est « partagée » (WPA *personal* – WPA-PSK)
- KEK (*Key Encryption Key*) : sert à l'AP pour distribuer sous forme cryptée la clef unique utilisée pour les trafics *broadcast* et *multicast* (GTK - *Group Transcient Key*)
- Clef de session : sert à générer la clef WEP
- Clef intégrité 1 & 2 : utilisées pour le calcul du MIC (code d'intégrité propre au WPA)

TKIP plus en détails

Génération de la clef WEP via un double *hashage*



Avantages de TKIP

- Ne demande pas plus de puissance matériel que le WEP statique
- La clef partagée pour l'authentification PSK (clé KEK) n'est pas celle utilisée pour le chiffrement des trames 802.11 (clé WEP PPK)
- La clef WEP utilisée pour le chiffrement est unique pour une association donnée
  - Utilisation des @MAC et de clefs aléatoires à l'initialisation
- L'utilisation de clefs dans le calcul de la MIC rend très difficile la modification de la trame
  - La seule attaque possible devient le déni de service = rejouer du trafic non modifié
  - A priori, une collision (deux vecteurs d'IV sur 48 bits, identiques, et portés par des trames corrects) est peu probable dans une période de temps faible
  - Rejouer du trafic non modifié provoque des collisions
  - ☹ Pour détecter cela, s'il y a plus d'une collision en 60s (deux vecteurs d'IV identiques), l'association est automatiquement rompue !

Chiffrement et intégrité par AES

AES / CCMP

- AES (*Advanced Encryption Standard*) / CCMP (*CBC-MAC protocol*) = chiffrement + intégrité
- AES = Moteur de chiffrement remplaçant de TKIP
- Nécessite une évolution du composant en charge du chiffrement
  - Demande plus de puissance que WEP/TKIP
  - Une simple évolution logicielle ne suffit pas, les APs et les adaptateurs client doivent être changés
  - Le support natif de l'AES est maintenant généralisé
- AES est un algorithme de chiffrement de type symétrique
  - Excellente résistance aux attaques statistiques, ainsi qu'au attaque par dictionnaire
- Depuis Mars 2015, la WiFi alliance recommande l'abandon de TKIP au profit de l'AES (passage de WPA à WPA2 « AES only »)

http://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_Alliance_Technical_Note_TKIP_v1.0.pdf

Lien vérifié Fév. 2017

Mise en œuvre de la sécurité dans les réseaux 802.11

Rappel de la problématique générale

➢ **Présentation des mécanismes intégrés aux produits WiFi**

- Mécanismes d'entrée dans un réseau WiFi
- Mécanismes de chiffrement WEP, TKIP, AES
- Mécanismes d'authentification 802.1x
- Spécifications WPA et WPA2, norme 802.11i

Déploiement d'un réseau multi SSID

Filtrage par adresse MAC

Sécurisation d'un réseau WiFi « public »

Rappel - authentification 802.11

Dans la norme IEEE 802.11 d'origine (1997),
deux types d'authentification 802.11 : *open* et *shared (PSK)*

Limite de l'authentification PSK

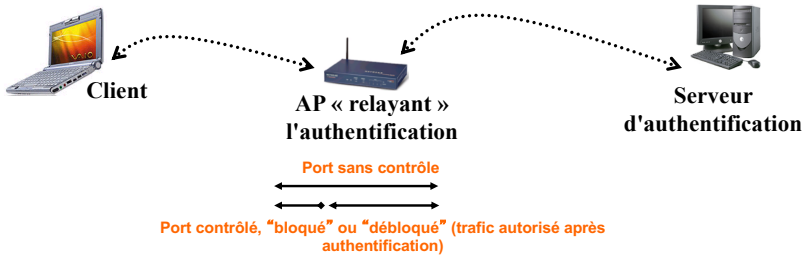
- Le mode *open* est réservé aux accès WiFi publics
  - Pas de chiffrement / Pas d'authentification
  - Un accès WiFi (personnel ou entreprise) doit être protégé
- L'authentification *PSK* ne convient pas s'il faut gérer un nombre important de clients mobiles et d'APs
  - Impossible de partager efficacement le même mot de passe TKIP ou AES pour un groupe d'utilisateurs = un secret difficile à conserver
  - Nécessité de dupliquer le mot de passe TKIP et/ou AES au niveau de tous les APs si le réseau est étendu

Authentification EAP/802.1x

- EAP/802.1x fournit un mécanisme s'appuyant sur la gestion d'un port logique au sein de l'AP
  - Ce port relaie vers les messages d'authentification vers un serveur externe à l'AP = un serveur d'authentification
- EAP/802.1x permet l'authentification sur les réseaux 802.11 a/b/g/n/ac
  - Ne modifie pas la norme d'origine, qui supporte les deux modes d'authentification open ou PSK
  - L'authentification EAP/802.1x est exploité **après** le mode open … open puis EAP/802.1x

Authentification EAP/802.1x

- Un mode open + EAP (open puis 802.1x/EAP)
  - Le client peut accrocher le SSID et s'y associer
  - Tant qu'il n'est pas authentifié, le client ne peut pas avoir accès au réseau « après l'AP »
  - Avant cela, seuls les échanges liés au processus d'authentification sont relayés vers le serveur d'authentification, via l'AP



Trois acteurs principaux

Principes généraux de 802.1x

1. Le client (*supplicant 802.1x*), composant logiciel
2. Le matériel d'accès au réseau local : AP WiFi a/b/g/n/ac supportant la spécification 802.1x
3. Le serveur d'authentification (**Radius**)

Radius

Remote Authentication Dial-In User Service

- Protocole d'authentification standard
  - Largement utilisé dans le monde Télécom pour traiter la problématique AAA (*Authentification, Authorization, Accounting*)
    - Utilisé par ex. par les FAIs pour l'authentification ADSL au delà du BAS
  - Défini par un certain nombre de RFCs
- Le client radius (NAS – Network Access Server) fait office d'intermédiaire entre l'utilisateur et le serveur
  - Dans le cas de 802.1x, **client Radius = NAS = AP WiFi**
  - Les échanges Radius sont chiffrés par un mot de passe configuré dans le serveur Radius et dans l'AP

Radius

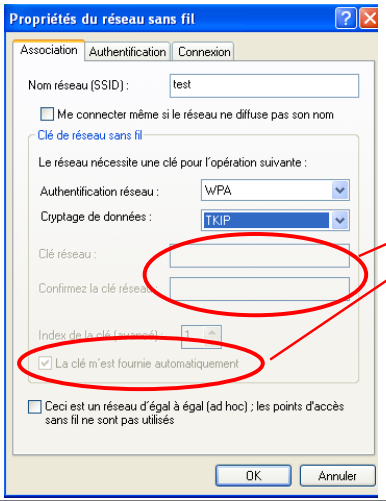
Remote Authentication Dial-In User Service

- Le serveur radius peut utiliser une base d'authentification pour référencer les utilisateurs autorisés
  - Base de données locale, annuaire LDAP …
- Les données Radius peuvent être transmises via un réseau IP entre l'AP et le serveur
  - Encapsulation IP -> UDP -> Radius

Gestion du chiffrement

- Les méthodes d'authentification 802.1x reconnue par WiFi permettent au client mobile de récupérer automatiquement une clé de chiffrement WEP statique, TKIP ou AES
- Une clé « maître » PMK est générée par le serveur Radius et renvoyé à l'AP dans un message
  - Utilisation d'un VSA (*Vendor Specific Attributes*) dans un message d'authentification Radius
  - L'authentification 802.1x est donc associée au mode *open*, sans clé de chiffrement configurée
  - Pas d'utilisation du mode *partagé* (PSK) dans ce cadre

Gestion du chiffrement



Ici, WPA = WPA *enterprise*

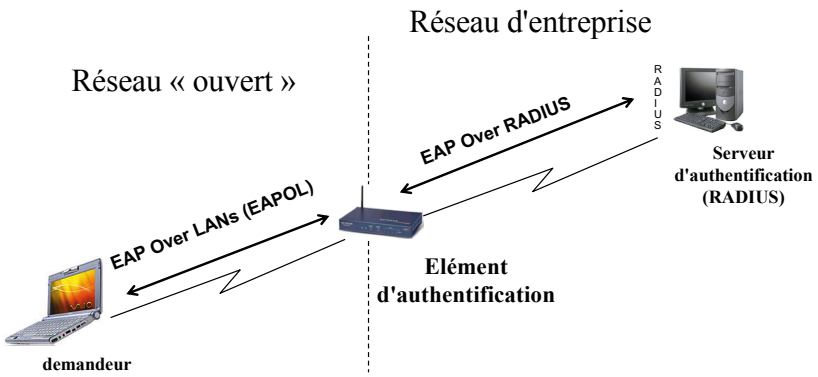
La clé PMK (utilisée par les moteurs de *hashage* TKIP ou AES) est générée par le serveur Radius, l'utilisateur n'a pas à fournir de clé de chiffrement

EAP

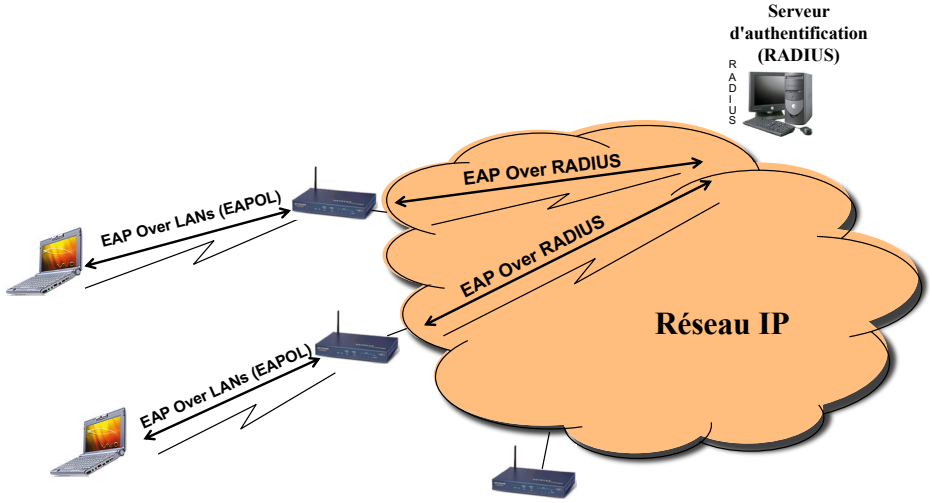
Extensible Authentification Protocol

- 802.1x spécifie l'utilisation du protocole EAP (rfc 2284), pour le transport des messages d'authentification
- EAP peut s'encapsuler dans différents protocoles : 802.3, 802.11, Radius …
- 802.1x utilise deux types de trafic EAP
  - **EAP over LAN** (EAPOL) = messages EAP encapsulées dans des trames LANs (encapsulation 802.11 | EAP)
  - **EAP over Radius** = messages EAP encapsulés dans des paquets Radius (encapsulation L2 | IP | UDP | Radius | EAP)

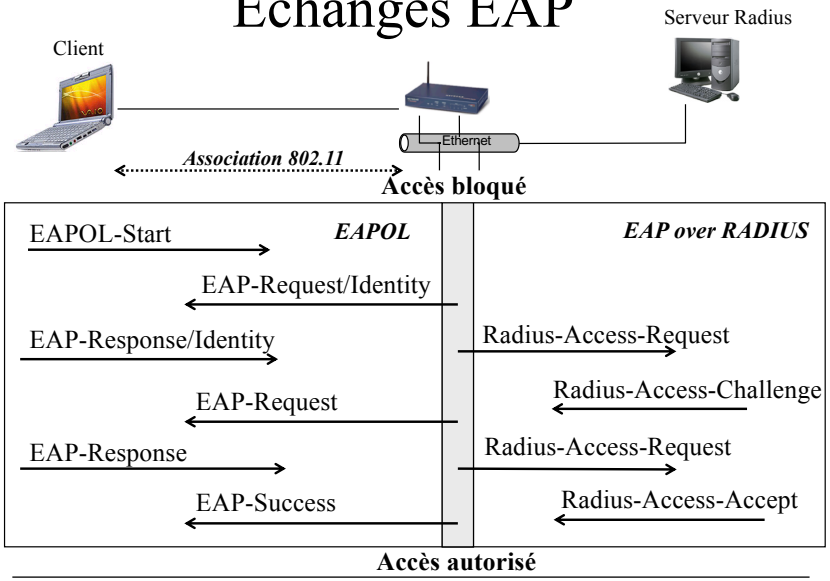
Encapsulation EAP



Encapsulation EAP



Echanges EAP



Au final … trois méthodes d'authentification

- Open
  - Réseau ouvert, pas de chiffrement, pas d'authentification
- PSK
  - Mot de passe configuré hors échange réseau sur l'AP et le client mobile, utilisé pour l'authentification et le chiffrement du lien radio
- EAP / 802.1x
  - En réalité, open + 802.1x
  - Authentification via des échanges EAP échangés entre le client mobile et un serveur Radius
  - Clé de chiffrement distribuée automatiquement au client mobile

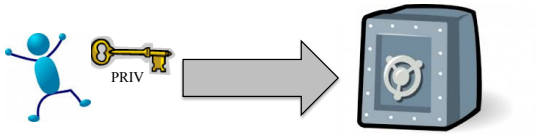
Support de différentes méthodes d'authentification

- EAP permet d'authentifier le client mobile, et éventuellement le serveur (authentification mutuelle)
- EAP supporte différentes méthodes d'authentification
  - Login / mot de passe
  - Certificat électronique
  - Token Card OTP (*One Time Password*)
  - Puce SIM
  - Ou une combinaison de plusieurs éléments, par ex. certificats et login / MdP
- De plus, la plupart des versions d'EAP gèrent la distribution dynamique des clefs de session WEP statique / TKIP / AES

Chiffrement asymétrique (1)

- Deux clés dissociées : une clé publique, et une clé privée

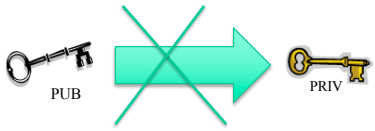
- La clé privée est conservée de manière confidentielle par son possesseur



Chiffrement asymétrique (2)

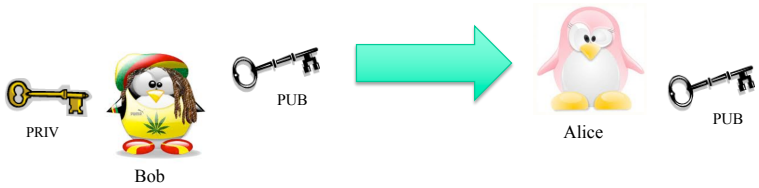
- La clé publique peut être diffusée

- Point très important : il n'est pas possible de retrouver la clé privée à partir de la clé publique !



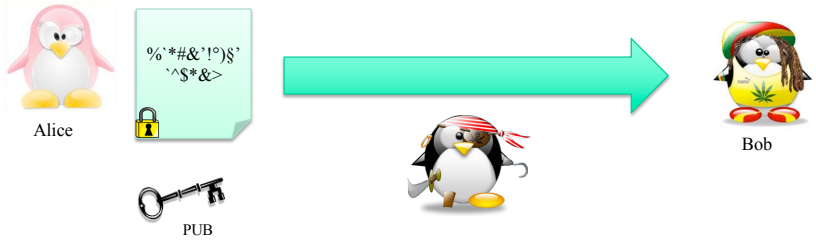
Chiffrement asymétrique (3)

- Création d'un couple (clé privée, clé publique) pour Bob, Bob diffuse sa clé publique



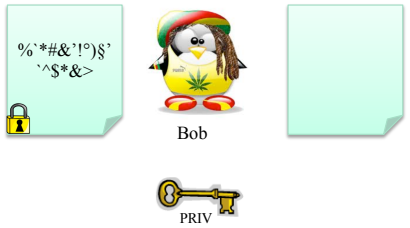
Chiffrement asymétrique (4)

- Alice envoie un message chiffré à Bob avec la clé publique de Bob



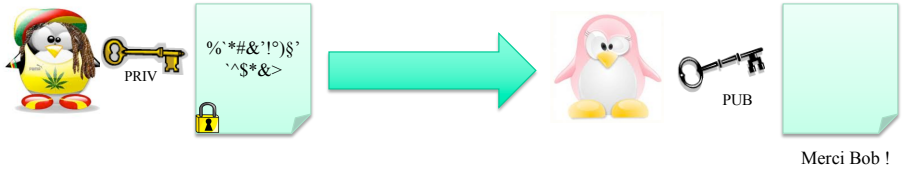
Chiffrement asymétrique (5)

- Bob déchiffre le message avec sa clé privée
- Seul Bob peut le faire



Chiffrement asymétrique (3)

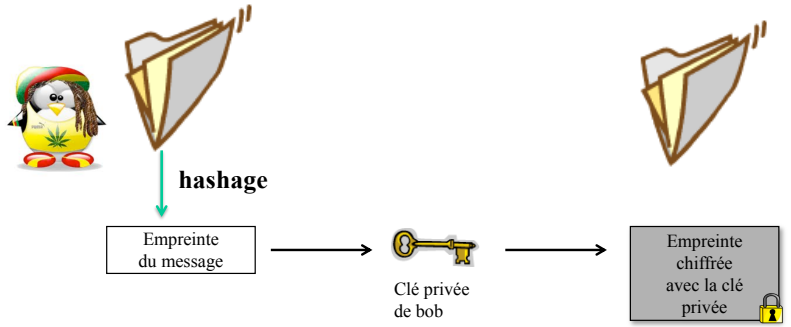
- La clé privée peut aussi servir à chiffrer, la clé publique sert alors à déchiffrer
- Bob envoie un message à Alice, chiffré avec sa clé privée
- Alice décode le message avec la clé publique de Bob
- Le message n'a pu être chiffré que par Bob



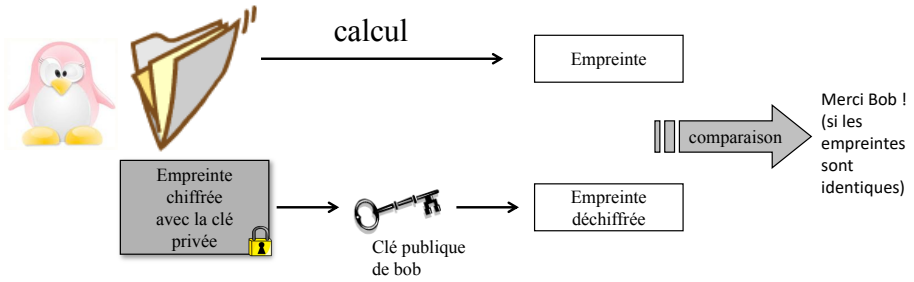
Signature électronique

- Utilisé pour prouver l'identité de l'auteur d'un document électronique
  - Par ex. un mail
- On utilise
  1. Sur un mécanisme de chiffrement asymétrique (clé privée, clé publique)
  2. Sur un mécanisme de *hashage*

Signature d'un document par Bob



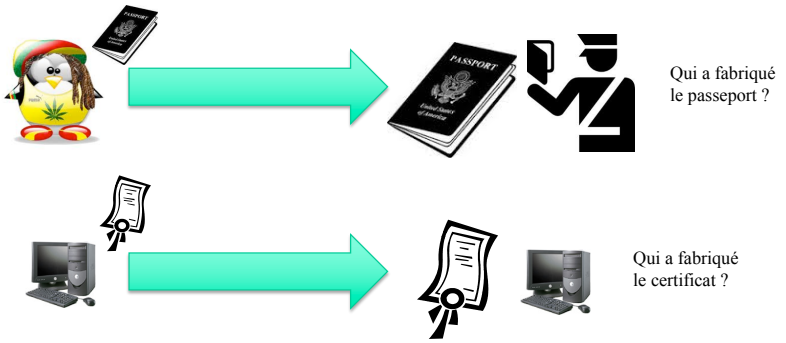
Vérification de la signature par Alice



Certificat électronique

- Certifier qu'une clé publique est bien celle d'une personne identifiée
  - Pour éviter des attaques du type « man in the middle » où quelqu'un se fait passer pour le correspondant et transmet de façon transparente pour l'émetteur les données au vrai destinataire
- Certificat = passeport numérique

Certificat électronique



Problème de confiance

- Comment certifier que le nom dans un certificat est bien celui du propriétaire de la clé publique ?
- Problème analogue à l'émission d'une carte d'identité …

Problème de confiance

- Comment certifier que le nom dans un certificat est bien celui du propriétaire de la clé publique ?
- Une autorité de certification (AC) ou autorité de confiance est en charge de délivrer le certificat, en vérifiant l'identité du demandeur

Problème de confiance

- Comment être certain qu'un certificat est émis par une autorité de certification ?

Problème de confiance

- Comment être certain qu'un certificat est émis par une autorité de certification ?
- Une autorité de certification possède une clé publique et une clé privée
- Elle signe les certificats qu'elle émet
- Si un certificat signé par cette autorité est modifié, cela peut être détecté par le récepteur du certificat

Problème de confiance

- Quand on reçoit un certificat signé, comment faire confiance à l'autorité de certification qui l'a émis ?

Problème de confiance

- Quand on reçoit un certificat signé, comment faire confiance à l'autorité de certification qui l'a émis ?
- On charge sur sa station le certificat de l'AC dans lequel on décide d'avoir confiance
  - Dans le certificat, on trouve la clé publique de l'AC qui va permettre de valider la signature des certificats émis par cette AC
- Sur quel(s) critère(s) charge-t-on le certificat de l'AC ?
  - On connaît en principe l'AC

Format d'un certificat X.509

- Fichier stocké sur un ordinateur, une carte à puce …
- Fichier publique, librement distribué
- Renferme une date de validité
- Signé numériquement par une autorité de certification (AC)
- Le propriétaire du certificat est le seul à posséder la clé privée associée

Clef publique Nom du propriétaire Période de validité Attributs Nom de l'AC Signature du certificat avec la clef privée de l'AC

Exemple d'utilisation

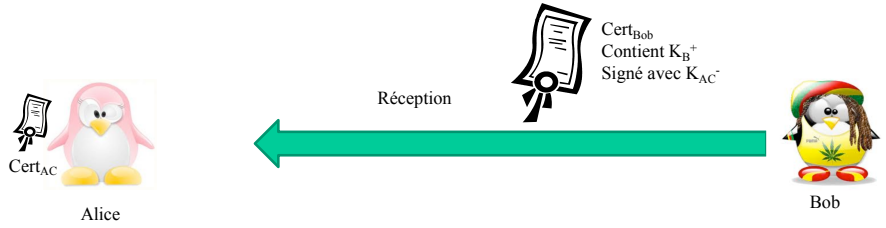
Alice

Alice possède le
certificat de l'autorité de confiance avec K_{AC}^{+}

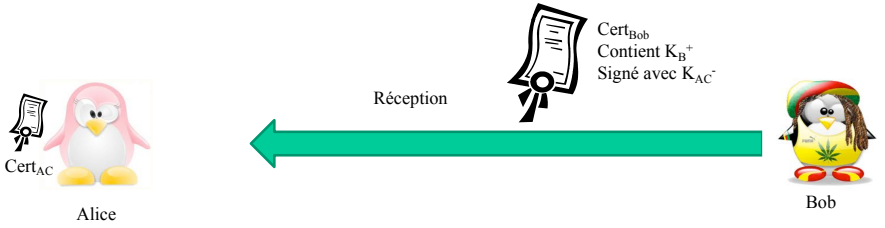
Bob

$Cert_{Bob}$
Contient K_B^{+}
Signé avec K_{AC}^{-}

Exemple d'utilisation



Exemple d'utilisation



Valide la provenance de $Cert_{Bob}$ signé par l'AC
Fait confiance à K_B^+ -> considère que c'est bien Bob qui possède K_B^-
Envoi du contenu chiffré que seul Bob peut déchiffrer
Par exemple, envoi de la clé de chiffrement K_{A-B}

$K_B^+(K_{A-B})$

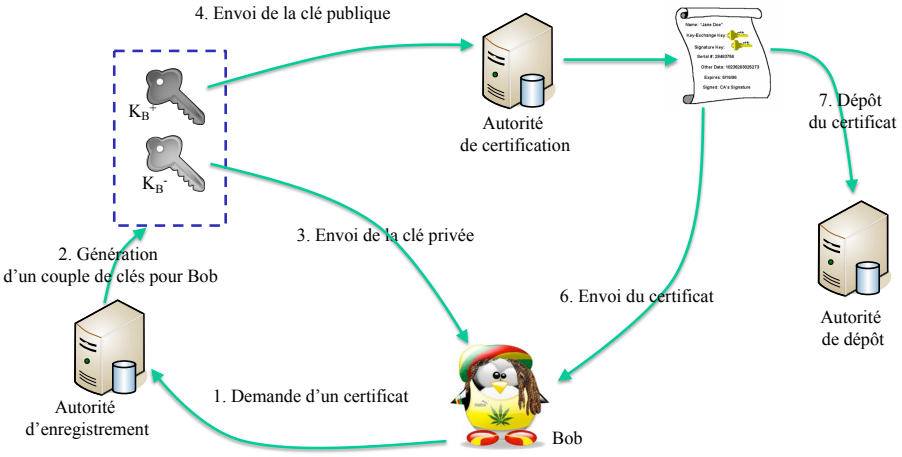
PKI

- PKI : Public Key Infrastructure
- Infrastructure nécessaire au fonctionnement d'un ou plusieurs ACs, afin de délivrer des certificats
  - Locaux (avec la protection qui y est attachée)
  - Ordinateurs
  - Logiciels (technologies clés : SSL/TLS, X.509)
  - Personnels
  - Mécanismes organisationnels : délivrance, révocation
  - Mécanismes administratifs : désignation d'un responsable moral

Services d'une PKI

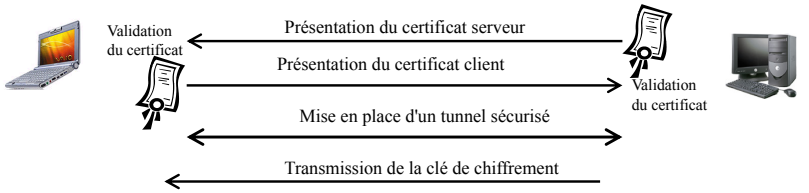
- Vérification de l'identité du titulaire lors de la création d'un certificat
- Publication du certificat
  - Mise en œuvre d'une interface de publication des certificats émis (par ex. Web)
- Renouvellement du certificat
- Révocation des certificats
- Publication des listes de certificats révoqués auprès des ACs

PKI : schéma fonctionnel



Les principaux algorithmes d'authentification supportés par EAP (1)

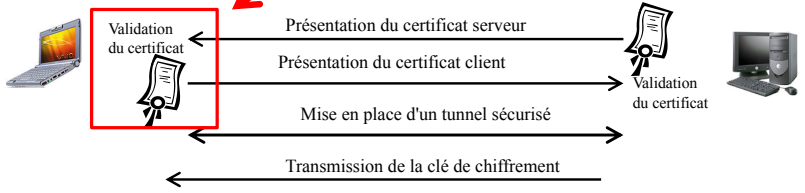
- **EAP-TLS** (*Transport Layer Security*)
  - Intégré à la certification WiFi en Mai 2005
  - Authentification mutuelle du client et du serveur par le biais de certificats (côté client et côté serveur)
  - S'appuie sur les phases d'authentification de SSL / TLS (*Secure Sockets Layer*)
  - Très sécurisé, mais complexe (et souvent coûteux) à mettre en œuvre - nécessité d'une PKI ou infrastructure à clé public pour gérer la distribution des certificats en direction des clients mobiles
  - Utilisé par free dans le cadre de son SSID « freephonie »



Les principaux algorithmes d'authentification supportés par EAP (1)

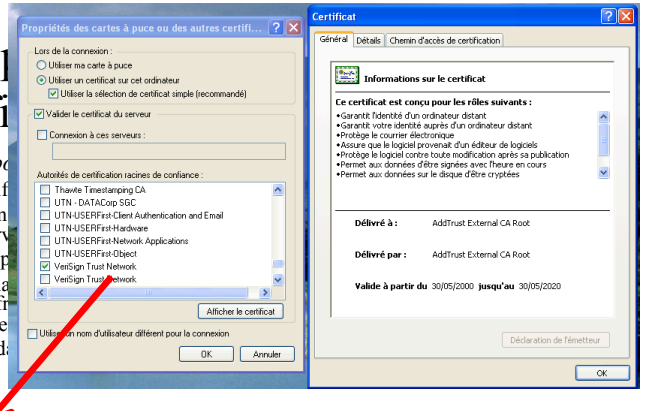
- **EAP-TLS** (*Transport Layer Security*)
  - Intégré à la certification WiFi
  - Authentification mutuelle du client et côté serveur)
  - S'appuie sur les phases d'auth
  - Très sécurisé, mais complexe d'une PKI ou infrastructure à direction des clients mobiles
  - Utilisé par free dans le cadre de son SSID « freephonie »

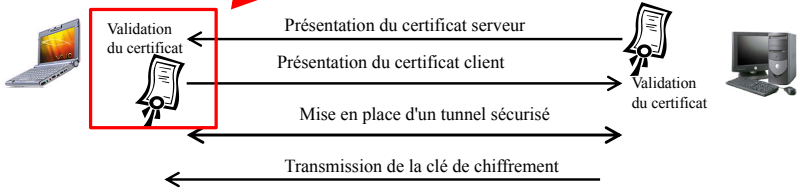
Le client valide le certificat, car il fait confiance à l'autorité qui a signé le certificat = le client a installé la clé publique de l'autorité de certification



Les p… d'authentifi…

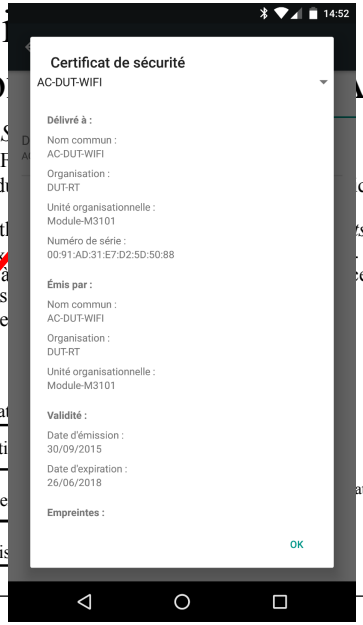
- **EAP-TLS** (*Transpo…*)
  - Intégré à la certif…
  - Authentification … client et côté serv…
  - S'appuie sur les p…
  - Très sécurisé, ma… d'une PKI ou infr… direction des clie…
  - Utilisé par free d…





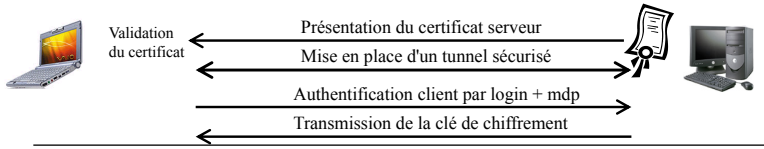
Les princi… d'authentificatio… …AP (1)

- **EAP-TLS** (*Transport Layer S…*
  - Intégré à la certification WiF…
  - Authentification mutuelle d… …cats (côté client et côté serveur)
  - S'appuie sur les phases d'aut… …*s Layer*)
  - Très sécurisé, mais complex… …nécessité d'une PKI ou infrastructur… …certificats en direction des clients mo…
  - Utilisé par free dans le cadre…



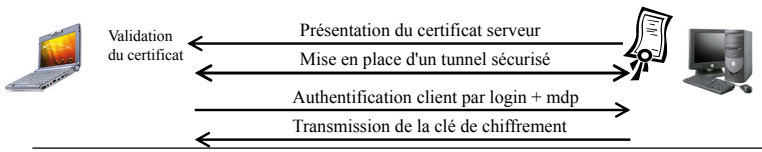
Les principaux algorithmes d'authentification supportés par EAP (2)

- **EAP-TTLS** (*Tunneled TLS*) et **EAP-PEAP** (*Protected EAP*)
  - Deux méthodes très proches, intégrées à la certification WiFi en Mai 2005
  - Utilisation d'un certificat coté serveur
  - Etablissement d'un tunnel chiffré TLS entre le client et le serveur Radius, puis envoi de l'authentification client
  - Deux sous-versions introduites PEAP dans la certification WiFi en Mai 2005 : PEAPv0 et PEAPv1
    - Standard ouvert (IETF) soutenu par Microsoft (PEAPv0), Cisco, et RSA Security
    - PEAPv0 s'appuie sur *MSCHAPv2* (login + mdp), et PEAPv1 sur GTC (Generic Tocken Card)
  - EAP-TTLS s'appuie sur un *hashage* MS-CHAPv2 (login + mdp)
  - Plus faciles à déployer que TLS, pas de certificats à distribuer aux clients
  - Possibilité de connecter le serveur Radius à une base LDAP existante dans le cas d'une authentification par login + mdp



Les principaux algorithmes d'authentification supportés par EAP (2)

- **EAP-TTLS** (*Tunneled TLS*) et **EAP-PEAP** (*Protected EAP*)
  - Deux méthodes très proches, intégrées à la certification WiFi en Mai 2005
  - Utilisation d'un certificat coté serveur
  - Etablissement d'un tunnel chiffré TLS entre le client et le serveur Radius, puis envoi de l'authentification client
  - Deux sous-versions introduites PEAP dans la certification WiFi en Mai 2005 : PEAPv0 et PEAPv1
    - Standard ouvert (IETF) soutenu par Microsoft (PEAPv0), Cisco, et RSA Security
    - PEAPv0 s'appuie sur *MSCHAPv2* (login + mdp), et PEAPv1 sur GTC (Generic Tocken Card)
  - EAP-TTLS s'appuie sur un *hashage* MS-CHAPv2 (login + mdp)
  - Plus faciles à déployer que TLS, pas de certificats à distribuer aux clients
  - Possibilité de connecter le serveur Radius à une base LDAP existante dans le cas d'une authentification par login + mdp



Les principaux algorithmes d'authentification supportés par EAP (3)

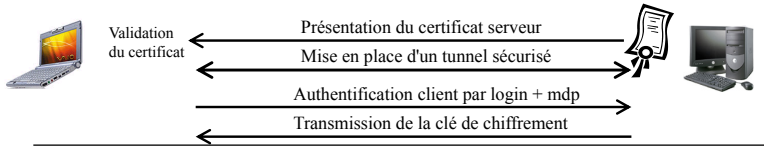
2007	3.720310	c8:85:50:95:1c:93	00:12:01:b5:6c:d0	EAP	80	Response, Identity
11366	28.140914	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	EAP	122	Request, Identity
11379	28.213160	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	EAP	73	Request, Protected EAP (EAP-PEAP)
11382	28.250929	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	TLSv1	1091	Server Hello, Certificate, Server Key Exchange, Ignored Unknown Record
11385	28.278780	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	TLSv1	1087	Server Hello, Certificate, Server Key Exchange, Ignored Unknown Record
11392	28.304835	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	TLSv1	1087	Server Hello, Certificate, Server Key Exchange, Ignored Unknown Record
11400	28.331207	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	TLSv1	1087	Server Hello, Certificate, Server Key Exchange, Ignored Unknown Record
11414	28.360475	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	TLSv1	1087	Server Hello, Certificate, Server Key Exchange, Ignored Unknown Record
11415	28.377553	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	TLSv1	1087	Server Hello, Certificate, Server Key Exchange, Ignored Unknown Record
11417	28.387322	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	TLSv1	1087	Server Hello, Certificate, Server Key Exchange, Ignored Unknown Record
11445	28.484846	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	TLSv1	132	Server Hello, Certificate, Server Key Exchange, Ignored Unknown Record
11469	28.496308	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	TLSv1	110	Application Data
11475	28.506301	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	TLSv1	142	Application Data
11478	28.520585	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	TLSv1	158	Application Data
11481	28.530985	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	TLSv1	110	Application Data
11483	28.540654	00:12:43:4e:18:91	00:ee:bd:9e:5f:e7	EAP	71	Success
12304	31.270343	00:12:43:4e:18:91	30:75:12:e2:80:fd	EAP	122	Request, Identity
12306	31.272426	30:75:12:e2:80:fd	00:12:43:4e:18:91	EAP	90	Response, Identity
12312	31.333537	00:12:43:4e:18:91	30:75:12:e2:80:fd	EAP	73	Request, Tunneled TLS EAP (EAP-TTLS)
12314	31.342053	30:75:12:e2:80:fd	00:12:43:4e:18:91	TLSv1	271	Client Hello
12323	31.416009	00:12:43:4e:18:91	30:75:12:e2:80:fd	TLSv1	1101	Server Hello, Certificate, Server Key Exchange, Server Hello Done
12326	31.421887	30:75:12:e2:80:fd	00:12:43:4e:18:91	EAP	73	Response, Tunneled TLS EAP (EAP-TTLS)
12352	31.489836	00:12:43:4e:18:91	30:75:12:e2:80:fd	TLSv1	1101	Server Hello, Certificate, Server Key Exchange, Server Hello Done
12354	31.497207	30:75:12:e2:80:fd	00:12:43:4e:18:91	EAP	73	Response, Tunneled TLS EAP (EAP-TTLS)
12360	31.567319	00:12:43:4e:18:91	30:75:12:e2:80:fd	TLSv1	1101	Server Hello, Certificate, Server Key Exchange, Server Hello Done
12376	31.576949	30:75:12:e2:80:fd	00:12:43:4e:18:91	EAP	73	Response, Tunneled TLS EAP (EAP-TTLS)
12405	31.678910	00:12:43:4e:18:91	30:75:12:e2:80:fd	TLSv1	1101	Server Hello, Certificate, Server Key Exchange, Server Hello Done
12408	31.685649	30:75:12:e2:80:fd	00:12:43:4e:18:91	EAP	73	Response, Tunneled TLS EAP (EAP-TTLS)
12417	31.745859	00:12:43:4e:18:91	30:75:12:e2:80:fd	TLSv1	1078	Server Hello, Certificate, Server Key Exchange, Server Hello Done

Les principaux algorithmes d'authentification supportés par EAP (4)

```
▶ Frame 12417: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▶ IEEE 802.11 QoS Data, Flags: ......F.C
▶ Logical-Link Control
▼ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: EAP Packet (0)
    Length: 1011
  ▼ Extensible Authentication Protocol
      Code: Request (1)
      Id: 7
      Length: 1011
      Type: Tunneled TLS EAP (EAP-TTLS) (21)
    ▶ EAP-TLS Flags: 0x80
      EAP-TLS Length: 5097
    ▶ [5 EAP-TLS Fragments (5097 bytes): #12323(1024), #12352(1024), #12360(1024), #12405(1024), #12417(1001)]
    ▼ Secure Sockets Layer
      ▶ TLSv1 Record Layer: Handshake Protocol: Server Hello
      ▶ TLSv1 Record Layer: Handshake Protocol: Certificate
      ▶ TLSv1 Record Layer: Handshake Protocol: Server Key Exchange
      ▶ TLSv1 Record Layer: Handshake Protocol: Server Hello Done
```


Les principaux algorithmes d'authentification supportés par EAP (5)

- **EAP-TTLS** *(Tunneled TLS)* et **EAP-PEAP** *(Protected EAP)*
  - Deux méthodes très proches, intégrées à la certification WiFi en Mai 2005
  - Utilisation d'un certificat coté serveur
  - Etablissement d'un tunnel chiffré TLS entre le client et le serveur Radius, puis envoi de l'authentification client
  - Deux sous-versions introduites PEAP dans la certification WiFi en Mai 2005 : PEAPv0 et PEAPv1
    - Standard ouvert (IETF) soutenu par Microsoft (PEAPv0), Cisco, et RSA Security
    - PEAPv0 s'appuie sur *MSCHAPv2* (login + mdp), et PEAPv1 sur GTC (Generic Tocken Card)
  - EAP-TTLS s'appuie sur un *hashage* MS-CHAPv2 (login + mdp)
  - Plus faciles à déployer que TLS, pas de certificats à distribuer aux clients
  - Possibilité de connecter le serveur Radius à une base LDAP existante dans le cas d'une authentification par login + mdp



Les principaux algorithmes d'authentification supportés par EAP (6)

- **EAP-MD5** *(Message Digest 5)*
  - Le client s'authentifie par mot de passe auprès du serveur
  - Même gestion des *challenges* que le protocole CHAP (utilisé par PPP)
  - Pas de support de distribution des clefs de session
  - Sécurité faible, non reconnu par la certification WiFi
- **EAP-LEAP** *(Lightweight EAP)*
  - Méthode propriétaire CISCO
  - Transmission d'une authentification chiffrée via *MSCHAPv2*
  - Meilleure sécurité que EAP-MD5, mais les attaques par dictionnaire sont toujours possibles
  - Non intégré à la certification WiFi
- **EAP-FAST** *(Flexible Authentication via Secure Tunneling)*
  - Méthode propriétaire CISCO, prise en charge par les bornes Aironet, et la suite logicielle « Cisco Fast Secure Roaming » (*cf.* partie « gestion de la mobilité »)
  - Amélioration de la sécurité par rapport à LEAP
  - Pas de certificat, authentification par login + mdp
  - Intégré à la certification WiFi

Les principaux algorithmes d'authentification supportés par EAP (7)

- **EAP-SIM**
  - Intégré à la certification WiFi, RFC 4186
  - Utilisation des informations de la puce SIM, pour effectuer l'authentification du client
  - Utilisé par des opérateurs (en France Free et SFR) pour l'authentification de leurs abonnées mobiles sur un SSID réservé sur chacune des Box ADSL
  - Très proche de EAP-TLS, utilisation d'un *credential* SIM
- **EAP-AKA et EAP-AKA'**
  - Intégré à la certification WiFi, RFC 4187
  - Utilisation des schémas d'authentification et des mécanismes de session de clé de chiffrement des réseaux cellulaires de 3ième génération (UMTS et CDMA2000)
  - Réponse EAP fournit le *subscriber's InternationalMobile Subscriber Identity* (IMSI) contenu dans le *UMTS Subscriber Identity Module* (USIM)
  - Très proche de EAP-TLS, utilisation d'un *credential* USIM

Récapitulatif

Principales méthodes d'authentification EAP (1)

Type EAP	Distribution dynamique des clefs de chiffrement	Méthode d'authentification	Certification WiFi	Remarques
EAP-TLS EAP-SIM EAP-AKA EAP-AKA'	Oui	Certificat (ou équivalent) côté client et serveur	Oui	Certificats complexes à gérer côté client Authentification mutuelle Largement supporté
EAP-MD5	Non	Login + MdP côté client	Non	Facile à mettre en œuvre Supporté par beaucoup de serveurs Pas d'authentification mutuelle
EAP-FAST	Oui	Login + MdP côté client	Oui	Solutions Cisco, utilisées dans le cadre du « Fast Secure Raoming »
EAP-TTLS	Oui	Login – MdP côté client + certificat (obligatoire côté serveur, optionnel côté client)	Oui	Création d'un tunnel TLS sûr Authentification mutuelle
EAP-PEAP	Oui	Différentes authentification côté client + certificat côté serveur	Oui	Création d'un tunnel TLS sûr, supporté par Microsoft Authentification mutuelle

Récapitulatif

Principales méthodes d'authentification EAP (2)

Type EAP	Distribution dynamique des clefs de chiffrement	Méthode d'authentification	Certification WiFi	Exploité dans Passpoint
EAP-TLS EAP-SIM EAP-AKA EAP-AKA'	Oui	Certificat (ou équivalent) côté client et serveur	Oui	Oui
EAP-MD5	Non	Login + MdP côté client	Non	Non
EAP-FAST	Oui	Login + MdP côté client	Oui	Non
EAP-TTLS	Oui	Login – MdP côté client + certificat (obligatoire côté serveur, optionnel côté client)	Oui	Oui
EAP-PEAP	Oui	Différentes authentification côté client + certificat côté serveur	Oui	Non

Support de 802.1x

- L'AP doit supporter le relai des messages 802.1x
  - L'ordre des séquences EAP dépend du type d'authentification retenu, il faut s'assurer que le type EAP visé est bel et bien supporté
- De nombreux clients supportent 802.1x, sans pour autant implémenter toutes les authentifications EAP
  - Fonctions nativement intégrées à Windows XP SP2, Vista, Seven et Windows 8 : TLS, SIM, PEAPv0
  - Fonctions intégrées à MAC OS X : TLS, TTLS, PEAPv0, LEAP, FAST, MD5
  - *Supplicant* spécifique fourni avec un composant WiFi (exemple Intel Centrino) …

Wi-Fi CERTIFIED Interoperability Certificate

This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing. Learn more: www.wi-fi.org/certification/programs

Certification ID: WFA16851 Page 1 of 2

Date of Last Certification	April 19, 2013
Company	Cisco Systems
Product	Cisco Aironet 2600 Series AIR-SAP2602
Model Number	AIR-SAP2602
Product Identifier(s)	
Category	Enterprise/Service Provider Access Point, Switch/Controller or Router
Hardware Version	Product: , Wi-Fi Component:
Firmware Version	Product: 15.2(20130305), Wi-Fi Component:
Operating System	Proprietary / Other:
Frequency Band(s)	2.4 GHz, 5 GHz - Concurrent

Summary of Certifications

CLASSIFICATION	PROGRAM
Connectivity	Wi-Fi CERTIFIED™ a, b, g, n
	WPA™ – Enterprise, Personal
	WPA2™ – Enterprise, Personal
Optimization	WMM®
	WMM®-Power Save

Wi-Fi CERTIFIED™ Interoperability Certificate

Certification ID: WFA16851 Page 2 of 2

Security

WPA™ – Enterprise, Personal
WPA2™ – Enterprise, Personal
EAP Type(s):
EAP-TLS
EAP-TTLS/MSCHAPv2
PEAPv0/EAP-MSCHAPv2
PEAPv1/EAP-GTC
EAP-SIM
EAP-AKA
EAP-AKA Prime
EAP-FAST

Wi-Fi CERTIFIED™ a

Wi-Fi CERTIFIED™ b

Wi-Fi CERTIFIED™ g

Wi-Fi CERTIFIED™ n

2.4 GHz, 5 GHz - Concurrent
Tx 3 tested Spatial Streams 2.4 GHz
Rx 3 tested Spatial Streams 2.4 GHz
Tx 3 tested Spatial Streams 5 GHz
Rx 3 tested Spatial Streams 5 GHz
Short Guard Interval
TX A-MPDU
STBC Transmit
40 MHz operation in 5 GHz

WMM®

WMM®-Power Save

Spectrum and Regulatory Features

802.11d
802.11h

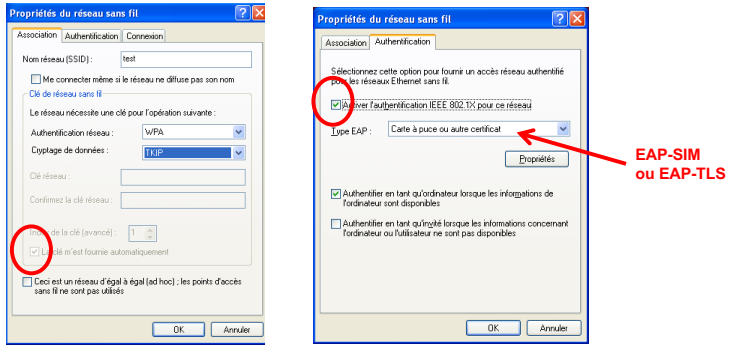
Support de 802.1x

- Côté OS mobile …
  - Iphone : EAP-SIM/AKA, EAP-TLS, EAP-TTLS, EAP-PEAP
  - Android (dépend des implémentations), mais le plus souvent : EAP-SIM/AKA, EAP-TLS, EAP-TTLS, EAP-PEAP
- Le problème se posent de manière identique au niveau du serveur Radius
  - Tous les modes d'authentification EAP ne sont pas toujours supportés, en fonction du serveur utilisé
    - FreeRadius : TLS, TTLS, PEAPv0, PEAPv1, LEAP
    - HP UX AAA Server : TLS, TTLS, PEAPv0, PEAPv1, MD5, SIM, AKA

Configuration de 802.1x (1)

Client / AP / Serveur

Au niveau du client, pour un SSID donné
- Activation de l'authentification 802.1x
- Choix de l'authentification EAP



Configuration de 802.1x (2)

Client / AP / Serveur

- Côté AP, configuration d'un SSID
  - Caché ou public
  - Authentification « EAP/802.1x »
  - Relai des messages EAP vers un serveur Radius défini par son adresse IP
  - Chiffrement des messages EAP/RADIUS via un mot de passe configuré dans l'AP et dans le serveur Radius

Configuration de 802.1x (2)

Client / AP / Serveur

- Configuration du serveur radius
  - Acceptation des messages EAP/Radius provenant d'un AP défini par son adresse IP
  - Chiffrement / déchiffrement des messages EAP/Radius via un mot de passe (identique à celui configuré dans l'AP)

Mise en œuvre de la sécurité dans les réseaux 802.11

Rappel de la problématique générale

➢ **Présentation des mécanismes intégrés aux produits WiFi**

Mécanismes d'entrée dans un réseau WiFi

Mécanismes de chiffrement WEP, TKIP, AES

Mécanismes d'authentification 802.1x

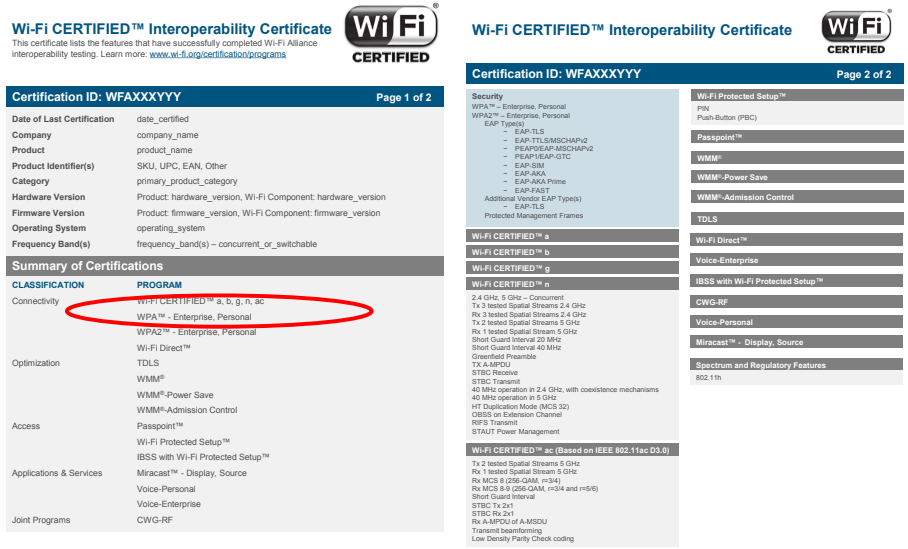
Spécifications WPA et WPA2, norme 802.11i

Déploiement d'un réseau multi SSID

WPA

WiFi Protected Access™

- Introduit dans la certification WiFi en 2003
- Supportée par de nombreux matériels (AP et cartes), et OS (depuis Windows XP SP1, MAC OS X.3, Linux, Android, IOS, WM)
  - Sur des matériels anciens, nécessitait une mise à jour du *firmware* (à condition que le constructeur la fournisse)
  - ☹ Des matériels anciens « marqués » du logo WiFi n'ont jamais supporté la spécification WPA (mais le problème n'existe plus pour les matériels récents)
  - Ne demande pas plus de puissance matériel que le WEP
  - Demande de son abandon progressif par la WiFi alliance en Mars 2015
- Deux versions : WPA *personal* (authentification PSK) et WPA *enterprise* (authentification EAP/802.1x)
- Deux caractéristiques majeurs
  - Support de **TKIP** (*Temporal Key Integrity Protocol*), compatibilité avec WEP
  - Utilisation de l'authentification **802.1x** pour la version enterprise



Wi-Fi CERTIFIED™ Interoperability Certificate

This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing. Learn more: www.wi-fi.org/certification/programs

Wi Fi CERTIFIED

Certification ID: WFAXXXYYY Page 1 of 2

Date of Last Certification	date_certified
Company	company_name
Product	product_name
Product Identifier(s)	SKU, UPC, EAN, Other
Category	primary_product_category
Hardware Version	Product: hardware_version, Wi-Fi Component: hardware_version
Firmware Version	Product: firmware_version, Wi-Fi Component: firmware_version
Operating System	operating_system
Frequency Band(s)	frequency_band(s) – concurrent_or_switchable

Summary of Certifications

CLASSIFICATION	PROGRAM
Connectivity	Wi-Fi CERTIFIED™ a, b, g, n, ac
	WPA™ - Enterprise, Personal
	WPA2™ - Enterprise, Personal
	Wi-Fi Direct™
Optimization	TDLS
	WMM®
	WMM®-Power Save
	WMM®-Admission Control
Access	Passpoint™
	Wi-Fi Protected Setup™
	IBSS with Wi-Fi Protected Setup™
Applications & Services	Miracast™ - Display, Source
	Voice-Personal
	Voice-Enterprise
Joint Programs	CWG-RF

Wi-Fi CERTIFIED™ Interoperability Certificate

Wi Fi CERTIFIED

Certification ID: WFAXXXYYY Page 2 of 2

Security
WPA™ – Enterprise, Personal
WPA2™ – Enterprise, Personal
EAP Type(s):
- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAP0/EAP-MSCHAPv2
- PEAP1/EAP-GTC
- EAP-SIM
- EAP-AKA
- EAP-AKA Prime
- EAP-FAST

Additional Vendor EAP Type(s)
- EAP-TLS

Protected Management Frames

Wi-Fi CERTIFIED™ a

Wi-Fi CERTIFIED™ b

Wi-Fi CERTIFIED™ g

Wi-Fi CERTIFIED™ n

2.4 GHz, 5 GHz – Concurrent
Tx 3 tested Spatial Streams 2.4 GHz
Rx 3 tested Spatial Streams 2.4 GHz
Tx 2 tested Spatial Streams 5 GHz
Rx 1 tested Spatial Stream 5 GHz
Short Guard Interval 20 MHz
Short Guard Interval 40 MHz
Greenfield Preamble
TX A-MPDU
STBC Receive
STBC Transmit
40 MHz operation in 2.4 GHz, with coexistence mechanisms
40 MHz operation in 5 GHz
HT Duplication Mode (MCS 32)
OBSS on Extension Channel
RIFS Transmit
STAUT Power Management

Wi-Fi CERTIFIED™ ac (Based on IEEE 802.11ac D3.0)

Tx 2 tested Spatial Streams 5 GHz
Rx 1 tested Spatial Stream 5 GHz
Rx MCS 8 (256-QAM, r=3/4)
Rx MCS 8-9 (256-QAM, r=3/4 and r=5/6)
Short Guard Interval
STBC Tx 2x1
STBC Rx 2x1
Rx A-MPDU of A-MSDU
Transmit beamforming
Low Density Parity Check coding

Wi-Fi Protected Setup™
PIN
Push-Button (PBC)

Passpoint™

WMM®

WMM®-Power Save

WMM®-Admission Control

TDLS

Wi-Fi Direct™

Voice-Enterprise

IBSS with Wi-Fi Protected Setup™

CWG-RF

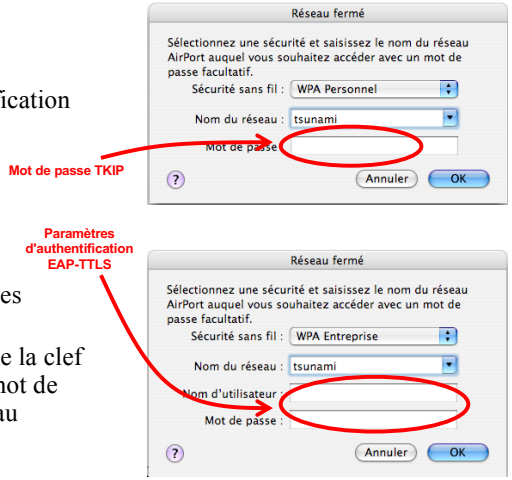
Voice-Personal

Miracast™ - Display, Source

Spectrum and Regulatory Features
802.11h

Les deux versions de WPA

- *Personal* ou WPA-PSK
  - Pas de serveur d'authentification
  - Pré-distribution des clefs (*pre-shared key*)
- *Enterprise* ou WPA
  - Nécessite un serveur d'authentification externe (Radius), qui authentifie les utilisateurs via 802.1x
  - Distribution dynamique de la clef (PMK) via EAP, pas de mot de passe TKIP à configurer au niveau du client



WPA2

WiFi Protected Access 2™

- Spécification par le consortium WiFi en Septembre 2004
  - WPA2 *personal* et WPA2 *enterprise*
- Compatible avec la spécification WPA
- Apparition des premiers produits WPA2 en Septembre 2004
- S'appuie sur les spécifications de la norme **802.11i**
  - TKIP est remplacé par AES - CCMP
  - Le support de TKIP/WEP est maintenu (compatibilité avec WPA), mais son utilisation est formellement déconseillée (pour WEP) et déconseillée (pour TKIP depuis Mars 2015)
- En résumé
  - WEP « statique » ⊂ WPA ⊂ WPA2
- Spécification de WPA3 en 2018

Wi-Fi CERTIFIED™ Interoperability Certificate

This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing. Learn more: www.wi-fi.org/certification/programs

Certification ID: WFAXXXYYY Page 1 of 2

Date of Last Certification	date_certified
Company	company_name
Product	product_name
Product Identifier(s)	SKU, UPC, EAN, Other
Category	primary_product_category
Hardware Version	Product: hardware_version, Wi-Fi Component: hardware_version
Firmware Version	Product: firmware_version, Wi-Fi Component: firmware_version
Operating System	operating_system
Frequency Band(s)	frequency_band(s) – concurrent_or_switchable

Summary of Certifications

CLASSIFICATION	PROGRAM
Connectivity	Wi-Fi CERTIFIED™ a, b, g, n, ac
	WPA2™ - Enterprise, Personal
Optimization	TDLS
	WMM®
	WMM®-Power Save
	WMM®-Admission Control
Access	Passpoint™
	Wi-Fi Protected Setup™
	IBSS with Wi-Fi Protected Setup™
Applications & Services	Miracast™ - Display, Source
	Voice-Personal
	Voice-Enterprise
Joint Programs	CWG-RF

Wi-Fi CERTIFIED™ Interoperability Certificate

Certification ID: WFAXXXYYY Page 2 of 2

Security
WPA™ – Enterprise, Personal
WPA2™ – Enterprise, Personal
EAP Type(s)
- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAP0/EAP-MSCHAPv2
- PEAP1/EAP-GTC
- EAP-SIM
- EAP-AKA
- EAP-AKA Prime
- EAP-FAST

Additional Vendor EAP Type(s)
- EAP-TLS

Protected Management Frames

Wi-Fi CERTIFIED™ a

Wi-Fi CERTIFIED™ b

Wi-Fi CERTIFIED™ g

Wi-Fi CERTIFIED™ n
2.4 GHz, 5 GHz – Concurrent
Tx 3 tested Spatial Streams 2.4 GHz
Rx 3 tested Spatial Streams 2.4 GHz
Tx 2 tested Spatial Streams 5 GHz
Rx 1 tested Spatial Stream 5 GHz
Short Guard Interval 20 MHz
Short Guard Interval 40 MHz
Greenfield Preamble
TX A-MPDU
STBC Receive
STBC Transmit
40 MHz operation in 2.4 GHz, with coexistence mechanisms
40 MHz operation in 5 GHz
HT Duplication Mode (MCS 32)
OBSS on Extension Channel
RIFS Transmit
STAUT Power Management

Wi-Fi CERTIFIED™ ac (Based on IEEE 802.11ac D3.0)
Tx 2 tested Spatial Streams 5 GHz
Rx 1 tested Spatial Stream 5 GHz
Rx MCS 8 (256-QAM, r=3/4)
Rx MCS 8-9 (256-QAM, r=3/4 and r=5/6)
Short Guard Interval
STBC Tx 2x1
STBC Rx 2x1
Rx A-MPDU of A-MSDU
Transmit beamforming
Low Density Parity Check coding

Wi-Fi Protected Setup™
PIN
Push-Button (PBC)

Passpoint™

WMM®

WMM®-Power Save

WMM®-Admission Control

TDLS

Wi-Fi Direct™

Voice-Enterprise

IBSS with Wi-Fi Protected Setup™

CWG-RF

Voice-Personal

Miracast™ - Display, Source

Spectrum and Regulatory Features
802.11h

Mise en œuvre de la sécurité dans les réseaux 802.11

Rappel de la problématique générale

Présentation des mécanismes intégrés aux produits WiFi

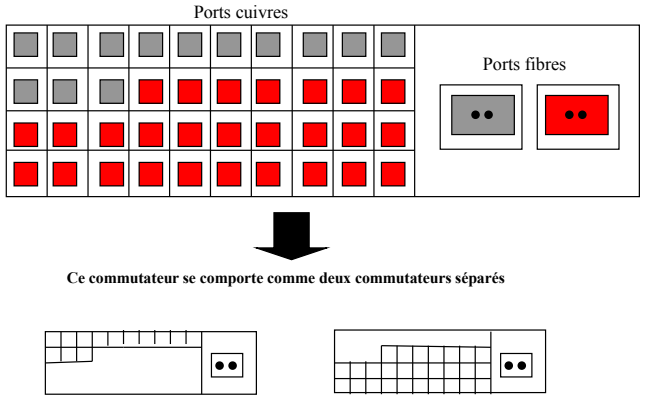
➢ **Déploiement d'un réseau multi SSID**

Utilisation de VLANs

Ethernet : problématique

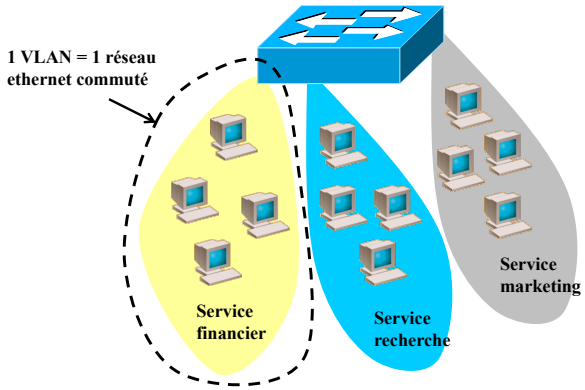
- Sur un réseau Ethernet
  - Un utilisateur a accès à toutes les stations de son réseau commuté
- Nécessité dans de nombreux cas de séparer les utilisateurs dans différents réseaux commutés
  - Grouper les utilisateurs qui ont de « bonnes raisons » d'échanger des données
  - Exemple : découpage d'une entreprise en services, un service = un réseau Ethernet commuté
    - Sécurité = les étudiants ne « voient » pas les enseignants (ex. Rennes 1)
    - Séparation des flux, permet d'éviter qu'un réseau n'en surcharge un autre

Séparation logique des flux en VLANs



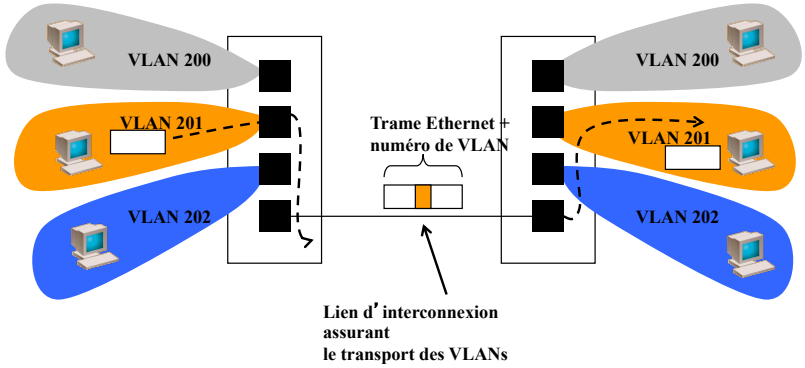
Configuration logicielle des ports du commutateur sur différents réseaux logiques (=VLAN ou *Virtual Lan*)
Exemple avec 2 VLANs :

Séparation logique des flux en VLANs

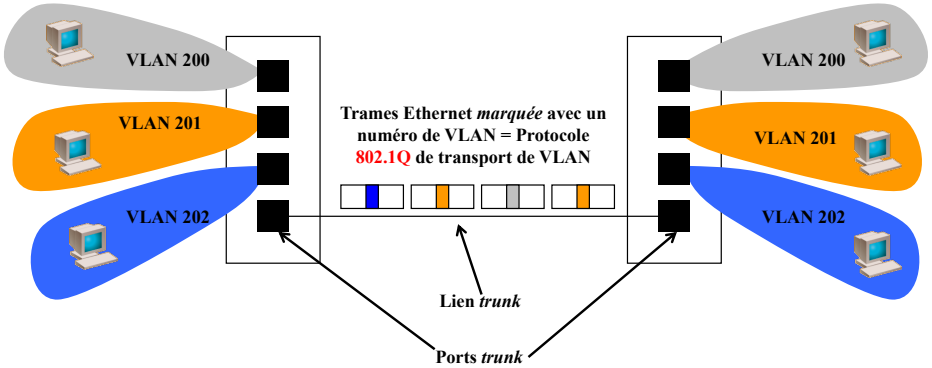


Transport de VLANs

- Un lien unique d'interconnexion transporte tous le trafic entre deux commutateurs

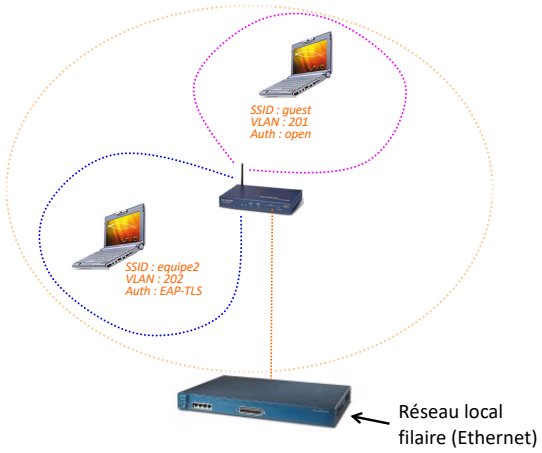


Transport de VLANs



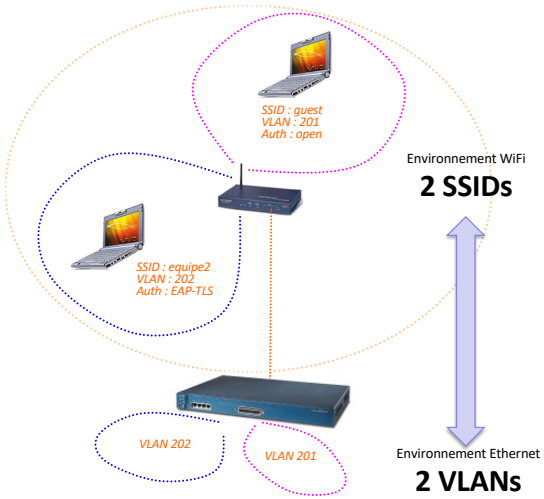
Exploitation multi-SSID

- Un SSID = une population spécifique d'utilisateurs
- Par exemple
  - un SSID ouvert pour les invités
  - un SSID avec une authentification forte EAP-TLS pour les personnels de l'entreprise



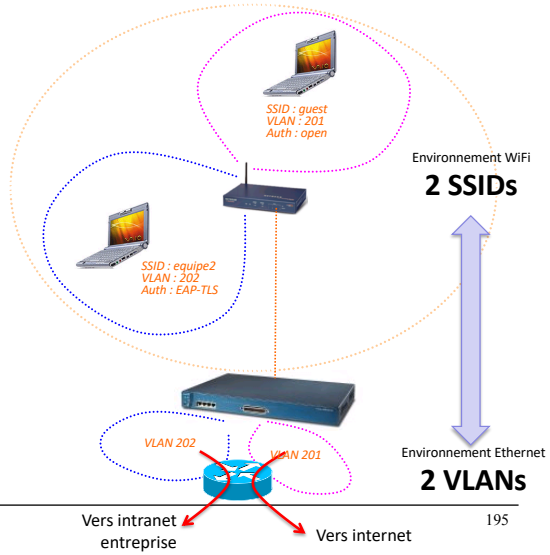
Lien SSID <-> VLAN

- Avoir plusieurs SSID n'a aucun intérêt si tous les utilisateurs se retrouvent sur le même réseau Ethernet
- En fonction du SSID de rattachement, l'utilisateur mobile se retrouve dans un VLAN spécifique

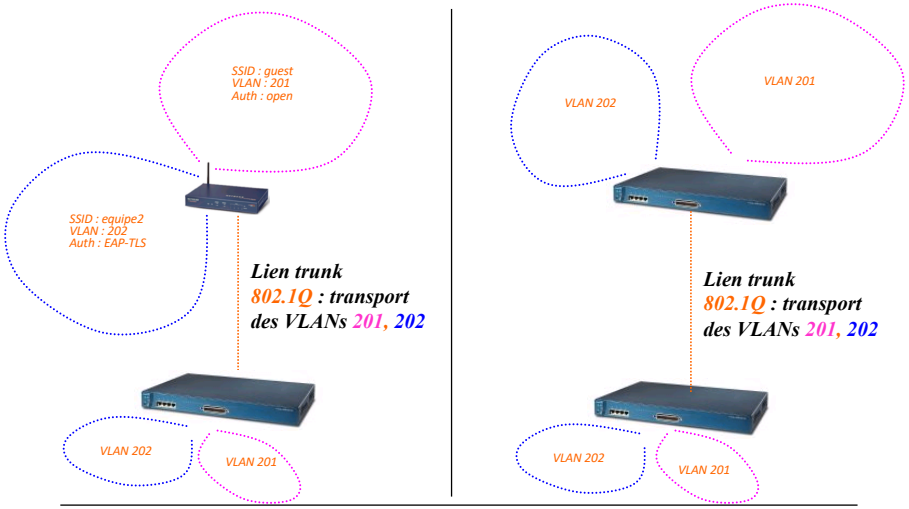


Lien SSID <-> VLAN

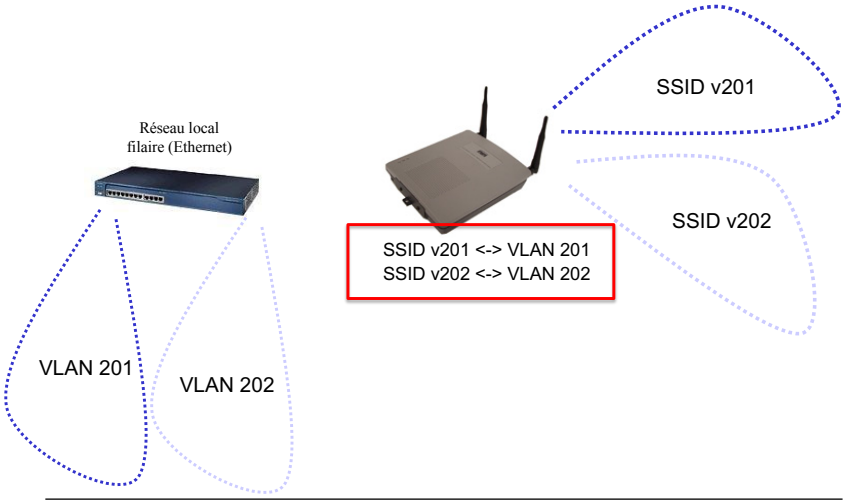
- Avoir plusieurs SSID n'a aucun intérêt si tous les utilisateurs se retrouvent sur le même réseau Ethernet
- En fonction du SSID de rattachement, l'utilisateur mobile se retrouve dans un VLAN spécifique
  - SSID ouvert <-> VLAN spécifique permettant d'aller uniquement vers Internet
  - SSID protégé par EAP-TLS <-> VLAN permettant d'accéder à l'intranet



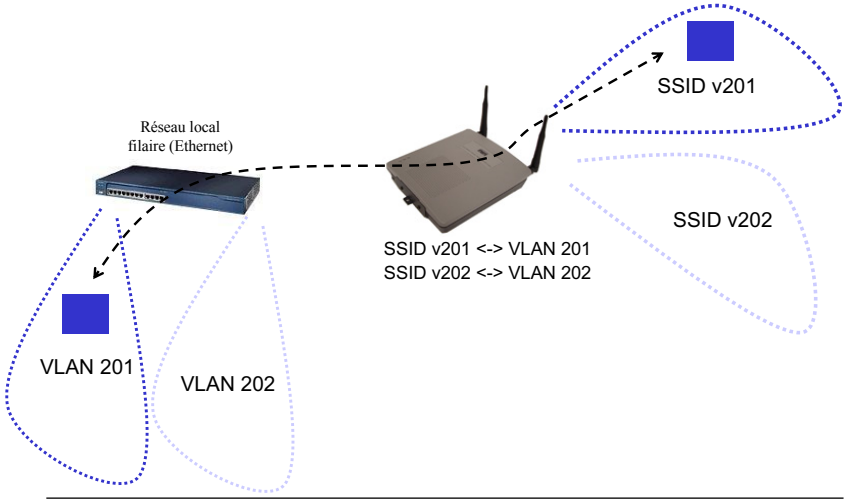
Principe



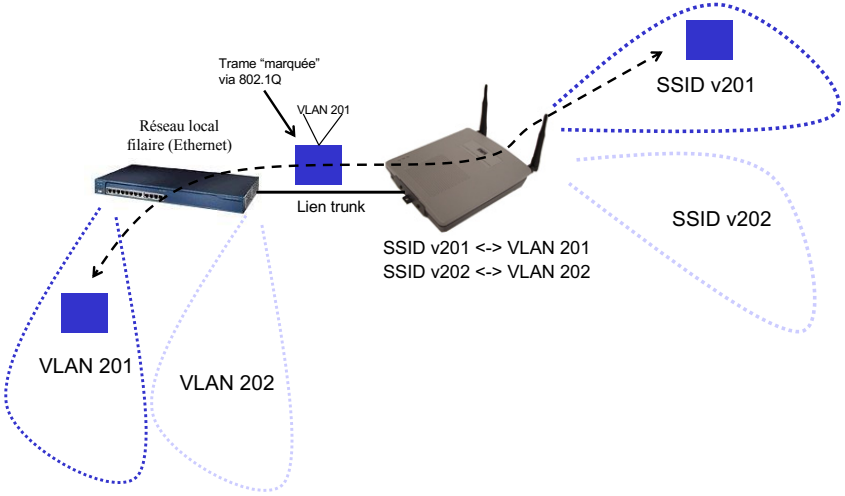
Utilisation des VLANs



Utilisation des VLAN



Utilisation des VLAN



En résumé …

Auth. 802.11	Auth. équip[t]	chiffrement	Radius nécessaire	Commentaire
open	non	non	non	Aucune sécurité. Ce mode peut être utilisé dans un Hot Spot public, en conjonction avec un VPN et/ou un portail captif, ou bien sur un WLAN « invité » d'une entreprise, ne donnant accès qu'aux réseaux externes à cette entreprise.
PSK	non	WEP	non	Solution complexe à utiliser, tant pour le client que pour l'administrateur de l'AP. Sécurité faible, exploitée uniquement par des matériels anciens 802.11b ne supportant pas la mise à jour WPA.
PSK	non	TKIP	non	Nécessite le support WPA personal, susceptible donc de ne pas pouvoir être mis en œuvre sur du matériel 802.11b ancien. Solution simple à utiliser, tant pour le client que pour l'administrateur. Bonne sécurité du lien. Pas d'authentification de l'utilisateur. Convient bien pour de petites configurations (cadre domestique, LAN sans fil avec un seul AP). Plus recommandé par la WiFi Alliance depuis Mars 2015.
PSK	non	AES	non	Nécessite le support WPA2 entreprise, ne fonctionne qu'avec des matériels récents. Même argument que le cas précédent, avec une sécurité du lien accru (chiffrement AES).
open	802.1x	WEP « statique »	oui	Authentification client grâce à un serveur Radius, l'efficacité repose sur la méthode retenue (TLS, TTLS, PEAP …). MD5 ne doit pas être retenu. La faiblesse de cette solution vient de l'utilisation du WEP statique. Doit être utilisé avec des matériels anciens 802.11b ne supportant pas la mise à jour WPA.
open	802.1x	TKIP	oui	Nécessite le support WPA enterprise. Solution adaptée pour un réseau d'entreprise. Une connexion 802.1x via EAP/TLS, EAP/TTLS ou EAP-PEAP à un WLAN, chiffré via TKIP, offre un niveau de sécurité suffisant pour accéder aux VLANs du réseau d'entreprise. . Plus recommandé par la WiFi Alliance depuis Mars 2015.
open	802.1x	AES	oui	Nécessite le support WPA2 enterprise. Même argument que le cas précédent. La solution « classique » pour accéder de manière sécurisé à un réseau WiFi d'entreprise.
open	@MAC	optionnel	optionnel	Méthode d'authentification obsolète et peu sécurisée.

Les stratégies de sécurité en résumé …

- Activer le WPA2 (plutôt que WPA en voie d'obsolescence)
  - Version *personal* (PSK) dans un cadre SOHO, le mot de passe est donné à un groupe restreint d'utilisateurs
  - Version *enterprise* en entreprise, en conjonction avec un serveur d'authentification Radius, utilisation d'une authentification forte (EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA)
- En accès « public » (HotSpot), ou sur un réseau invité dans une entreprise
  - Difficile dans l'immédiat d'utiliser l'authentification et le chiffrement WPA / WPA2
  - Adoption attendue de WiFi Passpoint (Hotspot 2.0) ?
- Faille *crack* publiée en Octobre 2017
  - Travaux en cours de la WiFi Alliance sur WPA3

Passpoint : vers des HotSpot « facilement » sécurisés ?

➢**Sécurisation d'un réseau WiFi « public »**
Exploitation d'un portail captif
Utilisation de tunnels VPNs
➢Mise en œuvre de WiFi *Passpoint*

Déploiement de réseaux WiFi ouverts

- Accès public à l'Internet via des cellules WiFi
  - Gare, hôtel, mairie, université …
  - Destinés à une population « non identifiable » *a priori*, contrairement aux réseaux d'entreprise
    - Pas de maîtrise sur le matériel client utilisé, sur le niveau de formation des utilisateurs
- Complexe dans ce contexte d'utiliser la sécurité WiFi *enterprise* / EAP 802.1x
  - Comment authentifier un utilisateur ?

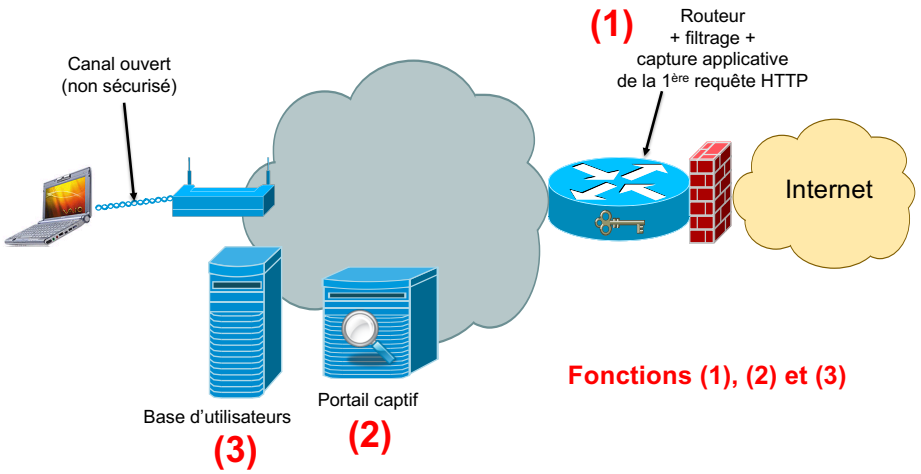
➔ Utilisation d'un portail captif et des technologies Web

Portail captif (1)

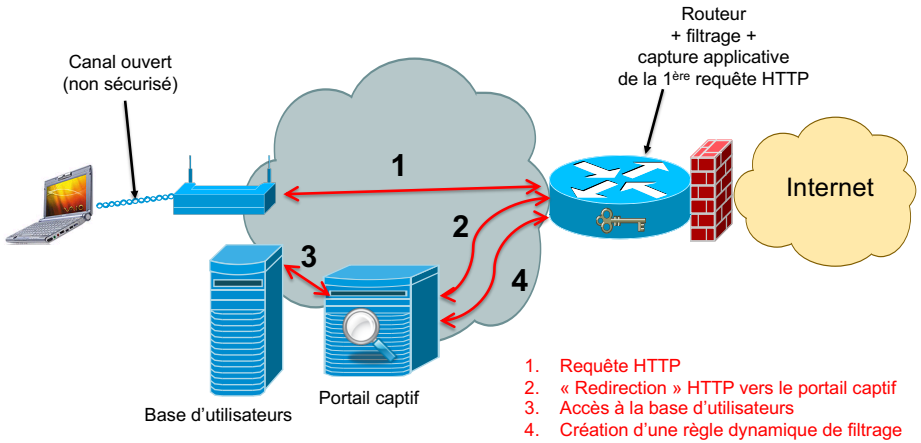
- SSID
  - Visible sans configuration, car diffusé dans les trames balises de l'AP
  - Ouvert, sans chiffrement, sans authentification
- Après rattachement au SSID, l'utilisateur obtient une configuration IP via DHCP
  - Tout le trafic IP est interdit sur le réseau WiFi, sauf http
- L'utilisateur lance son navigateur WEB (http ou https)
  - Quel que soit l'URL demandé, une page Web d'authentification lui est retournée
- Après l'authentification …
  - Les informations liées à l'adresse IP et l'adresse physique (adresse MAC) de l'utilisateur sont envoyées vers la passerelle IP (un routeur) afin d'ouvrir l'accès vers Internet

Portail captif (2)

Portail captif (3)



Portail captif (4)



1. Requête HTTP
2. « Redirection » HTTP vers le portail captif
3. Accès à la base d'utilisateurs
4. Création d'une règle dynamique de filtrage

Portail captif (5)

- Intégration de toutes ces fonctions (1)-(2)-(3) dans un seul « boitier » réseau
- Exemples
  - Intégré au contrôleur WiFi
  - Intégré à l'AP
  - Assemblage de logiciels *open source* sous Linux comme Alcasar - http://www.alcasar.net/
  - *Appliance* dédié (ou VM), par exemple gamme Ucopia

Portail captif (6)

- Repose sur un assemblage de techniques « plus ou moins » standard
  - Ex. : exploitation de la redirection http
- Anticipation de la 1ère requête http par les terminaux mobiles
  - Réseau ouvert –> envoi automatique d'une requête http « vide »
  - Comportement parfois aléatoire en fonction du terminal, automatisation difficile
- Problème de dimensionnement
  - Nombre d'accès simultanés, réglage du timeout des sessions

Passpoint : vers des HotSpot « facilement » sécurisés ?

➢**Sécurisation d'un réseau WiFi « public »**

Exploitation d'un portail captif

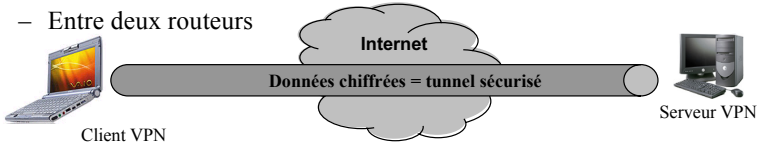
Utilisation de tunnels VPNs

➢Mise en œuvre de WiFi *Passpoint*

Réseaux privés virtuels (1)

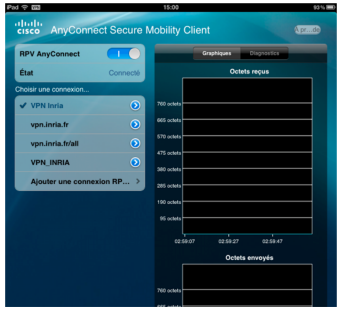
VPN - *Virtual Private Network*

- Les réseaux ouverts assurent l'authentification via le portail captif, mais pas le chiffrement
  - « Officiellement », la protection des données est à la charge de l'utilisateur, pas du réseau WiFi
  - ➔ Utilisation des technologies VPN, courantes dans le cadre des accès nomades (WiFi, xDSL, cellulaires)
- Etablissement d'un tunnel de communication chiffré entre deux extrémités, sur un réseau « ouvert » (par ex. Internet)
  - Entre un client et un serveur VPN
  - Entre deux routeurs



Réseaux privés virtuels (2)

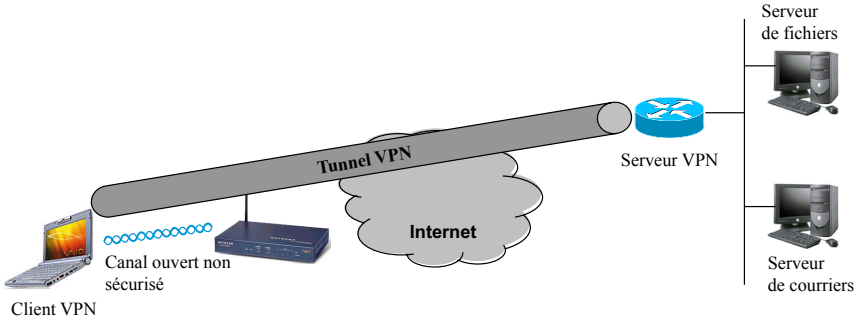
- De nombreux OS intègrent de manière native des clients VPN
  - Windows XP/Vista/Seven, Mac OS X, Linux
  - Intégration aux OS *Smartphones* : iphone, android
- Existence de clients VPN « externes »
  - Ex. client Cisco
- Différentes technologies possibles
  - IPSec (chiffrement des données au niveau IP)
  - SSL (chiffrement des données au dessus de la couche transport)
- Un VPN se traduit par un accès authentifié
  - MdP, certificats, carte à puce …
- Principaux inconvénients
  - Perte de débit
  - Surcharge logicielle au niveau client



Réseaux privés virtuels (3)

Utilisation dans le cadre d'un réseau WiFi

- HotSpot public, non sécurisé
- Réseau « invité » d'un réseau d'entreprise, accédé via un SSID public (annoncé dans les trames *beacon*) et sans authentification (*open*)



Passpoint : vers des HotSpot « facilement » sécurisés ?

- Sécurisation d'un réseau WiFi « public »
  - Exploitation d'un portail captif
  - Utilisation de tunnels VPNs
- **Mise en œuvre de WiFi *Passpoint***
  - **Problématique**

Certification WiFi

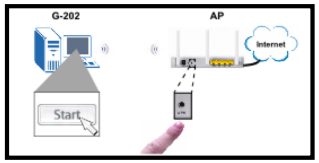
1. **Connectivité**
   - 802.11 a/b/g/n/ac, WiFi direct
2. **Sécurité**
   - WPA/WPA2

   → **Authentification + chiffrement du lien radio**
3. **Accès**
   - WPS, Passpoint

   → **Configuration de la sécurité**
4. **Applications et services**
   - Miracast, Voice Enterprise, Voice Personal, WiFi Aware
5. **Optimisation**
   - TDLS, WMM, WMM Power Save, WMM Admission Control
6. **Coexistence RF**
   - CWG-RF

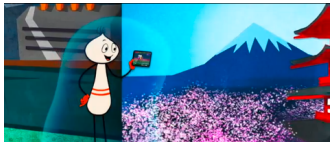
WPS - WiFi Protected Setup

- Hors normalisation IEEE, profil fonctionnel destiné à la sécurisation des accès WiFi domestiques (SOHO)
- Description fonctionnelle des différentes étapes côté AP et client WiFi pour sécuriser un lien WPA / WPA2 *personal*
  - Le mot de passe sert à l'authentification et au chiffrement, il est indispensable = éviter les réseaux WiFi « ouvert » dans un cadre SOHO
- WPS = Configuration « facile » d'un mot de passe à l'identique au niveau de l'AP et du client WiFi
- Deux modes
  - PIN - appairage (*peering*) par code
  - PBC - utilisation d'un bouton sur l'AP



WiFi Passpoint

- Certification hors IEEE, créée en 2012
  - Appelé également HotSpot 2.0
- Vidéo « officielle » de présentation
  http://www.youtube.com/watch?feature=player_embedded&v=hw2Z6OuNQE4#
- Accès transparent et automatisé et sécurisé aux *Hotspots* (accès WiFi public)



source Wi-Fi Alliance

WiFi Passpoint®

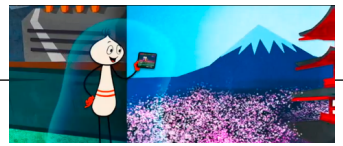
- Accès à un réseau WiFi public (ex. une gare)
  - Authentification « hors sécurité WiFi »
  - Portail captif Web
  - Pas de chiffrement

WiFi Passpoint

- Accès à un réseau WiFi protégé via des mécanismes de sécurité WPA2 *enterprise*
  - Authentification forte (EAP/802.1x)
  - Chiffrement (AES)
- … difficile à mettre en œuvre/configurer automatiquement quand
  - Le réseau ne connaît pas la population d'utilisateurs (qui ? quand ? avec quel terminal mobile ?)
  - Le terminal ne connaît pas le réseau (quel SSID ? Pour quel opérateur ?)

WiFi Passpoint – première vue « simple »

- S'appuie sur 802.11u pour la découverte et la sélection d'un réseau WiFi public d'opérateur = transmission par l'AP de balises spécifiques
- Prise en charge transparente de WPA2 *enterprise*
  - WPA2 *enterprise* = authentification EAP « externalisée » vers un serveur externe AAA Radius
  - Comment l'exploiter dans un réseau WiFi public (réseau WiFi opérateur par exemple) sans pré-configuration complexe ?
    - Ex. récent : EAP-SIM exploité sur le réseau ***Free_WiFi_secure*** des Freebox
- ***WiFi Passpoint*** = prise en charge transparente de différents types d'authentification EAP, à partir du moment où le réseau WiFi est visible via des balises étendus 802.11u envoyées par les APs du réseau public
  - Prise en charge d'EAP-TLS, EAP-SIM, EAP-AKA, EAP-AKA', EAP-TTLS



WiFi Passpoint – première vue « simple »

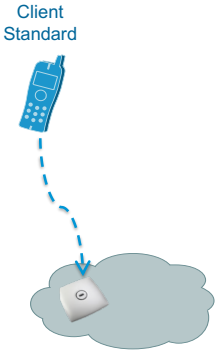
WiFi Passpoint – première vue « simple »

- La certification WiFi offre deux mécanismes d'authentification : PSK et 802.1x/EAP
- *WPS* simplifie la configuration de la clé PSK
- A priori, *Passpoint* est le « pendant » de WPS pour l'authentification 802.1x/EAP
  - Les *beacon* étendus 802.11u de Passpoint sont l'équivalent du « *push button* »
- … pas si simple
  - Passpoint est complexe et dépasse largement le cadre d'une simple autoconfiguration de la sécurité WPA2

Scénario classique

Configuration manuelle

1. Sélection du réseau WiFi (vulnérabilité au rogue AP)
2. Aller à la page d'authentification Web
3. Parcourir la page Web et saisir les données d'identification (*credential*), le plus souvent Id + password
4. Accéder à Internet



Au final, deux approches possibles pour un terminal

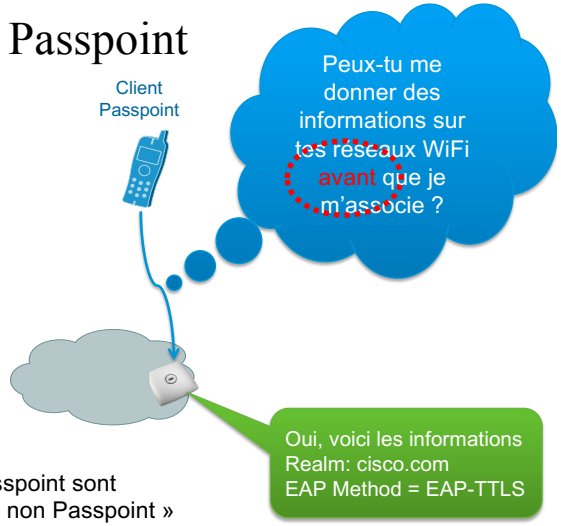
1. Exploiter un SSID connu et préconfiguré (réseaux favoris du terminal)
2. S'associer à chaque réseau découvert et ouvert en testant l'accès à Internet

Limite -> impossible d'exploiter un réseau protégé (i.e. sécurisé) non connu a priori par le terminal, le terminal doit être « pré-autorisé » à utiliser le réseau

Scénario Passpoint

Configuration automatique

1. Le terminal valide automatiquement le réseau et initie la connexion



Aspect essentiel : les réseaux Passpoint sont compatibles avec des terminaux « non Passpoint »

Administration d'un réseau WiFi

➢**APs lourds vs. APs légers**

Gestion centralisée via le protocole CAPWAP

Approche à base d'APs « lourds » (1)

- Tous les mécanismes permettant la mise en œuvre du réseau WiFi se trouvent dans l'AP
  - Gestion individuelle des canaux utilisés par chaque AP
    - 802.11h n'offre qu'une « vision locale » des canaux utilisés
    - Peu efficace dans le cas d'un déploiement dense
  - Gestion de la QoS au niveau MAC (voir la partie QoS du cours)
    - Pas de notion d'AP « busy » et d'AP « empty »
  - Décision de déclenchement du *roaming*
    - Déclenchement sur la base de l'état du lien avec le client
    - Dialogue inter-AP via le réseau filaire
  - Sécurité
    - Relais des messages d'authentification
    - Relais des clés de chiffrement
    - Chiffrement / déchiffrement des trames

Approche à base d'APs « lourds » (2)

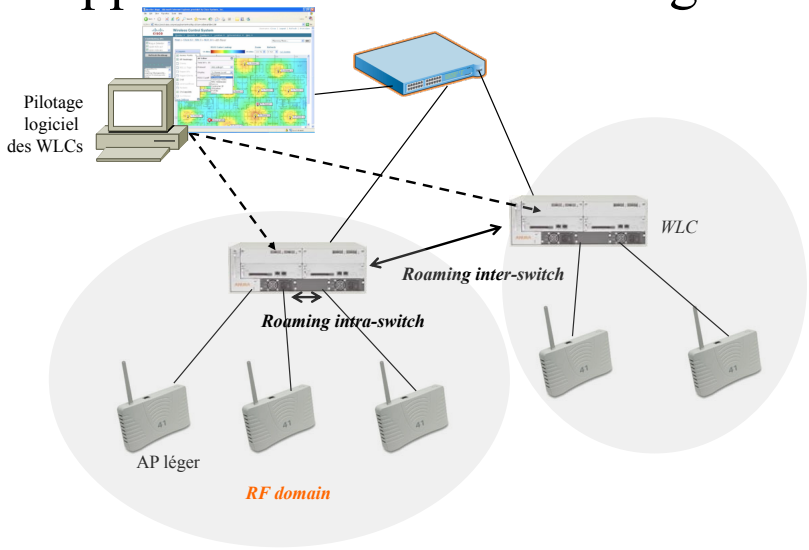
- Approche fortement distribuée, qui présente plusieurs inconvénients
  - Impossibilité d'avoir une vue globale du réseau WiFi, difficulté de déploiement
    - Complexité de la planification radio
      - Comment choisir la fréquence de fonctionnement d'un AP ?
    - Difficulté d'étendre l'architecture WiFi, un nouvel AP peut perturber les APs déjà présents, sachant que le nombre de fréquences disponibles reste limité
  - Configuration et administration
    - Chaque AP est configuré individuellement
      - Mise à jour logicielle, ajout d'un SSID, d'un VLAN, d'une politique de chiffrement …
  - Supervision
    - Mise en œuvre de la sécurité
      - Comment détecter un AP « intrus » (*rogue AP*)
  - Complexité du *roaming* inter-AP
    - Le maintien des clef de chiffrement et de la QoS nécessite une entité centralisée

Approche à base d'APs « légers »

Thin AP

- L'« intelligence » est déportée de l'AP vers le commutateur
  - L'AP devient un simple pont radio
  - C'est un équipement spécifique sur le réseau Ethernet, le **WLC** (*Wireless Lan Controller*), qui gère la couche MAC, ainsi qu'un groupe de points d'accès
- Possibilité de configuration automatique (*plug and play*) des APs
- Ex. de produit : Aruba AP130 series + 6000 mobility controler
  - Mesure de l'intensité du signal entre la station mobile et l'AP léger
  - La décision de *hand-over* est prise par le commutateur central
  - Latence annoncée par le constructeur : moins de 2-3 ms *intra-switch*, 10-15 ms *inter-switch*
- Des approches propriétaires pour gérer la signalisation entre un AP et son WLC
  - Airespace, racheté par Cisco (protocole LWAPP), Aruba (protocole PAPI) et Trapeze (protocole SLAPP)

Approche à base d'APs « légers »



Les principaux acteurs

- Cisco (Airspace)
  http://www.cisco.com/c/en/us/products/wireless/index.html
- Juniper (Trapeze) http://www.juniper.net/fr/fr/products-services/wireless/
- Zebra technology (Motorola/Symbol)
  https://www.zebra.com/qb/en/products/networks/wireless-lan.html
- HP (Aruba) http://www.arubanetworks.com/solutions/all-wireless-workplace/
- Ruckus
  http://www.ruckuswireless.com/

Liens vérifiés Nov. 2015

Administration d'un réseau WiFi

APs lourds vs. APs légers

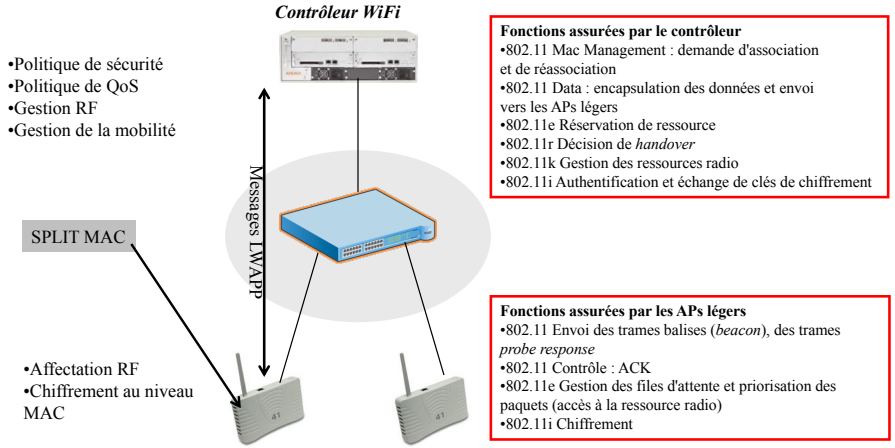
➢**Gestion centralisée via le protocole CAPWAP**

Normalisation CAPWAP

Control And Provisionning of Wireless Access Points

- Normalisation conduite par l'IETF
- Protocole de contrôle entre un contrôleur LAN (WLC) et des APs légers
  - L'approche multi-constructeurs doit devenir possible
  - **Ne modifie en rien les normes existantes côté station mobile** (802.11 a/b/g/n/ac, 802.11 e/i/r/k/v …)
- Le protocole LWAPP (Airspace, racheté par Cisco) a été choisi par l'IETF pour servir de base à la normalisation CAPWAP
  - Première version finalisée en Mars 2009, RFC 5416 - *CAPWAP binding for IEEE 802.11*
  - Intégration CAPWAP dans les produits Cisco, pas d'adoption « forte » des autres constructeurs pour le moment
  - Par ex. ARUBA attend officiellement la maturation de CAPWAP, et conserve son protocole PAPI

« Vision » CAPWAP



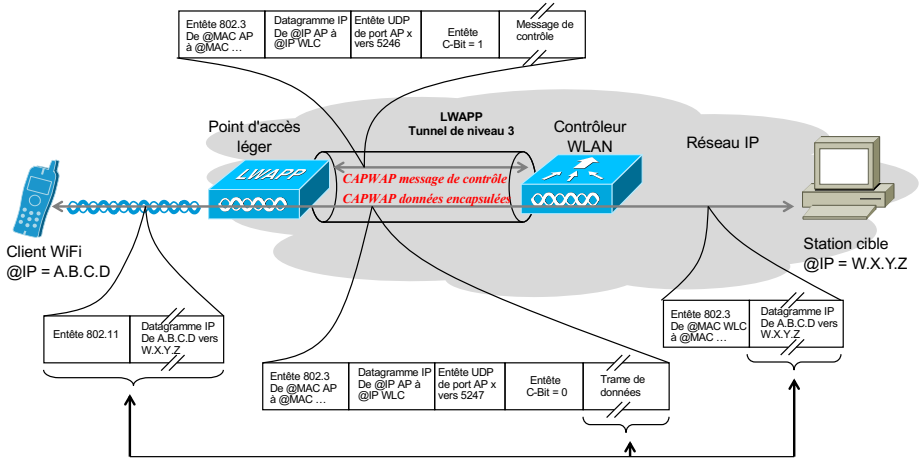
Ex. de solution Cisco
WLC série 2500

- Différentes licences
  - Un contrôleur permet de piloter de 5, 15, 25 ou 50 Aps
- 4 ports 802.3, dont 2 ports PoE réservés à des branchements d'APs
- Peut être couplé avec le logiciel WCS permettant de piloter des groupes de WLCs

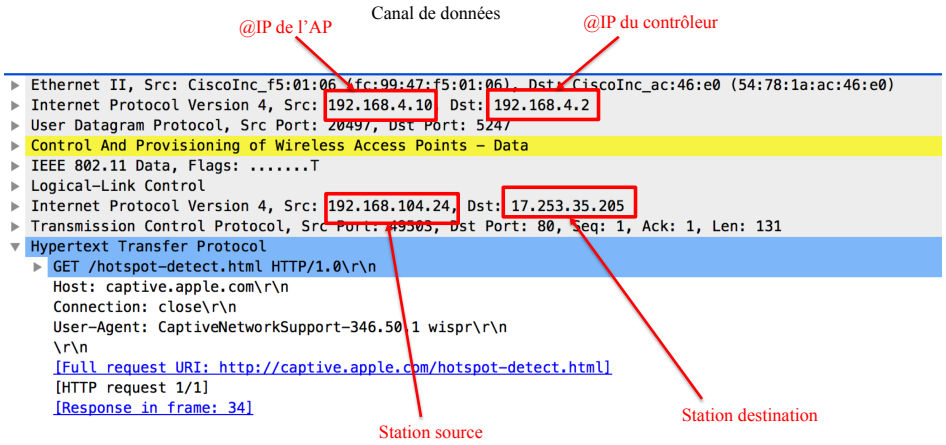
Ex. de solution Cisco
WLC série 8540

- Différentes licences
  - Permet de piloter jusqu'à 6000 APs et 64000 clients mobiles
  - 4 ports 1Gb/s ou 10Gb/s
  - Fonctionnement centralisé ou *Flexconnect*
  - Support 802.11ac, Passpoint

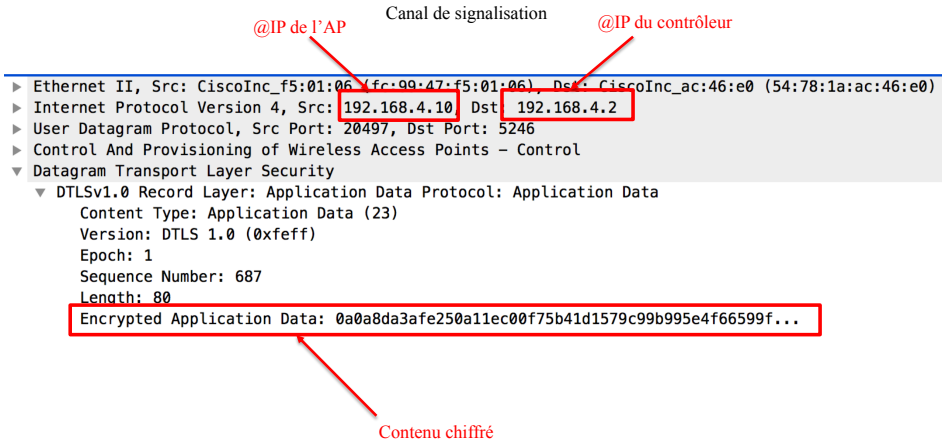
Transport CAPWAP au niveau 3



Exemple d'encapsulation CAPWAP



Exemple d'encapsulation CAPWAP



Fonctionnement CAPWAP

- Deux canaux de communication entre l'AP et le WLC
  - Un canal de signalisation chiffré en AES
  - Un canal de données non chiffré, le réseau filaire est considéré comme un réseau de confiance (séparation des flux via des VLANs par ex.)
- Fourniture à l'AP par le WLC de la configuration : SSID, sécurité, QoS …
- Le WLC interroge périodiquement l'AP via le canal de signalisation pour récupérer des statistiques
  - Mise en œuvre du *dynamic radio resource management* (RRM), gestion des alarmes …
- L'AP envoie périodiquement un message de présence au WLC toutes les 30 secondes
  - En cas d'indisponibilité du WLC, l'AP relance une phase de découverte de WLC

Exemples de fonctions évoluées

- Surveillance des ressources radio
- Assignation dynamique des canaux
- Détection et gestion des interférences
- TPC dynamique
- Equilibrage de charge entre les WLCs
- IDS, détection des *APs rogue*
- *Roaming* de niveau 3

Exemples de fonctions évoluées

Assignation dynamique d'un canal en réaction à une interférence