La sécurité des réseaux sans fil

Slides préparés depuis le livre :

WiFi Professionnel, La norme 802.11, le déploiement, la sécurité, de Aurélien Géron.

Dunod, 2009

1. Objectif

- La question de la sécurité est sans doute la première que se pose une société lorsqu'elle se penche sur le WiFi.
- Si l'on communique à travers les ondes, tout le monde peut capter les communications.
- Heureusement, il existe à présent des solutions très robustes pour rendre un réseau sans fil tout aussi sécurisé qu'un réseau filaire.

1. Objectif

- Dans ce chapitre, nous commencerons par définir ce qu'est la sécurité dans un environnement sans fil, et nous ferons le tour des solutions de sécurité existantes.

2. Les services de sécurité

- **La confidentialité :** l'accès aux données doit être réservé aux personnes autorisées.
  - Cela suppose un mécanisme **d'identification des utilisateurs**, la définition des **règles d'accès**, et la **protection des données pendant leur transport**, par le biais d'un cryptage.
- **L'intégrité :** Il faut en particulier pouvoir s'assurer que ce qui est reçu correspond bien à ce qui a été envoyé.
- **La disponibilité** : le réseau doit être accessible en tout temps et dans des conditions acceptables.
- **Authentification** : entity authentication or identification : corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.)

3. Une politique globale

- Assurer la sécurité d'un système impose une vision globale et pas uniquement technique : cela implique de mettre en place une organisation de sécurité transversale et indépendante dans l'entreprise, de définir une politique globale, et d'assurer la sécurité à tous les échelons : en particulier aux niveaux organisationnel, humain, données, logiciels, réseau et physique.

3. Une politique globale

- L’ensemble du système informatique doit être compartimenté et les droits des utilisateurs doivent être restreints pour éviter qu’une personne connectée au réseau, comme un visiteur ou même un employé, puisse tout faire.

4. Les attaques contre le réseau wifi

1. **L'espionnage:'l'écoute'**
    1. un pirate se poste à proximité et surveille les échanges. On dit qu'il « sniffe » le réseau sans fil.
    2. Avec le WiFi, chacun peut écouter ce qui est transmis par les autres. Il suffit pour cela de disposer d'un **adaptateur WiFi gérant le mode *monitor,*** c'est-à-dire capable de lire tous les messages, et pas uniquement ceux qui lui sont adressés. Ensuite, il faut utiliser un logiciel d'analyse du réseau.
    3. Écouter une communication WiFi est à la portée de presque tout le monde.

Sniffing..

- L'espionnage peut aboutir à la divulgation d'informations confidentielles : mots de passe, documents secrets, numéros de cartes bancaires, etc.
- Aussi, pour sécuriser les échanges, il est indispensable de crypter les communications avec un algorithme aussi puissant que possible, sans que cet algorithme ne ralentisse trop la communication.

2. L’intrusion

- Une autre attaque consiste à s’introduire au sein du réseau WiFi pour consulter voire modifier les données du système informatique (bases de données, fichiers, e-mails...) ou encore pour profiter de la connexion à Internet.
- L’intrusion est bien sûr tout à fait triviale si aucune sécurité n’est mise en œuvre : il suffit de s’associer normalement à l’un des AP du réseau. Si non le pirate :
  - ouvre une nouvelle session en se faisant passer pour un utilisateur légitime ;
    - *Attaque de dictionnaire.*
  - détourne une session existante (*hijacking).*

a. Attaque de dictionnaire

- Si les mots de passe sont échangés « en clair » ,il suffit d'attendre qu'un utilisateur légitime se connecte et d'espionner l'envoi de son mot de passe.
- Si le mot de passe est crypté, on peut essayer de s'attaquer à l'algorithme de cryptage utilisé.
- Une autre technique consiste à essayer des millions de mots de passe jusqu'à trouver le bon ! On parle donc d'attaques de « dictionnaire ».

Attaque de dictionnaire

- Il existe deux variantes de l'attaque de dictionnaire:
  - l'attaque « en ligne » et
  - l'attaque « hors-ligne ».
- Solution :
  - Idéalement, les mots de passe des utilisateurs doivent être assez long et complexes pour qu'il soit impossible de les deviner en quelques tentatives
  - Le système doit détecter et bloquer les attaques de dictionnaire en ligne, et il doit également utiliser un protocole d'authentification invulnérable aux attaques de dictionnaire horsligne.
  - Attention au *verifier*.

b. *Détourner une session existante*

- L'identification des utilisateurs est souvent un mécanisme assez coûteux en temps et en ressources informatiques : elle suppose en général l'accès à une base de données des utilisateurs.
- Il serait inconcevable de mettre en œuvre le mécanisme complet d'identification à chaque fois qu'un paquet de données est reçu.

b. *Détourner une session existante*

- Une solution courante consiste à utiliser simplement l'adresse MAC, du poste de l'utilisateur qui a été identifié.
- Par exemple, si on a bien identifié l'utilisateur « Ali» à l'adresse « 00:04:23:8B:B5:0B », on accepte dorénavant tous les paquets de données en provenance de cette adresse.

Scénario d'usurpation d'adresse MAC

- Malheureusement, il existe des adaptateurs WiFi dont on peut changer l'adresse MAC!!

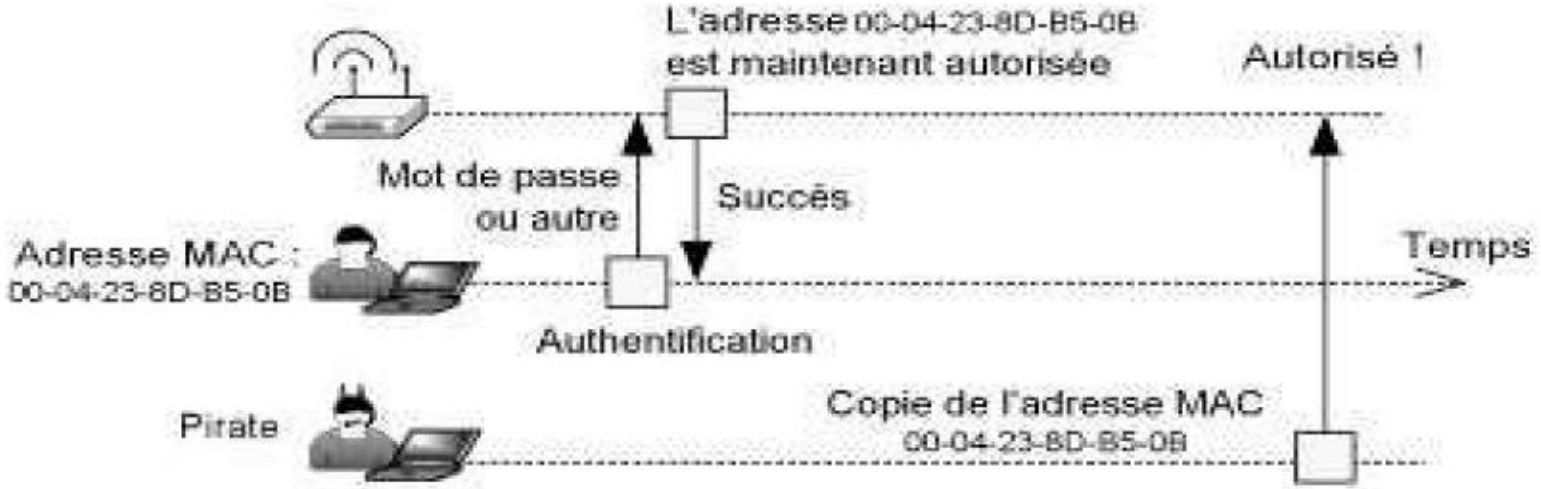


Figure 6.3 — Détournement de session par « *spoofing* » de l'adresse MAC.

Solution

- Les solutions les plus robustes, mises en œuvre par le **WPA et le WPA2**, consistent à négocier, lors de l'identification primaire, l'échange sécurisé de clés de cryptage. De cette façon, un pirate ne peut pas détourner une session en cours, car il ne connaît pas les clés de cryptage à utiliser.

d. Attaque de relecture (rejoue)

- Une autre façon d'ouvrir une nouvelle session consiste à enregistrer les paquets émis par une station légitime au moment où elle se connecte, puis de les émettre un peu plus tard.
- Aussi, cette simple attaque peu endommager tous le réseau sans fi!
  - Solution : freshness mechanism.

e. Le déni de service
DoS

- L'objectif de l'attaquant est d'empêcher le réseau de fonctionner normalement.
- Attaques à la couche physique comme à la couche MAC.
  - rien n'empêche l'attaquant d'arrêt d'envoyer des paquets CTS en se faisant passer pour l'AP : tous les utilisateurs croiront que l'AP a donné le droit à un autre utilisateur d'envoyer son paquet de données, et ils se mettront donc en attente.

Solutions

- Limiter la portée radio (le signale radio ne sort pas de l'entreprise).
- Masquer le SSID
- Le filtrage par adresse MAC
- ***WPA : Wi-Fi Protected Access.***
- Virtual local area networks (VLAN)
- Les réseaux privés virtuels (VPN)

II. WAP vs WAP2

- WPA et le WPA2, voir d'une part comment les déployer et d'autre part comment ils fonctionnent.
- Nous verrons qu'elles mettent en œuvre un cryptage puissant (TKIP ou AES), un mécanisme permettant d'assurer la **distribution et la protection des clés de cryptage**, un contrôle d'**intégrité** puissant et une bonne résistance aux **attaques de relecture**.

WPA vs WPA2

- Le WPA et le WPA2 reposent sur la même architecture.
- Le WPA repose sur un algorithme de cryptage défini par le protocole *Temporal Key Integrity Protocol (**TKIP**), lui-même basé sur l'algorithme* RC4
- Le **WPA2** repose, au choix, sur le TKIP ou sur *Advanced Encryption Standard* (**AES**).
- WPA apparu deux ans avant le WPA2.
- WPA ne peux pas sécuriser un réseaux ad hoc.

Sécurité

- Deux solutions WPA:
  - Personnel
  - Entreprise

Le WPA Personal

- Utiliser une clé partagée, ou ***P**re-**S**hared **K**ey (PSK) de 256 bits.*
- *Méthode :*
  - Saisir un mot de passe : *passphrase*
  - *PSK = PBKDF2(HMAC–SHA1, passphrase, ssid, 4096, 256)*

- Solution recommandée pour les particuliers ou les très petites entreprises car elle ne suppose l'installation d'aucun serveur d'authentification et elle offre un niveau de sécurité bien supérieur au WEP.

***PBKDF2 :* Password-Based Key Derivation Function version2**

Le WPA Personal avantages , inconvénients

avantages

- La solution PSK est de loin la plus simple à mettre en place, mais elle ne convient que pour les petits réseaux Infrastructure ou les réseaux Ad Hoc (pour ad hoc seul WAP2).

inconvénients

1. **Si le mot de passe choisi est trop court, un pirate peut lancer une attaque de dictionnaire hors-ligne pour le retrouver.**
2. Tous les utilisateurs partagent la même clé.

PSK = PBKDF2(HMAC−SHA1, passphrase, ssid, 4096, 256)

Services de sécurité assurés

- Trouvez les services de sécurités assurés par WPA pour les réseaux sans fils personnels?

Le WPA Enterprise

- Méthode:
  - installer et configurer un **serveur RADIUS** compatible avec l'**EAP** ;
  - activer la gestion du **802.1x** et du WPA (ou du WPA2) dans tous les **AP**;
  - configurer la connexion 802.1x et le WPA (ou le WPA2) sur le poste de chaque utilisateur. Bien entendu, il faut configurer le **poste** pour qu'il utilise le même algorithme de cryptage que les AP.
  - Choisir une ou plusieurs **méthodes d'authentification** EAP, et les configurer dans le serveur RADIUS et dans l'interface de connexion des utilisateurs.

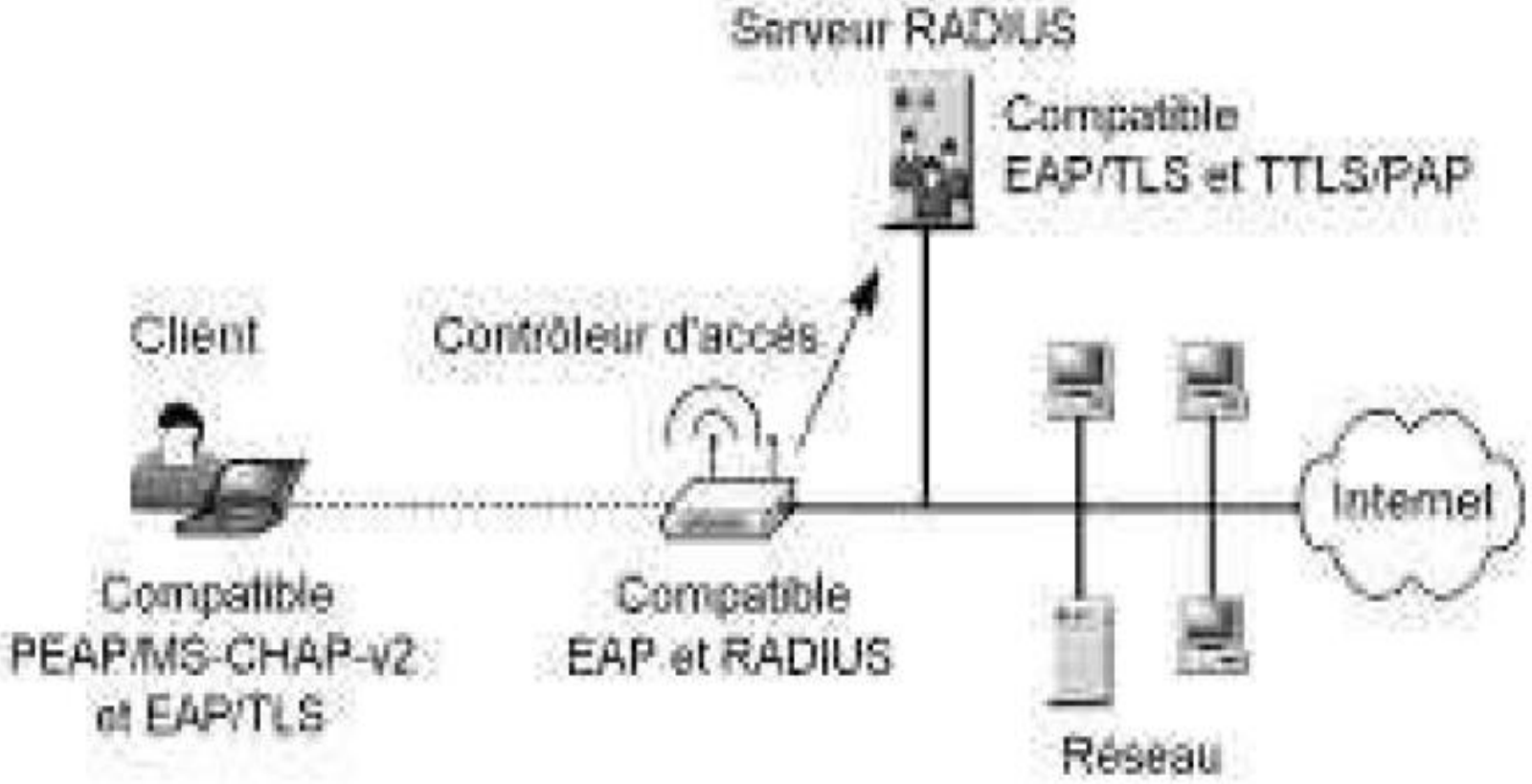
EAP ?

- *Extensible Authentication Protocol.*
- *Protocole très générique permettant* l'identification d'utilisateurs selon diverses méthodes (**mot de passe, certificat, carte à puce…**).
- Normalisé par l'IETF comme extension du protocole PPP, l'EAP est maintenant également à la base du 802.1x, lui même à la base du WPA Enterprise.

Principe de Fonctionnement d'EAP
L'architecture : trois acteurs

- Le principe d'EAP est très simple : si un utilisateur cherche à accéder au réseau, un contrôleur d'accès lui barrera le chemin jusqu'à ce qu'il s'identifie auprès du serveur d'authentification.
- Le contrôleur d'accès sert d'intermédiaire pour la communication entre le client et le serveur d'authentification.
- A l'issu du résultat final (le succès ou échec de l'authentification) il décidera à ouvrir la porte du réseau ou à la laisser fermée.
- S'il l'ouvre, l'ensemble du trafic du client vers le réseau passera par lui.
- Dans le cadre du WiFi, lorsque le 802.1x est utilisé, chaque AP est un contrôleur d'accès.

Un exemple de configuration EAP



802.1x

- **L'EAP et le 802.1x**
- Le protocole EAP est à la base du 802.1x, sur lequel reposent à leur tour les nouvelles solutions de sécurité du WiFi, le WPA Enterprise et le WPA2 Enterprise.
- Le WPA Personal et le WPA2 Personal reposent sur une simple clé partagée, ils n'utilisent donc pas les mécanismes d'authentification du 802.1x.

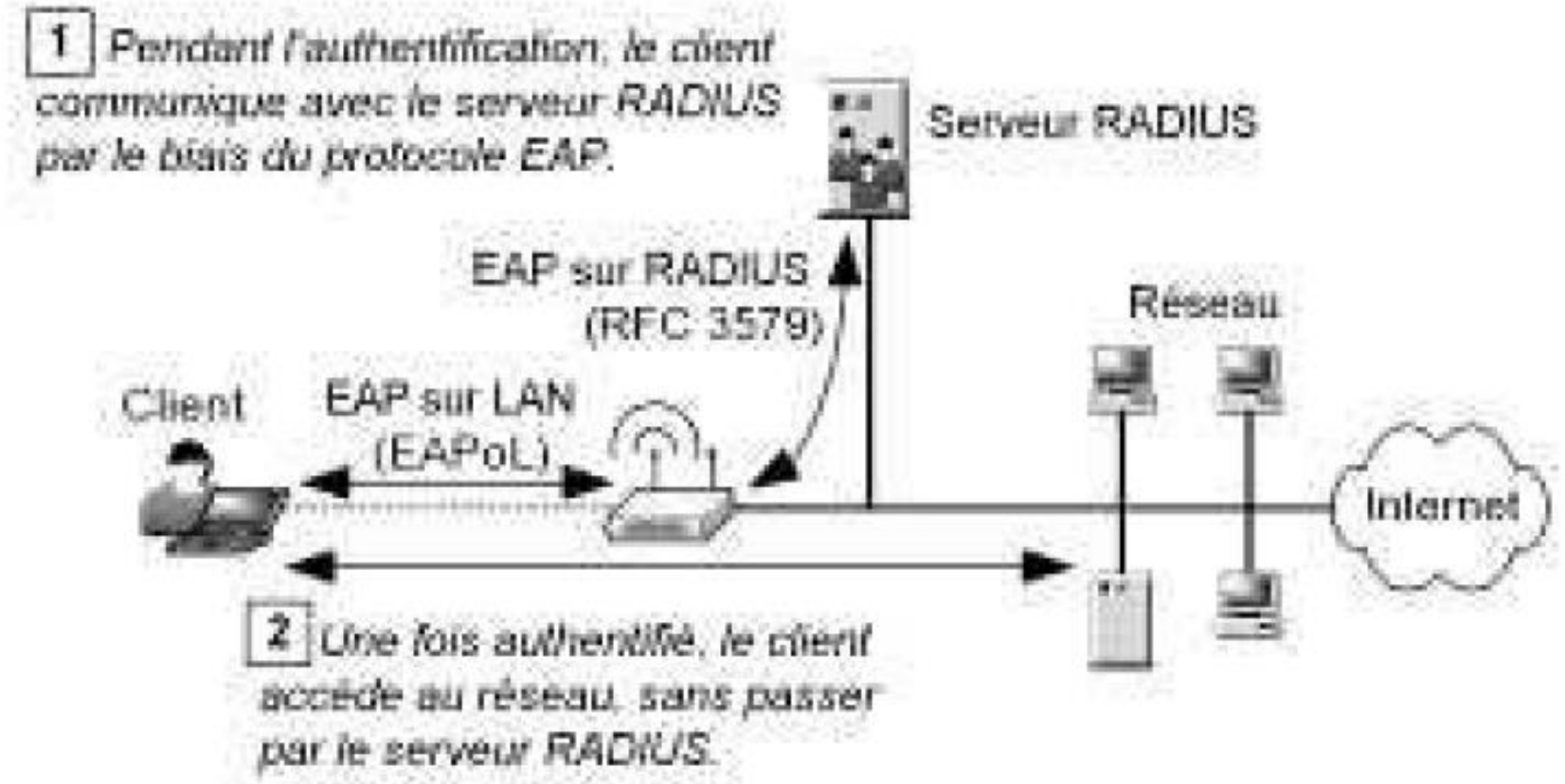
802.1x

- La seule présupposition est qu'il existe un lien de communication entre le client et le contrôleur d'accès et un lien *sécurisé* entre le contrôleur d'accès et le serveur d'authentification **RADUIS**.
- **Le standard 802.1x définit le protocole *EAPoL* (*EAP over LAN***): un protocole de communication entre le poste et le contrôleur d'accès.
- En outre, le 802.1x définit quelques nouveaux types de messages : **EAPoL-Start, EAPoL-Packet , EAPoL-Key,…**

802.1x

- La communication entre le contrôleur d'accès (c'est-à-dire l'AP) et le serveur d'authentification (le serveur RADIUS) se fait avec le protocole RADIUS.
- Les paquets EAP échangés entre le contrôleur d'accès et le serveur RADIUS sont donc encapsulés dans des requêtes RADIUS
- L'**RFC 3579** détaille cette encapsulation.

Les protocoles du 802.1x



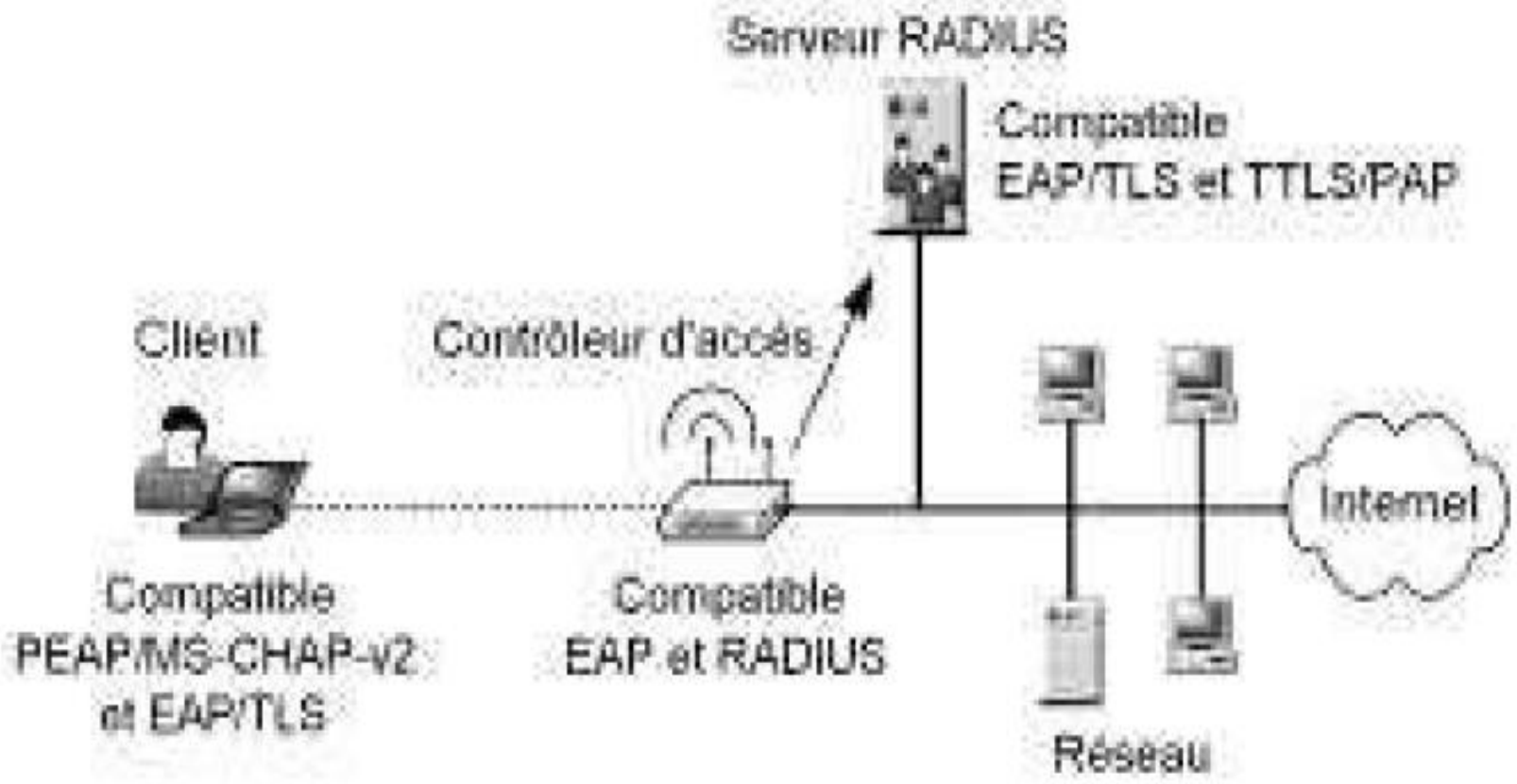
Exemple de configuration

- Le client possède un logiciel de connexion fourni avec son adaptateur WiFi compatible avec le 802.1x (donc avec l'EAP) et supporte **deux méthodes d'authentification**: *PEAP/MS-CHAP-v2* et *EAP/TLS*.
- Le contrôleur d'accès est un AP compatible 802.1x.
- Le serveur d'authentification est un serveur RADIUS compatible avec EAP. Il gère les méthodes d'authentification EAP/TLS et TTLS/PAP.

Exemple de configuration

- Le serveur demandera au client de s'identifier selon une méthode.
- Si le client ne la gère pas, le serveur en suggérera une autre et ainsi de suite jusqu'à ce que le client en accepte une.
- Dans cet exemple, ils tomberont d'accord sur la méthode d'identification EAP/TLS

Un exemple de configuration EAP



Avantages

- Les clés de cryptage sont distribuées automatiquement.
- Les clés de cryptage sont différentes pour chaque utilisateur et pour chaque session, et peuvent même changer automatiquement en cours de session.
- Sécurité bien plus élevée qu'avec des clés partagées.

Notes

- Si l'on veut bénéficier de la distribution automatique des clés de cryptage, la méthode EAP utilisée doit être capable de générer une clé secrète entre le client et le serveur d'authentification.
- on dit que la méthode est « génératrice de clés » (*Key Generating).*
- Exemple :
  - EAP/TLS, TTLS, PEAP, EAP/FAST.

Notes

- La difficulté de la solution 802.1x réside surtout dans l'installation et la configuration du serveur RADIUS. Cependant, une fois que cette architecture est mise en place, elle est beaucoup plus facile à administrer et beaucoup plus sûre que le WEP, le WPA-PSK ou le WPA2-PSK.

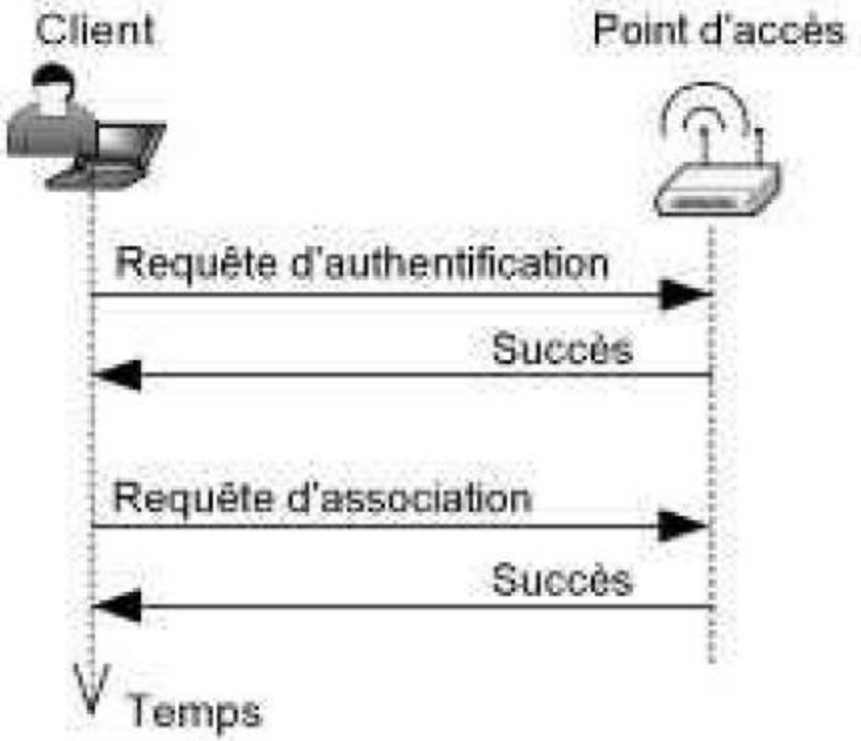
Procédure de connexion complète d'une station WAP entreprise

- Admettons qu'un utilisateur ait configuré son logiciel de connexion WiFi pour utiliser le WPA Enterprise.
- Que se passe-t-il lorsqu'il cherche à se connecter au réseau ?
- Il y a trois étapes :
  a. l'association WiFi,
  b. l'authentification 802.1x
  c. et la négociation des clés temporaires entre le client et l'AP.

a. L’association Wi-Fi

- le client détecte l’AP le plus proche.
- il envoie alors une requête d’authentification.
  - l’AP devrait toujours être en mode « ouvert »
- l’AP répondra que l’authentification est réussie
- Le client envoie une requête d’association à l’AP;
- l’AP accepte l’association.
- Bien qu’à ce stade l’utilisateur soit associé à l’AP, ne le laisse pas encore accéder au réseau .

a. L’association Wi-Fi



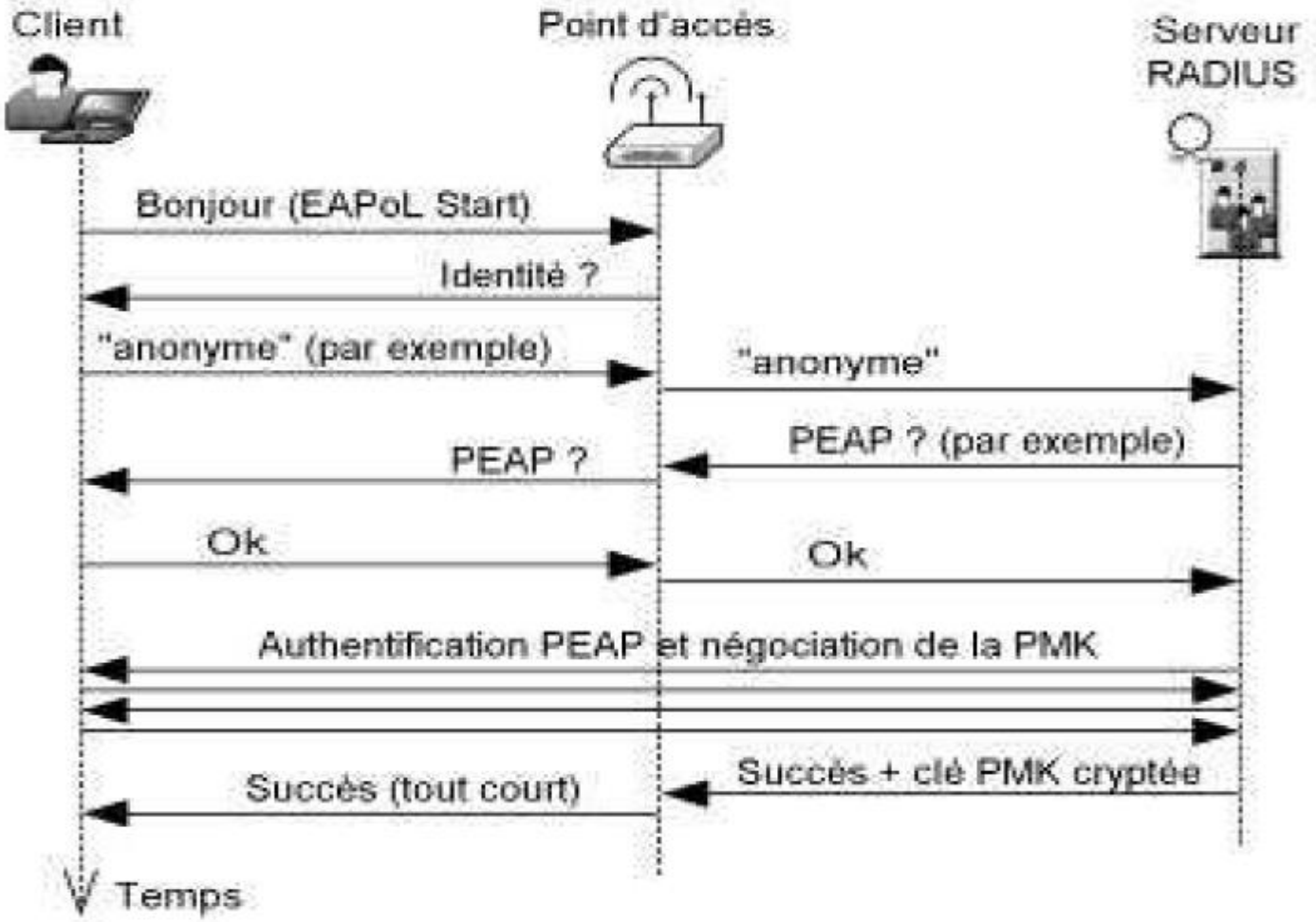
b. L’authentification 802.1x

- Le poste de l’utilisateur envoie maintenant une requête EAPoL-Start à l’AP, ce qui démarre une séquence d’échanges 802.1x ***pendant laquelle l’utilisateur doit être authentifié auprès du serveur d’authentification*** ;
- Selon la méthode génératrice de la clé, le client et le serveur se mettent d’accord secrètement sur une clé de 256 bits , dérivée de la clé secrète générée par l’authentification : on l’appelle la *Pairwise Master Key (PMK).* (*la clé secrète était d’abord générée par le client, puis cryptée à l’aide de la clé publique du serveur d’authentification et enfin envoyée au serveur*)

b. L’authentification 802.1x

- le serveur d’authentification transmet la PMK à l’AP, à l’aide d’un paquet RADIUS prévu à cet effet. De cette façon, le client et l’AP possèdent tous deux la même clé PMK, qui leur permettra d’établir entre eux un **tunnel sécurisé**.
- Si le client est bien authentifié, le serveur lui envoie un paquet EAP de type Succès, que le contrôleur d’accès voit passer.

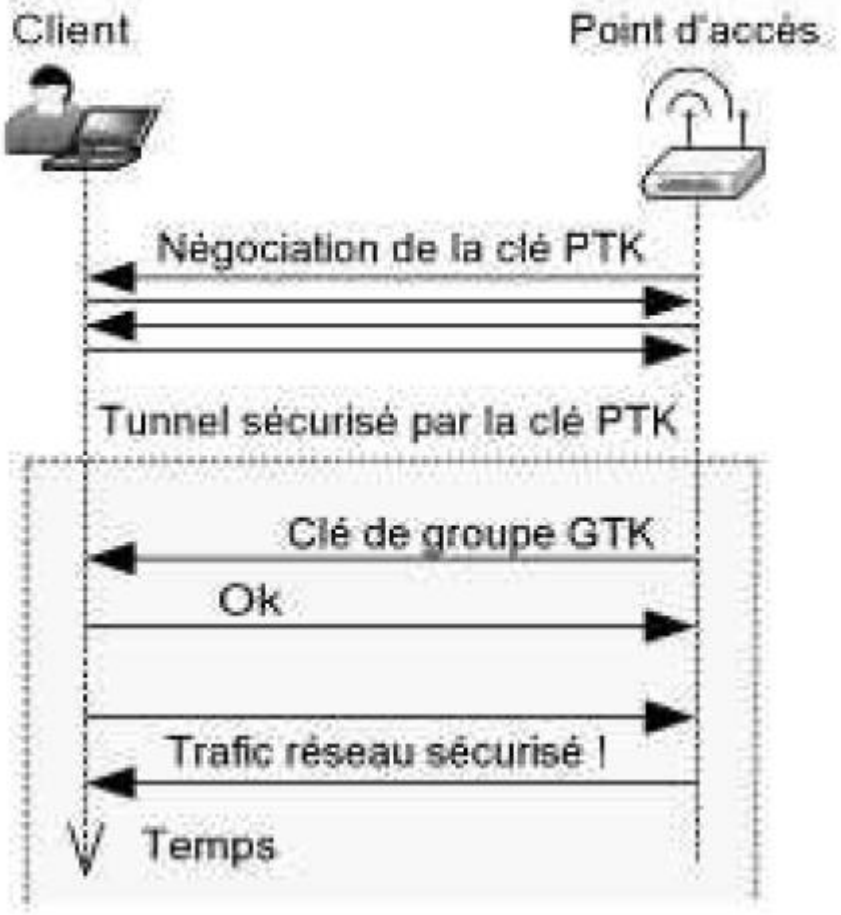
b. L'authentification 802.1x



c. Négociation des clés temporaires entre le client et l'AP.

- Le client et l'AP se mettent maintenant d'accord sur une nouvelle clé dérivée de la clé PMK : cette clé temporaire s'appelle la *Pairwise Transient Key (PTK).*
- Ils en profitent pour vérifier qu'ils possèdent bien la même clé de départ PMK.
- Dorénavant, tous leurs échanges sont cryptés avec la clé PTK.
- L'AP peut envoyer secrètement au client la clé qu'il utilise pour crypter le trafic **broadcast** et **multicast** : la *Group Transient Key (GTK).*

c. Négociation des clés temporaires entre le client et l'AP.



La méthode d’authentification PEAP

- *Protected EAP été* Développée par Cisco et Microsoft.
- PEAP se déroule en deux phases :
- La phase 1 ou '***identification externe***' permet l'authentification du serveur grâce à une infrastructure à clés publiques. Une fois le serveur authentifié il y a création d'un tunnel sécurisé.
- La phase 2 ou *'**identification interne***' permet l'authentification du client au travers du tunnel chiffré.

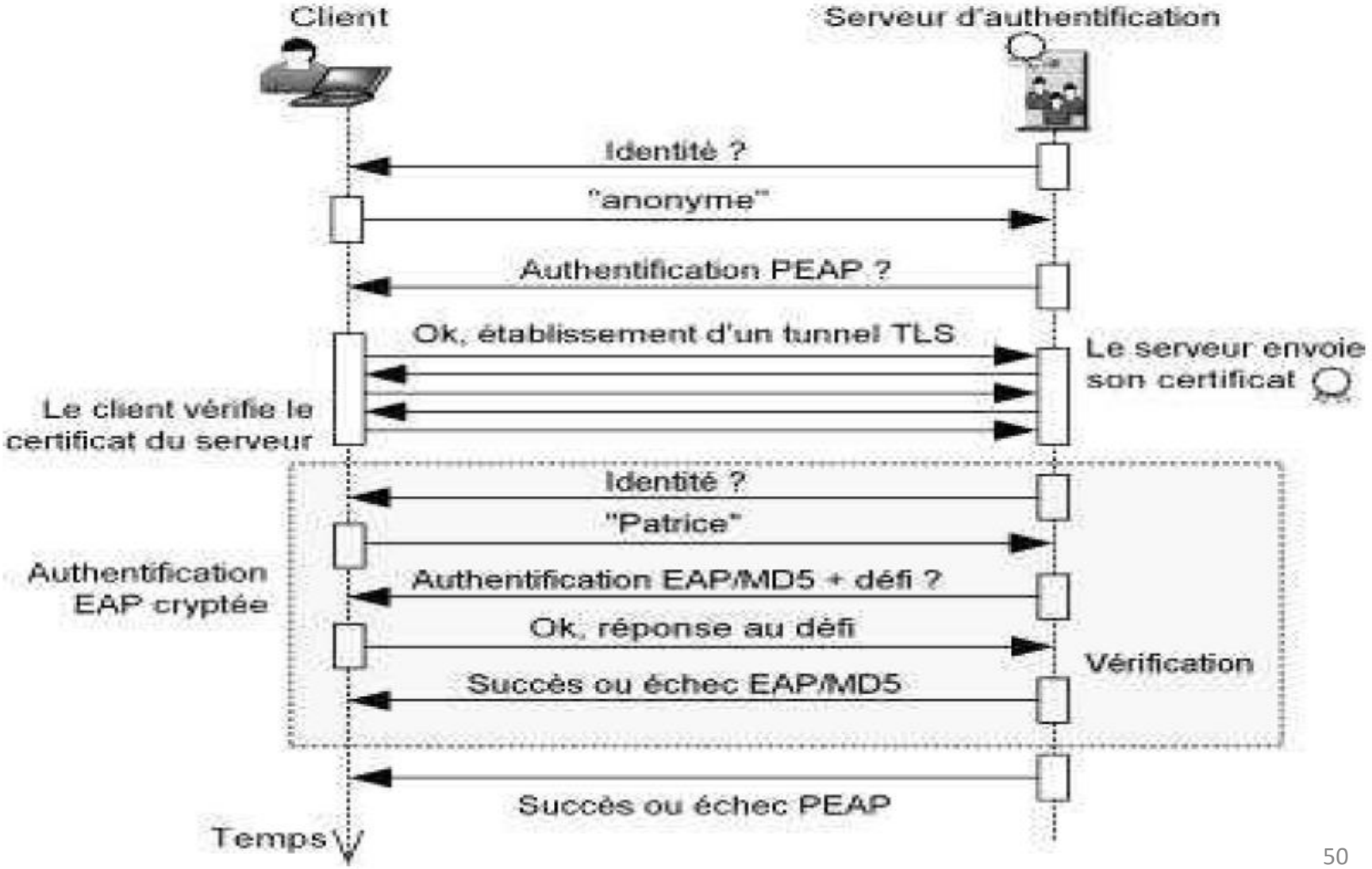
L’authentification PEAP

- Le serveur demande l’identité au client.
- Le client n’est pas obligé de fournir son vrai identité.
- le serveur fournir un certificat pour prouver son identité au client.
- **Etablir un tunnel TLS**.
- Dans ce tunnel, une nouvelle négociation EAP complète a lieu : c’est ici que le client fournit son identité et la preuve de cette identité. La méthode utilisée peut être n’importe quelle méthode EAP.

L’authentification PEAP

- Une fois que l’identification EAP « interne » est terminée par un paquet de succès ou d’échec, le tunnel TLS est fermé et le serveur renvoie un nouveau paquet de succès ou d’échec au client, en clair cette fois-ci.

L’authentification PEAP



EAP/MD5

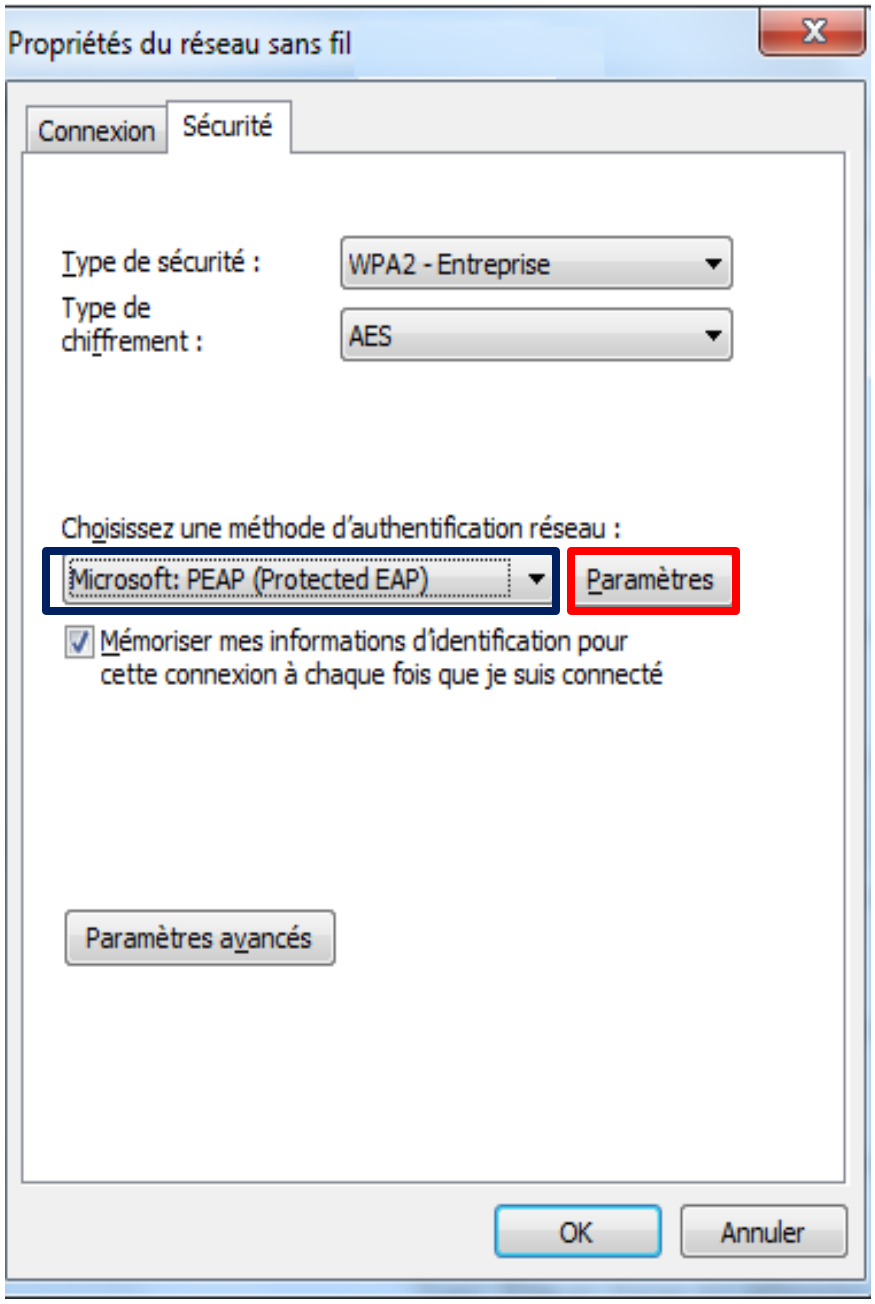
- **Le serveur envoie un CHALLENGE aléatoire**
  - Envoyer *Challenge* au client
- **Le client calcule une réponse**
  - Réponse=MD5(ID+Password*+Challenge*)
- **Le serveur vérifie**
  - Calcule la même valeur MD5
  - Compare.

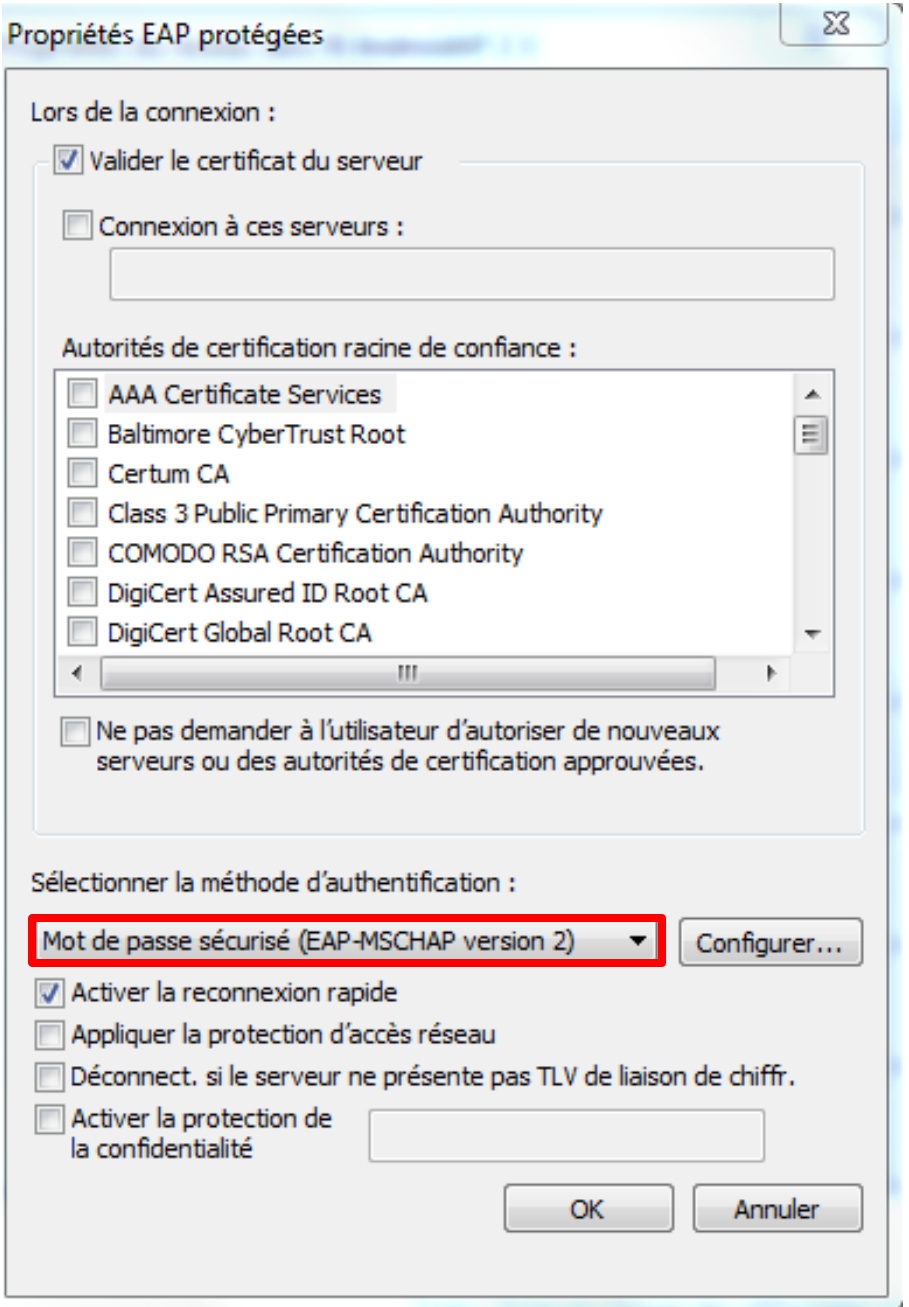
Remarque

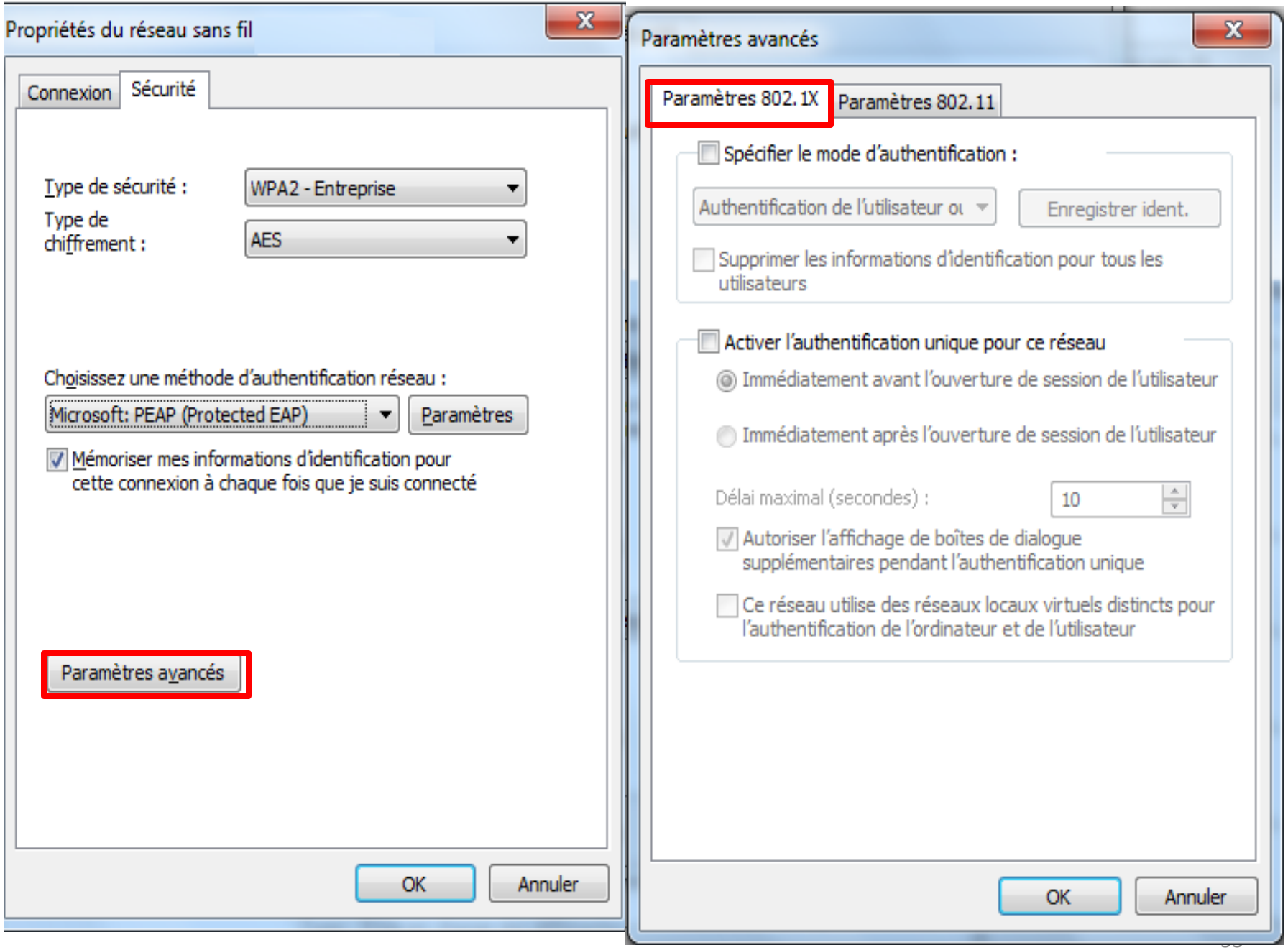
- **La méthode d'authentification EAP/MD5 est définie dans la RFC 3748**.

Conclusion

- En entreprise, une architecture 802.1x, et mise en place.
- Choisir une méthode d'authentification comme PEAP/MD5.
- Installer et configurer un serveur RADIUS gérant la méthode choisie.
- Résultats
  - distribution automatique de PMK
  - Négociation automatique de PTK
  - Cryptage AES
  - un compteur incrémenté à chaque paquet pour contrer les attaques de relectures.
  - Le WPA2/AES est tout à fait apte à assurer la sécurité d'un réseau sans fil d'entreprise.


Propriétés du réseau sans fil
Connexion
Sécurité
Type de sécurité :
WPA2 - Entreprise
Type de chiffrement :
AES
Choisissez une méthode d'authentification réseau :
Microsoft: PEAP (Protected EAP)
Paramètres
Mémoriser mes informations d'identification pour cette connexion à chaque fois que je suis connecté
Paramètres avancés
OK
Annuler


Propriétés EAP protégées
Lors de la connexion :
Valider le certificat du serveur
Connexion à ces serveurs :
Autorités de certification racine de confiance :
AAA Certificate Services
Baltimore CyberTrust Root
Certum CA
Class 3 Public Primary Certification Authority
COMODO RSA Certification Authority
DigiCert Assured ID Root CA
DigiCert Global Root CA
Ne pas demander à l'utilisateur d'autoriser de nouveaux serveurs ou des autorités de certification approuvées.
Sélectionner la méthode d'authentification :
Mot de passe sécurisé (EAP-MSCHAP version 2)
Configurer...
Activer la reconnexion rapide
Appliquer la protection d'accès réseau
Déconnect. si le serveur ne présente pas TLV de liaison de chiffr.
Activer la protection de la confidentialité
OK
Annuler


Propriétés du réseau sans fil
Connexion
Sécurité
Type de sécurité :
WPA2 - Entreprise
Type de chiffrement :
AES
Choisissez une méthode d'authentification réseau :
Microsoft: PEAP (Protected EAP)
Paramètres
Mémoriser mes informations d'identification pour cette connexion à chaque fois que je suis connecté
Paramètres avancés
OK
Annuler
Paramètres avancés
Paramètres 802.1X
Paramètres 802.11
Spécifier le mode d'authentification :
Authentification de l'utilisateur ou
Enregistrer ident.
Supprimer les informations d'identification pour tous les utilisateurs
Activer l'authentification unique pour ce réseau
Immédiatement avant l'ouverture de session de l'utilisateur
Immédiatement après l'ouverture de session de l'utilisateur
Délai maximal (secondes) :
10
Autoriser l'affichage de boîtes de dialogue supplémentaires pendant l'authentification unique
Ce réseau utilise des réseaux locaux virtuels distincts pour l'authentification de l'ordinateur et de l'utilisateur
OK
Annuler

VLAN : *Virtual local area networks*

- Si les AP le permettent (ou les commutateurs auxquels ils sont reliés), il est bon d'associer le trafic sans fil à un VLAN particulier. Ceci facilitera par la suite la maintenance et l'administration du réseau.
- Certains AP peuvent associer un utilisateur donné à un VLAN particulier au moment de l'identification (grâce au protocole RADIUS).
  - Un commercial se connecte au réseau sans fil, il peut automatiquement être associé au VLAN numéro 10. qui lui donne accès aux serveurs généraux de l'entreprise ainsi qu'à des serveurs spécifiques aux commerciaux
  - Comptable ➔ VLAN numéro 20 : accès aux serveurs généraux et aux serveurs réservés aux comptables.
  - simple visiteur➔ VLAN numéro 30 : uniquement un accès limité et contrôlé à Internet.

Homework

- Quels services de sécurité assurés par WPA Per & Entr
- D’autres solutions
  - VLAN
  - VPN
  - …

VLAN autre exemple

SSID Wi-Fi	VLAN ID	Usage
WiFi-Etudiants	VLAN 10	Accès internet
WiFi-Enseignants	VLAN 20	Accès prioritaire
WiFi-Administration	VLAN 30	Accès interne
WiFi-Invités	VLAN 40	Internet isolé

VLAN

- Différentes politiques de qualité de service (QoS) peuvent être mises en œuvre sur les différents VLAN :
  - un visiteur n'aura droit qu'à une très faible bande passante, alors que les commerciaux en auront suffisamment pour participer, par exemple, à des vidéoconférences.
  - Beaucoup de compagnies utilisent un VLAN parce que cela leur donne la possibilité de contrôler le débit de leur trafic wifi. On empêche que le trafic wifi soit utilisé par des sources de l'extérieur du réseau de la compagnie.

Les réseaux privés virtuels

- Isoler le réseau sans fil et obliger les utilisateurs à passer par des tunnels VPN.

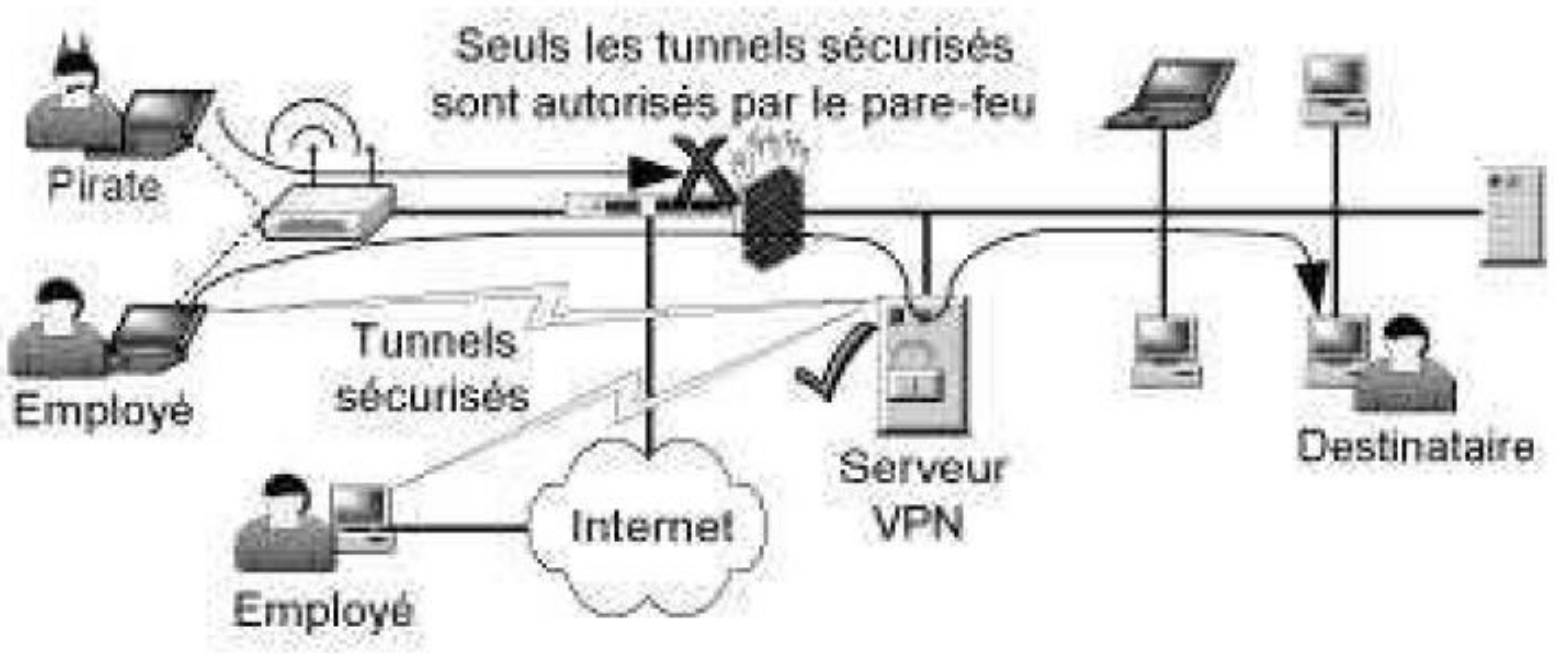


Figure 6.9 — La solution VPN.