Le Wi-Fi

Module 146

ICT Berufsbildung
Formation professionnelle
Formazione professionale

Chapitres :

1. Introduction
2. Fonctionnement du Wi-Fi
3. Les Limites du Wi-Fi
4. La sécurité

Chapitre : Le Wi-Fi

- 1. Introduction

La norme **IEEE 802.11** est un standard international décrivant les caractéristiques d'un réseau local sans fil.

Le nom « **Wi-Fi** » est la contraction de **Wi**reless **Fi**delity.

Le « **Wi-Fi** » permet de relier tout type de périphérique.

La portée varie de plusieurs **dizaines de mètres** à plusieurs **centaines de mètres**.

Le débit varie de 11 Mb/s à plus de 1300Mb/s.

La **norme 802.11** se situe au niveau des **couches 1 et 2** du système OSI.

Chapitre : Le Wi-Fi

▪1. Introduction

Représentation des principales révisions de la norme 802.11:

Norme	Description
802.11a	La norme 802.11a permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.
802.11b	La norme 802.11b propose un débit théorique de 11 Mbps (6 Mbps réels). La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles.
802.11g	La norme 802.11g offre un haut débit (idem 802.11a) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b.
802.11n	La norme 802.11n offre un débit théorique atteint les 540 Mbit/s (débit réel de 100 Mbit/s dans un rayon de 90 mètres) grâce aux technologies **MIMO** et **OFDM** Le 802.11n utilisera simultanément les fréquences 2,4 et 5GHz. Il saura combiner jusqu'a 8 canaux non superposés.
802.11ac	IEEE 802.11ac est la dernière évolution du standard de transmission sans fil 802.11, qui permet une connexion sans fil haut débit dans la bande de fréquences inférieure à 6 GHz (communément appelée bande des 5 GHz). Le 802.11ac offre jusqu'à 1 300 Mbit/s de débit théorique, en utilisant des canaux de 80 MHz, soit jusqu'à 7 Gbit/s de débit global dans la bande des 5 GHz (de 5170 MHz à 5835 MHz).

Chapitre : Le Wi-Fi

- 1. Introduction

Les différentes parties de l'équipement du Wi-fi :

- l'**adaptateur sans fils** ou **carte d'accès** - on appelle station (**STA**) tout équipement possédant une telle carte.

- le **point d'accès** – notés **AP**

Les deux **modes opératoires** du standard 802.11 :

- le **mode infrastructure** - clients connectés à un point d'accès

- le **mode ad hoc** - clients connectés à d'autres clients

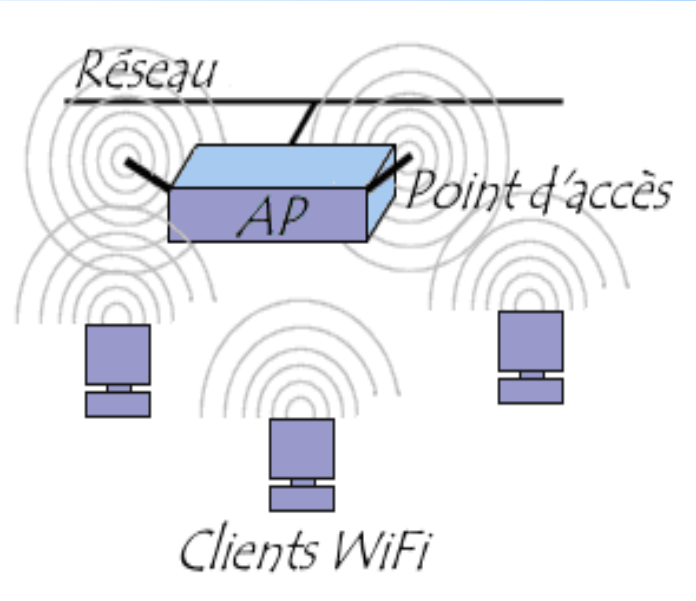
Chapitre : Le Wi-Fi

- 2. Fonctionnement du Wi-Fi

En **mode infrastructure** chaque station (**STA**) se connecte à un point d'accès (**AP**).

Chaque élément est identifié par un identifiant de 6 octets (**BSSID**).

Le **BSSID** correspond à l'adresse MAC du point d'accès.



Chapitre : Le Wi-Fi

- 2. Fonctionnement du Wi-Fi

La liaison de plusieurs points d'accès est appelée **E**nsemble de **S**ervices **E**tendu (Extended Service Set, **ESS**).

Le **ESSID** (Service Set Identifier) est un identifiant servant de nom pour le réseau.

Lors d'un déplacement, au sein de l'**ESS**, la station est **capable de changer de point d'accès**.

Les points d'accès communiquent entre eux afin d'échanger des informations sur les stations.

Cette caractéristique permet aux stations de **« passer de façon transparente »** d'un point d'accès à un autre (**itinérance** ou **roaming**).

Chapitre : Le Wi-Fi

- 2. Fonctionnement du Wi-Fi

La communication avec un point d'accès

Pour se connecter, la station diffuse une requête de sondage.

La requête contient l'**ESSID** et le débits de sa carte d'accès.

Chaque **AP** diffuse une trame de balise (**beacon**).

Une station située entre plusieurs **AP** pourra choisir le meilleur.

Chapitre : Le Wi-Fi

- 3. Les Limite du Wi-fi

Propagation des ondes radio

Les ondes radio se propagent en ligne droite dans plusieurs directions.

La vitesse de propagation des ondes dans le vide est de 3’108 m/s.

Dans tout autre milieu, le signal subit un affaiblissement dû à la réflexion, la réfraction, la diffraction, l'absorption.

La réflexion : *phénomène qui se produit lorsque des ondes rencontrent un obstacle qui le force de suivre une autre direction.*

La réfraction : *c’est la déviation des ondes passant obliquement d'un milieu transparent dans un autre.*

Chapitre : Le Wi-Fi

- 3. Les Limite du Wi-Fi (2)

La diffraction : *phénomène de déviation des ondes lorsqu'elles passent au voisinage d'un obstacle physique (trou de serrure).*

L'absorption : *processus par lequel l'énergie d'un photon est prise par une autre entité, par exemple, un atome qui fait une transition entre deux niveaux d'énergie électronique.*

Propriétés des milieux

L'affaiblissement de la puissance du signal est en grande partie dû aux propriétés des milieux traversés par l'onde.

Chapitre : Le Wi-Fi

- 3. Les Limites du Wi-Fi

MIMO

La technologie **Mimo** (**M**ultiple **I**n, **M**ultiple **O**ut) améliore les performances des réseaux sans fil en multipliant les signaux.

Peu importe la dégradation des ondes, les paquets de données sont réorganisés à l'arrivée pour reconstituer l'information d'origine.

Pour multiplier les signaux, les produits **Mimo** utilisent plusieurs antennes.

Le système MIMO améliore la portance et le débit.

Chapitre : Le Wi-Fi

- 4. La sécurité

Les ondes radioélectriques ont intrinsèquement une grande capacité à se propager dans toutes les directions.

Le danger est qu'un réseau sans fil peut très bien être installé dans une entreprise sans que le service informatique ne soit au courant !

Il est très facile de circuler en ville avec un ordinateur portable équipé d'une carte réseau sans fil à la recherche de réseaux sans fils (**war driving**).

Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples, ***l'interception de données, le détournement de connexion, le brouillage des transmissions, les dénis de service, l'intrusion réseau, déni de service sur batterie***.

Chapitre : Le Wi-Fi

- 4. La sécurité

Une infrastructure adaptée consiste à positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir.

Les paramètres par défaut sont tels que la sécurité est minimale.

Il est indispensable de connaître l'identifiant du réseau (**SSID**).

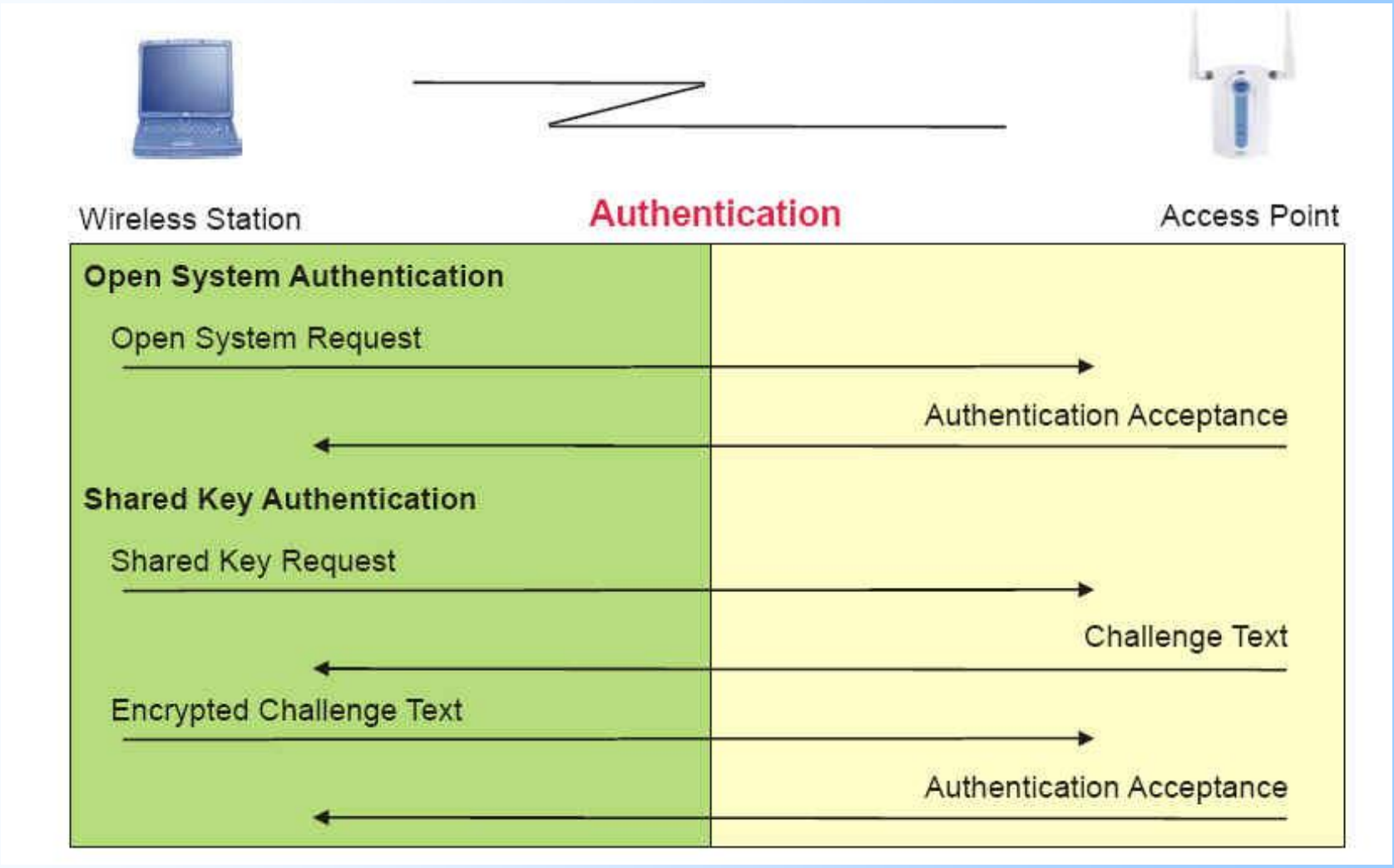
Il est vivement conseillé de modifier le **nom du réseau**, de **désactiver la diffusion** (broadcast), **changer l'identifiant réseau**.

Les points d'accès permettent de gérer une liste de droits d'accès (**ACL**) basée sur les adresses **MAC**.

Les réseaux sans fils peuvent être cryptés de plusieurs manières dont le **WEP**, le **WPA** (**W**ifi **P**rotected **A**ccess) et le **WPA2** (**W**ifi **P**rotected **A**ccess, seconde génération).

Chapitre : Le Wi-Fi

- 4. La sécurité, authentification WEP



Chapitre : Le Wi-Fi

- 4. La sécurité, authentification WEP

Améliorer l'authentification

Afin de gérer plus efficacement les authentifications, les autorisations et la gestion des comptes utilisateurs, il est possible de recourir à un serveur RADIUS (Remote Authentication Dial-In User Service).

Le protocole RADIUS est un système client/serveur permettant de gérer de façon centralisée les comptes des utilisateurs et les droits d'accès associés.

Pour toutes les communications nécessitant un haut niveau de sécurisation, il est préférable de recourir à un chiffrement fort des données en mettant en place un réseau privé virtuel (VPN).

Chapitre : Le Wi-Fi

- 4. La sécurité

WPA-PSK - Wifi Protected Access Pre Shared Key est une variante du « **WPA** ».

La configuration du **WPA-PSK** commence par la détermination d'une clé statique ou « passphrase » tout comme le **WEP**.

A la différence du **WEP**, le **WPA** va utiliser **TKIP** pour faire une rotation des clés.

WPA est une solution de sécurisation de réseau **Wi-fi** permettant de combler les lacunes du **WEP**.

Chapitre : Le Wi-Fi

- 4. La sécurité

WPA2 - Wifi Protected Access, seconde génération vient renforcer la sécurité des réseaux sans-fil sans pour autant remiser la version précédente.

La seule amélioration visible est la présence du chiffrement par **AES**, le nouvel algorithme de chiffrement.

Le support de ce protocole lui permet ainsi de prétendre à la certification **FIPS-140-2**.

WPA2 est donc la déclinaison du très attendu protocole 802.11i.

Ce protocole était attendu comme la pierre fondatrice des réseaux **Wi-Fi** sécurisés.

Chapitre : Le Wi-Fi

- 4. La sécurité, authentification WPA2 (4 way handshake)

Lorsqu'un client se connecte à un point d'accès protégé par le protocole WPA2, il y a un échange de 4 messages qui est effectué.

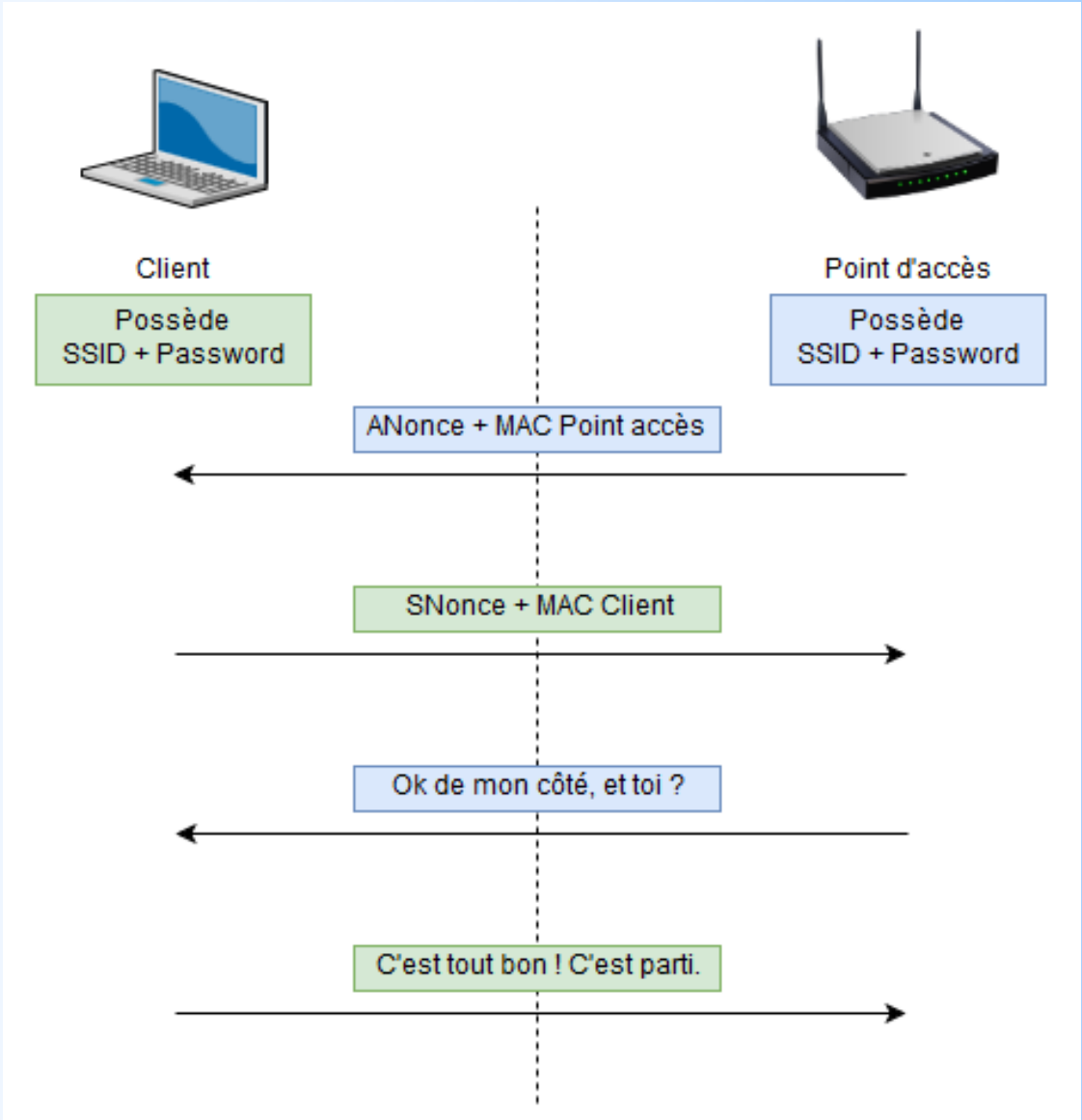
Pour pouvoir construire une clé, chaque partie aura besoin :

- du SSID
- de la clé du point d'accès
- l'adresse MAC des deux parties
- Un nombre aléatoire généré par le client ANonce
- Un nombre aléatoire généré par le Point d'accès

SNonce

Chapitre : Le Wi-Fi

- 4. La sécurité, authentification WPA2 (4 way handshake)



Chapitre : Le Wi-Fi

- 4. La sécurité, authentification WPA2 (4 way handshake)

Message 1 : ***Point d'accès*** - Je t'envoie un numéro aléatoire (Anonce) et mon adresse MAC. Moi j'ai déjà mon SSID et la clé du réseau, me permettant de calculer une clé commune à tous (PMK).

Message 2 : ***Client*** - Reçus ! J'ai fait une tambouille avec ton numéro (Anonce), un numéro que j'ai généré (Snonce), ton adresse MAC, mon adresse MAC, ton SSID et la clé (qui me donnent aussi la PMK), ça m'a donné la clé de chiffrement (PTK). Et du coup, je t'envoie mon numéro généré (Snonce) et mon adresse MAC pour que tu fasses la même tambouille.

Message 3 : ***Point d'accès*** - Reçus aussi. J'ai fait la même tambouille, donnant la clé de chiffrement (PTK).

Message 4 : ***Client*** - Parfait ! Allez, discutons.

Chapitre : Le Wi-Fi

- 4. La sécurité, authentification WPA2 (4 way handshake)