Ecole Nationale Polytechnique d’Oran- Maurice AUDIN
Département de Génie des Systèmes

Intitulé de la matière: **Technologies des Réseaux Sans Fil**

Chapitre 2: Les Réseaux Locaux Sans Fil (WLAN)

Mme Nawel BENDIMERAD

Année universitaire 2023/2024

Contenu du Chapitre 2

1/ Introduction

2/ Définition

3/ Les norme IEEE 802.11

4/ Les équipements Wi-Fi

5/ Topologies sans fil

6/ Connexion d’une station

7/ Les couches protocolaires

8/ Les trames Wi-Fi

9/ Mécanismes de sécurité

1/ Introduction

- De nos jours les WLAN sont de plus en plus sollicités dans de nombreux domaines tels que les entreprises, les universités, les usines, les aéroports, les hôpitaux, etc.
- Les points d'accès Wi-Fi existent dans des lieux dits de passage: « Hotspots ».
- Les WLANs représentent une bonne solution pour diverses raisons telles que :

➢ extension à des LANs filaires

➢ sites difficiles à câbler (bâtiments anciens, musées, monuments historiques, etc.)

➢ réalisations temporaires (pour des périodes de surcharge ou des projets spéciaux)

➢ mise en place rapide de réseaux

➢ environnement en évolution constante

➢ conférences, etc.

2/ Définition

- Un réseau Wi-Fi est un réseau répondant à une des normes IEEE 802.11 qui offre les fonctionnalités des réseaux locaux LAN traditionnels (Ethernet), mais en utilisant une technologie sans fil.
- Le nom Wi-Fi (contraction de ***Wireless Fidelity***) correspond initialement au nom donnée à la certification délivrée par la WECA (*Wireless Ethernet Compatibility Alliance*), l'organisme chargé de maintenir l'interopérabilité entre les matériels de la norme 802.11.
- C’est la Wi-Fi Alliance qui pose le label “ **Wi-Fi** ” et certifie les produits des constructeurs.
- Donc, uniquement les matériels certifiés par la Wi-Fi Alliance ont la possibilité d’utiliser le logo de la certification Wi-Fi.
- Un WLAN permet de relier des ordinateurs portables ou autres périphériques à une liaison haut débit sur un rayon de plusieurs dizaines de mètres en intérieur et de centaines de mètres en environnement ouvert.

3/ Les norme IEEE 802.11 (1)

- Les normes IEEE 802.11 définissent la manière dont les radiofréquences sont utilisées pour les liaisons sans fil.
- La plupart des normes spécifient que les appareils sans fil ont une antenne pour transmettre et recevoir des signaux sans fil sur la fréquence radio spécifiée (2,4 GHz ou 5 GHz).
- Il s’agit de nouvelles spécifications qui continuent de croître à mesure que de nouvelles fréquences deviennent disponibles.
- Certaines des nouvelles normes qui transmettent et reçoivent à des vitesses plus élevées nécessitent que les points d'accès (AP) et les clients sans fil disposent de plusieurs antennes utilisant la technologie à entrées et sorties multiples (MIMO).
- MIMO utilise plusieurs antennes comme émetteur et récepteur pour améliorer les performances de communication. Jusqu’à quatre antennes peuvent être prises en charge.

3/ Les norme IEEE 802.11 (2)

- Diverses implémentations de la norme IEEE 802.11 ont été développées au fil des ans. Les principales sont les suivantes:

Norme IEEE	Radio fréquence	Description
802.11 (1997)	2,4 GHz	première norme Wi-Fi vitesses allant jusqu'à 2 Mbit/s
802.11a (1999)	5 GHz	appelée Wi-Fi 2 des vitesses allant jusqu'à 54 Mbit/s petite zone de couverture non interopérable avec les 802.11b et 802.11g
802.11b (1999)	2,4 GHz	appelée Wi-Fi 1 des vitesses allant jusqu'à 11 Mbit/s théorique portée plus longue que 802.11a (50m en intérieur et 300m en extérieur)

3/ Les norme IEEE 802.11 (3)

802.11g (2003)	2,4 GHz	appelée Wi-Fi 3 des vitesses allant jusqu'à 54 Mbit/s compatible avec 802.11b avec une capacité de bande passante réduite
802.11n (2009)	2,4 GHz 5 GHz	appelée Wi-Fi 4 les débits de données varient de 150 Mbit/s à 600 Mbit/s avec une distance jusqu'à 70 m les points d'accès et les clients sans fil ont besoin de plusieurs antennes utilisant la technologie MIMO compatibilité avec les appareils 802.11a/b/g à débit de données limité
802.11ac (2013)	5 GHz	fournit des débits de données allant de 450 Mbit/s à 1,3 Gbps utilisant la technologie MIMO jusqu'à huit antennes peuvent être prises en charge compatible avec les appareils 802.11a / n avec limitation des débits de données est appelée Wi-Fi 5 par la Wi-Fi Alliance

3/ Les norme IEEE 802.11 (4)

802.11ax (2021)	2,4 GHz 5 GHz	publié en 2019 - également connu sous le nom de High-Efficiency Wireless (HEW) des débits de données plus élevés gère de nombreux appareils connectés efficacité énergétique améliorée offre une meilleure stabilité dans les zones encombrées est connue sous le nom de Wi-Fi 6
802.11ay (2021)	60 GHz	offre un débit de 20 Gbit/s et peut atteindre jusqu'à 176 Gbit/s vise à augmenter la portée et la fiabilité

3/ Les norme IEEE 802.11 (5)

802.11ax (2022)	2,4 GHz 5 GHz 6 GHz	apparition du Wi-Fi 6E une extension sur une nouvelle fréquence du Wi-Fi 6 offre un débit de 10,5 Gbit/s
802.11be (2024)	2,4 GHz 5 GHz 6 GHz	apparition du Wi-Fi 7 offre un débit de 46 Gbit/s utilisation simultanée de plusieurs fréquences gère plus d’utilisateurs

3/ Les norme IEEE 802.11 (6)

Les nouvelles normes Wi-Fi permettent d’améliorer les débits, de diminuer la latence et de supporter toujours plus d’utilisateurs simultanés.

4/ Les équipements Wi-Fi (1)
Le point d’accès (AP: Access Point)

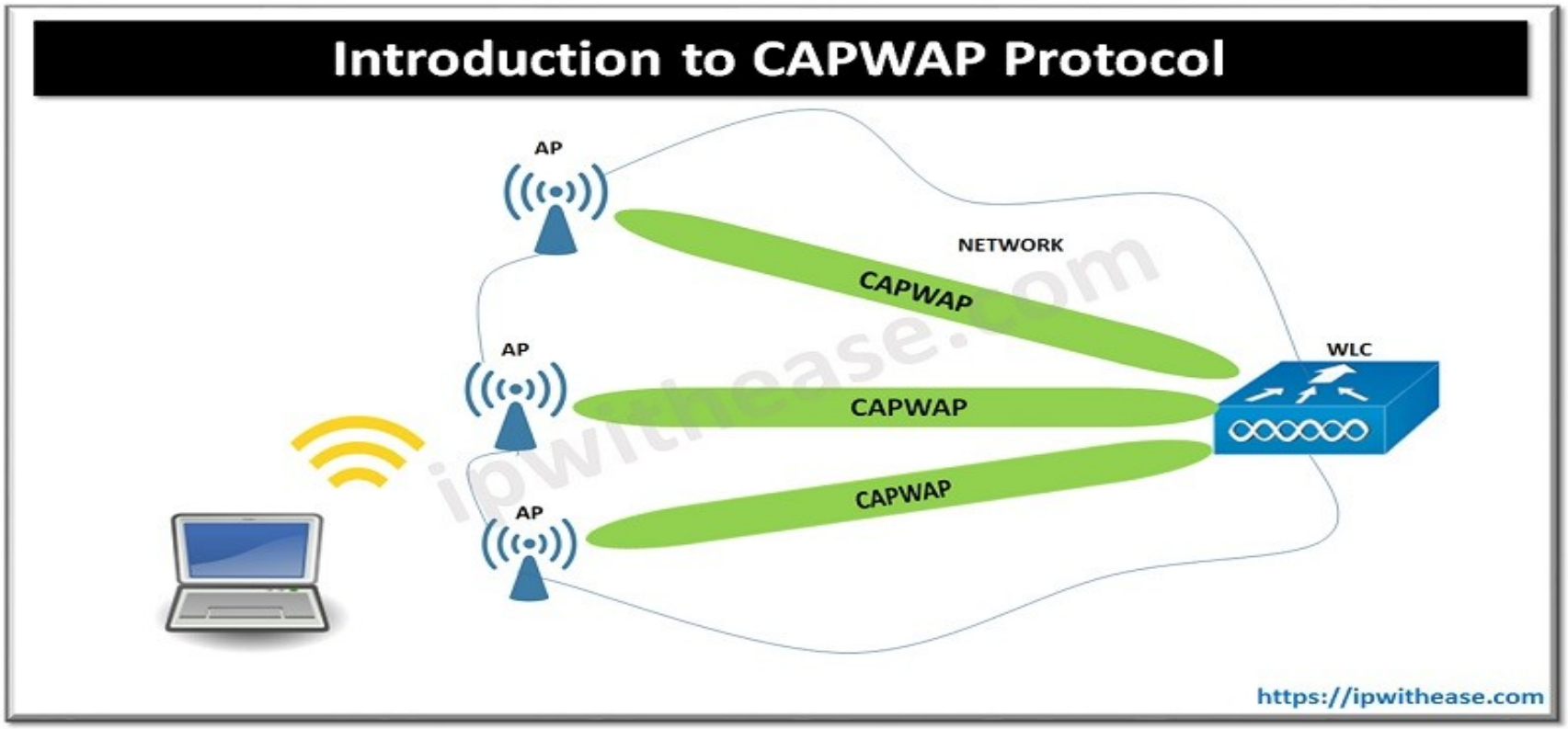
- Appelé aussi **borne sans fil**, il permet aux stations équipées de cartes Wi-Fi d’obtenir une connexion au réseau.
- Chaque station doit tenter de s’associer et de s’authentifier avec l’AP.
- Les trames d’information envoyées par un client sont réémises par l’AP, ce qui permet à la station de joindre un autre client qu’elle ne peut pas forcément voir directement (éloignement, obstacle).
- Les APs sont nécessaires lorsque le réseau sans fil fonctionne en mode infrastructure.
- Ce sont des boîtes qui contiennent une carte Wi-Fi, une ou plusieurs antennes et du logiciel embarqué dans une puce.
- Le logiciel présent permet de fournir des services supplémentaires liés à la sécurité et l’identification des autres AP connectés.

4/ Les équipements Wi-Fi (2)
Le point d’accès (AP: Access Point)

- Les points d’accès peuvent être classés comme des **points d'accès autonomes (Autonomous Access Points)** ou des **points d'accès basés sur un contrôleur (Lightweight Access Points)**.
- **Les points d’accès autonomes** sont considérés comme des périphériques autonomes configurés à l’aide d’une interface de ligne de commande ou d’une interface graphique.
- Les points d’accès autonomes sont utiles dans les situations où seuls quelques points d’accès sont requis dans l’organisation.
- Un routeur domestique est un exemple d’AP autonome car la configuration complète de l’AP réside sur l’appareil.
- **Les points d’accès basés sur un contrôleur** sont des périphériques dépendants d’un serveur, qui ne nécessitent aucune configuration initiale. Les points d’accès basés sur un contrôleur sont utiles dans les cas où de nombreux points d’accès sont nécessaires sur l’ensemble du réseau. Chaque nouveau point d’accès ajouté est automatiquement configuré et géré par un contrôleur WLAN.

4/ Les équipements Wi-Fi (2)
Le protocole CAPWAP

- CAPWAP (Control And Provisioning of Wireless Access Points) est un protocole standard IEEE, basé sur LWAPP (LightWeight Access Point Protocol). Il permet à un WLC de gérer plusieurs AP et WLAN.
- CAPWAP est également responsable de l'encapsulation et de la transmission du trafic client WLAN entre un AP et un WLC avec un tunnel.



4/ Les équipements Wi-Fi (3)

Cartes Wi-Fi

- Ce terme désigne les périphériques actifs Wi-Fi/Antenne directement branchés à un ordinateur client. Ils jouent exactement le même rôle que les cartes réseaux traditionnelles à la différence près qu'on ne branche pas de câble dessus, puisque la liaison est assurée par radio. Elles existent en trois formats:

- **PCMCIA:** Il s'agit du format le plus répandu puisque ce format est spécifique aux portables dont les propriétaires étaient les premiers intéressés par la technologie sans fil.
- **PCI:** C'est le format standard pour les ordinateurs de bureau mais les cartes restent au format PCMCIA. Il y a donc un adaptateur PCMCIA-PCI sur lequel est logée une carte PCMCIA.
- **USB:** Ce format s'est rapidement popularisé pour sa simplicité d'utilisation et les constructeurs n'ont pas tardé à proposer également des cartes Wi-Fi à ce format.

4/ Les équipements Wi-Fi (4)
Antennes sans fil

- L'antenne intégrée à l'AP ou à la carte Wi-Fi peut être remplacée par une antenne externe plus puissante.
- Le choix d'une antenne est important et doit être déterminé par le rôle qu'elle devra assurer, c'est à dire les interactions souhaitées avec les autres éléments Wi-Fi distants.
- Il existe trois grandes familles d'antennes :

➢ Les antennes omnidirectionnelles

➢ Les antennes directionnelles

➢ Les patchs ou antennes sectorielles

- En fonction des caractéristiques du terrain et des zones à couvrir, il est possible de réaliser des liaisons point à point via deux antennes directionnelles ou utiliser un élément omnidirectionnel dans le cas où nous avons des stations plus dispersés et rapprochés.

5/ Topologies sans fil (1)

- La norme 802.11 distingue deux modes principaux de topologies sans fil:

➢ Le mode **Ad Hoc**: C'est lorsque deux appareils se connectent de manière poste à poste (mode point à point) via Wi-Fi direct, sans utiliser de points d’accès ou de routeurs sans fil.

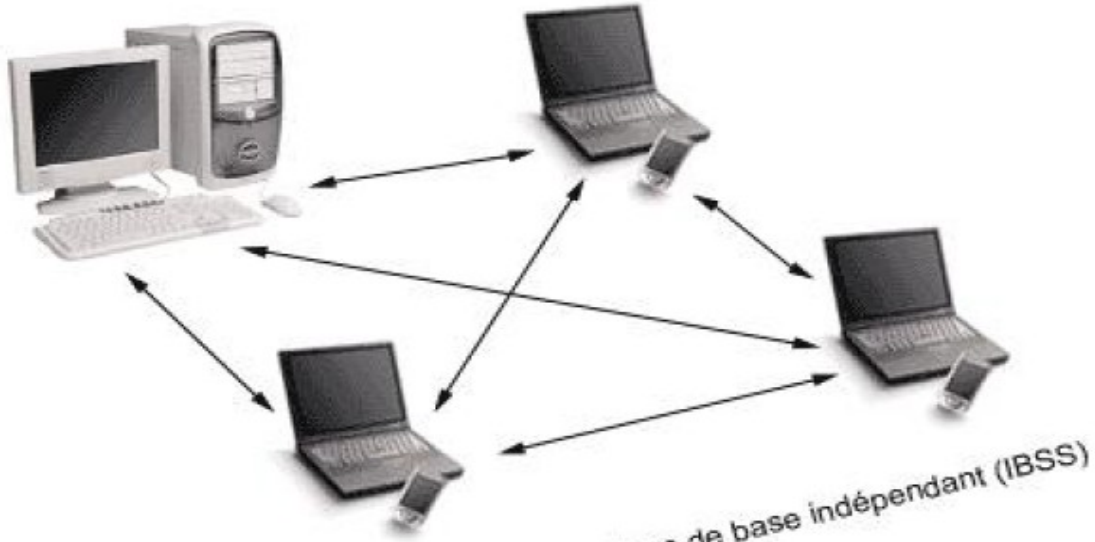
➢ Le mode **Infrastructure**: Dans lequel le réseau est composé d’une infrastructure permettant l’échange d’information entre les stations. Cette infrastructure correspond au point d’accès.

➢ Le mode partage de connexion (Tethering): qui est un mode parfois utilisé pour fournir un accès sans fil rapide.

5/ Topologies sans fil (2)

5.1 Le mode Ad Hoc

- Représente un groupe de PC avec chacun un adaptateur sans-fil connecté entre eux via le signal radio et sur le même canal, sans point d'accès.
- Dans ce mode, le réseau fonctionne de façon complètement distribuée.
- La norme désigne l'ensemble des stations à portée radio mutuelle par l'appellati



Ensemble de services de base indépendant (IBSS)

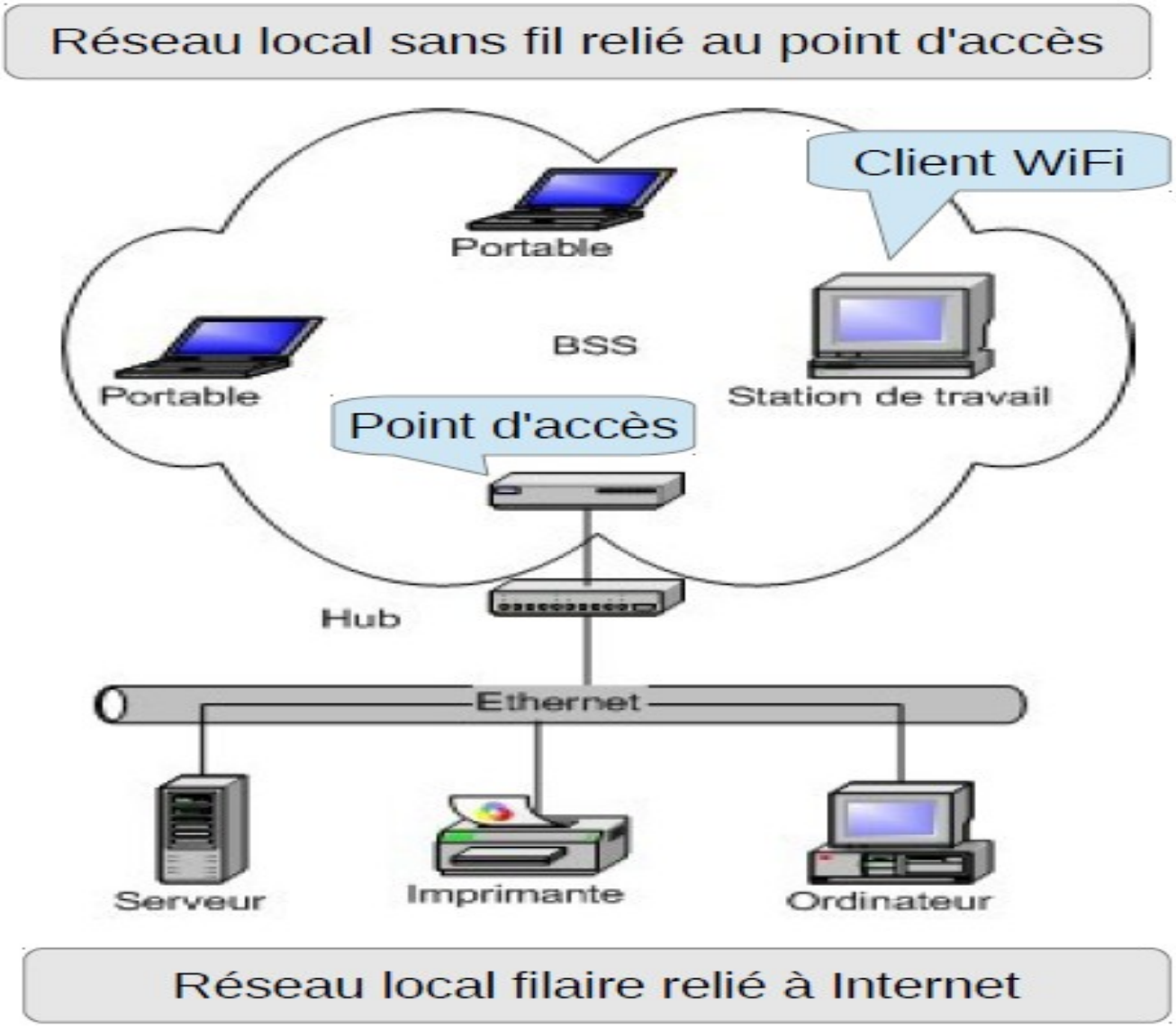
5/ Topologies sans fil (3)

5.2 Le mode Infrastructure

- En mode infrastructure, le réseau est composé de:
  - Clients Wi-Fi qui possèdent un matériel avec une interface sans fil.
  - Un Point d'accès WiFi (AP) qui gère les liaisons sans fil suivant la norme WiFi, le plus souvent connecté à Internet via un réseau filaire.
- L’ensemble formé par le point d’accès et les stations situées dans sa zone de couverture est appelé ensemble de services de base: **BSS (Basic Service Set)**
- L’adresse MAC du point d’accès est utilisée pour identifier de manière unique chaque BSS, qui est appelé l'identificateur de l'ensemble de services de base **BSSID**. Par conséquent, le BSSID est le nom formel du BSS et est toujours associé à un seul AP.

5/ Topologies sans fil (4)

5.2 Le mode Infrastructure



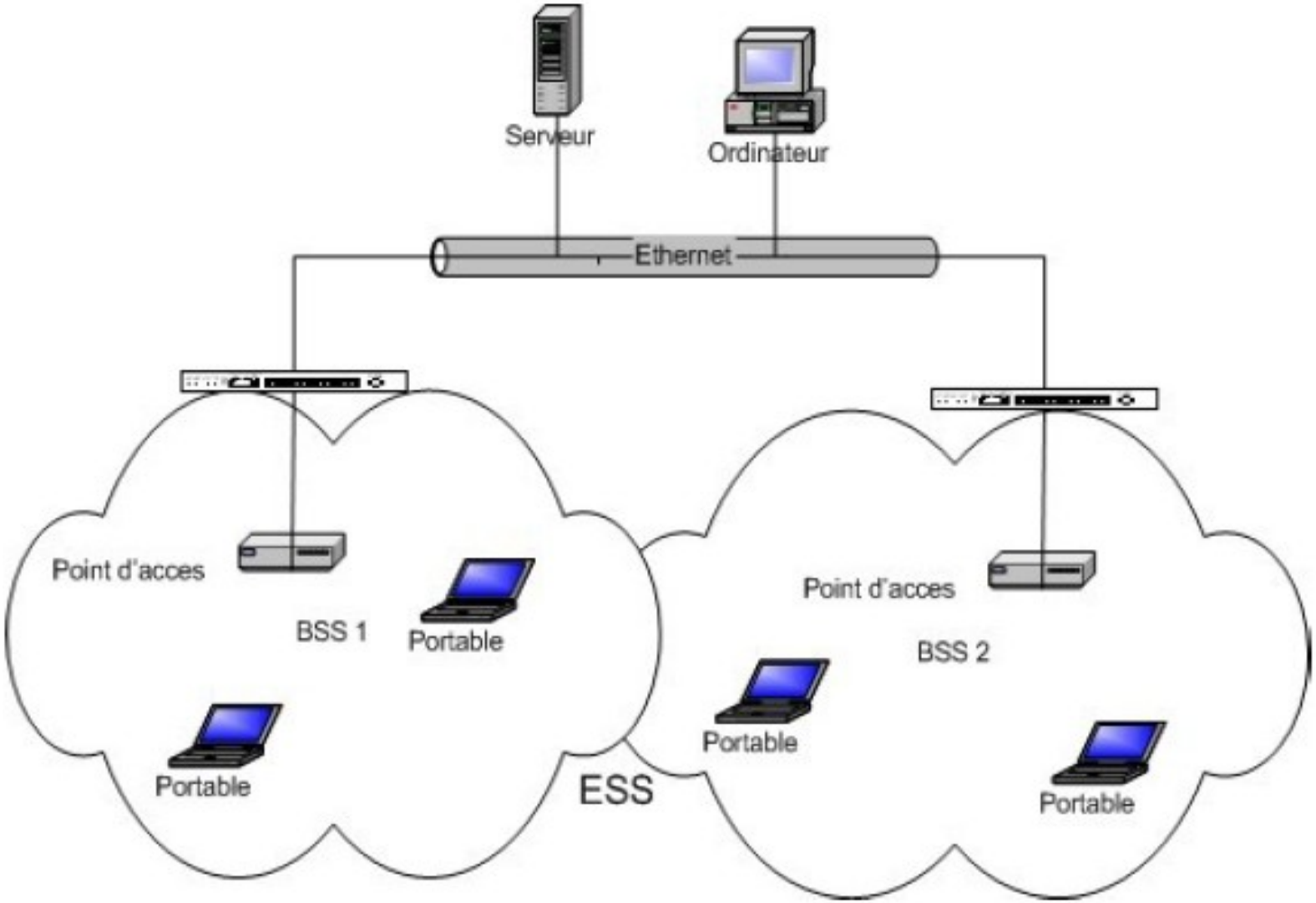
5/ Topologies sans fil (5)

5.2 Le mode Infrastructure

- Lorsque le réseau est relié à plusieurs BSS, chacun d'eux est relié à un système de distribution **DS (Distribution System)** par l'intermédiaire de leur point d'accès.
- Le système de distribution (DS) peut être aussi bien un réseau filaire (Ethernet), qu'un câble entre deux points d'accès ou bien même un réseau sans fil.
- Un groupe de BSS interconnectés par un système de distribution forme un ensemble de services étendu **ESS (Extended Service Set)**.
- Un ESS est identifié par un nom ESSID, appelé simplement SSID, qui est configuré manuellement sur les stations clients ou automatiquement par détection grâce à sa diffusion via le point d'accès.
- Un utilisateur nomade a la possibilité de passer de façon transparente d'un BSS à l'autre, ce qui est appelé **service d'itinérance (roaming)**, en utilisant le mécanisme du **« Handover »**.

5/ Topologies sans fil (6)

5.2 Le mode Infrastructure



6/ Connexion d'une station (1)

6.1 Synchronisation

- Lorsqu'une station a besoin d'accéder à un BSS ou un IBSS, soit après démarrage ou après un passage en mode veille, des informations de synchronisation sont nécessaire de la part du point d'accès, ou des autres stations dans le cas d'un réseau Ad Hoc. Ces informations peuvent être obtenues par l'une des deux techniques suivantes:

- **Ecoute active** : dans ce cas, la station tente de trouver un point d'accès en transmettant une trame de demande de synchronisation et attend une trame balise (Beacon Frame) de la part du point d'accès. La trame balise est une trame contenant des informations de synchronisation telles que la valeur de l'horloge du point d'accès au moment de la transmission.
- **Ecoute passive** : dans ce cas, la station attend simplement de recevoir une trame balise, celle-ci étant envoyée périodiquement par le point d'accès. Les stations réceptrices vérifient la valeur de leur horloge au moment de la réception, et la corrige afin de rester synchronisées.

6/ Connexion d’une station (2)
6.2 Authentification

- Une fois qu’une station a trouvé un point d’accès et une cellule (BSS) associée, le processus d’authentification s’enclenche. Il existe deux mécanismes d’authentification:

- **Open System Authentification** : Authentification par défaut, du moment que le réseau est ouvert, le terminal peut s’associer à n’importe quel point d’accès et écouter toutes les données qui transitent au sein du BSS.
- **Shared Key Authentification** : Il s’agit d’un véritable mécanisme d’authentification, utilisé dans le cas d’une sécurité WEP (Wired Equivalent Privacy) qui est basée sur une clé secrète communiquée aux utilisateurs autorisés du réseau, ainsi que de nouvelles politiques de sécurité telles que WPA (Wireless Protected Access), WPA2, etc. qui sécurisent les données avec le mécanisme de cryptage.

6/ Connexion d’une station (3)

6.3 Association

- Une fois la station authentifiée, nous passons au processus d’association. Celui-ci consiste en un échange d’informations concernant les différentes stations, les capacités de la cellule et enfin l’enregistrement de la position actuelle de la station par le point d’accès.
- C’est seulement après la fin du processus d’association que la station peut transmettre et recevoir des trames de données.
- Etant associée à une cellule, la station reste synchronisée avec le point d’accès par écoute passive. Le point d’accès transmet régulièrement les trames appelées trames "balises", qui contiennent la valeur de son horloge interne et qui permettent aux stations de synchroniser leur horloge.
- En cas de déplacement, l’attachement entre la station et le point d’accès est rompu grâce à la désassociation.

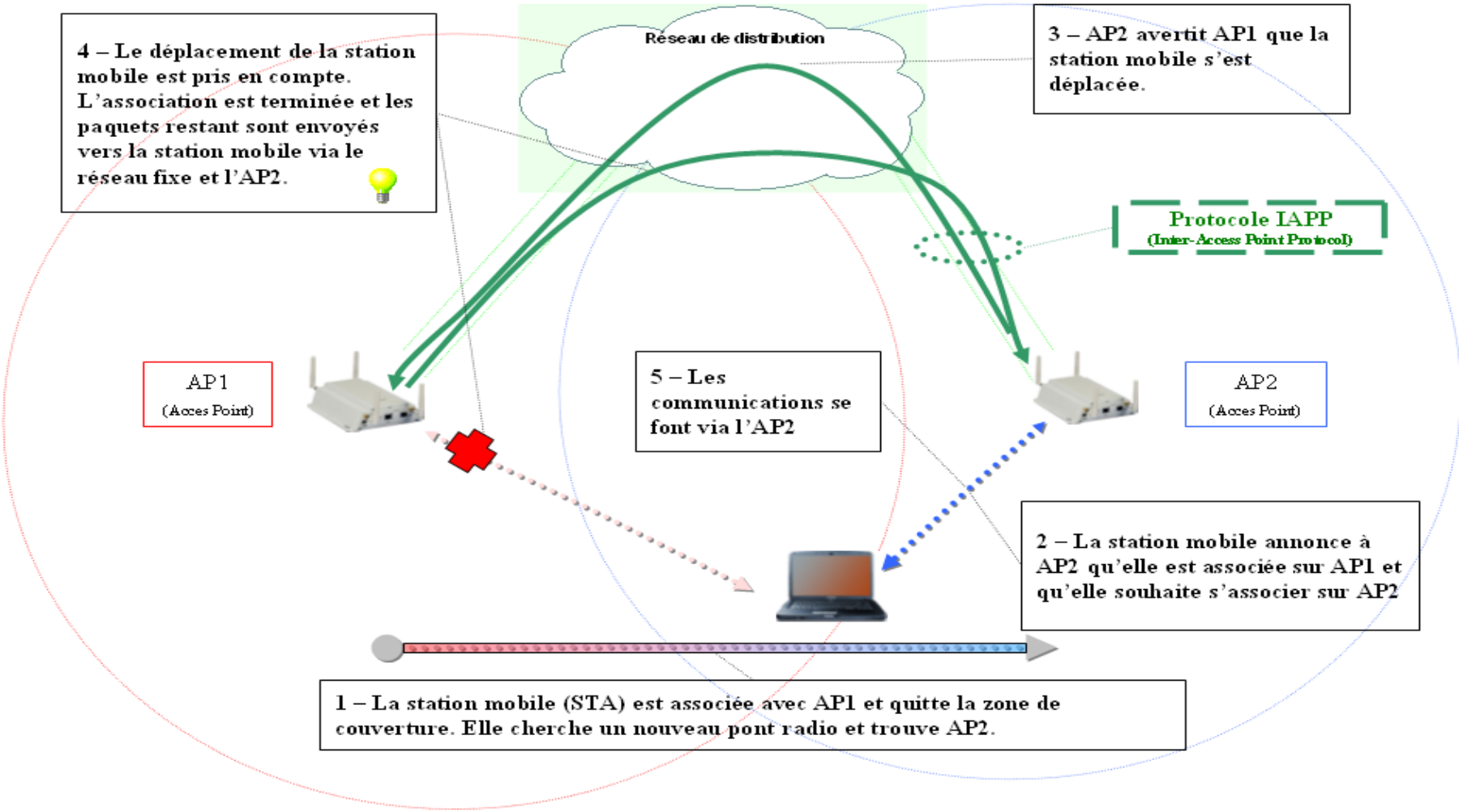
6/ Connexion d’une station (4)

6.4 Le roaming

- Le **roaming** est le processus de mouvement d’une cellule vers une autre sans perdre la connexion au réseau. Cette fonction est similaire au "**handover**" des téléphones portables, mais avec deux différences majeures :
- Sur un LAN, qui est basé sur une transmission par paquets, la transition d’une cellule à une autre doit être faite entre deux transmissions de paquets, contrairement à la téléphonie où la transition peut subvenir au cours d’une conversation.
- Dans un système vocal, une déconnexion temporaire peut ne pas affecter la conversation, alors que dans un environnement de paquets, les performances seront considérablement réduites à cause de la retransmission qui sera exécutée par les protocoles des couches supérieures.

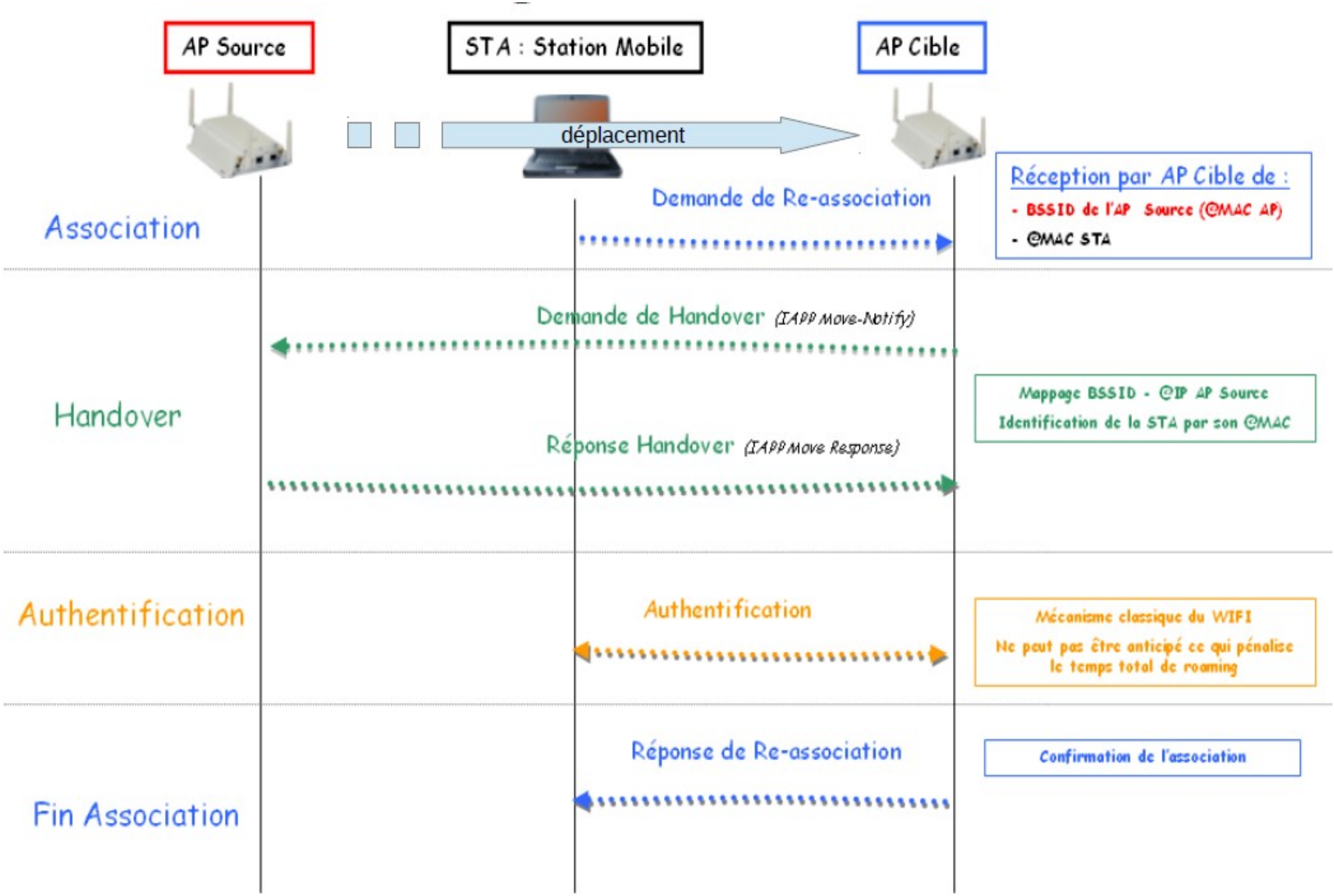
6/ Connexion d'une station (5)

6.4 Le roaming



6/ Connexion d'une station (6)

6.4 Le roaming



7/ Les couches protocolaires (1)

- La norme 802.11 définit seulement les deux couches les plus basses du modèle OSI (Les couches 1 et 2).
- La couche liaison de données est subdivisée en deux sous-couches: LLC et MAC.
- La couche physique est découpée en deux sous-couches: PLCP et PMD.

Modèle OSI	**Modèle 802.11**
Couche 2 **Couche liaison de données**	**LLC (Logical Link Control)**
	MAC (Medium Access Control)
Couche 1 **Couche physique**	**PLCP (Physical Layer Convergence Protocol)**
	PMD (Physical Medium Dependent)

7/ Les couches protocolaires (2)
7.1 La couche physique (1)

- La couche physique de la norme 802.11 est l'interface située entre la couche MAC et le support qui permet d'envoyer et de recevoir des trames.
- Chaque couche physique 802.11 est divisée en deux sous-couches :
  - la sous-couche **PMD** (Physical Medium Dependent) qui gère l'encodage des données et effectue la modulation.
  - La sous-couche **PLCP** (Physical Layer Convergence Protocol) qui s'occupe de l'écoute du support et fournit un signal appelé CCA (Clear Channel Assessment) à la sous-couche MAC pour lui indiquer si le canal est libre.
- Il existe 3 types de modulation utilisés au niveau de la couche physique: le **FHSS** ou étalement de spectre par saut de fréquence, le **DSSS** ou étalement de spectre par séquence directe, et le **OFDM** ou multiplexage par répartition en fréquences orthogonales.

7/ Les couches protocolaires (3)

7.1 La couche physique (2)

FHSS (Saut de fréquence)

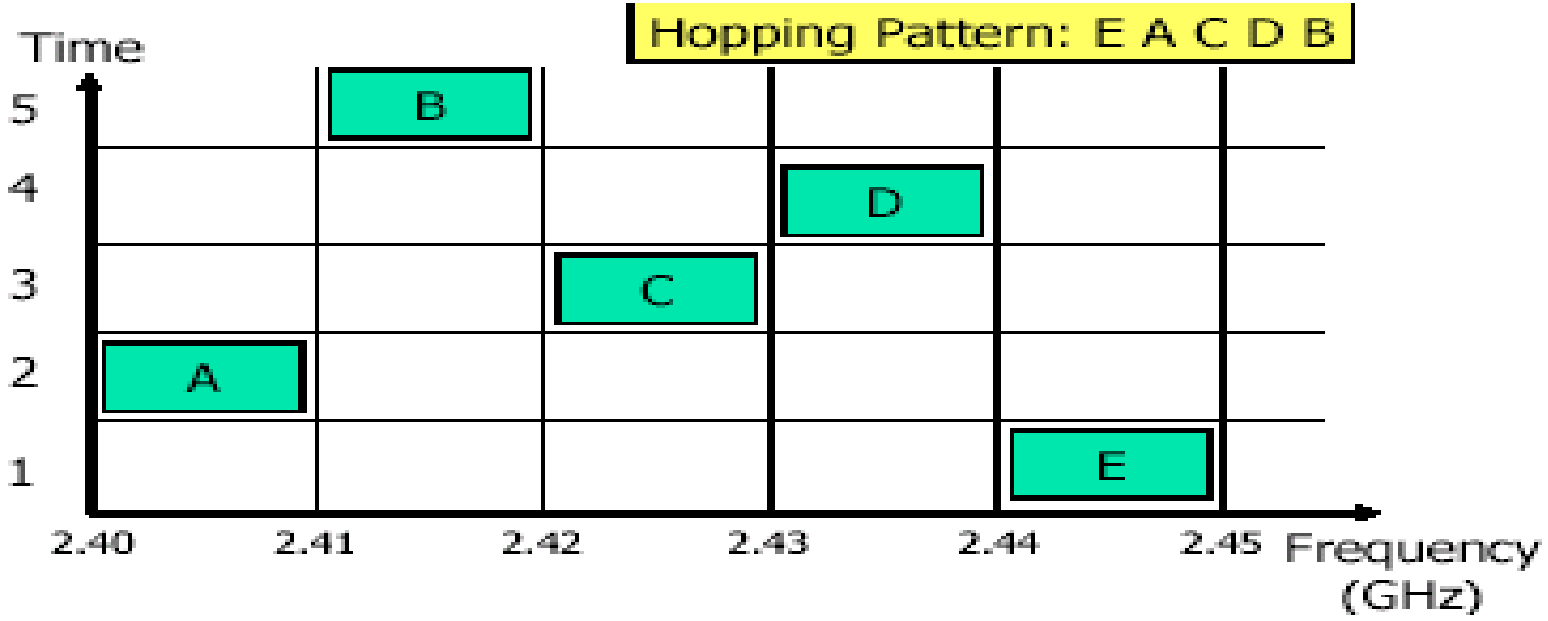
- Le FHSS (Frequency Hopping Spread Spectrum) est une technique qui est basée sur le saut de fréquence périodique de l'émetteur, suivant un ordre cyclique prédéterminé.
- La bande de fréquences 2.4 - 2.4835 GHz est divisée en 79 canaux de 1 MHz chacun.
- La transmission est ainsi réalisée en émettant successivement sur un canal puis sur un autre pendant une courte période de temps (d'environ 400 ms).
- Le fait de ne jamais rester sur le même canal engendre une bonne tolérance aux bruits.
- Il s'agit d'une méthode de transmission relativement simple mais qui est limitée par son débit maximum de 2 Mbits/s.
- Elle introduit une certaine complication au niveau MAC, ce qui se traduit en termes de multiplication d'en-têtes et donc de réduction de débit.

7/ Les couches protocolaires (4)

7.1 La couche physique (3)

FHSS (Saut de fréquence)

- Chaque conversation sur le réseau 802.11 s'effectue suivant un schéma de saut différent, et ces schémas sont définis de manière à minimiser le risque que deux expéditeurs utilisent simultanément le même sous-canal.
- La séquence de fréquences utilisée est donc publique.



Négociation du schéma de transmission (Hopping Pattern)

7/ Les couches protocolaires (5)

7.1 La couche physique (4)

DSSS (Direct-Sequence Spread Spectrum)

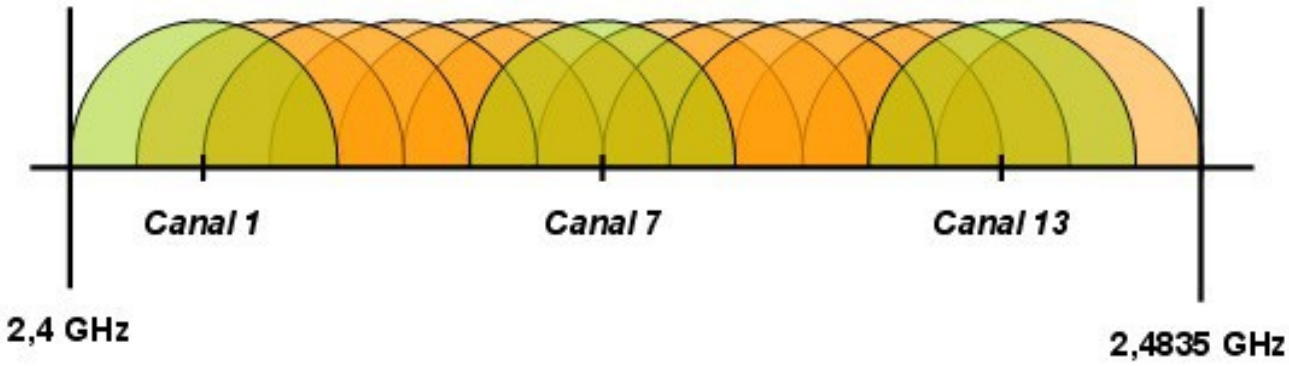
- Comme le FHSS, l'étalement de spectre à séquence directe (DSSS) divise la bande des 2.4 GHz en sous bandes. Cependant la division se fait ici en 14 canaux de 20 MHz chacun espacés de 5 MHz.
- Pour communiquer, l'émetteur et le récepteur doivent se mettre d'accord sur un seul canal fixe à utiliser.
- La largeur de la bande ISM étant égale à 83.5 MHz, il est impossible d'y placer 14 canaux adjacents de 20 MHz. Les canaux se recouvrent donc.
- Comme la transmission ne se fait que sur un canal, les systèmes DSSS sont plus sensibles aux interférences que les systèmes FHSS, qui utilisent toute la largeur de bande.
- L'utilisation d'un seul canal pour la transmission est un inconvénient si différents réseaux 802.11 DSSS se superposent.

7/ Les couches protocolaires (6)

7.1 La couche physique (5)

DSSS (Direct-Sequence Spread Spectrum)

- Pour permettre à plusieurs réseaux d'émettre sur une même cellule, il faut allouer à chacun d'eux des canaux appropriés, qui ne se recouvrent pas.
- Sachant que la largeur de bande n'est que de 83.5 MHz, il ne peut donc y avoir au maximum que trois réseaux 802.11 DSSS émettant sur une même cellule sans risque d'interférences.



7/ Les couches protocolaires (7)

7.1 La couche physique (6)

DSSS (Direct-Sequence Spread Spectrum)

- Son principe consiste à transmettre pour chaque bit une séquence Barker (ou bruit pseudo-aléatoire, en anglais pseudo-random noise noté PN) de bits.
- Ainsi chaque bit valant 1 est remplacé par une séquence de bits et chaque bit valant 0 par son complément. La nouvelle séquence ainsi constituée est dénommée « chip » ou « chipping code».
- Le DSSS provoque ainsi des transitions d'état très rapide (chipping) qui tendent à étaler le spectre du signal : en effet, la largeur du spectre correspond au double du débit de la source. En provoquant artificiellement un débit très élevé, le spectre est étalé.
- Dans le standard 802.11, le code d'étalement a une longueur de 11 bits, et la séquence d'étalement remplace un bit à 1 par la séquence «10110111000» et un bit à 0 par son complément, soit «01001000111».

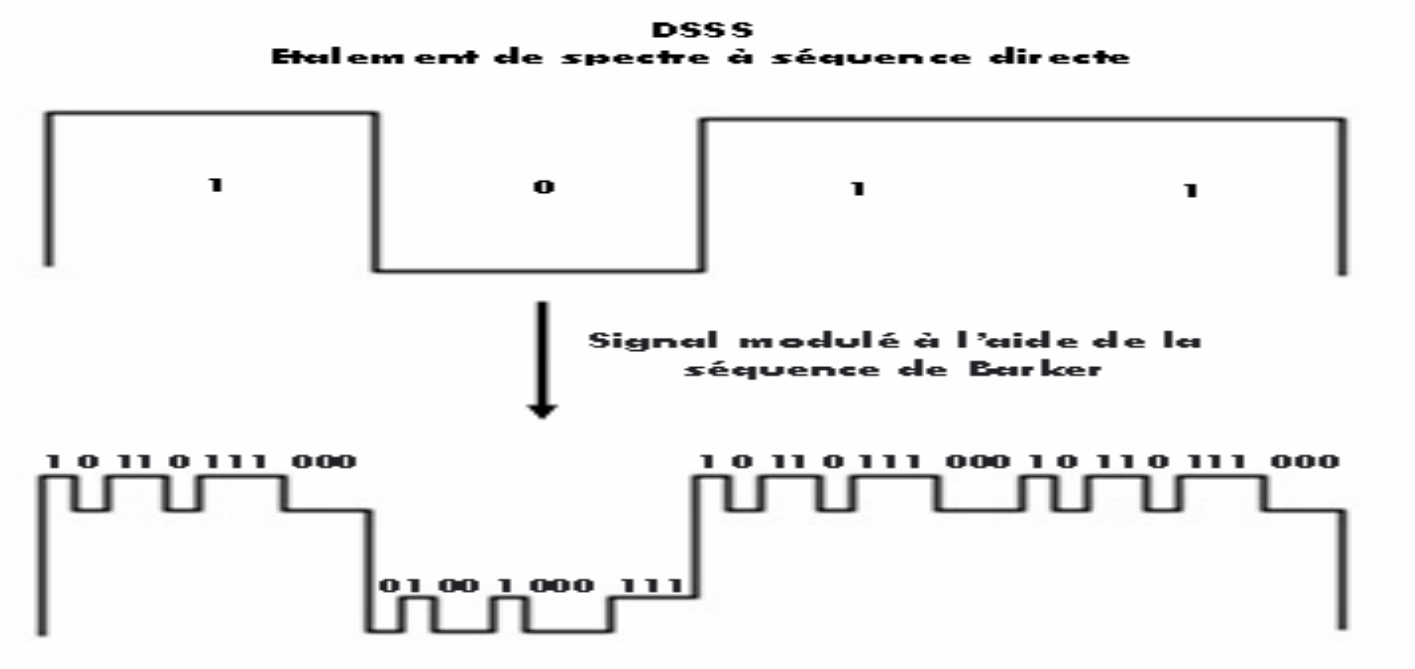
7/ Les couches protocolaires (8)

7.1 La couche physique (7)

DSSS (Direct-Sequence Spread Spectrum)

- Ces séquences de Barker ne permettent que de coder deux états (0 ou 1) avec un débit de 1 Mbit/s à 2 Mbit/s.
- En codant plusieurs bits de données par chip, la technique dite du CCK (Complementary Code Keying) (8 bits) permet d'atteindre des débits plus élevés (5,5 ou 11 Mbit/s) : c'est ce qu'on appelle le DSSS à haute vitesse ou High-Rate DSSS (HR-DSSS).

Technique de chipping



7/ Les couches protocolaires (9)

7.1 La couche physique (8)

OFDM (Orthogonal Frequency Division Multiplexing)

- Se base sur le principe du multiplexage fréquentiel, qui permet la transmission simultanée de plusieurs communications sur une même bande de fréquences.
- Le canal de transmission est découpé en sous-canaux et les données sont émises simultanément sur chaque sous-porteuse.
- Malheureusement, il est possible d'avoir des interférences entre les sous-porteuses, ce qu'on appelle l'Inter-Carrier Interference (ICI).
- Pour résoudre ce problème, l'OFDM utilise une fonction mathématique assez complexe pour rendre les sous-porteuses «orthogonales », c'est-à-dire pour qu'elles n'interfèrent pas les unes avec les autres.

7/ Les couches protocolaires (10)

7.1 La couche physique (9)

OFDM (Orthogonal Frequency Division Multiplexing)

- Comme pour le DSSS, la bande disponible est divisée en canaux de 20 MHz et sa transmission se fait que sur un canal.
- Chaque canal est divisé en 52 sous-canaux ayant pour largeur 300Khz. 48 sous-canaux sont utilisés pour la transmission des données tandis que les quatre autres sont chargés de la correction d'erreur ou FEC (Forward Error Correction). A chaque sous-canal est appliquée une technique de modulation définissant ainsi un canal à très bas débit.
- L'avantage d'OFDM vient de la formation d'un canal très haut débit de ces sous-canaux à très faible débit, permettant ainsi d'atteindre des vitesses de transmission jusqu'à 54 Mbit/s pour 802.11a.
- Un autre avantage d'OFDM est le mécanisme de correction d'erreur sur l'interface physique, évitant ainsi la gestion des retransmissions au niveau de la couche MAC.

7/ Les couches protocolaires (11)

7.1 La couche physique (10)

Les évolutions de la couche physique 802.11

- Au fil des années, des améliorations importantes concernant la couche physique ont été apportées au standard 802.11.

Norme	Fréquence radio (GHz)	Techniques d'étalement et/ou de modulation
802.11	2,4	FHSS, DSSS
802.11a	5	OFDM
802.11b	2,4	DSSS, HR-DSSS
802.11g	2,4	DSSS, HR-DSSS ou OFDM
802.11n	2,4 ou 5	OFDM
802.11ac	5	OFDM

Principales améliorations concernant les couches physiques de la norme 802.11

7/ Les couches protocolaires (12)

7.2 La couche liaison de données (1)

- La couche liaison de données définit l'interface entre le bus de la machine et la couche physique.
- Elle est composée de deux sous-couches :
  - La sous-couche de contrôle de liaison logique (**LLC** : Logical Link Control).
  - La sous-couche de contrôle d'accès au support (**MAC** : Medium Access Control):
- Défis:
  - Dans un réseau filaire, chaque machine envoyant un message vérifie qu'aucun autre message n'a été envoyé en même temps par une autre machine. Si c'est le cas, les deux machines patientent pendant un temps aléatoire avant de recommencer à émettre.
  - Dans un réseau sans fil, ce procédé n'est pas possible dans la mesure où deux stations communiquant avec un récepteur ne s'entendent pas forcément mutuellement en raison de leur rayon de portée.

7/ Les couches protocolaires (13)

7.2 La couche liaison de données (2)

La sous-couche LLC

- Représente le lien logique entre la couche MAC et la couche réseau (OSI 3) via le LSAP (Logical Service Access Point) qui permet de rendre interopérables des réseaux différents au niveau MAC ou physique mais possédant la même sous-couche LLC.
- Utilise les mêmes propriétés que la sous-couche LLC 802.2
- Son but est de permettre aux protocoles réseaux de niveau 3 de reposer sur une couche unique (la couche LLC) quel que soit le protocole sous-jacent utilisé, dont le Wifi ou l'Ethernet, par exemple.
- Tous les paquets de données WiFi transportent donc un paquet LLC.
- Il est alors possible d'avoir en même temps, sur un même réseau plusieurs protocoles de niveau 3, et donc relier un WLAN à tout autre réseau local appartenant à un standard de l'IEEE.
- Utilise deux types de fonctionnalités: Système de contrôle de flux et reprise sur erreur.

7/ Les couches protocolaires (14)

7.2 La couche liaison de données (3)

La sous-couche MAC

- Son rôle est assez similaire à celui de la couche MAC 802.3, puisque les stations écoutent la porteuse avant d'émettre. Si la porteuse est libre, le terminal émet, sinon il se met en attente.
- Cependant, la couche MAC 802.11 intègre un grand nombre de fonctionnalités, telles que :

- Le contrôle d'accès au support,
- L'adressage et le formatage des trames,
- Le contrôle d'erreurs par CRC (Cyclic Redundancy Check),
- La fragmentation et le réassemblage des trames,
- La qualité de service,
- La gestion de l'énergie,
- La gestion de la mobilité,
- La sécurité, etc.

7/ Les couches protocolaires (15)

7.2 La couche liaison de données (4)

La sous-couche MAC

- La sous-couche MAC définit deux méthodes d'accès différentes: et intègre un grand nombre de fonctionnalités, telles que :

➢ **PCF** (Point Coordination Function): Il s'agit d'un mode de contrôle centralisé dans le point d'accès (PCF : Point CF), donc, le AP gère les émissions et distribue les autorisations d'émissions en interrogeant successivement les stations présentes (Polling).

Inconvénient: Paquets de signalisation supplémentaires

Avantages: - Il n'y a plus de collision

- Possibilité de gérer des qualités de services: priorité possible entre les stations

➢ **DCF (**Distributed Coordination Function): est basé sur le **CSMA/CA** (Carrier Sense Multiple Access/Collision Avoidance), contrairement au réseaux Ethernet où on utilise le **CSMA/CD**.

7/ Les couches protocolaires (16)

7.2 La couche liaison de données (5)

La sous-couche MAC

- Le **CSMA/CD** ne peut pas être utilisé dans les environnements sans fil pour les raisons suivantes:

➢ Pour détecter une collision, une station doit être capable d'écouter et de transmettre en même temps.

➢ Dans les systèmes radio, la transmission couvre la réception des signaux sur la même fréquence et ne permet pas à la station d'entendre la collision (les transmissions radio ne sont jamais Full Duplex)

➢ Comme une station ne peut écouter sa propre transmission, si une collision se produit, la station continue à transmettre la trame complète, ce qui entraine une perte de performance du réseau.

- Le protocole **CSMA/CA** tente d'éviter les collisions en imposant un accusé de réception (Acknowledgement, ACK) systématique des paquets, ce qui signifie que pour chaque paquet de données arrivé intact, un paquet ACK est émis par la station de réception.

7/ Les couches protocolaires (17)

7.2 La couche liaison de données (6)

La sous-couche MAC (Le Protocole CSMA/CA)

- Le principe de fonctionnement du protocole CSMA/CA est le suivant:

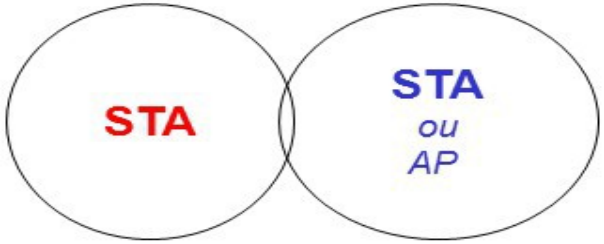
1. La station voulant émettre écoute le réseau. Si le réseau est encombré, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé **DIFS** pour Distributed Inter Frame Space), alors la station peut émettre.
2. La station transmet un message appelé Ready To Send (noté **RTS** signifiant prêt à émettre) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission.
3. Le récepteur (généralement un point d'accès) répond un Clear To Send (**CTS**, signifiant: le champ est libre pour émettre), puis la station commence l'émission des données.

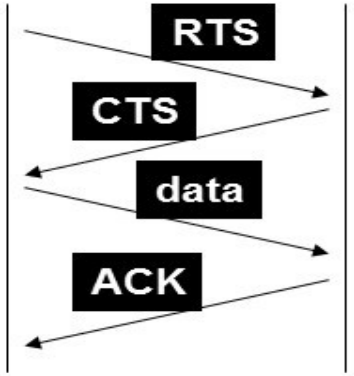
7/ Les couches protocolaires (18)

7.2 La couche liaison de données (7)

La sous-couche MAC (Le Protocole CSMA/CA)

4. A la réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (ACK).
5. Toutes les stations avoisinantes patientent alors pendant un temps qu'elle considère être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.

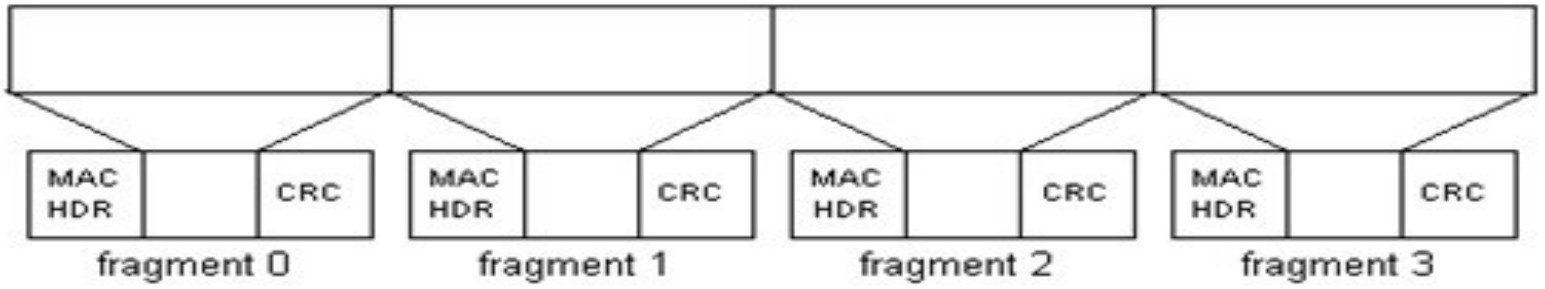




8/ Les trames Wi-Fi (1)

- La fragmentation et le réassemblage des trames sont gérés au niveau de la couche MAC.
- Les paquets sont fractionnés en trames pour les raisons suivantes:
  - La probabilité d'erreur augmente avec la taille du paquet (taux d'erreur supérieur par rapport à celui généré dans les réseaux filaires).
  - Moins de bande passante gâchée par retransmission.

Trame initiale



- La couche liaison doit assurer une transmission exemptée d'erreurs sur un canal de communication.

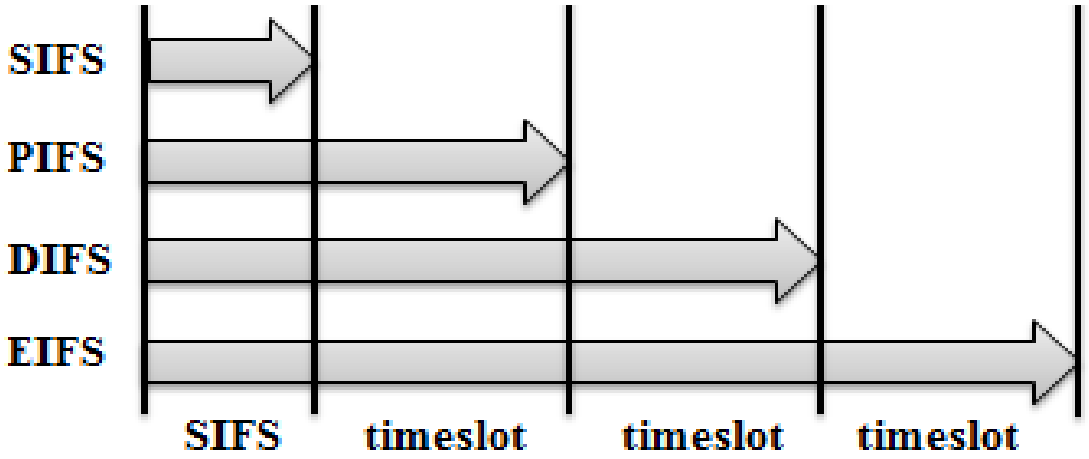
8/ Les trames Wi-Fi (2)
Espaces inter-trame (IFS)

- Les modes d'accès définis au niveau de la sous couche MAC sont contrôlés par l'utilisation d'espaces ou de silence inter-trames IFS (Inter-Frame Spacing),
- Les IFS correspondent à l'intervalle de temps entre la transmission de deux trames. Les intervalles IFS sont des périodes d'inactivité sur le support de transmission.
- Pour définir les différents types d'IFS, la norme a tout d'abord introduit la notion de Slot Time, dont la valeur dépend de la couche physique utilisée. Par exemple, pour la couche PMD à étalement de spectre à séquence directe, cette valeur est de 20 µs.
- Chaque IFS correspond à la valeur de son précédent augmentée du Slot Time.

8/ Les trames Wi-Fi (3)
Espaces inter-trame (IFS)

- Il existe 4 types d'espace inter-trame:

1. SIFS (Short Inter Frame Space)
2. PIFS (PCF IFS)
3. DIFS (DCF IFS)
4. EIFS (Extended IFS



- **Remarque**: Toutes les autres stations à l'écoute déclenchent un timer appelé NAV (Network Allocation Vector) pour une certaine durée, permettant de retarder toutes les transmissions prévues et passent en mode économie d'énergie.

8/ Les trames Wi-Fi (4)

Espaces inter-trame (IFS)

SIFS (Short Inter Frame Space)

- C’est le plus petit écart entre deux trames
- Il est utilisé pour séparer les transmissions appartenant à un même dialogue, par exemple:
  - entre des données et ACK,
  - RTS et CTS,
  - différents fragments d’une trame segmentée,
  - trame de polling en mode PCF.
- Il y a toujours, au plus, une seule station pour transmettre à cet instant, ayant donc la priorité sur toutes les autres
- Cette valeur est fournie par la couche physique, par exemple, pour le FHSS de 802.11, le SIFS=28 microsecondes.

8/ Les trames Wi-Fi (5)
Espaces inter-trame (IFS)
PIFS (PCF IFS)

- Il est utilisé en mode PCF. Il permet aux transmissions PCF de gagner l'accès au médium par l'utilisation d'un IFS plus petit que celui utilisé pour la transmission des trames en DCF. Ce qui permet aux AP d'accéder avec priorité au support.
- La valeur du PIFS est égale à celle du SIFS plus un certain temps (Slot Time), soit 78 microsecondes pour la couche physique FHSS et 30 microsecondes pour la couche physique DSSS.
- En mode PCF, une station « sélectionnée » doit répondre dans un intervalle de temps prédéterminé (PIFS), sinon le point d'accès passe à la station suivante. À tout moment, le point d'accès peut mettre fin à la période de PCF et basculer en mode DCF.
- La méthode PCF est conçue essentiellement pour la transmission de données sensibles, telles que la voix ou la vidéo. C'est pour cette raison que la valeur du PIFS est inférieur à celle du DIFS.

8/ Les trames Wi-Fi (6)
Espaces inter-trame (IFS)
DIFS (DCF IFS)

- Il est utilisé par une station voulant commencer une nouvelle transmission
- Le DIFS est le plus couramment utilisé (avec le SIFS). Il est utilisé en mode DCF comme temps minimal d'attente avant transmission.
- Les valeurs des différents PIFS et DIFS sont calculées de la manière suivante :

➢ PIFS=SIFS + Slot Time

➢ DIFS= SIFS + 2 * Slot Time

- où Slot Time correspond à l'intervalle minimal entre deux opérations de détection physique de porteuse. Cette valeur est dépendante des caractéristiques de la couche physique considérée.

8/ Les trames Wi-Fi (7)
Espaces inter-trame (IFS)
Algorithme de Backoff

- Une procédure de backoff est mise en place suite à la détection de l'occupation du canal par la fonction d'accès DCF pour une durée supérieure à DIFS.
- Cette procédure permet aux stations de réduire la probabilité de collision.
- Le temps de backoff correspond à l'attente pendant une durée aléatoire avant le prochain envoi.
- Cette durée d'attente aléatoire est calculée de la manière suivante :

Temps de Backoff (i) = Random (0, CW_i) * Slot Time

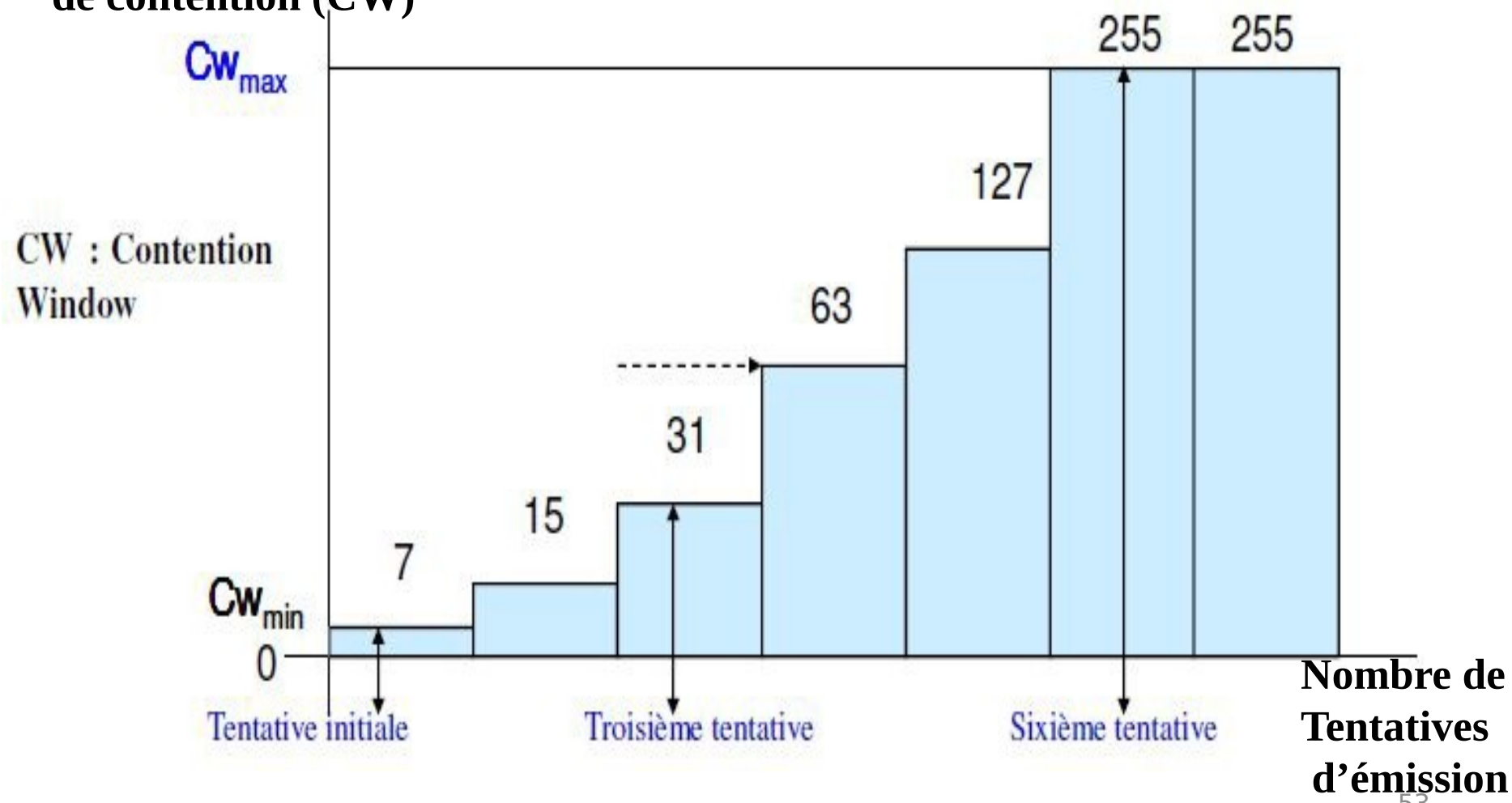
Avec :

$CW_i = 2^{2+i} - 1$, où i correspond au nombre de tentatives de transmission.

8/ Les trames Wi-Fi (8)

Espaces inter-trame (IFS)

Algorithme de Backoff



8/ Les trames Wi-Fi (9)
Espaces inter-trame (IFS)
Algorithme de Backoff

- La valeur de CW évolue dans l'intervalle [CW_{min}, CW_{max}] qui est définie par le standard. Par exemple:
  - Pour la norme 802.11a et g : CWmin = 15, CWmax = 1023.
  - Pour la norme 802.11b : CWmin = 31, CWmax = 1023.
- La valeur de CW est initialisée à CW_{min}, lorsqu'un paquet vient d'être envoyé avec succès ou lorsqu'un paquet est rejeté suite au dépassement de la limite des retransmissions.
- Après la détection d'une collision, la valeur de CW est augmentée de façon exponentielle jusqu'à atteindre la borne maximale CW_{max} afin de réduire le taux de collision.
- Rappel: Le Slot Time Varie aussi de norme en norme : Dans 802.11a : 9 microsecondes / 802.11b : 20 microsecondes / 802.11g : 10 microsecondes, etc.

8/ Les trames Wi-Fi (10)
Espaces inter-trame (IFS)
Algorithme de Backoff

- Une fois la valeur du temps de Backoff calculée, elle est décrémentée de 1 à chaque slot libre.
- Lorsque le temps de Backoff atteint 0, et si le médium est toujours libre, la station tente l'envoi sur le médium.
- Si en cours de décrémentation du temps de Backoff le médium devient occupé, la valeur courante du Backoff est mémorisée et la décrémentation reprendra au point où elle s'était arrêtée lorsque la station observera à nouveau un intervalle DIFS d'inoccupation du médium.
- Note: Plusieurs travaux de recherche ont été menés dans la perspective d'améliorer l'algorithme de backoff utilisé par le protocole CSMA/CA.

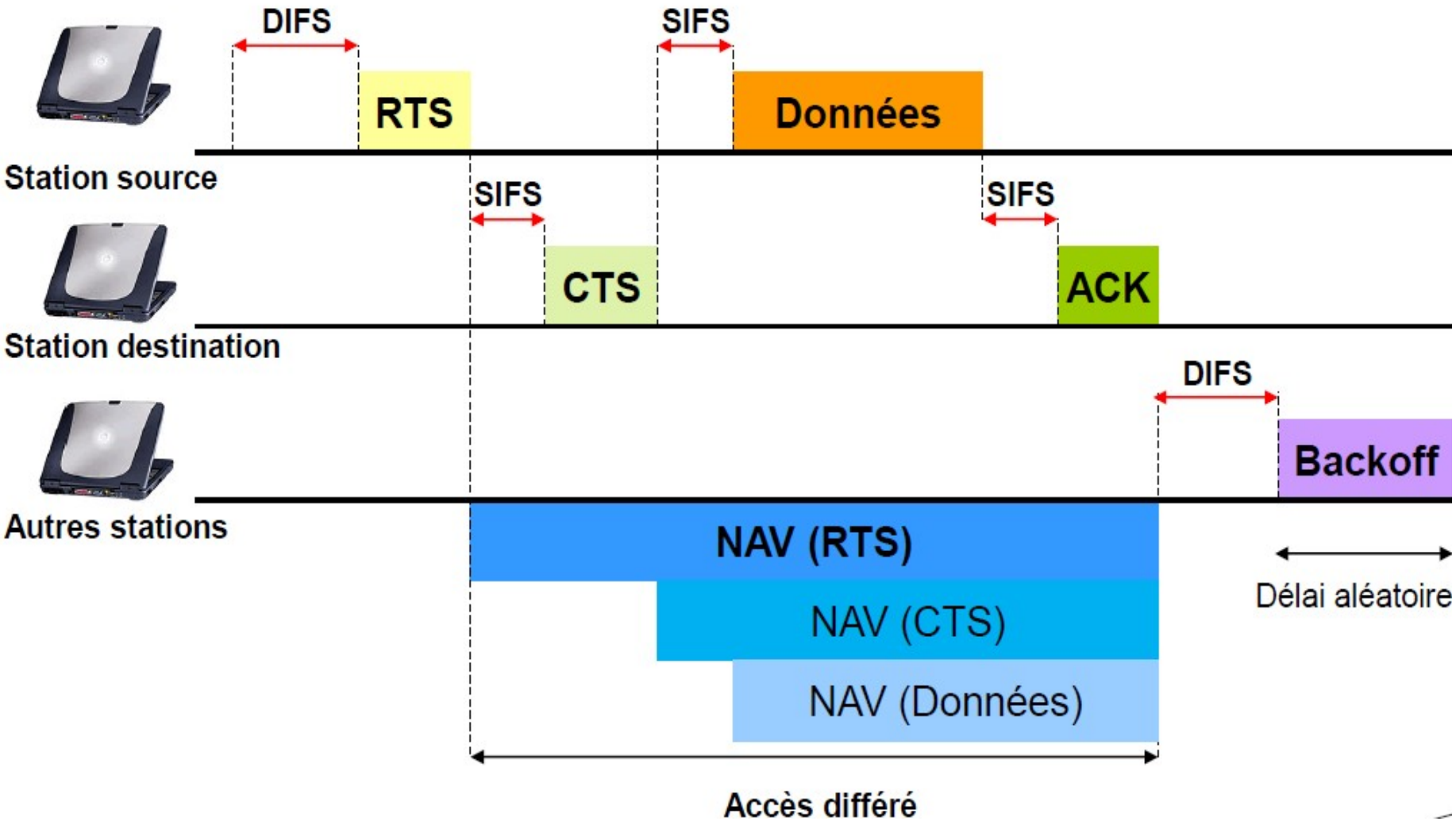
8/ Les trames Wi-Fi (11)
Espaces inter-trame (IFS)
EIFS (Extended IFS)

- Le quatrième IFS est le plus long.
- Lorsqu'une station reçoit une trame erronée, elle doit attendre pendant un EIFS l'acquittement de cette trame.
- Il est utilisé lorsqu'il y a détection de collision.
- Ce temps relativement long par rapport aux autres IFS est utilisé comme inhibiteur pour éviter des collisions en série.
- Il est utilisé uniquement en mode DCF
- **Note**: Les différents IFS permettent de définir des degrés de priorité. Lorsque plusieurs stations souhaitent émettre simultanément, la station souhaitant émettre les trames les plus prioritaires comme les acquittements pourra les envoyer en premier. Puis seront transmises d'autres trames jugées prioritaires comme celles liées au trafic qui a des contraintes de délai.

8/ Les trames Wi-Fi (12)

Espaces inter-trame (IFS)

Exemple



8/ Les trames Wi-Fi (13)

Format

Au niveau MAC

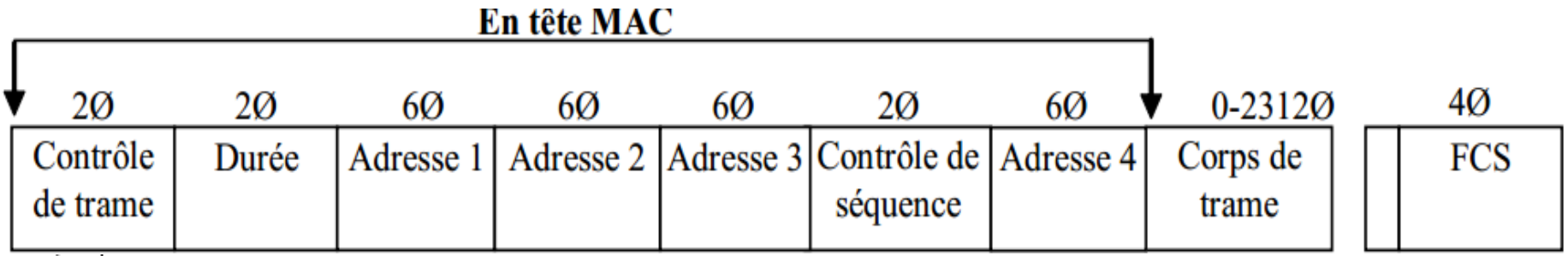
- Il existe trois types de trames MAC 802.11:
- **Les trames de données**: utilisées pour la transmission des données
- **Les trames de contrôle:** utilisées pour contrôler l'accès au support (ex: RTS, CTS, ACK) (contribuent au bon acheminement des trames de données.
- **Les trames de gestion**: transmises de la même façon que les trames de données pour l'échange d'informations de gestion, mais qui ne sont pas transmises aux couches supérieures (ex: trame balise (beacon), association, authentification, etc.).
- Chacun de ces trois types est subdivisé en différents sous-types, selon leurs fonctions spécifiques.

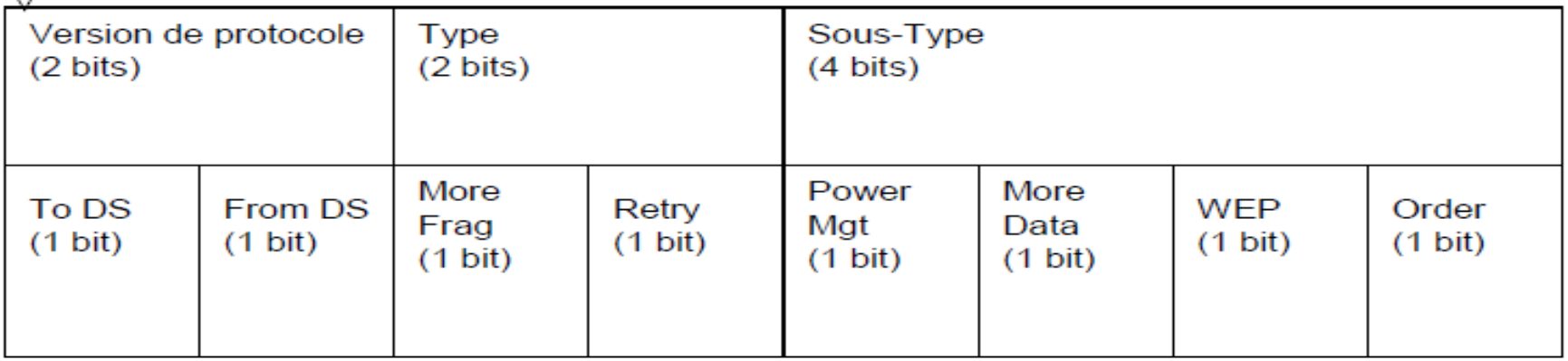
8/ Les trames Wi-Fi (14)

Format

Au niveau MAC

- Le format général d'une trame MAC 802.11 est le suivant:





8/ Les trames Wi-Fi (15)
Format
Au niveau MAC

- Le champ **contrôle de trame** est composé des champs suivants:
  - **Version de protocol** : identifier la version du protocole IEEE 802.11.
  - **Type** : 3 types possibles : trames de gestion, de contrôle ou de données.
  - **Sous-type** : pour chaque type il existe des sous-types
  - **To DS** : 1 si la trame est adressée à l'AP, 0 sinon.
  - **From DS** : 1 lorsque la trame vient du DS (système de distribution)
  - **More Fragment** : 1 si d'autres fragments suivent le fragment en cours.
  - **Retry** : 1 si le fragment est une retransmission (utile pour le récepteur si le ACK est perdu)
  - **Power Management** : la station sera en mode de gestion d'énergie après cette trame.
  - **More Data** : pour la gestion d'énergie, l'AP indique qu'il a d'autres trames pour cette station.
  - **WEP** : le corps de la trame sera chiffré selon l'algorithme WEP
  - **Order** : trame envoyée en utilisant la classe de service « strictement ordonné ».

8/ Les trames Wi-Fi (16)
Format
Au niveau MAC

- Le champ **durée** :
  - Dans la plupart des trames, indique la durée, en microsecondes, de la prochaine trame transmise, pour le calcul du NAV.
  - En mode économie d'énergie, dans les trames de contrôle, indique l'ID de la station en association.
- Les champs **Adresse 1, 2, 3 et 4** :
  - **Adresse 1**: Adresse du récepteur. Si To DS est à 1 c'est l'adresse de l'AP, sinon, c'est celle de la station.
  - **Adresse 2**: Adresse de l'émetteur. Si From DS est à 1 c'est l'adresse de l'AP, sinon, c'est celle de la station.
  - **Adresse 3**: Adresse de l'émetteur original, quand le champ From DS est à 1, sinon, si To DS est à 1 c'est l'adresse destination.
  - **Adresse 4**: Est utilisé dans le cas où une trame est transmise entre deux points d'accès (le système de distribution DS est utilisé), alors To Ds et From DS =1 et il faut renseigner à la fois l'émetteur original et le destinataire.

8/ Les trames Wi-Fi (17)

Format

Au niveau MAC

- Le champ Contrôle de séquence (2 octets) est composé en 2 sous-champs :

- Le numéro de séquence (12 bits) : numéro assigné à chaque trame afin d'éliminer les trames dupliquées.

- Le numéro de fragment (4 bits) : numéro assigné à chaque fragment, si la trame est fragmentée.

- Corps de la trame (données) (0-2312 octets) : La taille peut être supérieure à 1500 octets à cause du chiffrement WEP. Il n'y a pas de données pour les trames de contrôle et de gestion.

- FCS (Frame Check Sequence) (4 octets) : CRC de 32 bits, pour le contrôle d'intégrité de la trame.

8/ Les trames Wi-Fi (18)

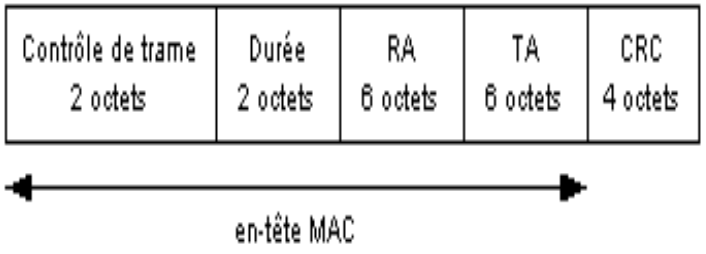
Format (**Au niveau MAC)**

Les trames de contrôle

- Les trames de contrôle permettent l'accès au support et ont pour fonction d'envoyer les commandes et informations de supervision aux éléments du réseau. Dans la partie contrôle de trame, les champs de "To DS" à "order" sont à 0.

- Trames principales :

➢ **RTS (Request to send)** est utilisé pour réclamer le droit de transmettre une trame de données.



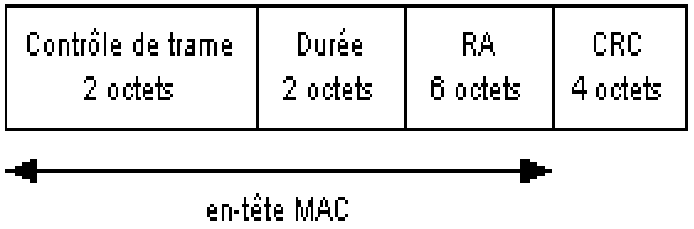
- **RA** est l'adresse du récepteur de la prochaine trame de données.
- **TA** est l'adresse de la station qui transmet la trame RTS.
- **Durée** est le temps de transmission de la prochaine trame, +CTS, + ACK, +3SIFS.

8/ Les trames Wi-Fi (19)

Format (**Au niveau MAC)**

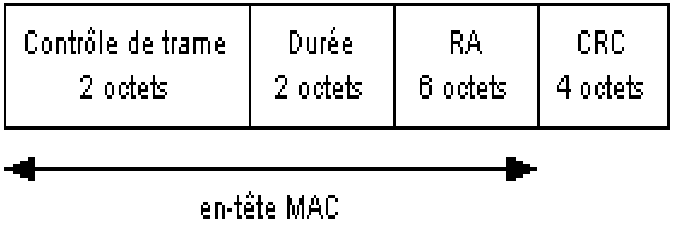
Les trames de contrôle

- **CTS (Clear to send)** correspond à la réservation du canal pour émettre une trame de données.



  - **RA** est l'adresse du récepteur de la trame CTS, copiée du champ TA de RTS.
  - **Durée** est la valeur obtenue dans RTS, moins le temps de transmission de CTS et d'un SIFS.

- **ACK** permet l'acquittement des trames de données.



  - **RA** est l'adresse de la trame précédant cette trame ACK.
  - **Durée** est à 0 si le bit MoreFragment était à 0 dans le champ contrôle de la trame précédente, sinon, c'est la valeur précédente moins le temps de transmission de ACK et d'un SIFS.

8/ Les trames Wi-Fi (20)

Format

Au niveau physique

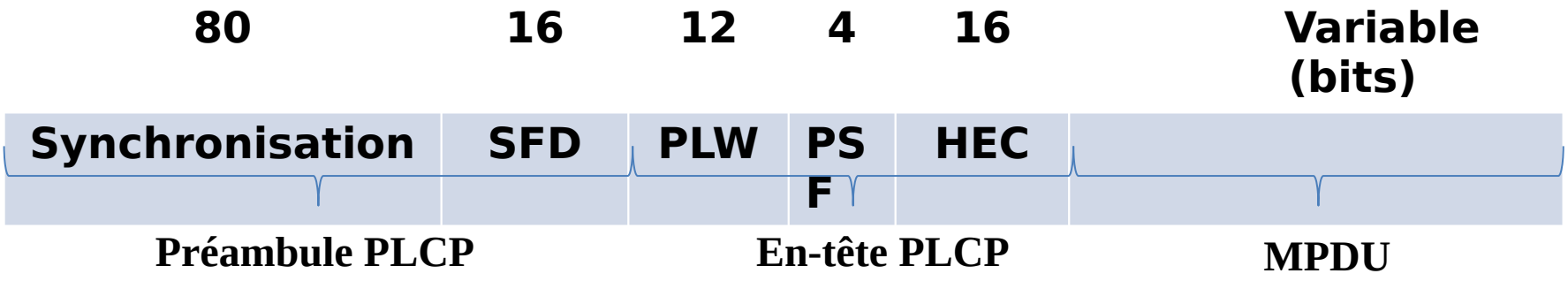
- Les paquets de données, provenant de la couche réseau, sont encapsulés au niveau 2 par un en-tête MAC, formant une MPDU (Mac Protocol Data Unit).
- Cette MPDU est ensuite encapsulée dans une seconde trame au niveau 1 (physique) pour permettre la transmission sur le média.
- Cette encapsulation consiste à rajouter un préambule et un en-tête à la MPDU, cet ensemble forme une PLCP-PDU.
- Le préambule permet la détection du début de trame, la prise du canal pour l'émission, la synchronisation, etc.
- L'en-tête contient diverses informations comme le débit, variable suivant l'interface physique utilisée.
- Le préambule et l'en-tête varient en fonction de la couche physique utilisée: FHSS, DSSS, OFDM.

8/ Les trames Wi-Fi (21)

Format

Au niveau physique

Trame FHSS



- **Préambule PLCP**: est composé de 2 champs:

1. **Synchronisation**: une séquence de 80 bits (alternance de 0 et de 1), permettant de sélectionner et de synchroniser avec un AP ou une station.
2. **SFD (Start Frame Délimiter)**: une suite de 16 bits (0000 1100 1011 1101) définissant le début de la trame.

8/ Les trames Wi-Fi (22)

Format

Au niveau physique

Trame FHSS

- **En-tête PLCP**: est composé de 3 champs:

1. **PLW (PLCP-PDU Length Word)**: une séquence de 12 bits, définissant la longueur (en nombre d'octets) de la trame. Cela permet à la couche physique de déterminer la fin de la trame.
2. **PSF (PLCP Signaling Field)**: est défini sur 4 bits, il indique le débit utilisé sur l'interface radio (1 ou 2 Mbits/s pour la transmission des données MPDU).
3. **HEC (Header Error Check)**: est un CRC représenté sur 16 bits, permettant de détecter les erreurs des champs de l'en-tête (PLW et PSF).

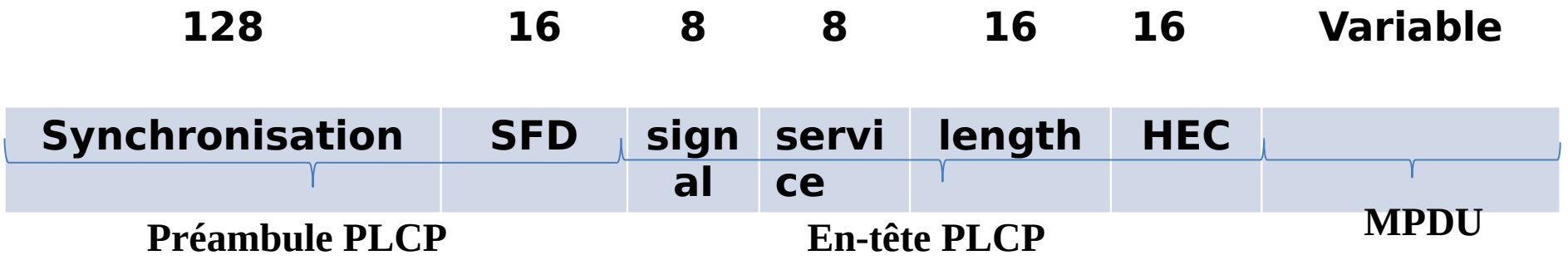
- **Remarque**: Le préambule et l'en-tête sont toujours transmis à 1 Mbits/s.

8/ Les trames Wi-Fi (23)

Format

Au niveau physique

Trame DSSS



- **Préambule PLCP**: identique à la trame FHSS, si ce n'est une longueur de synchronisation plus longue, et une suite de 16 bits différents (1111 0011 1010 0000) pour le SFD.

8/ Les trames Wi-Fi (24)

Format

Au niveau physique

Trame DSSS

- **En-tête PLCP**: est composé de 4 champs:

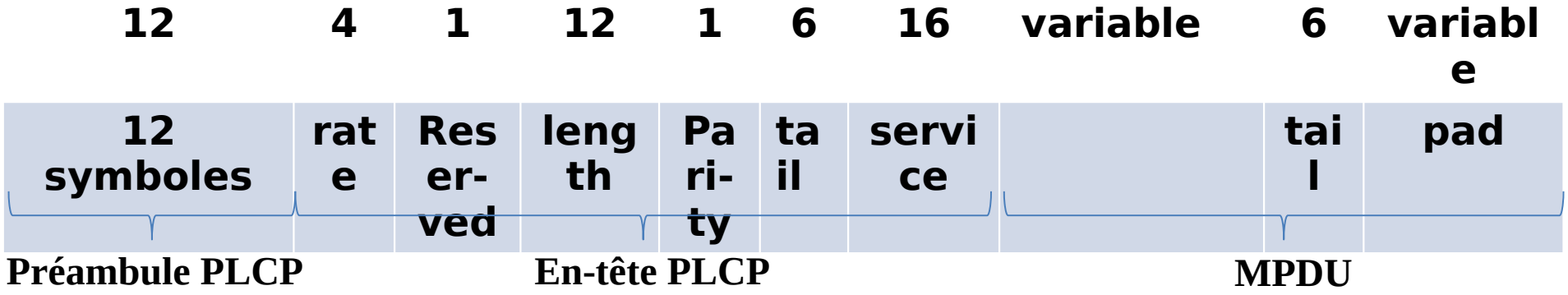
1. **signal**: une séquence de 8 bits, définissant le débit utilisé pour la transmission des données (MPDU).
2. **service**: une suite de 8 bits réservée pour un usage futur, ne contient que des 0.
3. **length**: est défini sur 16 bits, permettant d'indiquer la longueur (en nombre d'octets) de la trame à suivre. Cela permet à la couche physique de déterminer la fin de la trame.
4. **HEC (Header Error Check)**: est un CRC représenté sur 16 bits, permettant de détecter les erreurs des champs de l'en-tête (signal, service et length).

8/ Les trames Wi-Fi (25)

Format

Au niveau physique

Trame OFDM



- **Préambule PLCP**: différent par rapport au format des trames précédentes. Le préambule d'une trame OFDM est réalisé grâce à une séquence de douze symboles permettant la détection du signal par le récepteur et le début de la trame.

8/ Les trames Wi-Fi (26)

Format

Au niveau physique

Trame OFDM

•**En-tête PLCP**: est composé de 6 champs:

1rate: une séquence de 4 bits, définissant le débit de transmission.

2reserved: un bit réservé, toujours à 0.

3length: permet d'indiquer la longueur (en nombre d'octets) dans la trame.

4parity: un bit de parité des trois champs précédents pour la détection d'erreur.

5tail : un champ réservé pour un usage futur, ne contient que des 0.

6service: réservé pour un usage futur, ne contient que des 0.

•**MPDU**: on trouve les champs suivants:

1tail : un champ réservé pour un usage futur, ne contient que des 0.

2pad: un champ de padding (remplissage) de 6 bits minimum, permettant une structure se comptant en octets.

9/ Mécanismes de sécurité (1)

- Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples, parmi lesquels, nous pouvons citer :

➢ L'interception de données en écoutant les transmissions des différents utilisateurs du réseau sans fil.

➢ Le détournement de connexion dont le but est d'obtenir l'accès à un réseau local ou à Internet.

➢ Le brouillage des transmissions en envoyant des signaux radio de telle manière à produire des interférences.

➢ Les mêmes risques existent sur un réseau filaire mais il faut pouvoir accéder au matériel réseau (prises, câbles, etc.).

- En résumé les services sécurisés indispensables aux extensions IP sans fil sont les suivants:

➢ Identification et authentification des utilisateurs du réseau.

➢ Signature des trames échangées (**intégrité**, **authentification**).

➢ Chiffrement des données (**confidentialité**).

9/ Mécanismes de sécurité (2)

- Exemple de règles de protection élémentaires :

- **SSID** : Changement du SSID par défaut et désactivation du broadcast du SSID.
- **Filtrage d'adresses MAC**: N'autoriser que les communications contrôlées par une liste d'adresses MAC, ou ACL (Access Control List).

- Deux modes d'authentification ont été introduit dans la norme 802.11 d'origine :

- **Système ouvert (Open System authentication)**: l'authentification est explicite. Un terminal peut donc s'associer avec n'importe quel point d'accès et écouter toutes les données qui transitent au sein du BSS.
- **Authentification par clé partagée (Shared Key authentication)** : Fournit des mécanismes, tels que WEP, WPA, WPA2 et WPA3 pour

9/ Mécanismes de sécurité (3)
Le chiffrement WEP (Wired Equivalent Privacy)

- Le protocole **WEP** est un protocole chargé du chiffrement des trames 802.11utilisant l'algorithme RC4 (Ron's Cipher 4).
- Cet algorithme permet de générer à partir d'une clé **partagée** et d'un vecteur d'initialisation **IV (Initialization Vector)** une séquence pseudo-aléatoire (d'une longueur égale à la longueur de la trame), cette séquence est **la clé effective** du cryptage.
- L'opération de cryptage est effectuée par un ou-exclusif (XOR) du texte en clair couplé à son CRC et de la clé effective du cryptage.
- Les clés utilisées dans ce protocole sont d'une longueur de 64 bits ou 128 bits (des implémentations récentes vont même jusqu'à pousser cette longueur à 232 bits). Les 24 bits de la clé servent pour le Vecteur d'Initialisation, ce qui signifie que seul 40 bits ou 104 bits sont réservés pour la clé.

9/ Mécanismes de sécurité (4)

Le chiffrement WEP (Wired Equivalent Privacy)

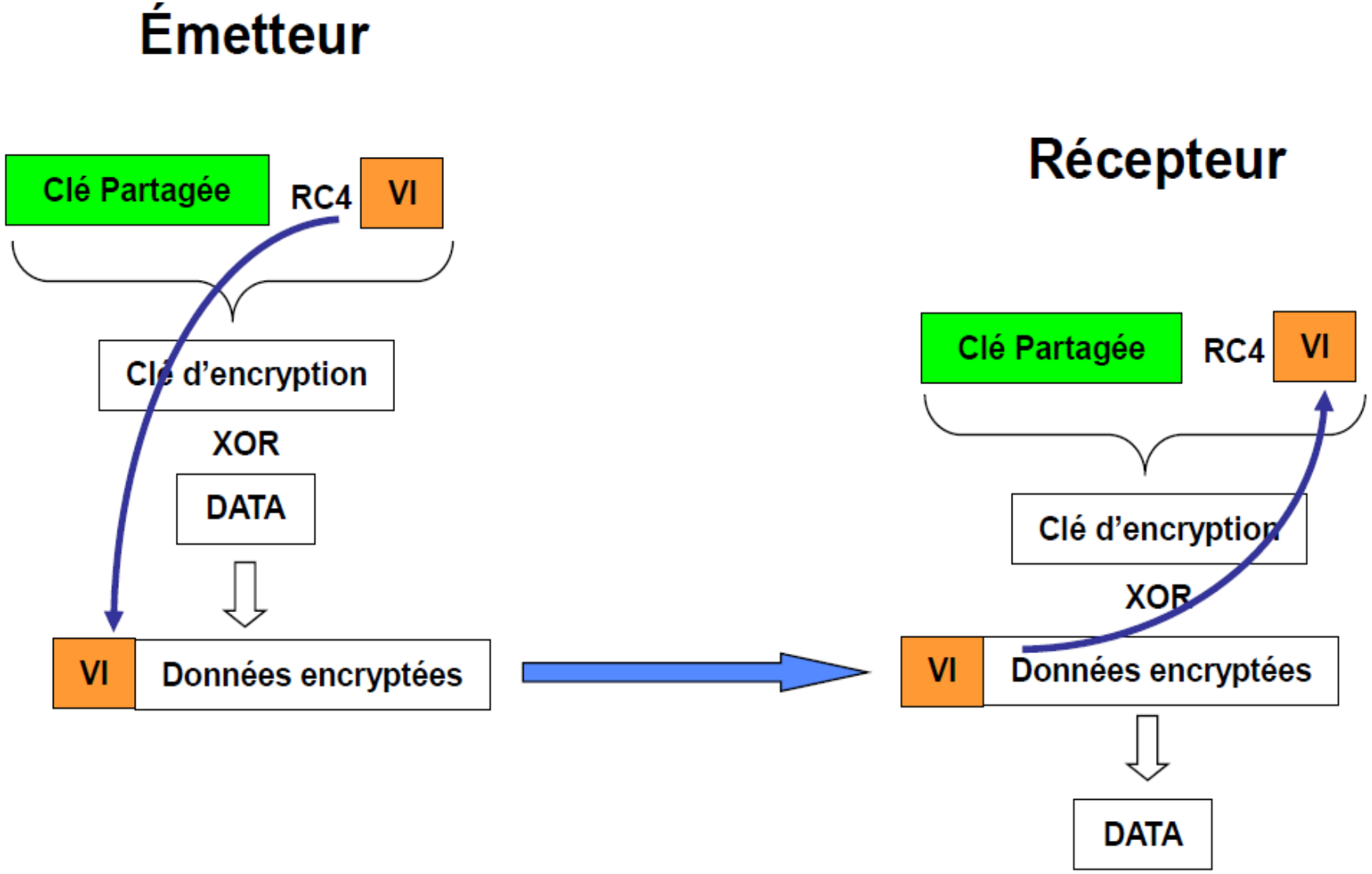
Principe

- Après avoir identifié un AP, l'émetteur (la station) commence par émettre une requête d'authentification (Authentication Request).
- Lorsque le récepteur (le point d'accès ou la station en mode ad hoc) intercepte cette requête, il génère un texte aléatoirement par dérivation de la clé WEP qu'il connaît.
- Ce texte qui est appelé «challenge» est envoyé à l'émetteur qui se charge de le crypter avec sa propre clé WEP. Il renvoie ensuite le challenge crypté au récepteur ainsi qu'un nouveau IV.
- Lorsque le récepteur reçoit le challenge crypté, il le décrypte à l'aide de sa clé WEP et de l'IV reçu et compare le résultat obtenu au challenge d'origine. Si la comparaison aboutit à une similarité totale, l'émetteur est authentifié, sinon il ne l'est pas.
- Problème: la clé ne change jamais lors de l'échange des paquets.

9/ Mécanismes de sécurité (5)

Le chiffrement WEP (Wired Equivalent Privacy)

Principe



9/ Mécanismes de sécurité (6)

Le chiffrement WPA (Wireless Protected Access)

- Dans le protocole WPA, les données sont toujours codées avec un algorithme de chiffrement par flot RC4 mais les vecteurs d'initialisation comportent désormais 48 bits et la clé primaire 128 bits.
- Le protocole WPA ajoute également un mécanisme de changement dynamique des clés de chiffrement appelé TKIP (Temporal Key Integrity Protocol). A l'aide de ce mécanisme, les clés de chiffrement sont donc périodiquement renouvelées lors des communications.
- Au niveau de l'authentification des utilisateurs, le protocole WPA utilise désormais un serveur d'authentification 802.1X et s'appuie sur la famille des protocoles EAP (Extensible Authentification Protocol) qui supporte de nombreux mécanismes d'authentification.
- A l'aide de ces différents mécanismes, le protocole WPA rend l'intrusion dans un réseau 802.11 beaucoup plus difficile mais pas impossible. C'est pourquoi le protocole WPA2 a été proposé.

9/ Mécanismes de sécurité (7)
Le chiffrement WPA 2

- Le protocole WPA2 est la version certifiée par la Wi-Fi Alliance de la norme 802.11i.
- Il supporte les différents mécanismes obligatoires de la norme, ce qui ne le rend pas forcément compatible avec certains anciens équipements sans fil.
- Il reprend les différents éléments du protocole WPA mais propose l'utilisation d'un nouvel algorithme de chiffrement appelé CCMP (Counter-Mode / CBC-Mac Protocol) qui est basé sur un chiffrement par bloc AES (Advanced Encryption System).
- Dans un chiffrement par bloc, les données sont découpées en blocs de taille généralement fixe, qui sont ensuite chiffrés les uns après les autres.
- L'algorithme CCMP utilise des clés et des blocs de 128 bits pour chiffrer les données.

9/ Mécanismes de sécurité (8)
Le chiffrement WPA 3

- Au cours des années 2017 et 2018, des attaques critiques de WPA2 (attaques KRACK) ont été publiées.
- Ce fait a déclenché l'annonce par la Wi-Fi Alliance de la spécification du protocole WPA3 (WPA3-v2.0 publié le 20/12/2019).
- Le protocole WPA3 a deux objectifs principaux.

➢ Le premier objectif est de certifier dans les produits Wi-Fi l'application correcte des contre-mesures proposées contre les attaques dites KRACK.

➢ Le deuxième objectif est de mettre à jour les mécanismes existants pour augmenter le niveau de sécurité.