

Cours 2 : réseaux sans fil

Plan

- Généralités
 - Wireless networks
 - Wireless LAN, normes 802.11
 - Architecture
 - Mode infrastructure (SSID)
 - Mode ad-hoc
 - Modèle OSI
 - Couche physique
 - Couche liaison
 - Sécurité
 - Conclusion
-



A dark blue vertical bar is positioned on the left side of the slide, spanning the height of the main content area.

Généralités

Réseaux sans fil (Wireless Networking)

► Définition

- Un réseau sans fil est un réseau de machines qui n'utilisent pas de cables. C'est une technique qui permet aux particuliers, aux réseaux de télécommunications et aux entreprises de limiter l'utilisation de cables entre diverses localisations.

► Applications

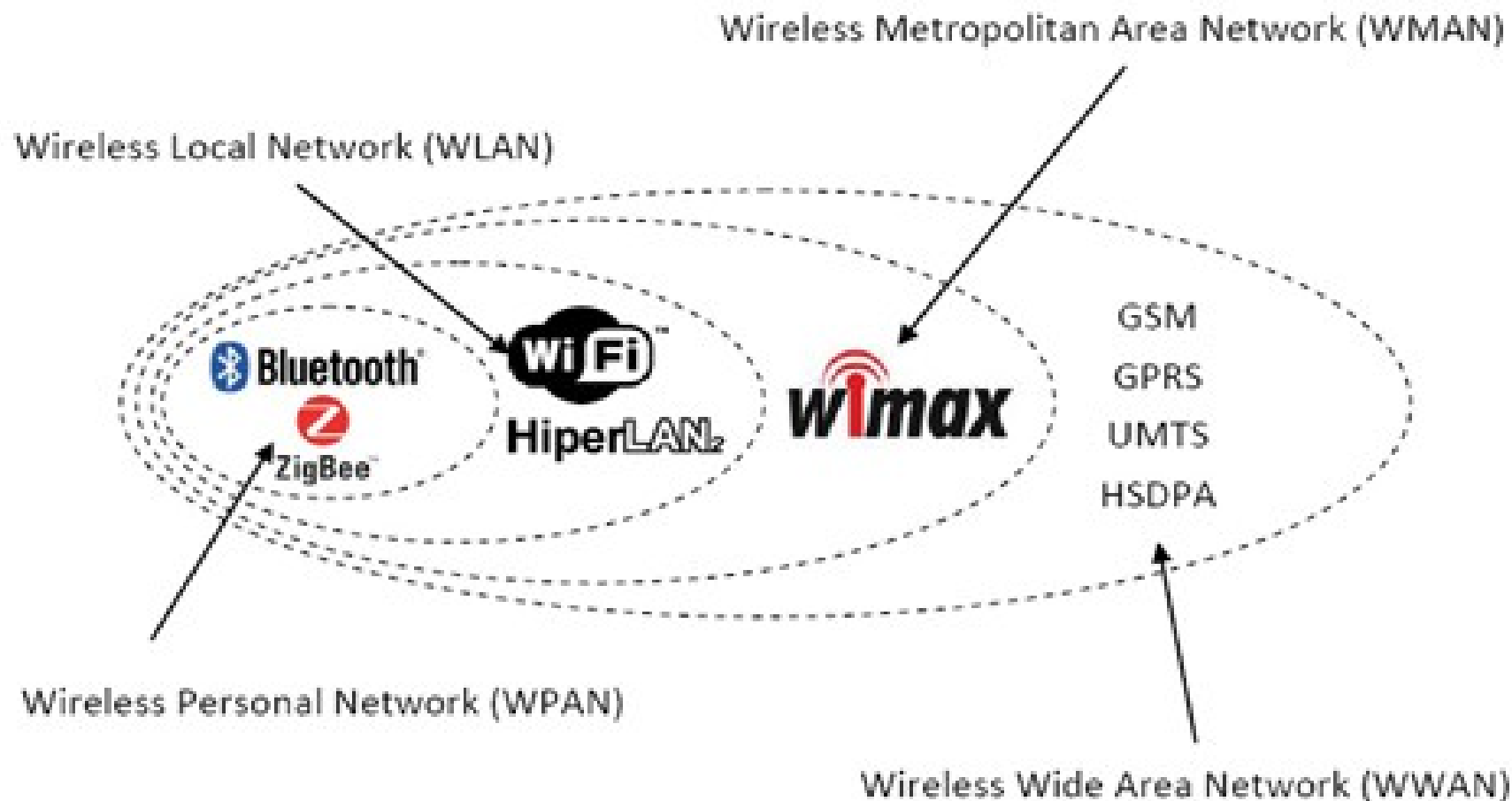
- Nomadisme (accéder à internet via un ordinateur portable, en mobilité)

► Classification

- Chaque solution correspond à un usage différent, en fonction de ses caractéristiques (vitesse de transmission, débit maximum, coût de l'infrastructure, coût de l'équipement connecté, sécurité, souplesse d'installation et d'usage, consommation électrique et autonomie...).



Classification des réseaux sans fil



WPAN

► Définition

- ▶ Réseau individuel sans fil (Wireless Personal Area Network)
- ▶ Faible portée (qqs dizaines de m)
- ▶ Permet la connexion de périphériques (pda, imprimante,), d'ordinateurs

► Bluetooth

- ▶ Technologie principale WPAN
- ▶ Lancée par Ericson en 1994
- ▶ Débit de 1Mbps pour 30m
- ▶ Très peu gourmand en énergie
- ▶ Norme 802.15.1



► HomeRF

- ▶ Home Radio Frequency group (1998).
- ▶ Débit 10Mbps pour 50 à 100m
- ▶ Abandonnée en 2003 au profit du WiFi



WLAN

► Définition

- Réseau local d'entreprise (Wireless Local Area Network)
- Couvre l'équivalent d'un réseau local d'entreprise (100 m)
- Relie entre eux les équipements présents dans la zone de couverture

► WiFi

- Wireless Fidelity
- Soutenu par l'alliance WECA
- Débit jusqu'à 54 Mbps,
- Portée de plusieurs centaines de m



► Hiperlan2

- High Performance Radio LAN 2.0
- Norme européenne
- Fréquence de 5150MHz à 5300Mhz
- Débit jusqu'à 54 Mbps,
- Portée de plusieurs centaines de m



WMAN

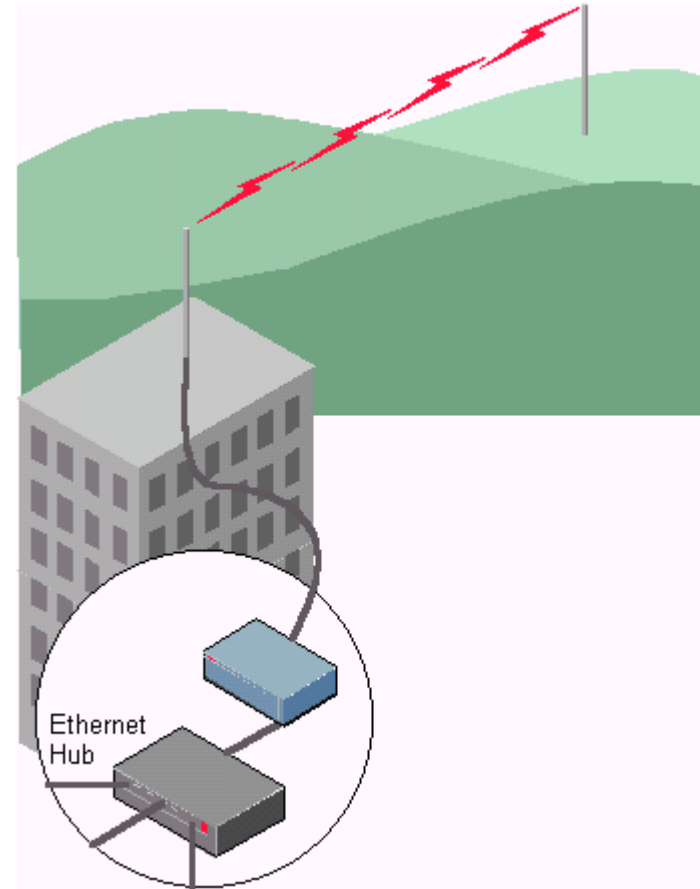
► Définition

- Réseau métropolitain (Wireless Metropolitan Area Network)
- Plus connu sous le nom de Boucle Local Radio (BLR)
- Permet à un particulier ou une entreprise d'être relié à son opérateur (téléphonie fixe, Internet, télévision...) via les ondes radio.
- Basé sur la norme 802.16

► Technologies

- Local Multipoint Distribution Service (LMDS)
- Multichannel Multipoint Distribution Service (MMDS)
- Worldwide Interoperability for Microwave Access (WiMAX)

From Computer Desktop Encyclopedia
© 2000 The Computer Language Co. Inc.



Pb du dernier km

WWAN

► Définition

- Réseau étendu sans fil (Wireless Wide Area Network)
- Plus connu sous le nom de « réseaux cellulaires mobile »
- Utilisé par les téléphones mobiles (cf cours I)

► Technologies

- GSM : Global System for Mobile communication
- GPRS : General Packet Radio Service
- UMTS : Universal Mobile Telecommunication System



Classification des réseaux sans fil

Cat.	Portée max	Débit	Usages	Normes
WPAN	Qqs m	1 Mbit/s	Réseau particulier	IEEE 802.15 (Bluetooth), NFC, ETSI HyperPan
WLAN	500 m	+ de 50 Mbit/s	Réseaux internes, propres à un bâtiment (soit comme réseau d'entreprise, soit comme réseau domestique).	IEEE 802.11 (a,b,c,...) ETSI HyperLan
WMAN	4 à 10 kilomètres	de 1 à 10 Mbit/s	Ville, Campus, ... Interconnecte plusieurs WLAN	IEEE 802.16 WiMax ETSI HyperMan
WWAN	Plusieurs centaines de kms	de 1 à 10 Mbit/s	Régional, National Interconnecte plusieurs villes	Basé sur des technologies cellulaires





WLAN ou Wi-Fi

Wireless LAN (WLAN)

► Définition

- Un réseau d'ordinateurs et de matériels sans fil qui offre les fonctionnalités des réseaux locaux LAN traditionnels (Ethernet), mais en utilisant une technologie sans fil.

► Dans la pratique

- Un WLAN permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA) ou même des périphériques à une liaison haut débit (de 11 Mbit/s en 802.11b à 54 Mbit/s en 802.11a/g) sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres) et de centaines de mètres en extérieur (500m)



Wireless LAN (WLAN) ou WiFi

► Normes IEEE 802.11 (WiFi)

- IEEE = Institute of Electrical and Electronics Engineers
- La norme initiale 802.11 a connu de nombreuses révisions notées 802.11a, 802.11b, 802.11g pour les principales.
- Ces révisions visent essentiellement une amélioration du débit et/ou une amélioration de la sécurité.

► Wi-Fi (Wireless Fidelity)

- Un « label » commercial décerné par un groupement de constructeurs (« Wireless Ethernet Compatibility Alliance », WECA) depuis 1999, renommé « Wi-Fi Alliance » en 2003.
- Valide le respect du standard et l'inter-opérabilité entre matériels
- Souvent en avance sur la normalisation IEEE



► Dans la pratique, les 2 sont confondus



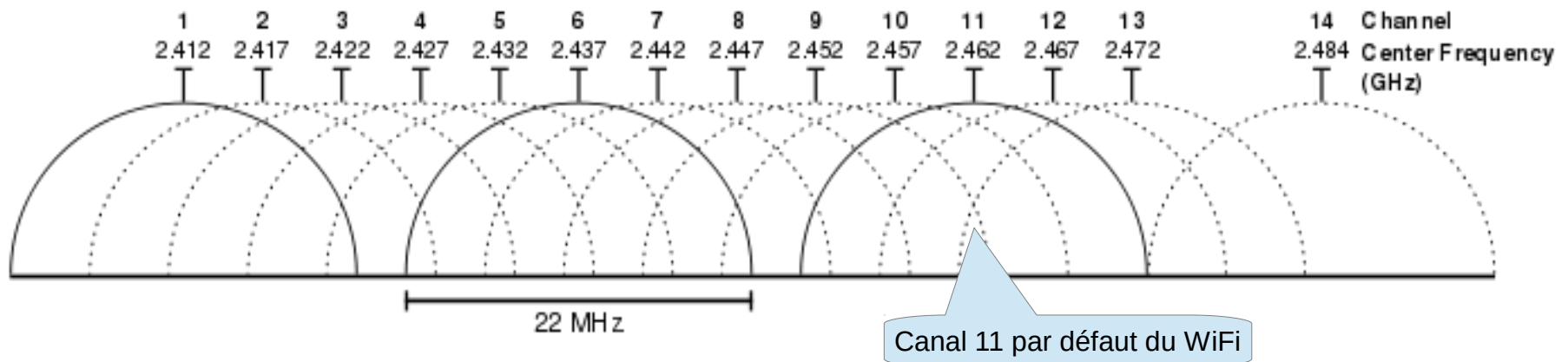
Supports de transmission du WiFi

► Infra-rouge

- Signal facilement bloqué, nécessite un espace dégagé, de faible portée, débit de seulement 4 Mbps
- Adapté aux transmissions de données entre ordinateurs et imprimante

► Fréquences radio

- Passe à travers la plupart des obstacles dans un bureau
- Bande des 2.4Gz organisée en 14 canaux de 22Mhz de large



Les normes WiFi

Normes	Débit max	Fréquence	Date	Description
802.11	1 à 2 Mb/s	2,4 Ghz	1997	Première norme WiFi
802.11a	54 Mb/s	5 GHz	1999	- haut-débit sur 8 canaux - de 50Mbs jusqu'à 10m à 6Mbps jusqu'à 70m
802.11b	11 Mb/s	2,4 GHz	1999	- fixe un débit moyen maximum à 11 Mb/s théorique - portée de 50m en intérieur à 300 mètres en extérieur - spécifie 3 canaux radio (1, 6 et 11)
802.11g	54 Mb/s	2,4 GHz	2001	- fixe un débit moyen maximum à 54 Mbits/s théorique une - portée de 25m en intérieur à 75 mètres en extérieur - spécifie 3 canaux radio (1, 6 et 11)
802.11i			2004	- améliore la sécurité (authentification, cryptage et distribution des clés) en s'appuyant sur la norme Advanced Encryption Standard.
802.11n	270 Mb/s	2,4 GHz ou 5 GHz	2009	- regroupement des canaux - agrégation des paquets de données
802.11s	1 G/s	5 GHz	2012	- en cours de normalisation - améliore 802.11n



Débits et distance

- ▶ Technologie dépendant de l'environnement
 - ▶ Type de construction (cloisons, murs, matériaux)
 - ▶ Implantation des antennes
 - ▶ Interférences (bluetooth, micro-ondes, autres réseau wifi)
- ▶ Comparaison des débits en fonction de la distance

Norme	débit théorique	portée en intérieur	usage
802.11a	54 Mbit/s	25 mètres	Accès au haut débit mais à courte portée.
802.11b	11 Mbit/s	35 mètres	Norme assez courante, utile pour le surf sur Internet. A éviter pour le streaming de vidéos ou le jeu en ligne.
802.11g	54 Mbit/s	25 mètres	Norme la plus répandue. Permet de jouer et de regarder des vidéos sur le Net avec un certain confort. Le transfert de fichiers volumineux reste long.
802.11n	540 Mbit/s	50 mètres	La norme à venir. Le très haut débit sans fil.

Organismes de contrôle français

► **ART** (Autorité de Régulation des Telecommunications)

- En France, mise en place le 5 janvier 1997.
- La création d'une autorité administrative indépendante pour réguler la concurrence dans le secteur des télécommunications est la conséquence de l'ouverture à la concurrence de ce secteur, auparavant en situation de monopole légal, en dehors du secteur de la téléphonie mobile.
- Devient **l'ARCEP** (Autorité de Régulation des Communications Electroniques et des Postes) en 2005

► Réglementation

- Depuis 2007, l'opérateur qui souhaite déployer un réseau wifi public doit se déclarer auprès de l'ARCEP
- Sauf les réseaux Wifi réservés à un usage privé, les réseaux internes ouverts au public (ex : cybercafés).



Architecture

- Mode infrastructure (SSID)
- Mode ad-hoc

Composants

► Points d'accès

- Routeurs WiFi et ponts Ethernet/802.11
- Prise en charge de la norme 802.11 avec un aspect sécuritaire (authentification et cryptage)
- Logiciel de configuration (ex : serveur web intégré)
- Serveur DHCP



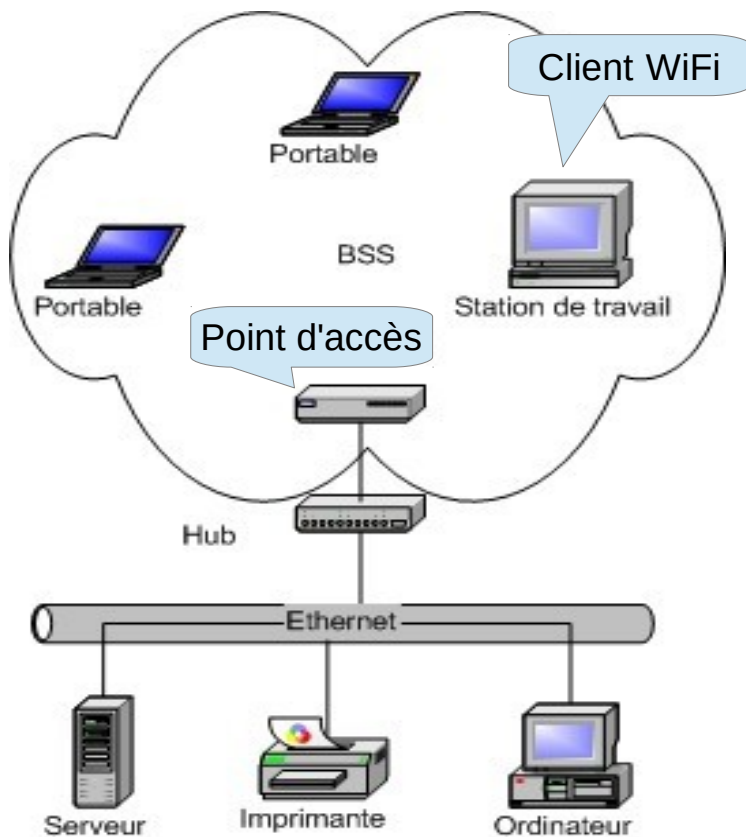
► Interface client

- WNIC (Wireless Controller) à insérer dans un slot PCI de la carte mère
- Adaptateurs Wifi USB
 - Plus facile à installer
 - Plus petite antenne que les WNIC donc moins fiable



Architecture Wifi Infrastructure

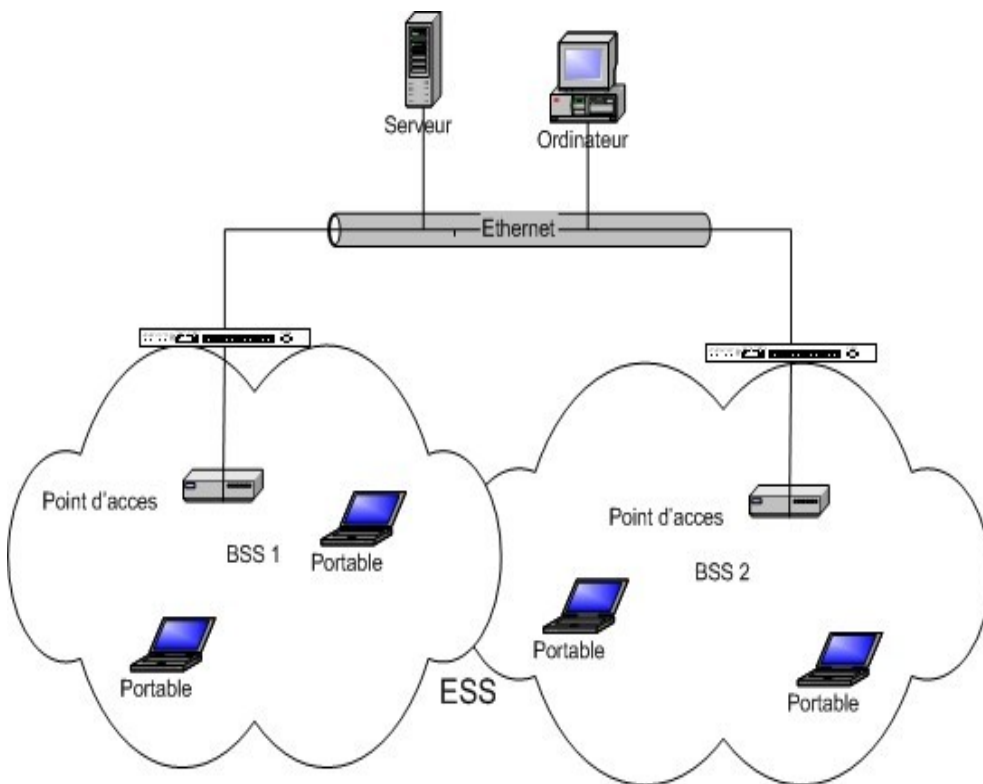
Réseau local sans fil relié au point d'accès



- ▶ Client WiFi
 - ▶ Possède un matériel avec une interface sans fil
- ▶ Point d'accès WiFi (AP)
 - ▶ Gère les liaisons sans fil suivant la norme WiFi
 - ▶ Le plus souvent connecté à Internet via un réseau filaire
- ▶ BSS (Basic Service Set)
 - ▶ L'ensemble des stations radio à portée d'un point d'accès.
 - ▶ Chaque BSS a un identifiant (BSSID), qui est l'adresse MAC du point d'accès.

Réseau local filaire relié à Internet

Architecture Wifi Architecture



- ▶ **ESS (Extended Service Set)**
 - ▶ Interconnecte plusieurs BSS
 - ▶ Identifié par un nom ESSID de 32 carac. max, appelé simplement SSID (ex : livebox-l2d3, eduroam, wifi-guest,...)
 - ▶ Il est configuré manuellement sur les stations clients ou automatiquement par détection grâce à sa diffusion via le point d'accès.
- ▶ **Itinérance (roaming)**
 - ▶ Un utilisateur nomade passe de façon transparente d'un BSS à l'autre.
 - ▶ (voir plus loin)

Connexion en mode infrastructure

► Authentification

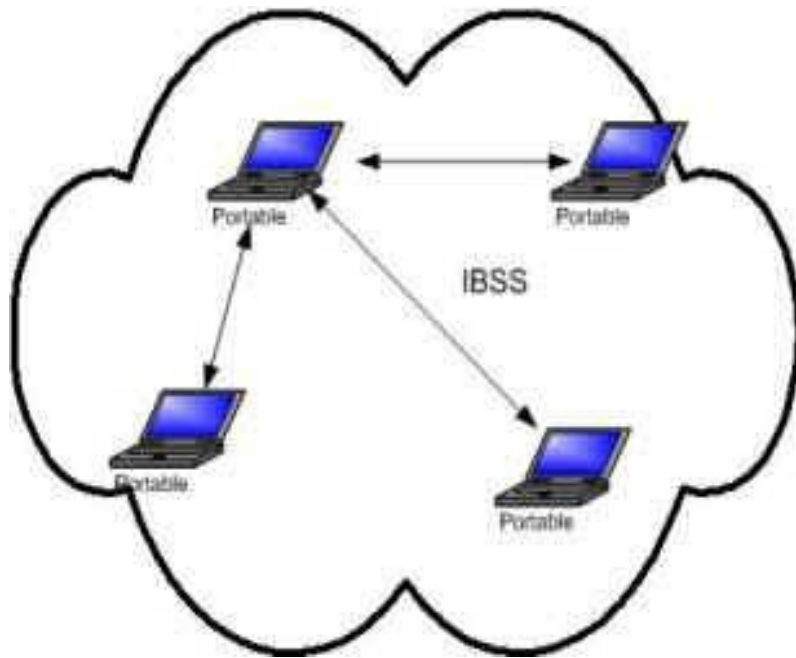
- La station désirant entrer sur le réseau Wi-Fi doit s'authentifier sur l'AP. Si le réseau est ouvert, cette phase est obligatoirement un succès.
- Les mécanismes actuels demandent un mot de passe, voire différents challenges pour s'authentifier sur
- un AP. (cf WEP, le WPA et le WPA2)

► Association

- Une fois authentifiée, une station est associée et peut commencer à émettre des trames sur le réseau.
- Toutes les trames contiennent le SSID de l'ESS : deux réseaux différents peuvent partager la même fréquence, s'ils n'ont pas le même SSID
- L'AP relaiera ces informations aux destinataires concernés



Architecture Wifi Ad-hoc



- ▶ Représente un groupe de PC (jusqu'à 5) 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 distribué.
- ▶ La norme désigne l'ensemble des stations à portée radio mutuelle par l'appellation IBSS (Independent Basic Service Set) .



Roaming

Roaming

► Définition

- ▶ Le roaming, ou handover, ou encore appelé l'itinérance en wifi représente l'action qui consiste pour une station à changer de point d'accès (AP) sans perdre sa connectivité réseau.
- ▶ Mécanisme de niveau 2 (et 3) : cf modèle OSI
- ▶ Protocole 802.11.f en 2003

► Applications

- ▶ Beaucoup d'apps peuvent supporter de perdre/récupérer la connexion Internet mais certaines doivent la conserver
- ▶ Exemples :VoIP, streaming, ...

► Classification

- ▶ Roaming intra-ESS (*Internal Roaming*) : le mobile passe d'un AP à un autre AP au sein du même réseau sans fil
- ▶ Roaming inter-ESS (*External Roaming*) : le mobile se déplace dans le Wlan d'un autre fournisseur de service internet sans fil ou Wireless Internet Service Provider (WISP)



Roaming

▶ Association – désassociation

- ▶ Une station qui souhaite utiliser le réseau doit s'associer avec le point d'accès. Grâce à cette association, la station fait partie du BSS du point d'accès. Elle peut alors, utiliser les services du point d'accès. L'attachement entre la station et le point d'accès est rompu grâce à la désassociation.

▶ Distribution

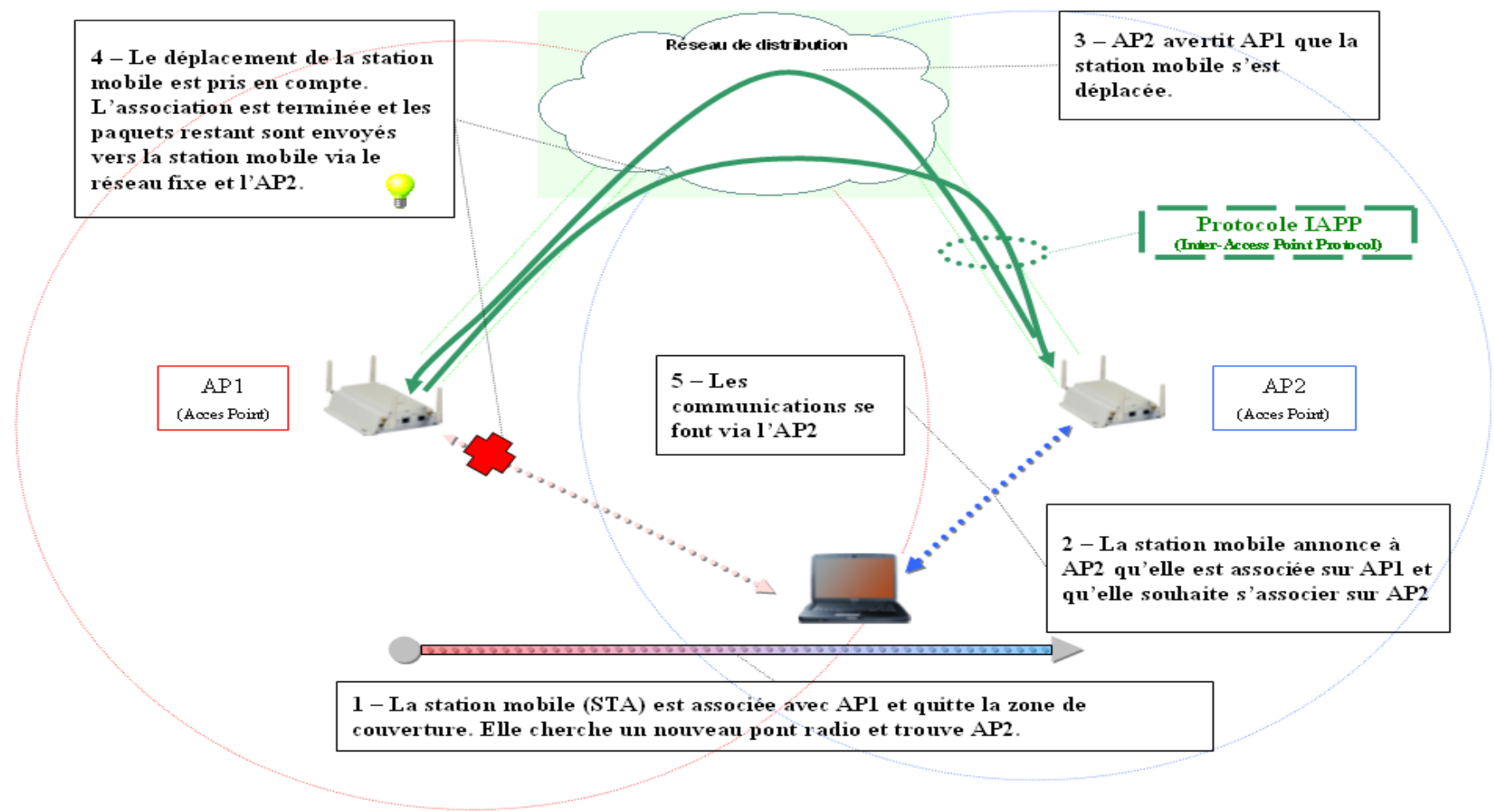
- ▶ C'est ce service qui aiguille les trames. Il permet à une station d'envoyer des trames à travers le système de distribution (DS) d'un BSS ou d'un ESS.

▶ Intégration

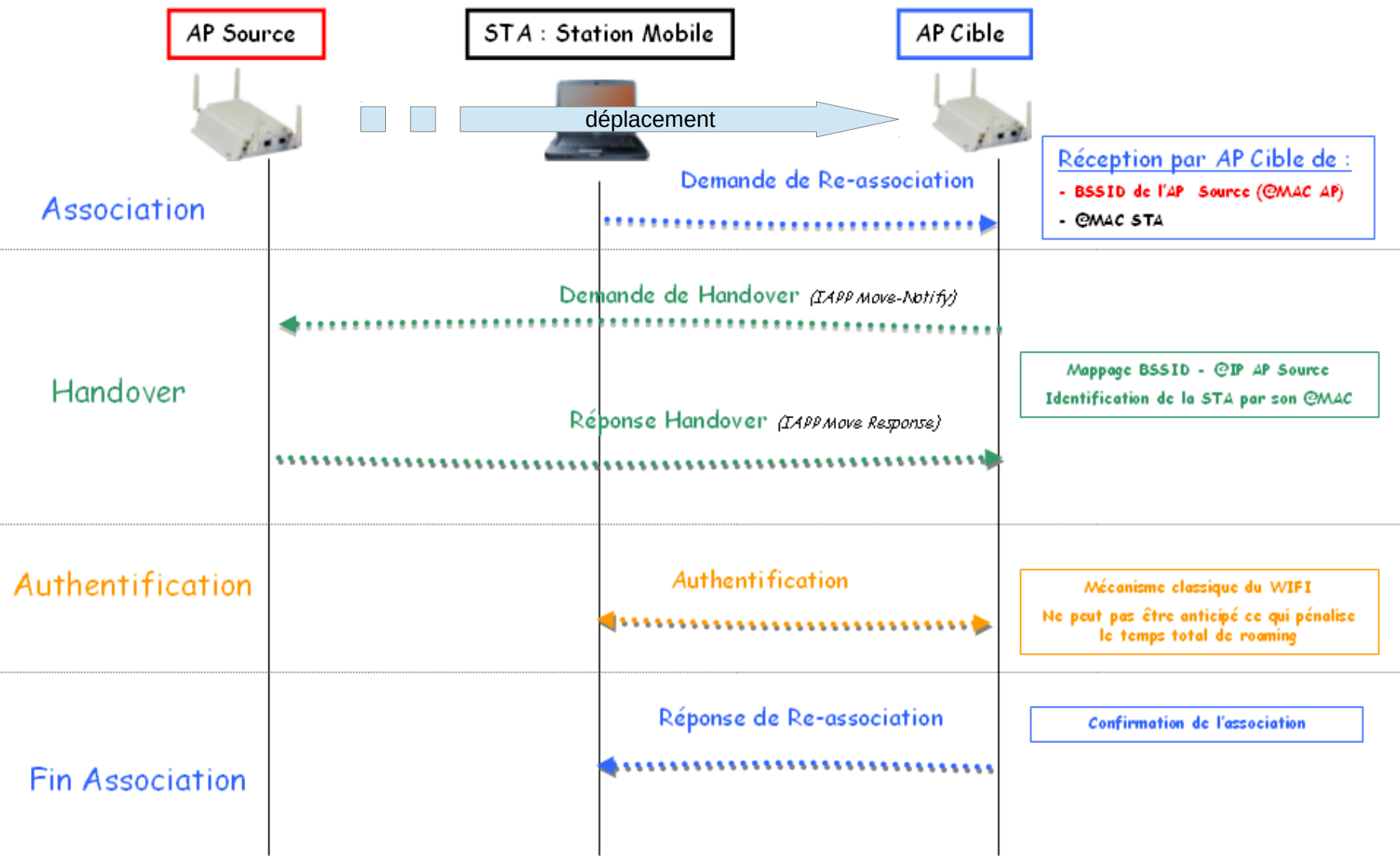
- ▶ Le service d'intégration permet aux différents points d'accès de communiquer par un canal différent de 802.11, le plus souvent il s'agit d'un réseau local.



Internal Roaming



Internal Roaming



Roaming

► Performances

- Le roaming, bien que fonctionnel, est très lent, trop pour la Voix sur IP (VoIP)
- Lenteur due principalement à la lenteur du mécanisme d'authentification
- Les normes additionnelles qui devaient améliorer le roaming n'ont pas été complètement finalisées.
- Désintérêt de la part des acteurs du marché, tant dans le logiciel libre que dans le logiciel propriétaire.
- Echec de la norme 802.11f qui a été retirée en 2006 par l'IEEE

► Evolution du roaming WiFi

- Evolution de la norme 802.11i (authentification par WPA2)
- Solutions propriétaires : obligation de choisir un constructeur pour roamer
- Afin de palier au problème du roaming avec la VoIP, l'IEEE se penche sur l'utilisation du réseau GSM associé au Wifi

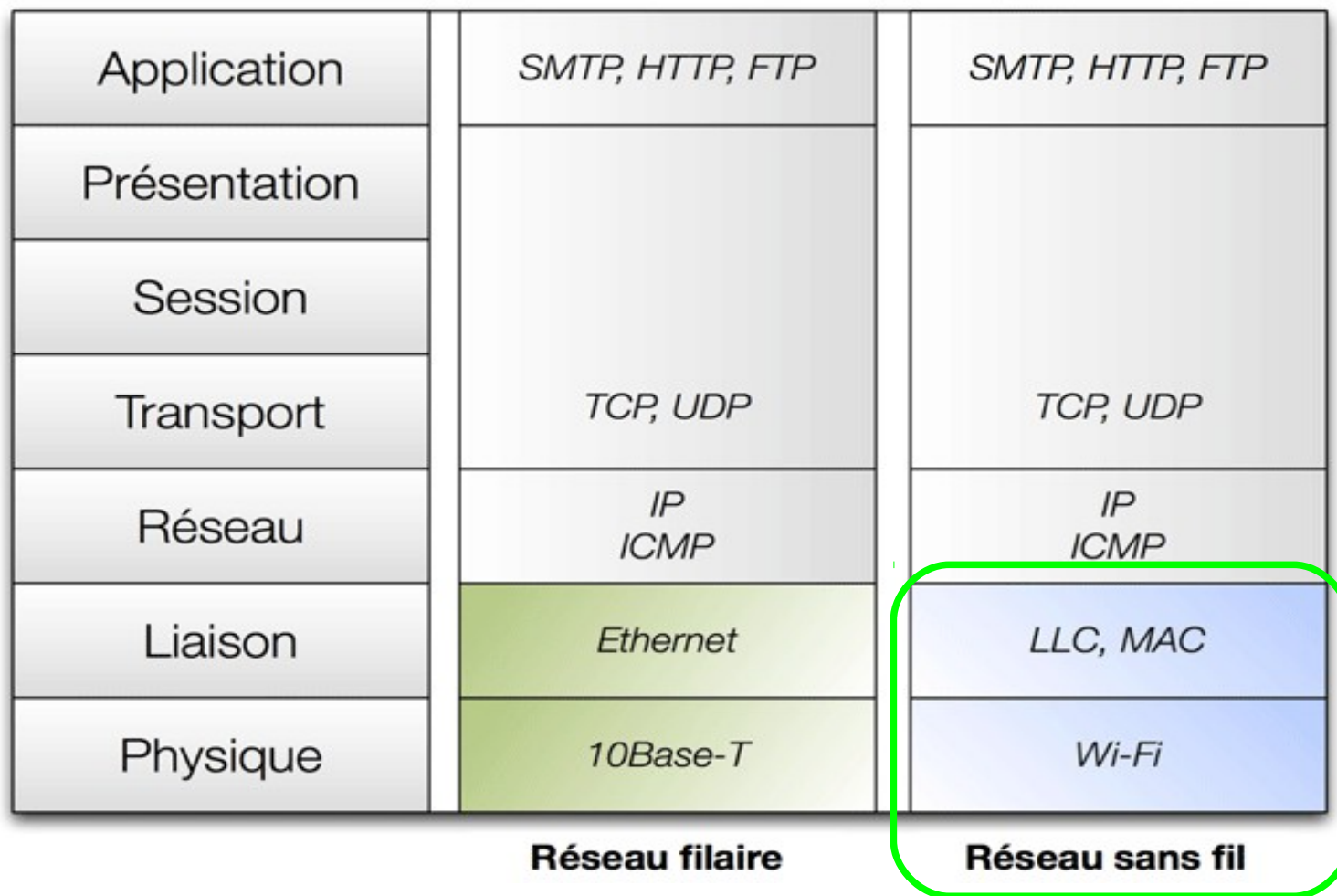




Modèle OSI

Modèle OSI

- Le WiFi concerne les couches 1 et 2 du modèle OSI



Modèle OSI

- Le WiFi concerne les couches 1 et 2 du modèle OSI

Couche

LIAISON

2 sous-couches

- LLC - Logical Link control
- Contrôle d'accès au support
- *Medium Access Control MAC*

Couche

PHYsique

3 couches physiques différentes

- DSSS
- FHSS
- Infra-rouge



Couche physique

► Transmission en bande étroite

- les différentes communications sur des canaux différents.
- La bande de fréquence utilisée doit être aussi petite que possible afin de limiter les interférences sur les bandes adjacentes.

► Problèmes d'interférences

- Partage de la bande passante entre les différentes stations présentes dans une même cellule.
- La propagation par des chemins multiples d'une onde radio.

► Techniques de transmission sans fil

- La technique de l'étalement de spectre à saut de fréquence
- La technique de l'étalement de spectre à séquence directe
- La technologie infrarouge



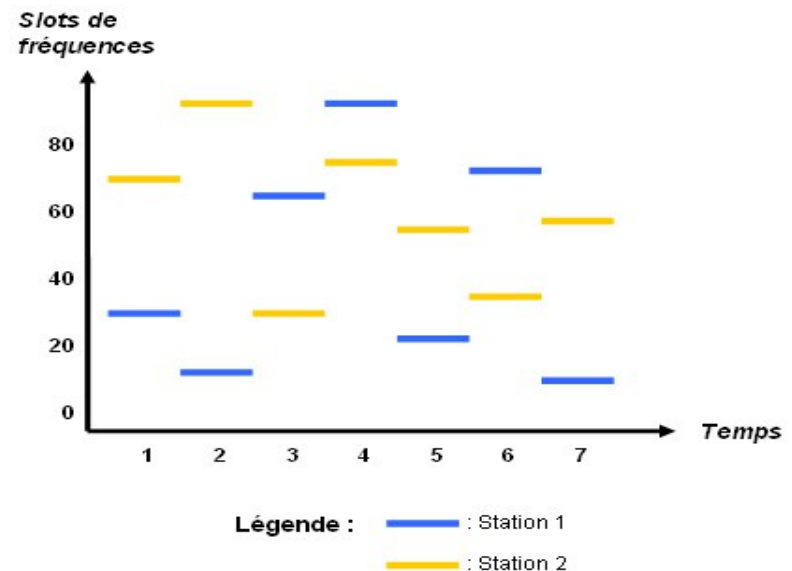
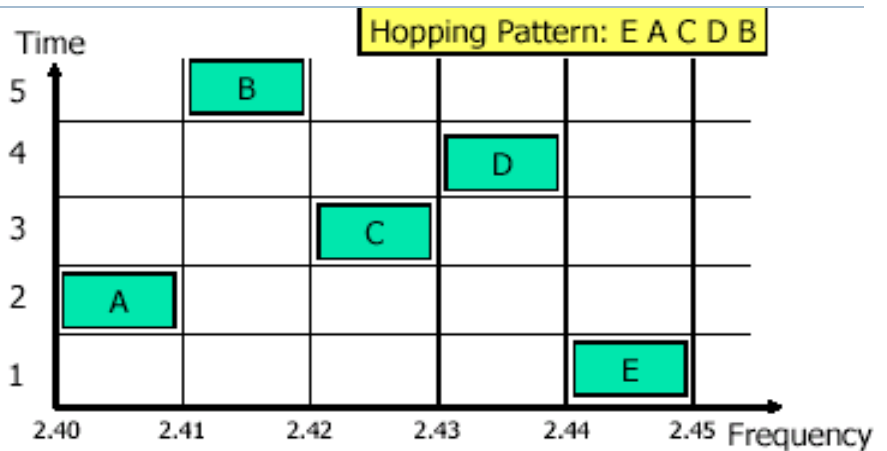
FHSS (Frequency Hopping)

► Bande ISM : 2,4/2,483 GHz

- 79 canaux disjoints de 1 Mhz
- Débit : 1 ou 2 Mb/s
- Données rapides ➡ taux d'erreurs élevé
- Utilise un changement de fréquence synchronisé toute les 0,4 s
- Négociation du schéma de transmission (Hopping Pattern)

► Performances

- Coût bas
- Petite consommation d'énergie
- Bonne tolérance aux bruits
- Débit faible



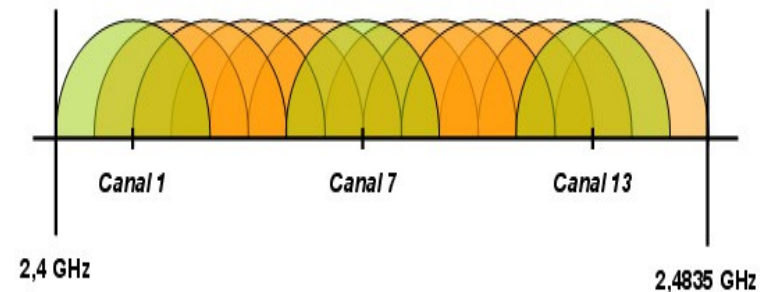
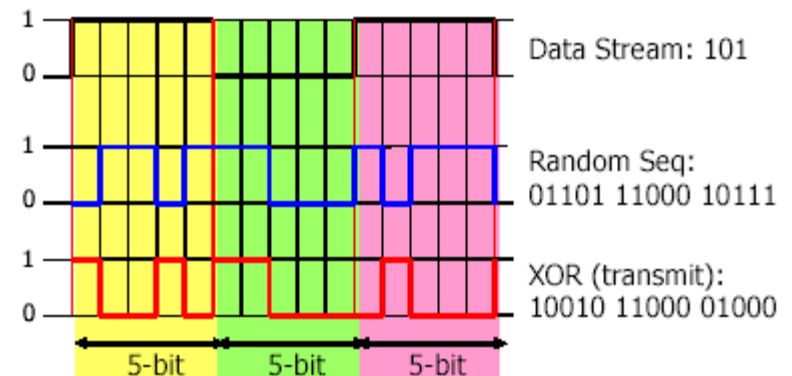
DSSS (Direct Sequence Spread Spectrum)

► Bande ISM : 2,4/2,483 GHz

- Débit : 1, 2, 5.5, 11 Mb/s
- Un bit \Rightarrow plusieurs bits (11)
- Transmission des données XOR une séquence de bits Chipping Code

► Performances

- Coût élevé
- Consommation d'énergie importante
- Débit important
- Redondance bits \Rightarrow diminution des retransmission



Couche liaison de données

- ▶ La couche Liaison de données de la norme 802.11 est composé de deux sous-couches
 - ▶ la couche de contrôle de la liaison logique (Logical Link Control, notée LLC)
 - ▶ la couche de contrôle d'accès au support (Media Access Control, ou MAC).
- ▶ La couche MAC définit deux méthodes d'accès différentes
 - ▶ La méthode CSMA/CA utilisant la Distributed Coordination Function (DCF)
 - ▶ La Point Coordination Function (PCF)
- ▶ Problématique
 - ▶ 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.



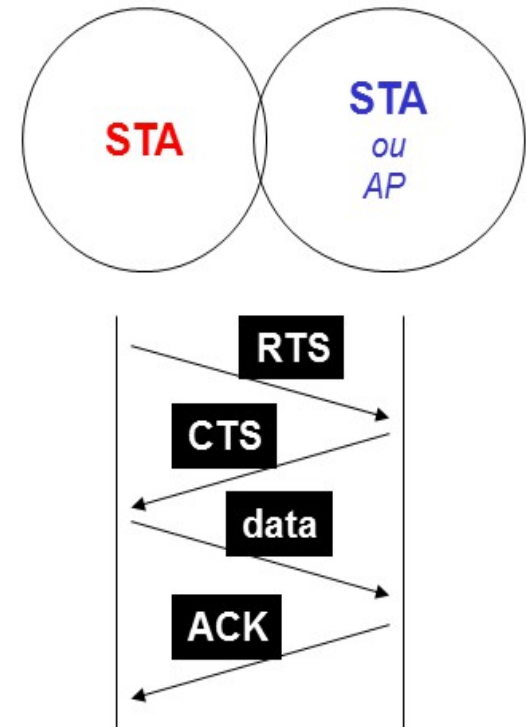
Sous-Couche MAC : CSMA/CA

- ▶ CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance))
- ▶ Le protocole CSMA/CA utilise un mécanisme d'esquive de collision basé sur un principe d'accusé de réceptions réciproques entre l'émetteur et le récepteur
 - ▶ Le taux d'erreur augmente avec la taille des paquets
 - ▶ Fragmentation des paquets en morceaux (fragments)
 - ▶ Mécanisme de contrôle des erreur et retransmission

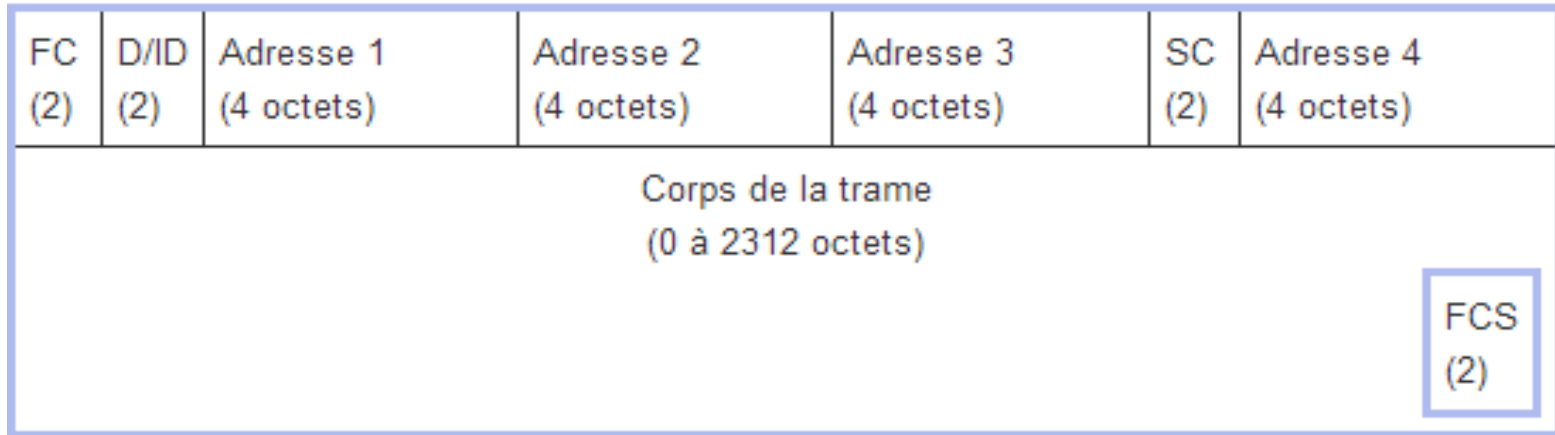


Sous-Couche MAC : CSMA/CA

- 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.
- 4) A 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.



Trame WiFi



- ▶ FC (Frame Control) : contient le numéro de version, des informations sur la fragmentation et l'authentification
- ▶ Durée / ID : durée d'utilisation du canal de transmission.
- ▶ Champs adresses : une trame peut contenir jusqu'à 3 adresses en plus de l'adresse de 48 bits
- ▶ Contrôle de séquence : ce champ permet de distinguer les divers fragments d'une même trame
- ▶ CRC : une somme de contrôle servant à vérifier l'intégrité de la trame



A dark blue vertical bar is positioned on the left side of the slide, spanning the height of the main content area.

Sécurité




Sécurité

- ▶ Les ondes se propage dans toutes les directions avec une portée assez grande. D'une pièce à l'autre mais également d'un étage à l'autre.
- ▶ Un simple logiciel permet de détecter les réseaux wifi de l'entourage
- ▶ Le War-driving localise et cartographie les réseaux ss fils et le publie sur internet
- ▶ Le war-chalking indique à la craie, à même la rue, le mur ou le trottoir, l'emplacement d'un réseau wifi avec différents symboles.
- ▶ Le « war-driving » (détection et piratage automatisé de réseaux sans-fil vulnérables à bord d'une voiture) devient une véritable mode dans les centres urbains.
- ▶ Aux Etat-Unis, certains sont même passés au « war-flying » (même principe à bord d'un hélicoptère)



Sécurité



Le CraieFiti ... !	
Type	Symbole
Noeud ouvert	ssid  bande passante
Noeud fermé	ssid 
Noeud WEP	ssid contact  bande passante
http://craiefiti.free.fr/	

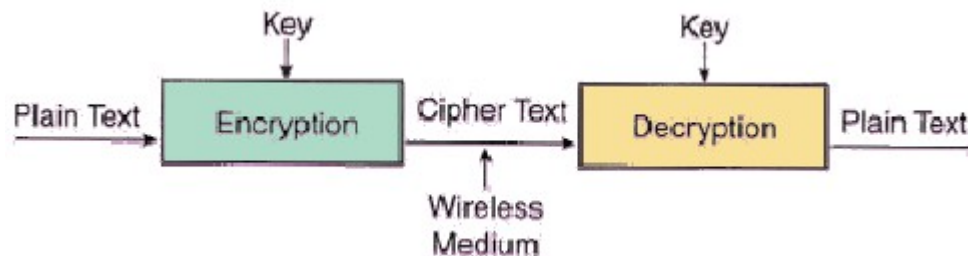
► Mécanismes de sécurité

- Désactivation des options de la trame balise (beacon) qui diffuse leSSID
- Utilisation des ACL accès control list qui contient les adresses Mac des adaptateurs pouvant se connecter
- Utilisation du cryptage des données WEP,WAP



Clé WEP

- ▶ Le WEP (Wired Equivalent Privacy) est un mécanisme de cryptage des données
 - ▶ Basé sur une clé secrète de 64 ou 128 bits Cette clé doit être connue de la station et du point d'accès.
 - ▶ Une clé de session générée de façon aléatoire.
 - ▶ Ce protocole a été cassé en 2001 via sa clé de session
- ▶ Authentification par clé partagée
 - ▶ Clé secrète partagée par toutes les stations (doit être renseigné par un autre canal, le plus souvent à la main)
 - ▶ WEP 64 : clé de 40 bit, WEP 128 : clé de 104 bits
 - ▶ Confidentialité par cryptage



WAP/WAP2

- ▶ juin 2004
- ▶ norme 802.11i
- ▶ WPA Wireless Protected Access
- ▶ WPA2 et le nom commercial de wpa
- ▶ 4 phases
 - 1) Mise en accord sur la politique de sécurité
 - 2) Authentification
 - 3) Dérivation et distribution des clés
 - 4) Chiffrement et intégrité de la RSNA (robust security network association)



Conclusion

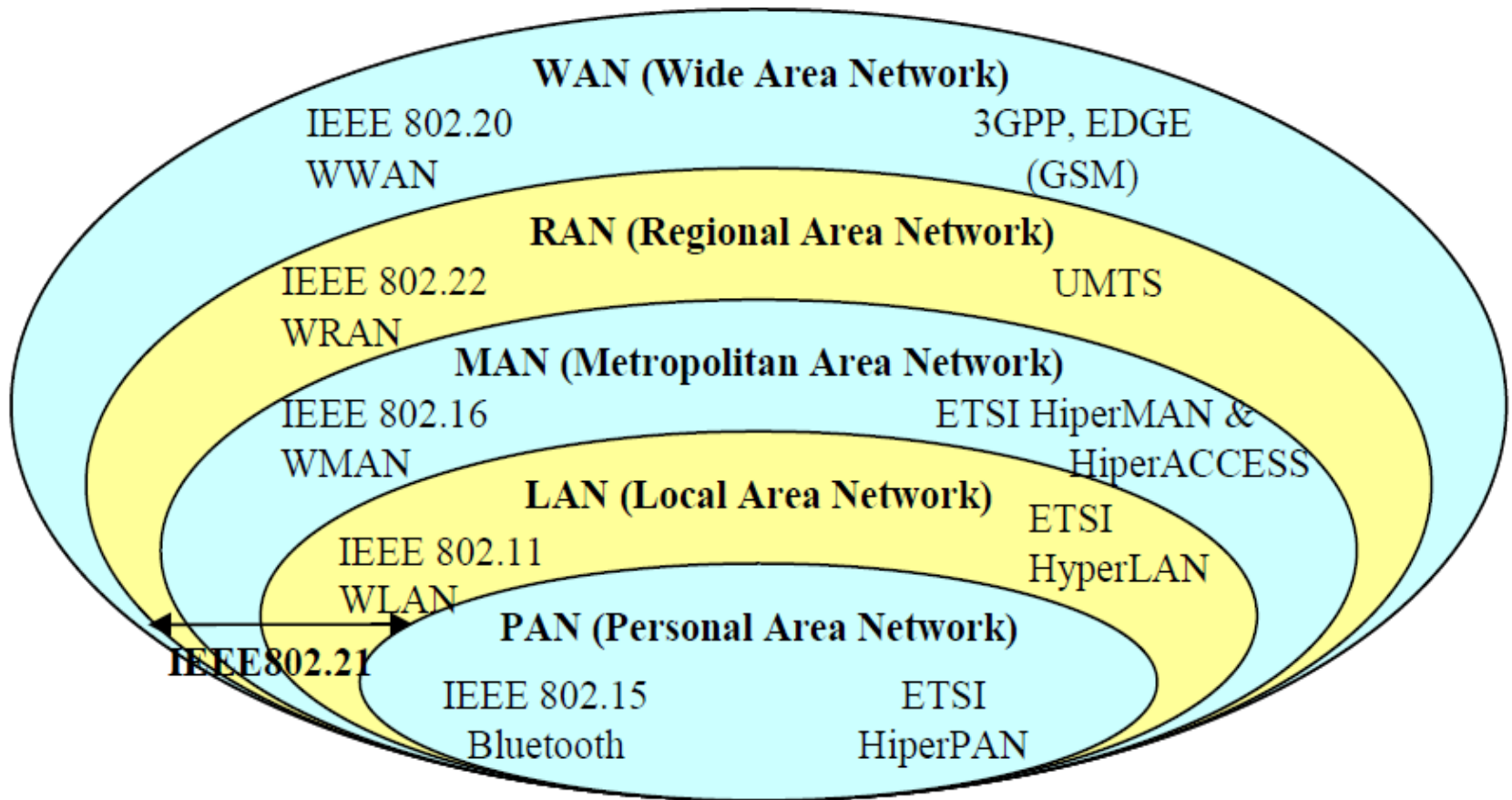
-
-
-

Objectifs, applications

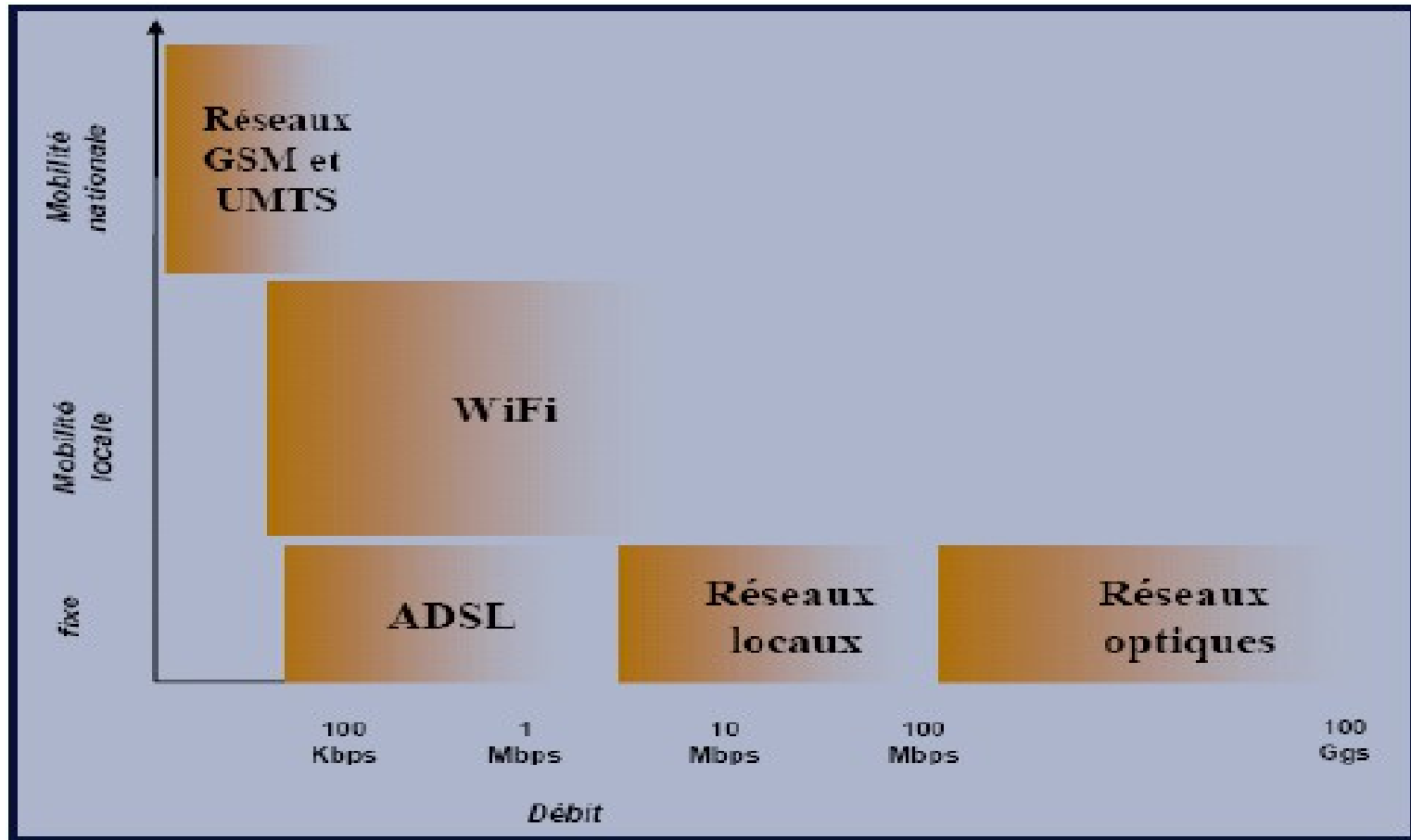
Définition Wireless LAN, normes 802.11

ARCEP, ART : attribution des fréquences

Panorama des réseaux sans fil



Types de réseaux / débits / portées



Différences entre 3G et WiFi

► Accès au réseau

- ▶ 3G : à partir d'une antenne, via son opérateur téléphonique
- ▶ WiFi : à partir de n'importe quelle borne WiFi (qui joue le rôle de modem) si on connaît la clé d'encryptage, via un fournisseur d'accès à internet

► Mobilité

- ▶ Un téléphone 3G conserve sa connexion à Internet tant qu'il est à portée d'une antenne radio de son réseau téléphonique.
- ▶ Une connexion Wi-Fi à Internet nécessite que le mobile reste à portée du routeur sans fil où il s'est connecté ; en cas de déplacement, le mobile est déconnecté d'Internet.

► Vitesse / coût

- ▶ La vitesse moyenne constatée en Wi-Fi architecture est de 3.9 Mbps en Wi-Fi contre 1 à 2 Mbps en 3G (14 Mbps en 3G+ et beaucoup plus avec la 4G).
- ▶ Longtemps les fournisseurs 3G limitaient le téléchargement (surfacturation en cas de dépassement) mais ce n'est plus le cas aujourd'hui ; en Wi-Fi les téléchargements sont illimités.



WiMax : applications



WiMax : caractéristiques

Technologie	Standard	Débit	Distance	Fréquence
Wifi	802.11 b	11 Mb/s	100m	2,4 GHz
Wifi	802.11 g	54 Mb/s	100m	2,4 GHz
WiMAX	802.16 - 2004	75 Mb/s	10 km	< 11 GHz
WiMAX	802.16e	30 Mb/s	<3,5 km	2 - 6 GHz
UMTS	3G	2 Mb/s	6 km	2,1 GHz
Edge	2,5G	348 kb/s	6 km	1,9 GHz
ADSL	xDSL	8 Mb/s	5 km	1,1 KHz
ADSL2+	xDSL	25 Mb/s	2,5 km	1,1 KHz



Evolution des réseaux sans fil

