PDF-XChange Product
Click to buy NOW!
www.tracker-software.com

Sécurité des Réseaux Sans Fil

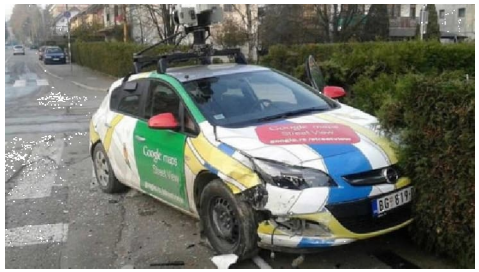
MP1SSR
Abir Ben Ali
www.elabedabir.weebly.com

Organisation de l'enseignement

- Cours : 21h
- TP : 21h

- Présentations orales
- Contrôle continu = 0.3 *Note_Exposé* + 0.7 *Note_DS*
- Site web du responsable de l'UE : www.elabedabir.weebly.com

Sécurité sans fil?



https://www.titanhq.fr/blog/attaques-reseau-wifi-courantes-se-proteger/

Sécurité sans fil?

IP Cam Attack:
https://www.youtube.com/watch?v=yTakZbiqsN0

Public WiFi:
https://www.youtube.com/watch?v=1OVTmrXGHyU

Car Attack :
https://www.youtube.com/watch?v=gJ2rQgoBKWE

Réseaux mobiles vs Réseaux de mobiles

- Les réseaux mobiles sont des réseaux à infrastructure (*backbone*) mobile
- Les réseaux de mobiles sont des réseaux où l'infrastructure est fixe, mais les utilisateurs sont mobiles
- Les réseaux mobiles de mobiles sont des réseaux où l'infrastructure et les utilisateurs sont mobiles

Réseaux sans fil vs Réseaux mobiles

- Réseaux sans fil

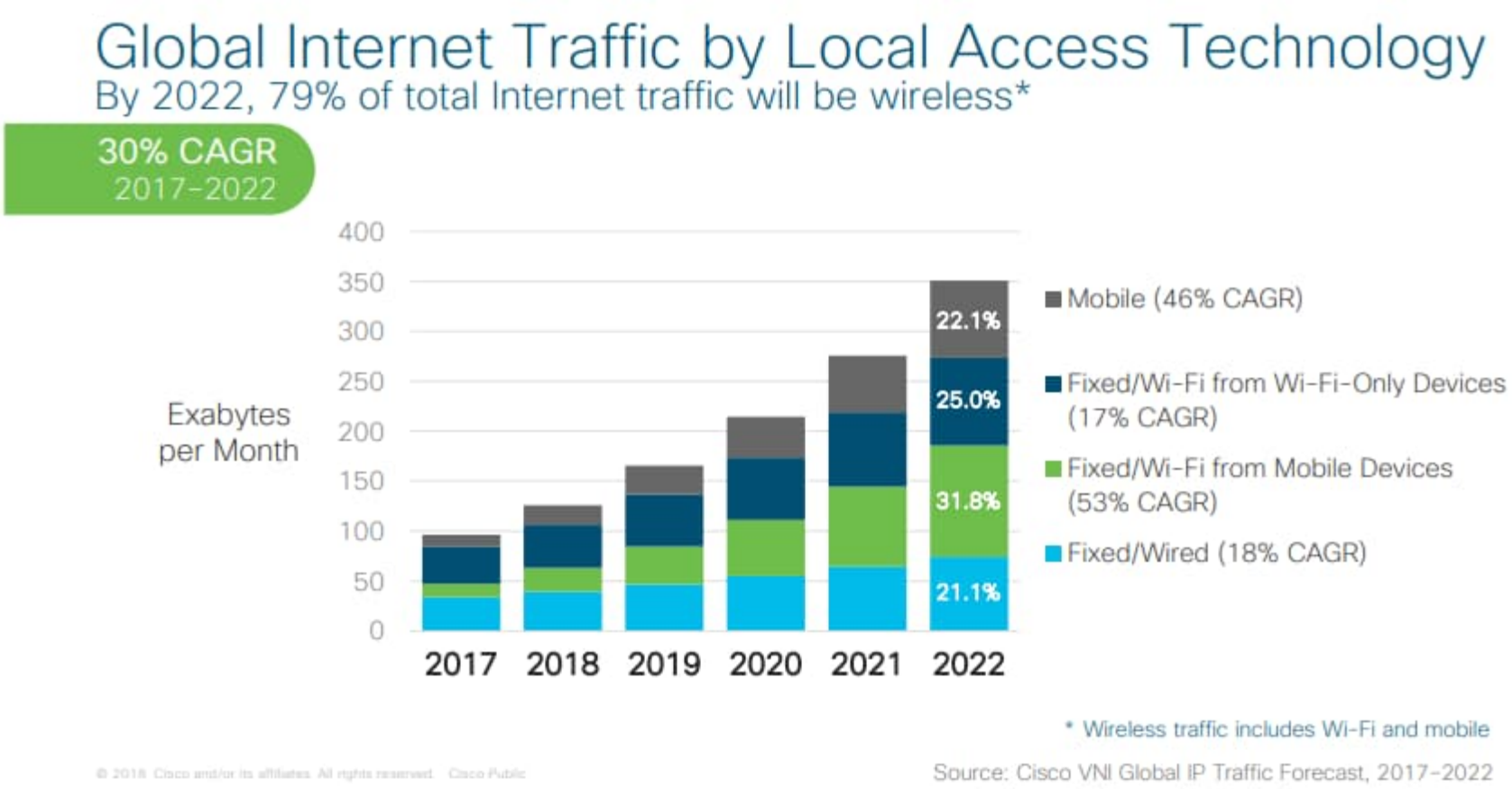
  ➔Communications sans câbles

  - Ondes radio
  - Lumière , infrarouge, laser

- Réseaux mobiles

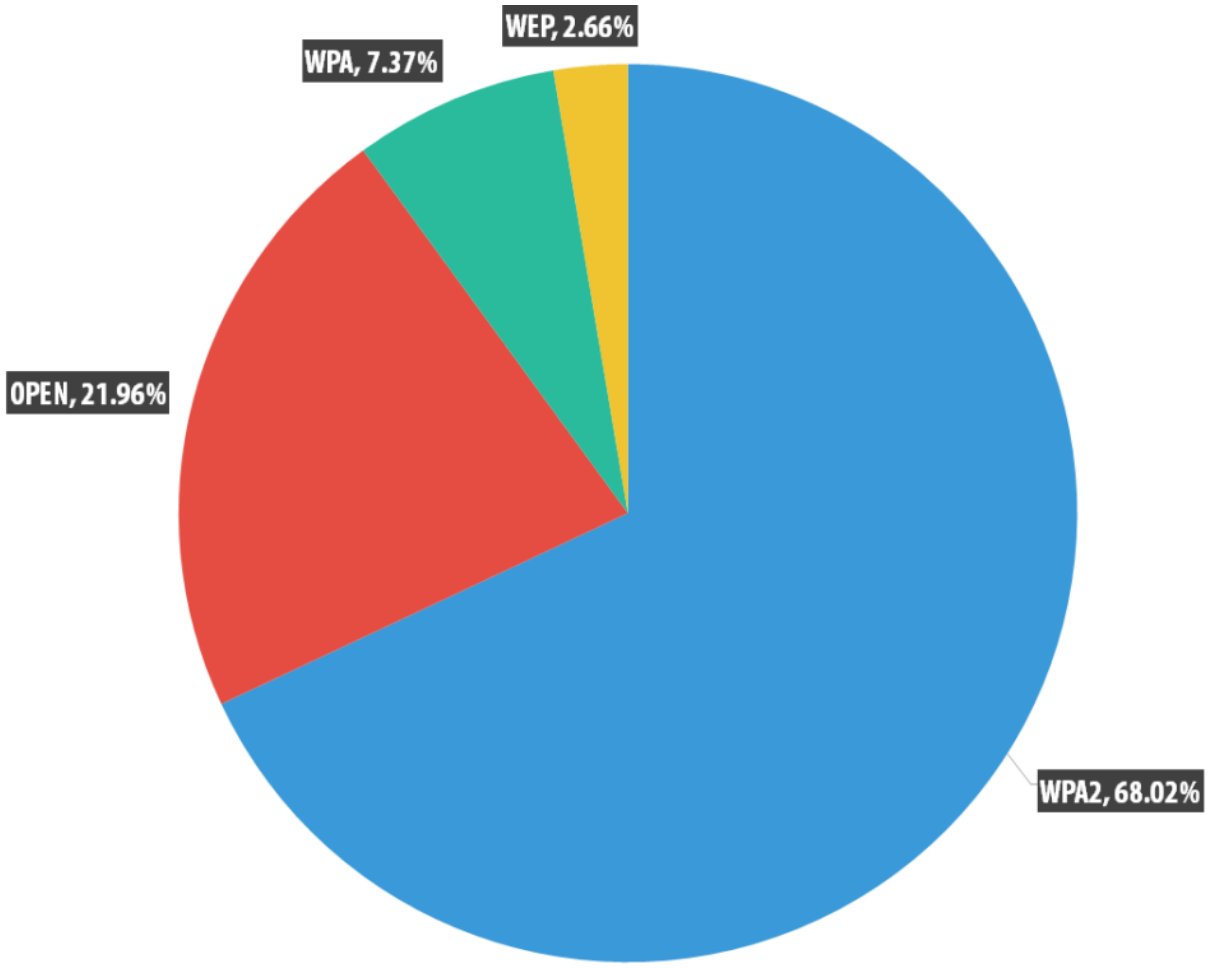
  ➔ Offrir aux utilisateurs mobiles (nomades) un accès itinérant depuis l'extérieur de son réseau en conservant la même adresse (IP mobile,...)

IP Traffic by Access Technology

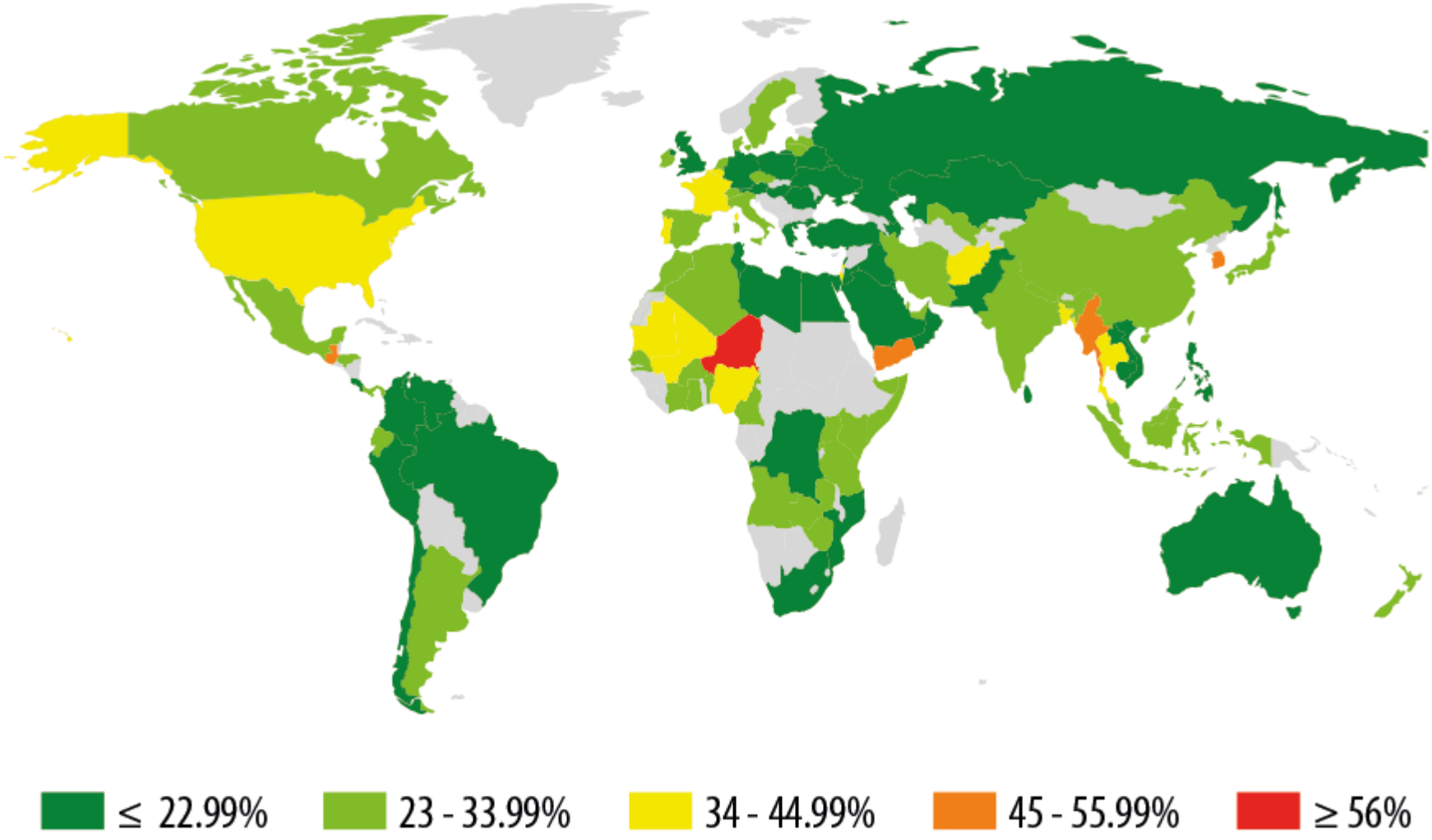


CAGR: Taux de Croissance Composé Annuel

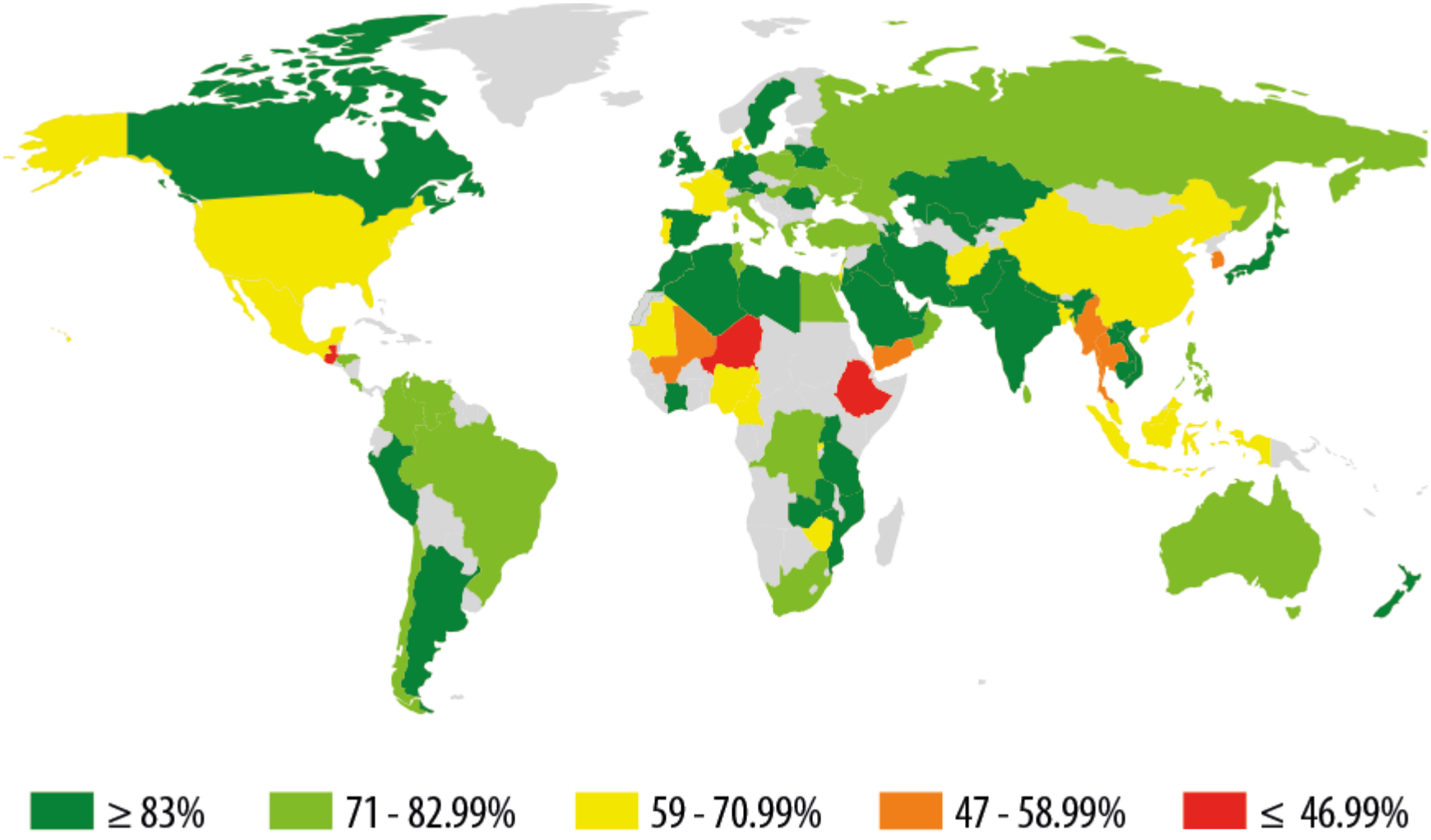
Encryption type used in Wi-Fi hotspots across the world



Share of Wi-Fi hotspots that use unreliable WEP or do not encrypt data (by country)



Share of Wi-Fi hotspots that use WPA/WPA2 (by country)



Contenu

- Caractérisation des réseaux sans fil
- Présentation de la norme Wi-Fi IEEE 802.11
- Vulnérabilités des réseaux Wi-Fi
- Solutions proposées pour la sécurité des réseaux Wi-Fi
- Sécurité Bluetooth?

Solutions internes pour la sécurité Wi-Fi

- WEP, WPA, WPA2, WPA3, WPS

Solutions externes pour la sécurité Wi-Fi

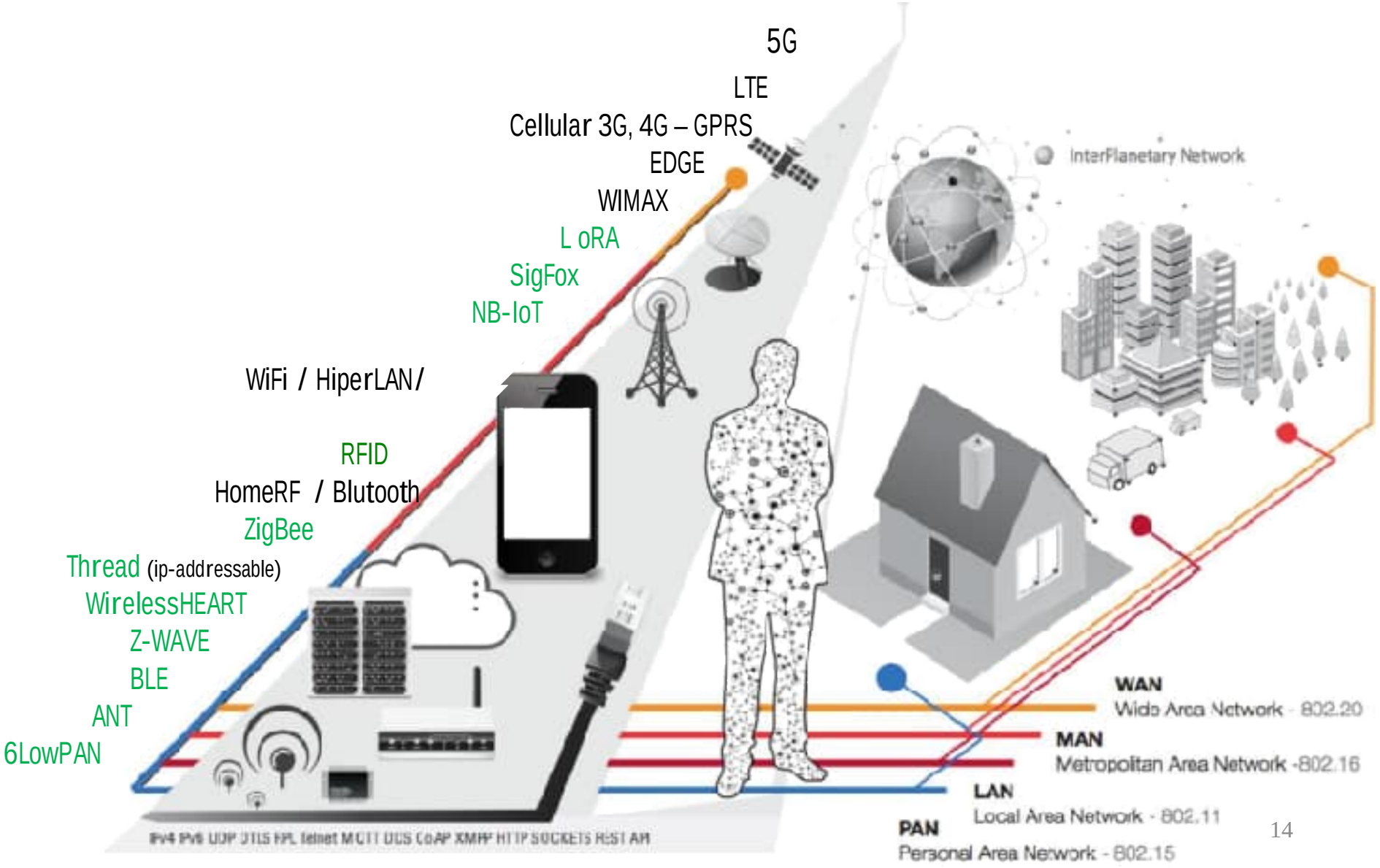
- VPN, firewalls, WIDS, WIPS, Pentest, SIEM ...

Sécurité d'autres normes sans fil

- Bluetooth
- Wi-Max
- ZigBee
- HiperLAN

Caractérisation des réseaux sans fil

Catégories des réseaux sans fil



Catégories des réseaux sans fil

- Réseaux personnels sans fil (WPAN)
  - Bluetooth (IEEE 802.15.1): lancée par Ericsson en 1994, proposant un débit théorique de 1 Mbps pour une portée maximale d'une trentaine de mètres. Très peu gourmande en énergie ➔ adaptée à aux petits périphériques.
  - HomeRF (pour *Home Radio Frequency*): lancée en 1998 par le HomeRF Working Group. Propose un débit théorique de 10 Mbps avec une portée d'environ 50 à 100 mètres. A été abandonnée en 2003.
  - ZigBee (IEEE 802.15.4) :permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie ➔ adaptée pour les petits appareils électroniques (appareils électroménagers, hifi, jouets, ...). Permet d'obtenir des débits pouvant atteindre 250 Kb/s avec une portée maximale de 100 mètres environ.
  - Infrarouge : peut monter à quelques mégabits par seconde pour une portée de quelques mçètres. Llargement utilisée pour la domotique mais très vulnérable aux interférences lumineuses.

Catégories des réseaux sans fil

- Réseaux locaux sans fil (WLAN)
  - Wifi (ou IEEE 802.11): soutenu par la WiFi Alliance offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres
  - HiperLAN2 (*High Performance Radio LAN 2.0*): norme européenne élaborée par l'ETSI (*European Telecommunications Standards Institute*). HiperLAN 2 permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 MHz.
- Réseaux métropolitains sans fil (WMAN)
  - Wi-Max (*IEEE 802.16*) : permettant d'obtenir des débits de l'ordre de 70 Mbit/s sur un rayon de plusieurs kilomètres.

Catégories des réseaux sans fil

- Réseaux étendus sans fil (WWAN)
  (réseaux cellulaires mobiles)

  - GSM (Global System for Mobile Communication): réseau cellulaire 2G offre des débits d'environ 10 Kbit/s grâce au GPRS.
  - GPRS (General Packet Radio Service)
  - UMTS (Universal Mobile Telecommunication System): réseau cellulaires de troisième génération permet des débits théoriques de l'ordre de 2 Mbit/s
  - 3G+ (3rd and 4th Generation Networks)

Spectre de fréquences

Fréquences situées dans les bands dites « sans license »:

- Bande ISM (*Industrial Scientific Medical*) de 2400 Mhz à 2483 Mhz
  - ➔ offre une bande passante de 83 Mhz
  - ➔ Bande divisée en 14 canaux de 20 Mhz ➔ Problème de recouvrement ➔ 3 réseaux adjacents sur une même zone
  - ➔ Largement utilisée par les autres standards
- Bande U-NII (Unlicensed National Information Infrastructure) de 5150 Mhz à 5720 Mhz
  - ➔ offre une bande passante de 300 Mhz
  - ➔ 8 canaux de 20 Mhz
  - ➔ Moins encombrée

Problèmes des réseaux radio

Un débit faible

- Les ressources sont limitées
- On ne peut pas utiliser n'importe quelle bande de fréquences

L'atténuation rapide du signal en fonction de la distance

- Empêche de détecter les collisions

Les interférences

- Les émetteurs fonctionnent sur des fréquences très proches
- L'environnement ouvert/fermé
  - → Atténuation
  - → chemins multiples

Un taux d'erreurs élevé

Problèmes des réseaux radio

L'énergie

- Souvent utilisés pour des applications nomades
- Consommation rapide des batteries
- Importance de la puissance d'émission

Faible sécurité

- Facilité d'espionner le réseau
- Protection physique impossible

➔ Protection logique (cryptographie)

La mobilité

- Doit être prise en compte avec des protocoles adaptés (handover)

Présentation de la norme IEEE 802.11

Définition

- Wi-Fi (Wireless-Fidelity) désigne une norme d'interopérabilité pour les produits de réseau sans fil utilisant les voies hertziennes issus de la norme IEEE 802.11 (norme qui évolue constamment).

Normalisations IEEE 802.11

■ IEEE 802.11a (WiFi2)	WiFi5 La norme 802.11a permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels).
■ IEEE 802.11b (WiFi)	Elle propose un débit théorique de 11 Mbps (6 Mbps rééls) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz
■ 802.11e	Une amélioration de la qualité de service pour une meilleure transmission de la voix et de la vidéo.

Normalisations IEEE 802.11 (2)

- **IEEE 802.11f** — Itinérance (roaming): est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits.
- **IEEE 802.11g** — Offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz, elle a une compatibilité ascendante avec la norme b.
- **IEEE 802.11h** — Vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, d'où le h de 802.11h) et être en conformité avec la réglementation européenne.

Normalisations IEEE 802.11 (3)

- **IEEE 802.11i** — A pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification) en s'appuyant sur l'AES (*Advanced Encryption Standard*) et propose un chiffrement des communication s pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
- **IEEE 802.11R** — Réalise des transmission infrarouges.
- **IEEE 802.11j** — Vise à se rapprocher de la norme japonaise.

Normalisation IEEE 802.11 (4)

- IEEE 802.11n (WiFi4) — Publié en 2009, opère sur les 2,4 GHz et 5 GHz, pour un débit allant jusqu'à 540 Mbps
- IEEE 802.11ac (WiFi5) — Publié en 2014, opère sur la bande 5 Ghz , pour un débit allant jusqu'à 1,3 Gbps
- IEEE 802.11ah — Publié en 2017, offre une économie d'énergie opère sur la bande 800 Mhz , pour un débit de 4 Mbps
  ➔ Conçu pour l'Internet des Objets
- IEEE 802.11p — Amendement du standard IEEE802.11 pour les communications véhiculaires V2X
- IEEE 802.11ax (WiFi6) — Publié en 2021, opère sur les 2,4 GHz et 5 GHz, pour un débit de 4,8 Gbps

Fonctionnement de WiFi

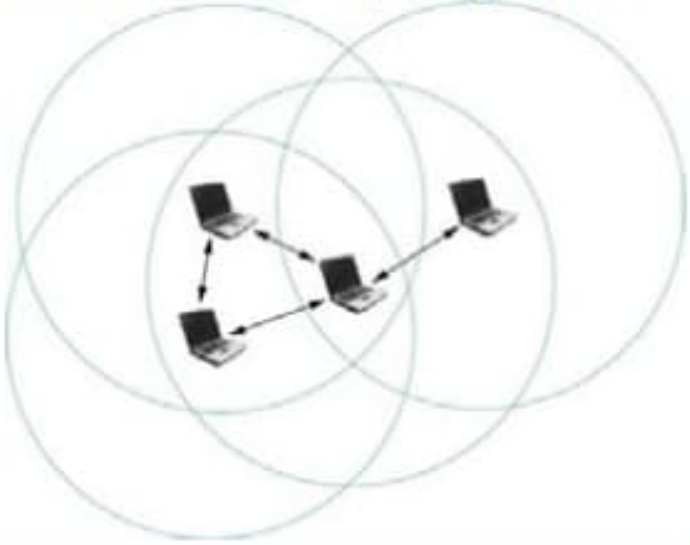
Mode ad hoc (spontané)

- Totalement distribué.
- Permet la communication entre deux machines sans l'aide d'une infrastructure
- Les stations se trouvant à portée de radio forment un IBSS (Independant Basic Service Set).
- La bande passante du réseau est basée sur

la vitesse de l'hôte le plus lent.

- La bande passante du réseau est divisée

par le nombre d'hôtes sur ce réseau.



Mode Ad hoc vs réseau Ad hoc

- Il n'y a pas de routage en mode ad hoc, contrairement à un réseau ad hoc

- Protocoles de routage spécifiques aux réseaux ad hoc (MANET: Mobile Ad hoc NETwork) :
  - proactifs (OLSR, ...)
  - réactifs (AODV, DSR,...)

Fonctionnement de WiFi (2)

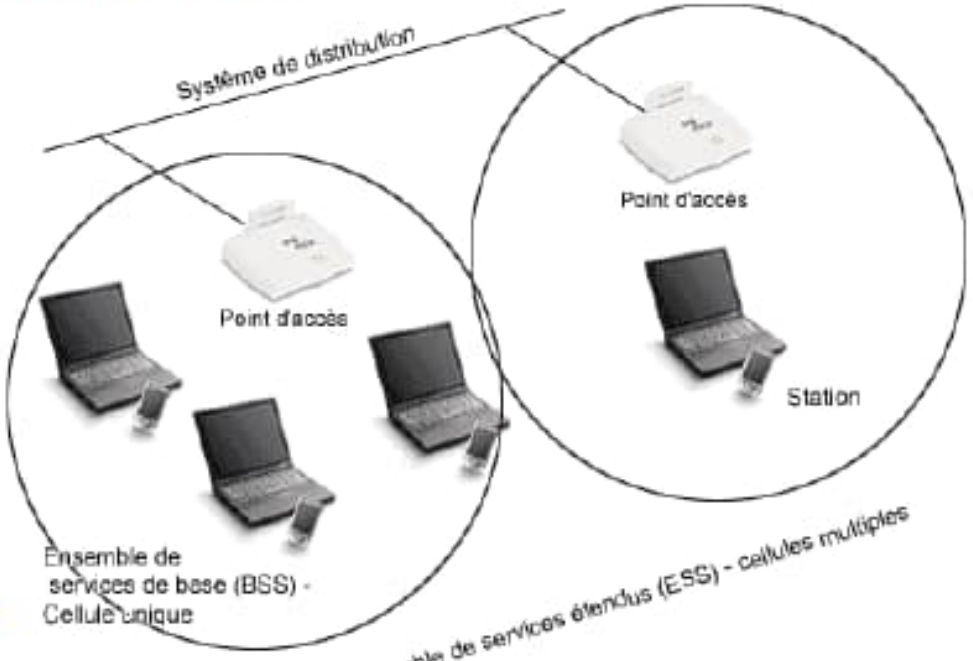
Mode infrastructure

- Se base sur une station spéciale appelée Point d'Accès (PA) .
- Permet à des stations wifi de se connecter à un réseau (généralement Ethernet) via un point d'accès
- L'ensemble des stations à portée radio du PA forme un BSS (Basic Service Set).
- Chaque BBS est identifié par un BSSID (BSS Identifier)

de 6 octets qui correspond à l'adresse MAC du PA.

Fonctionnement de WiFi (3)

- On peut composer un réseau avec plusieurs BSS, reliés entre eux par un système de distribution (DS).
- Ces différents BSS forment un ESS (Extended Service Set).
- Un ESS est identifié par un ESSID (SSID) qui est constitué d'un mot de 32 caractères qui représente le nom du réseau.



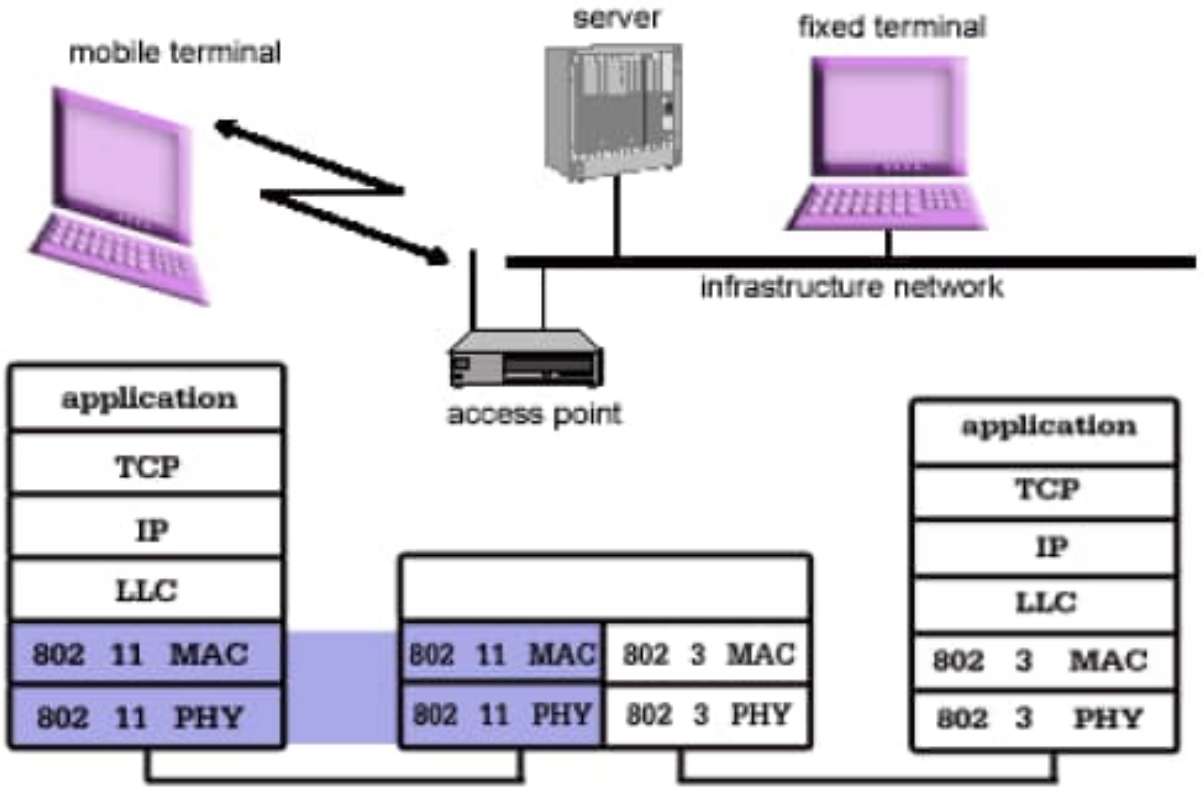
Mode Infrastructure

Spécifications IEEE 802.11

La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

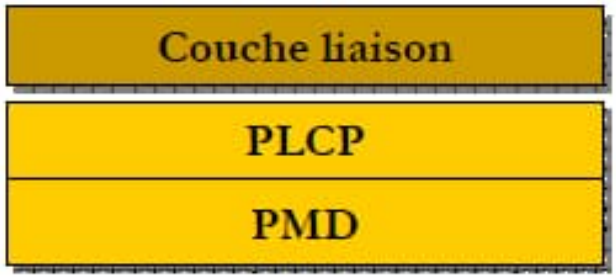
- La couche physique (notée parfois couche PHY), proposant trois types de codages de l'information
- La couche liaison de données, constituée de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC).

Spécifications IEEE 802.11



La couche PHY IEEE 802.11

- La couche physique définit la modulation des ondes radio-électriques et les caractéristiques de la signalisation pour la transmission de données.
- Décomposée en deux sous-couches:
  - PLCP (Physical Layer Convergence Protocol): s'occupe de l'écoute du support et de la signalisation en fournissant un CCA (Clear Channel Assessment) à la couche MAC,
  - PMD (Physical Medium Dependent) traite l'encodage des données et la modulation.



La couche PHY IEEE 802.11

Propose trois couches différentes suivant différentes techniques de transmission :

- Techniques à étalement de spectre:
  - FHSS *Frequency Hopping Spread Spectrum* (802.11)
  - DSSS *Direct Sequence Spread Spectrum* (802.11b)

  ➔ Bonnes performances contre le brouillage en changeant périodiquement la fréquence d'émission selon une séquence préétablie

- OFDM *Orthogonal Frequency Division Multiplexing* (802.11a,802.11g)

  ➔ Plus haut débit (54 Mbps), 802.11a totalement incompatible avec Wifi.

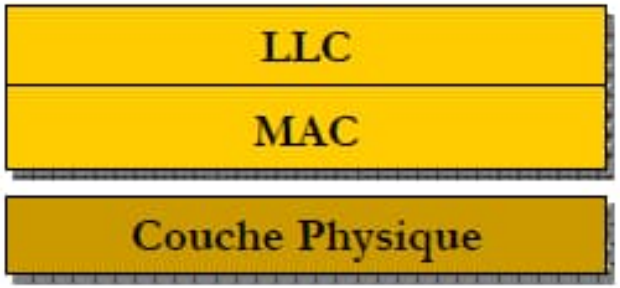
- IR (802.11)

La couche MAC IEEE 802.11

La couche MAC de WiFi est subdivisée en 2 sous-couches:

- LLC (*Logical Link Layer*): est identique à la couche 802.2 permettant une compatibilité avec n'importe quel autre réseau 802

- MAC (Medium Access Control) : caractérise l'accès au média de façon commune aux différentes normes 802.11 physiques, elle est équivalente à la norme 802.3 Ethernet avec des fonctionnalités nécessaires aux transmissions radio.



La couche MAC IEEE 802.11 (2)

DCF

- Distributed Coordination Function (DCF) ou CP (Contention Period) appelée aussi mode d'accès à compétition.
- similaire à Ethernet.
- Permettant le transport des données asynchrones où les stations ont une chance égale d'accéder au support.
- Utilisée par les modes Ad-Hoc et infrastructure

PCF

- Point Coordination Function (PCF) ou CFP (Contention Free Period) appelée mode d'accès contrôlé.
- Contrôlée par le point d'accès
- Fondée sur l'interrogation à tour de rôle des stations, ou polling.
- Une station ne peut émettre ou recevoir que si elle est autorisée.
- Méthode conçue pour les applications temps réel (vidéo, voix) nécessitant une gestion du délai lors des transmissions de données.
- Utilisée par le mode infrastructure.

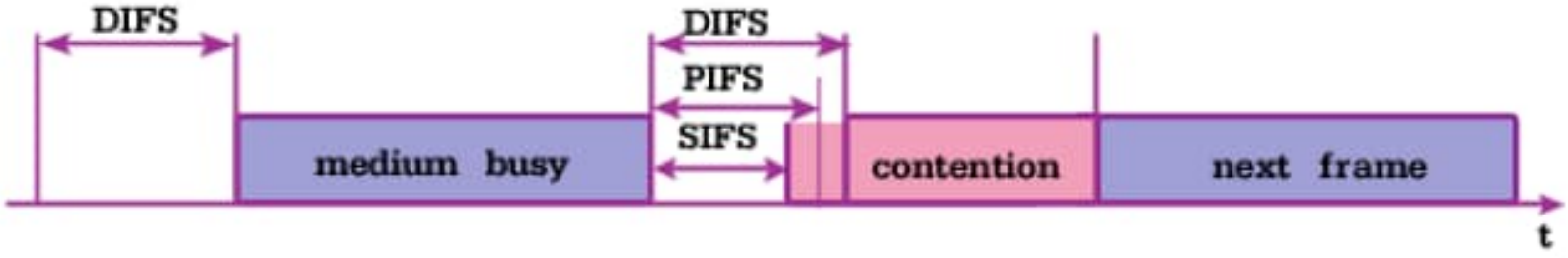
DCF (mode CSMA/CA)

Carrier Sense Multiple Access/ Collision Avoidance

- Méthode d'accès présentée comme alternative à CSMA/CA car les liaisons radio utilisées ne sont pas full-duplex et une machine qui écoute la porteuse n'est pas certaine d'écouter toutes les stations connectées au point d'accès (cas de la station cachée).

- Présente plusieurs techniques :
  - ✓ Système d'accès au support basé sur des temporisateurs.
  - ✓ Un système d'acquittement positif.
  - ✓ Une gestion de reprise sur collision par des timers.
  - ✓ Une technique optionnelle permettant de sécuriser la transmission des données et d'éviter les collisions avec les nœuds cachés.

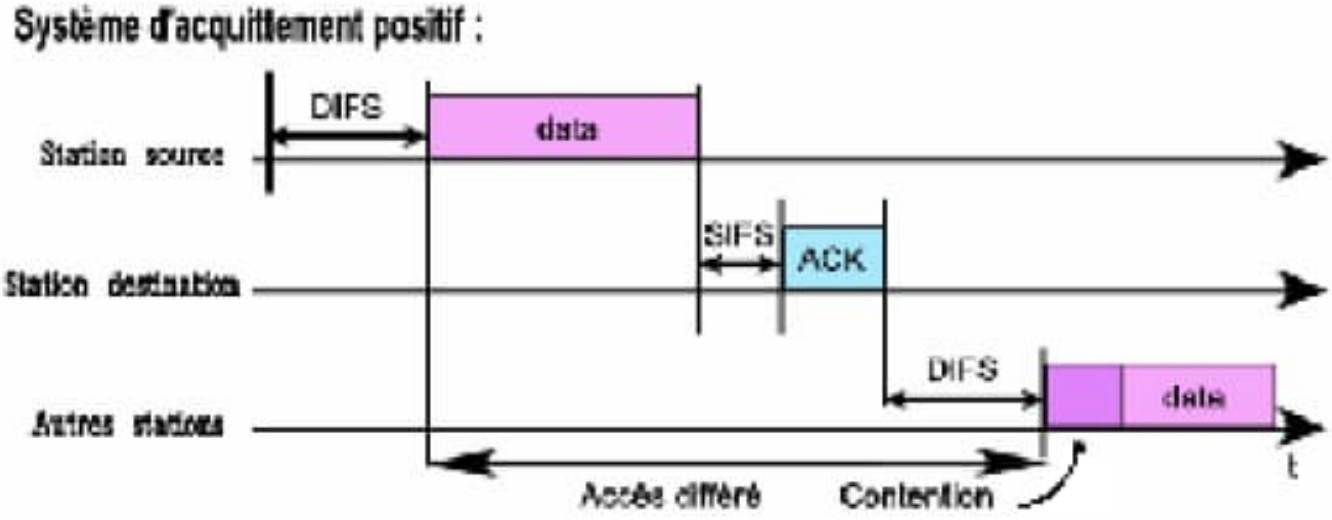
Accès au support



- SIFS (Short Interframe Sequence) le plus petit des IFS, donc le plus prioritaire. Il est utilisé pour la transmission d'un même dialogue (données/ACK).
- PIFS (PCF Short Interframe Sequence) : utilisé pour les trames PCF (accès contrôlé) par le point d'accès. Permet un accès prioritaire de ce PA sur les stations du réseau.
- DIFS (DCF Short Interframe Sequence) : utilisé par les stations pour accéder au support en mode DCF.

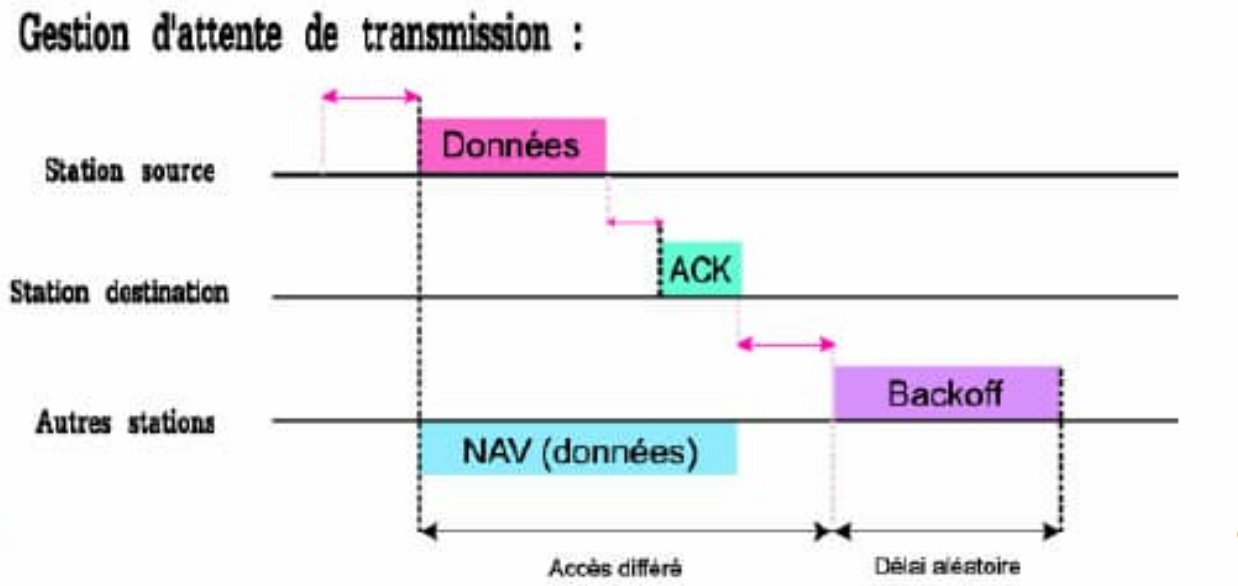
Système d'acquittement positif

La station destination vérifie le CRC de la trame et renvoie un ACK à l'émetteur. Si la station émettrice ne reçoit pas ce ACK, elle suppose qu'une collision s'est produite, la trame est donc retransmise suivant une gestion utilisant des timers.



Gestion d'attente de transmission

- Transmission après une écoute pendant un DIFS.
- Calcul de la durée de la transmission d'après le TTL contenu dans la trame ➔ calcul du NAV (Network Allocation Vector).
- Utilisation de backoff avant la transmission afin de minimiser le risque de collision entre les stations en contention.



Technique de sécurisation de transmission par réservation (option)

- Basé sur un mécanisme de réservation basé sur l'emploi de trames RTS / CTS (Request To Send / Clear To Send) entre hôte source et hôte destination.
- une station désirant émettre envoie un RTS
- La station destination répond, après un SIFS, par un CTS.
- Toutes les stations mettent à jour leurs NAV.

☺ Permet de résoudre le problème des nœuds cachés

☹ Dégrade les performances du réseau

➔ utiliser un RTS threshold

PCF (mode infrastructure)

- Mode Basé sur une scrutation successive des stations par le AP (polling).
- Le AP établit une liste d'interrogation (polling list) des stations associées fonctionnant en mode PCF.
- Organisé autour d'une super-trame découpée en deux périodes à l'alternat : une partie pour le mode CFP et une autre pour le mode CP.
- Le PA génère une balise, appelée Beacon Frame, pour indiquer le passage en mode PCF, après une inter trame PIFS.

Gestion des associations

Le processus d'association se déroule en plusieurs étapes :

① Ecoute du support (afin de découvrir les points d'accès):

- Ecoute active : Une station envoie une trame de requête (Probe Frame Request), contenant sa configuration (SSID auquel elle appartient, débit…), sur chaque canal et enregistre les caractéristiques des points d'accès (possédant le même SSID) qui y répondent et choisit le point d'accès offrant le meilleur compromis de débit et de charge. Si elle ne reçoit aucune réponse elle passe en écoute passive.

- Écoute passive : la station scanne tous les canaux et attend de recevoir une trame balise (beacon frame) du point d'accès.

Gestion des associations (2)

② Authentification :

- Open System Authentication : mode par défaut, n'importe quelle station se connectant est authentifiée.
- Shared Key Authentication : mode d'authentification basé sur un partage de clé secrète entre la station et le point d'accès. Ce mécanisme est activé avec le protocole WEP.

③ Association :

- La station envoie une requête d'association au PA (Assocation Request Frame)./
- Le AP répond par une trame de réponse qui contient un identificateur d'association (Association ID).
- Une fois acceptée, la station règle son canal sur le PA.

Formats de trames

FC 2octets	D/ID 2 octets	Adresse 1 6 octets	Adresse 2 6 octets	Adresse 3 6 octets	SC 2 octets	Adresse 4 6 octets
Corps de la trame (0 à 2312 octets)						FCS 4 octets

- FC (Frame Control): 11 champs sur 2 octets.
- D/ID : Duration /ID
- Adresses source et destination + adresses des DS intermédiaires
- Sequence Control : n° séquence + n° fragment
- FCS : CRC de 32 bits

Formats de trames (2)

Le champ FC