WLAN

Objectifs

- Pouvoir expliquer la différence entre les termes WLAN, 802.11 et Wi-Fi
- Savoir citer les avantages et les inconvénients des WLAN
- Savoir différencier les deux modes utilisés pour les WLAN
- Pouvoir expliquer le lien entre 802.11 et le modèle OSI
- Savoir expliquer les critères pour le choix de canaux
- Pouvoir expliquer le problème d'accès au medium dans le cadre d'un WLAN
- Savoir décrire la méthode d'accès au medium CSMA/CA

Objectifs (suite)

- Pouvoir expliquer les difficultés liées à CSMA/CA et les solutions qui permettent de l'améliorer (RTS/CTS)
- Savoir interpréter les principaux champs d'une trame 802.11 et expliquer à quoi correspondent le type et sous-type de trame
- Pouvoir expliquer l'utilité des différentes trames de gestion
- Savoir expliquer les différents problèmes de sécurité posés par les réseaux Wi-Fi
- Pouvoir citer les différents protocoles utilisés pour sécuriser les réseaux Wi-Fi et leurs forces/faiblesses

Définitions

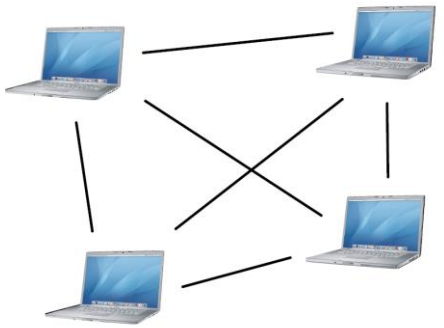
- WLAN: Wireless Local Area Network (réseau local sans fil)
  - Type de réseau
- 802.11: décrit les caractéristiques d'un WLAN
  - Standard international
- Wi-Fi: Wireless Fidelity, marque créée par la Wi-Fi Alliance
  - Initialement le nom d'une certification pour la compatibilité des équipements
  - Technologie / ensemble de protocoles basé sur les standards 802.11

Avantages et inconvénients

- Avantages
  - Mobilité
  - Facilité et coût d'installation
  - Adapté à toutes les plateformes
- Inconvénients
  - Débit faible et partagé
  - Problèmes liés à la transmission radio (interférences, couverture)
  - Sécurité

Architecture

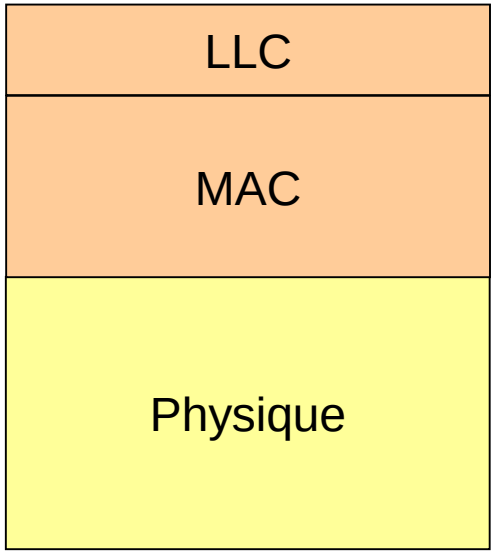
- 2 modes : infrastructure et ad hoc
- Mode ad-hoc:
  - Communication directe entre les clients
  - Pas de communication vers l'extérieur (p.ex. Internet)



- Mode infrastructure:
  - Communication entre les clients à travers un AP (Access Point)
  - Communication vers l'extérieur à travers l'AP

Lien avec le modèle OSI

- 802.11 définit les couches Physique et Liaison
- La couche liaison est divisée en 2 sous-couches:
  - MAC
  - LLC
- But initial de LLC: cacher les différences entre les versions à la couche supérieure
- Concrètement: identifie seulement le protocole de la couche supérieure



Normes principales

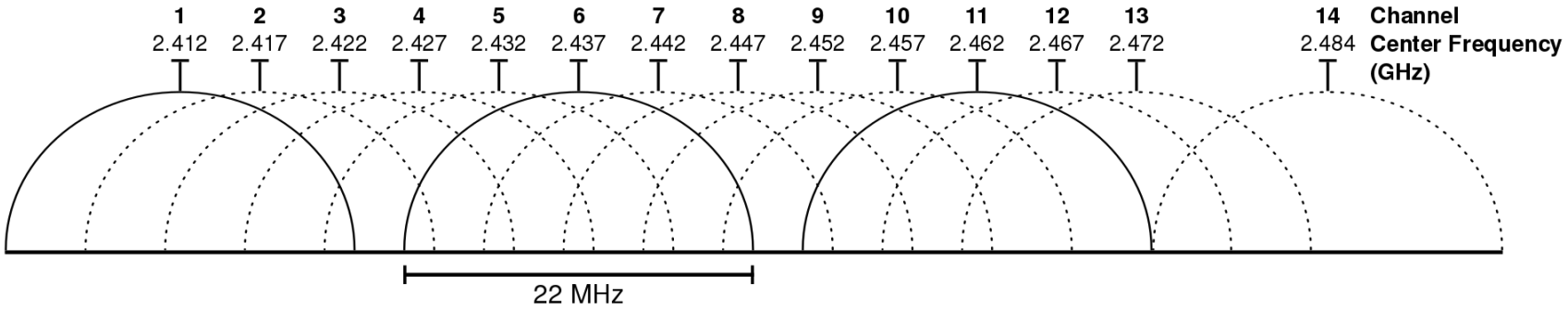
Norme	Débit maximal théorique	Bande de fréquences	Commentaire
IEEE 802.11	1, 2	2.4 GHz	Première norme
IEEE 802.11b	11 Mb/s	2.4 GHz	Compatible avec 802.11g. Peu utilisée
IEEE 802.11g	54 Mb/s	2.4 GHz	Très populaire
IEEE 802.11a	54 Mb/s	5 GHz	Portée plus faible, mais moins d'interférences
IEEE 802.11n	600 Mb/s	2.4 GHz ou 5 GHz	Utilise le MIMO (Multiple Input Multiple Output)

Choix de canal

- Les bandes de fréquences sont divisées en canaux
- Nombre de canaux utilisés :
  - 802.11b: 1
  - 802.11g: 1
  - 802.11a: 1
  - 802.11n: 1 ou 2
- Le choix des bons canaux est important pour éviter de mauvaises performances

Choix de canal: 802.11b/g/n (2.4GHz)

- 13 canaux en Europe + canal 14 seulement au Japon
- Chevauchement des canaux: bruit dans les canaux voisins
- Utilisation du même canal
  - Inconvénient: Partage de la bande passante
  - Avantage: permet au mécanismes de détection de collision de fonctionner
- Idéalement: 5 canaux d'écart pour éviter les interférences
  - Canaux les plus utilisés: 1, 6 et 11



Choix de canal: 802.11a/n (5GHz)

- 19 canaux en Europe
- Pas d'interférences mutuelles
- 802.11n peut utiliser un ou deux canaux
  - 5GHz: rien de spécial
  - 2.4GHz: les deux canaux doivent être séparés de 20 MHz
    - Par exemple 1 et 5 ou 6 et 10
    - Un seul réseau 802.11n à 2.4 GHz bloque 9 des 13 canaux

Accès au medium

- Pratiquement impossible de transmettre et écouter en même temps
  - Le signal reçu peut être très faible par rapport au signal émis
  - CSMA/CD ne peut pas être utilisé
- Les collisions doivent être évitées plutôt que détectées
- Deux modes d'opération:
  - DCF (Distributed Coordination Function)
  - PCF (Point Coordination Function)

- La méthode la plus courante est CSMA/CA, qui correspond à un DCF

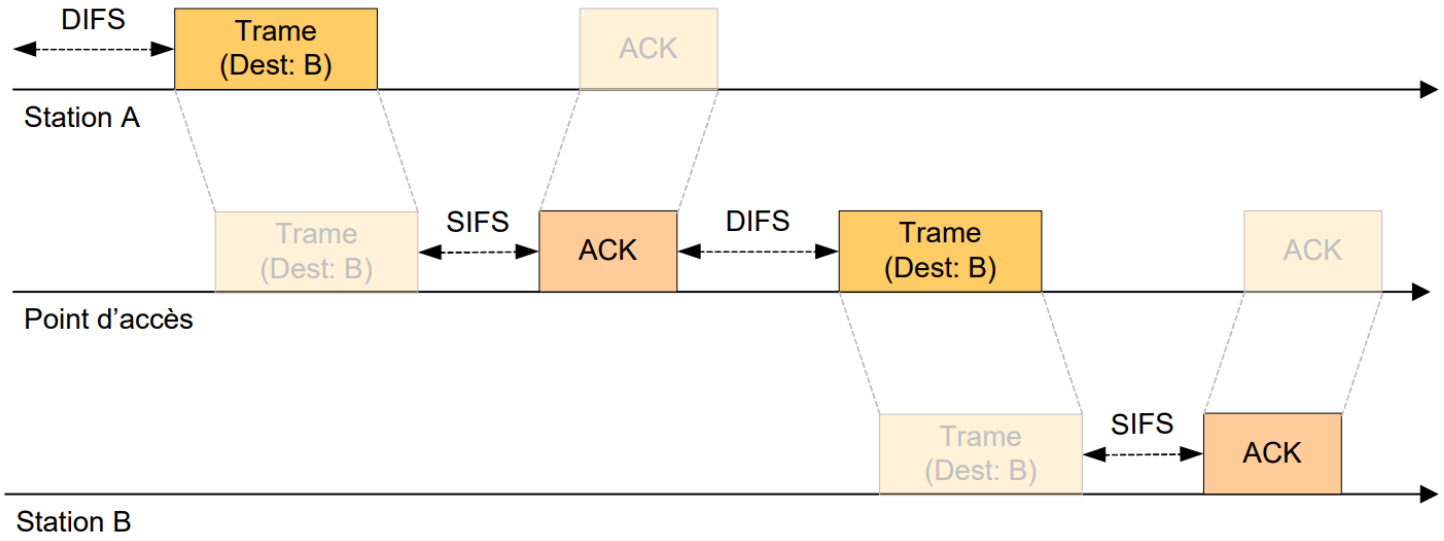
CSMA/CA

- CSMA/CA
  - Carrier Sense Multiple Access Collision Avoidance
- Principe:
  1. Ecouter le canal avant de transmettre
  2. Si le canal est libre pendant l'intervalle DIFS: transmission
  3. Si le canal est occupé: attente d'un délai aléatoire
  4. Une fois la trame transmise: attente d'un délai aléatoire
  5. Acquittement des trames après chaque transmission (intervalle SIFS entre la réception de la trame et l'acquittement)

CSMA/CA: intervalles

- **DIFS** (DCF InterFrame Spacing): intervalle standard entre les trames. Si cette durée est écoulée, une station peut essayer d'envoyer une trame.
- **SIFS** (Short InterFrameSpacing): intervalle plus court permettant par exemple d'envoyer un acquittement avant qu'une autre station n'envoie une trame.

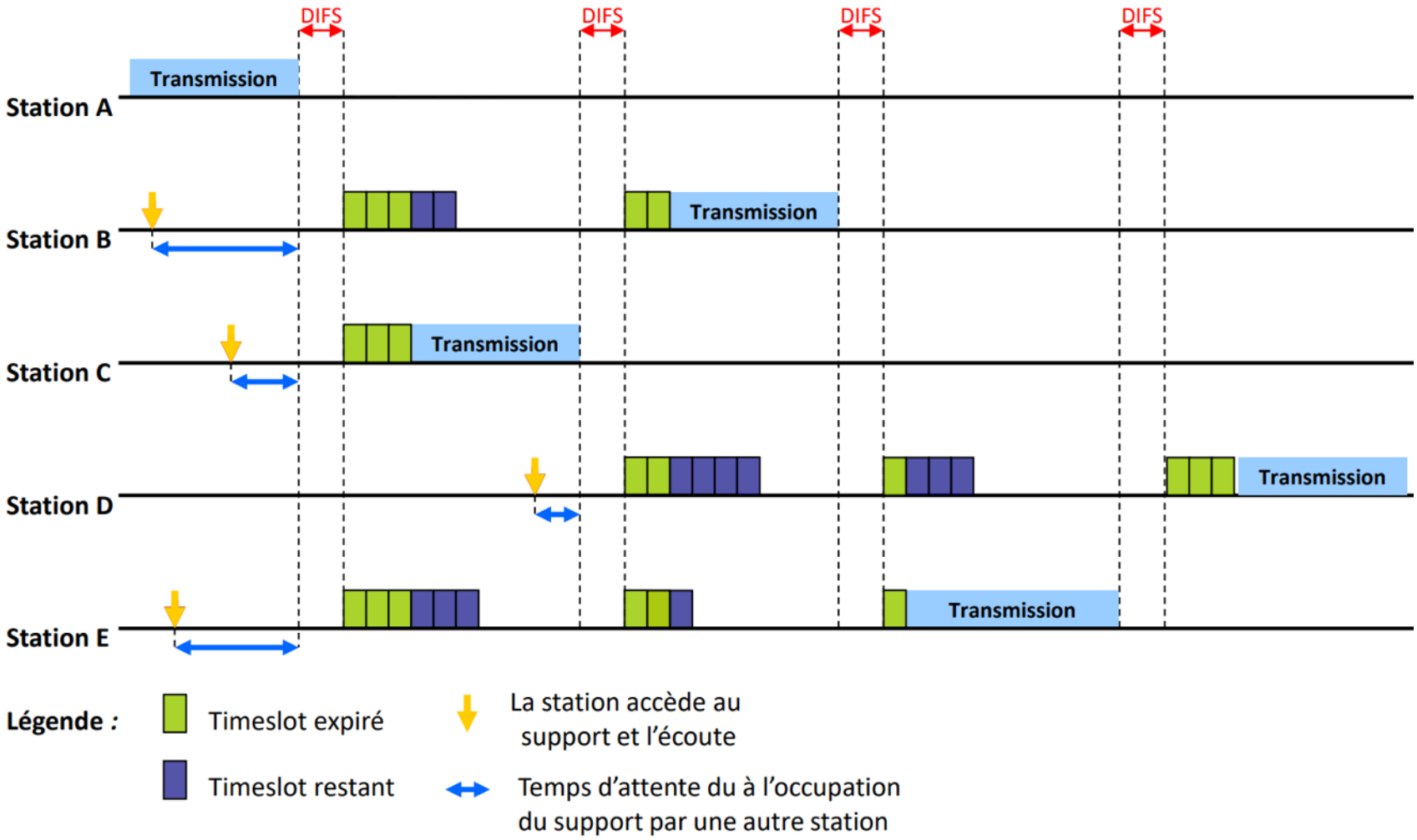
CSMA/CA: exemple 1



CSMA/CA: délai aléatoire

- Quand une station doit attendre un délai aléatoire, elle continue d'écouter le canal
- Si une autre station commence à émettre:
  - Interruption de l'attente
  - Reprise de l'attente après la fin de la transmission + DIFS

CSMA/CA: exemple 2

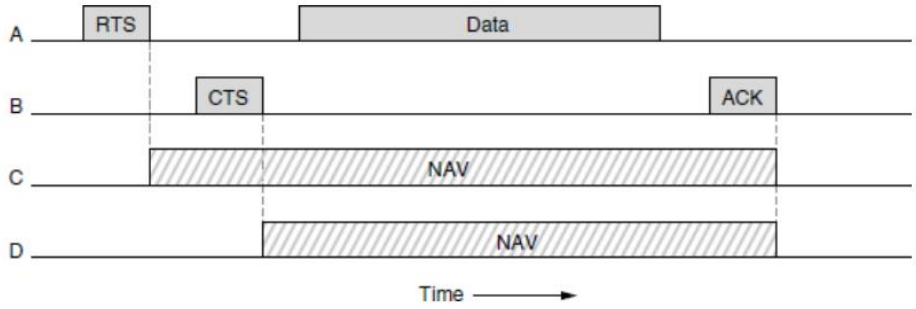


Problèmes de CSMA/CA

- Dans quels cas est-ce qu'il y a quand même des collisions?
  1. Deux stations qui terminent leur attente en même temps
  2. Deux stations émettent en même temps, mais sont trop éloignées pour détecter que l'autre émet aussi: problème de la station cachée
- Quelles solutions?
  1. On ne peut pas résoudre le problème, mais on peut diminuer la durée des collisions → ACK timer
  2. Utilisation du mode RTS/CTS pour éviter le problème

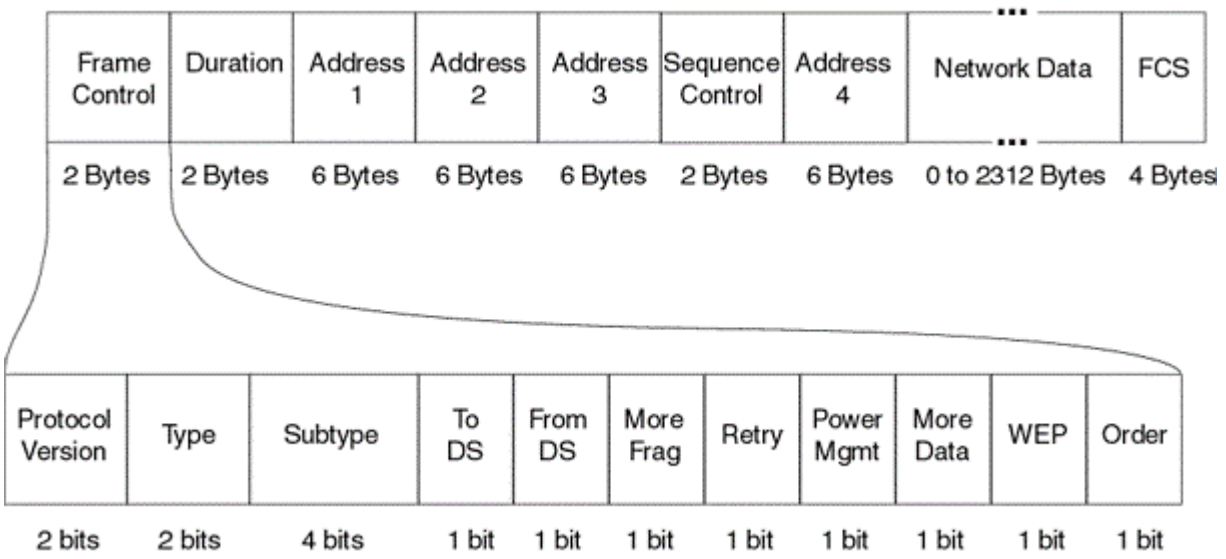
Mode RTS/CTS

- **RTS:** Request to send, message envoyé par une station A qui veut émettre au destinataire B
- **CTS:** Clear to send, message envoyé par la station B à la station A pour lui donner la permission d'émettre
- **NAV:** Network Allocation Vector, compteur maintenu par les stations permettant de savoir quand recommencer à écouter le canal.



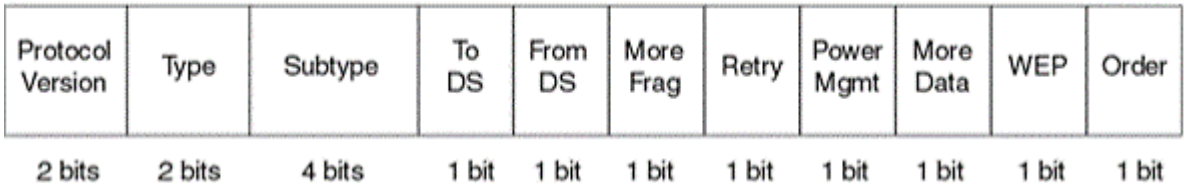
Format des trames

- **Duration:** utilisé par les stations pour définir le NAV
- **Address 1, 2 et 3:** destination, source et adresse distante
- **Sequence Control:** numérote les trames
- **Address 4:** généralement pas utilisé
- **FCS:** CRC-32



Format des trames: frame control

- **Protocol Version:** 0, devrait servir à concilier plusieurs versions
- **Type:** données, contrôle (RTS/CTS/ACK/..), gestion
- **Subtype:** p.ex. RTS pour une trame de contrôle
- **Autres champs:** donnent des détails sur la trame
  - Suivie par d'autres fragments ou trames
  - Retransmission
  - Contenu chiffré
  - …



Trames de gestions 802.11

- Utilisées pour la communication avec l'AP
- Scanning (trouver un réseau):
  - Scanning actif: Probe request et Probe response
  - Scanning passif: Beacon (envoyé régulièrement par l'AP)
- Authentification (prouver son identité):
  - Authentication
- Association (négocier les conditions):
  - Association request
  - Association response

Sécurité Wi-Fi

- Aucun chiffrement (p.ex. free hotspot)
  - Équivalent à un hub
- WEP
  - Basé sur un algorithme de chiffrement faible (RC4)
  - RC4 mal utilisé
  - Possible de récupérer la clé en environ une minute
- WPA
  - Amélioration de WEP
  - Meilleure utilisation de RC4
  - Passphrase: vulnérable aux attaques par dictionnaire

Sécurité Wi-Fi (suite)

- WPA2
  - Basé sur un algorithme de chiffrement sûr (AES)
  - Passphrase: vulnérable aux attaques par dictionnaire
- WPA2 Enterprise
  - Nécessite de fournir un username/password
  - Etape supplémentaire d'authentification → génération de clef
  - Pas de passphrase: résiste aux attaques par dictionnaire
- Problème du déni de service
  - Par définition les réseaux sans fil sont vulnérables aux attaques par déni de service
  - En créant du bruit, on empêche un réseau sans fil de fonctionner