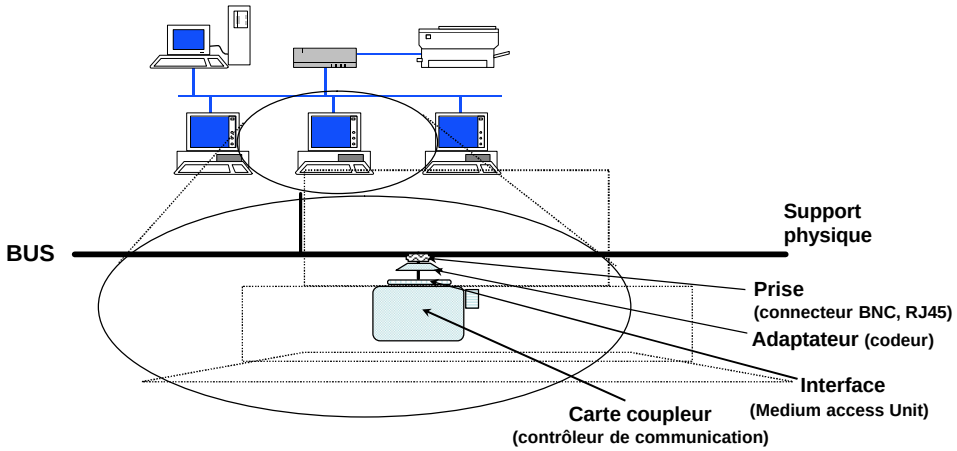
Partie 2

Sécurité des Réseaux Locaux Informatiques

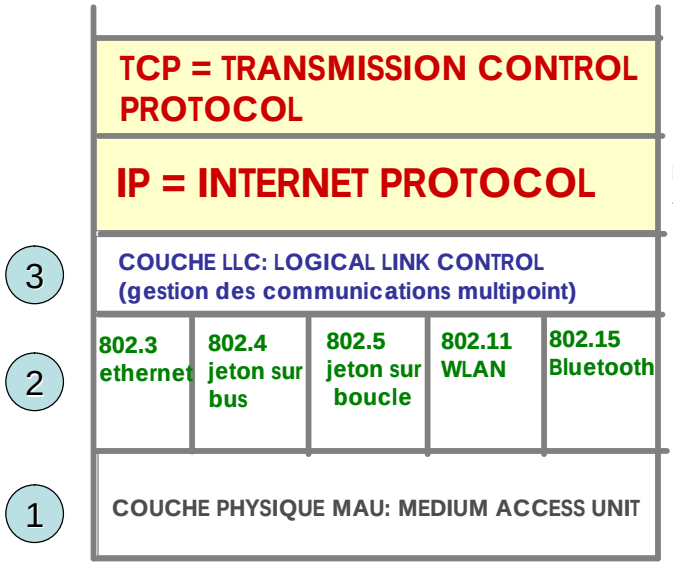
VLAN et WLAN

LES RESEAUX LOCAUX INFORMATIQUES
ETHERNET 10BASE5

- Utilisation d'un BUS
- Partage du support entre les stations au moyen d'un protocole de niveau 2 (Liaison) appelé MAC (Medium Access Control)



ARCHITECTURE
IEEE 802 LAN et WLAN

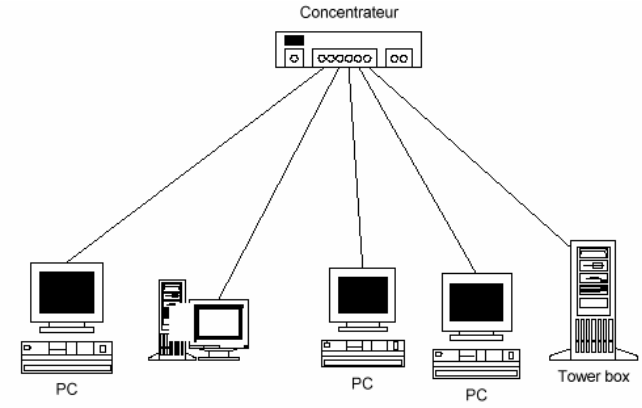


PROTOCOLE DE NIVEAU 4:
SERVICE DE TRANSPORT
CIRCUIT VIRTUEL CONNECTE
AVEC CONTROLE DE FLUX

PROTOCOLE DE NIVEAU 3:
ADRESSAGE ET ROUTAGE IP

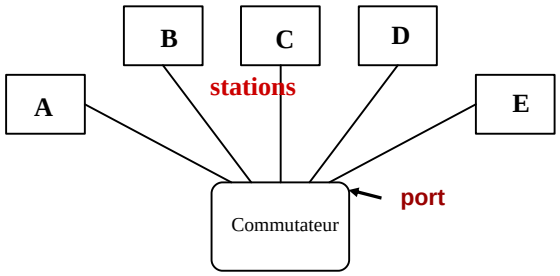
COUCHE MAC:
MEDIUM ACCESS CONTROL

ETHERNET 802.3
10 base T (1990)



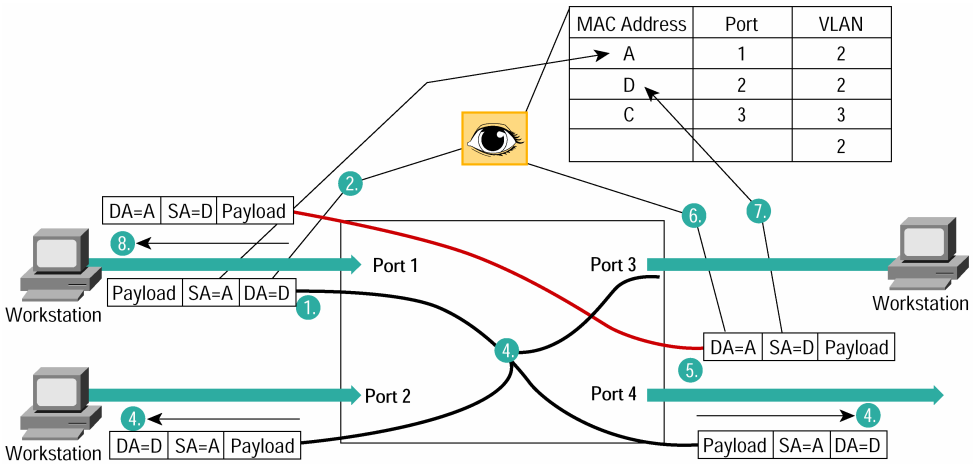
- Utilisation d'une topologie en étoile autour d'un HUB (migration facile)
- Faciliter la gestion du parc de terminaux
- Ne supprime pas les collisions
- Les stations se partagent les 10 Mbps

ETHERNET COMMUTE
PRINCIPES



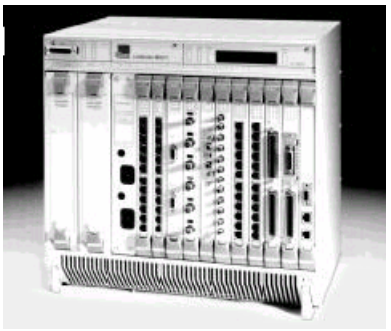
- **Réduire les collisions pour accroitre les débits**
- **Utilisation d'une topologie en étoile (migration facile)**
- **Remplacer le nœud central passif (HUB) par un commutateur.**
- **chaque station possède 10 Mbps entre elle et le Commutateur**
- **Mettre à peu de frais des réseaux virtuels (utilisation de table dans les commutateurs)**

SWITCH COMMUTE - APPRENTISSAGE



REPEATER / HUB / SWITCH

Répéteur/adaptateur (UNICOM)



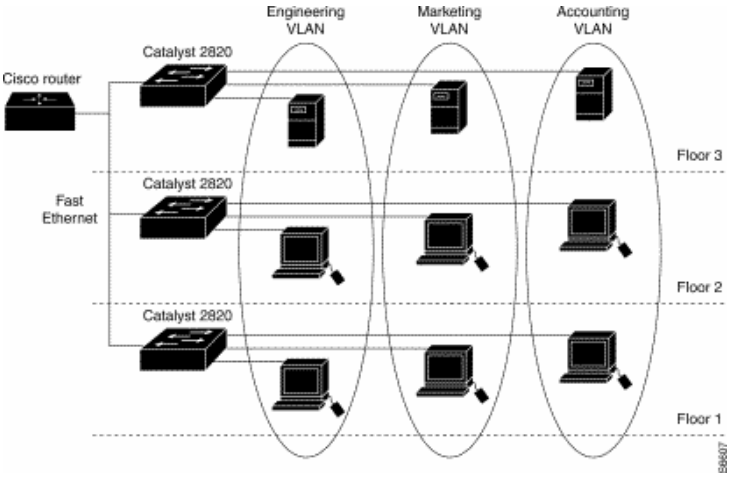
Switch multi Protocole (3com)

hubs 16/8 ports (HP)

Commutateur/ Switch Netgear

Switch empilables

VLAN



Typologie des VLAN

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

1. **Un VLAN de niveau 1 (aussi appelés VLAN par port, en anglais *Port-Based VLAN*) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur ;**
2. **Un VLAN de niveau 2 (également appelé VLAN MAC ou en anglais *MAC Address-Based VLAN*) consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station; le défaut est que chaque station doit être manuellement associée à un VLAN.**
3. **Un VLAN de niveau 3**

Typologie des VLAN (2)

3. Un VLAN de niveau 3 : on distingue plusieurs types de VLAN de niveau 3 :

- **Le VLAN par sous-réseau (en anglais *Network Address-Based VLAN*) associe des sous-réseaux selon l'adresse IP source des datagrammes. Solution souple car la configuration des commutateurs se modifient automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances car les informations contenues dans les paquets doivent être analysées plus finement.**
- **Le VLAN par protocole (en anglais *Protocol-Based VLAN*) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.**

VLAN et QOS

- IEEE 802.1p et 802.1q -

Tame Ethernet non 802.1p

Destination	Source	Type / Longueur

Tame Ethernet etendue 802.1p

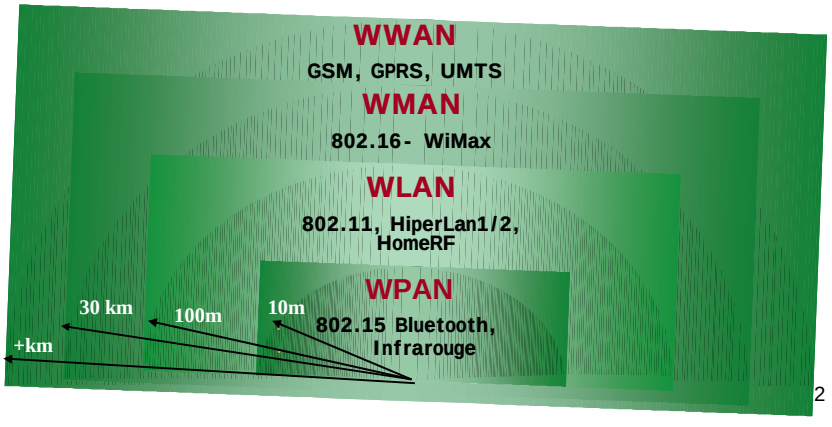
Destination	Source	Tag Control Info	Type / Longueur

Type de trame	Priorite	Cano-nical	802.1q VLQN identifiant
2 bytes	3 bits	3 bits	12 bits

Sous champ de controle	Description
Type de frame marquée	Toujours a 8100h (type trame Ethernet)
Champ priorité (802.1p)	Valeur representant le niveau de priorite
« Canonical »	Toujours a 0
802.1q VLQN identifiant	Numero d'identification du VLAN

Les réseaux WLAN

- **Réseaux locaux sans fil (Wireless Local Area Networks)**
- **Faire communiquer des dispositifs sans fil dans une zone de couverture moyenne**



Les standards réseaux sans fils

- **WPAN :**
  - **IEEE 802.15 (WiMedia)**
    - **IEEE 802.15.1 : Bluetooth**
    - **IEEE 802.15.3 : UWB (Ultra Wide Band)**
    - **IEEE 802.15.4 : ZigBee**
  - **HomeRF**
- **WLAN :**
  - **IEEE 802.11 (Wifi)**
    - **IEEE 802.11b**
    - **IEEE 802.11a**
    - **IEEE 802.11g**
    - **IEEE 802.11n**
  - **HiperLAN 1/2**
- **WMAN**
  - **IEEE 802.16 (WiMax)**
    - **IEEE 802.16a**
    - **IEEE 802. 16b**
  - **IEEE 802.20 (MBWA)**

Les technologies WLAN

- En 1985 les Etats-Unis ont libéré trois bandes de fréquence à destination de l'Industrie, de la Science et de la Médecine. Ces bandes de fréquence, baptisées **ISM (Industrial, Scientific, and Medical),** sont les bandes 902-928 MHz, 2.400-2.4835 GHz, 5.725-5.850 GHz.

- En Europe la bande s'étalant de 890 à 915 MHz est utilisée pour les communications mobiles (GSM), ainsi seules les bandes 2.400 à 2.4835 GHz et 5.725 à 5.850 GHz sont disponibles pour une utilisation radio-amateur.

- En 1990 : IEEE débute la spécification d'une technologie de LAN sans fil

Les technologies WLAN

- **IEEE 802.11 (IEEE)**
  - **Juin 1997: finalisation du standard initial pour les WLAN IEEE 802.11**
  - **Fin 1999 : publication des deux compléments 802.11b et 802.11a**
- **HiperLAN (ETSI)**
  - **1996: ratification de la norme HiperLAN/1 (bande des 5 GHZ, jusqu'à 24Mbs)**
  - **HiperLAN/2 (bande des 5 GHZ, jusqu'à 54Mbs)**
- **HomeRF**
  - **Mars 1998: HomeRF Working Group pour la domotique sans fil (supporte voix/données)**
  - **bande de 2,4 GHZ, 10 Mbs et passe à 20 Mbs**

Problèmes rencontrés dans les WLAN

- **Interférence avec d'autres ondes (Micro-ondes, équipements électroniques, autres réseaux sans fils adjacents)**
  - **Bandes de fréquences ISM : Industrial-Scientific-Medical**
  - **2,4 GHz comme Bluetooth (pas de licence d'exploitation requise)**
- **Longévité des batteries**
- **Inter-opérabilité**
- **Sécurité**
- **Qualité de Services**

La famille des standards IEEE 802

802.11x – Amendements

- **802.11a** - Vitesse de 54 Mbits/s (bande 5 GHz)
- **802.11b** - Vitesse de 11 Mbits/s (bande ISM 2,4 GHz)
- **802.11g** - Vitesse de 54 Mbits/s (bande ISM)
- **802.11n** - Vitesse de 100 Mbits/s (bande ISM)
- **802.11e** - Qualité de service
- **802.11x** – Amélioration de la sécurité (court terme) : WEP
- **802.11i** - Amélioration de la sécurité (long terme) : AES
- **802.11f** – itinérance : Inter-Access point roaming protocol

Wi-Fi ou 802.11b

- Basé sur la technique de codage physique DSSS : étalement de spectre à séquence directe (Direct Sequence Spread Spectrum);
- Mécanisme de variation de débit selon la qualité de l'environnement radio : débits compris entre 1 et 11 Mbits/s

Zone de couverture

Vitesses (Mbits/s)	Portée (Mètres)
11	50
5	75
2	100
1	150

À l'interieur des batiments

Vitesses (Mbits/s)	Portée (Mètres)
11	200
5	300
2	400
1	500

À l'extérieur des batiments

Sécurité dans le standard IEEE 802.11

Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :

1. **L'interception de données consistant à écouter les transmissions des différents utilisateurs du réseau sans fil**
2. **Le détournement de connexion dont le but est d'obtenir l'accès à un réseau local ou à internet**
3. **Le brouillage des transmissions consistant à émettre des signaux radio de telle manière à produire des interférences**
4. **Les dénis de service rendant le réseau inutilisable en envoyant des commandes factices**

Sécurité dans le standard IEEE 802.11

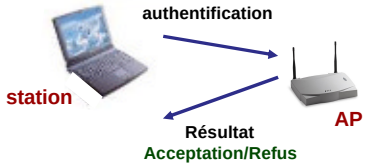
Tous les mécanismes de sécurité initiaux peuvent être déjoués : avec les Outils « AirSnort » or « WEPcrack »

- **A court terme**
  1. **Wired Equivalent Privacy (WEP) étendue**
     - **clé de cryptage passe de 64 à 128 bits**
     - **Défaut : une seule et même clé pour toutes les stations**
- **A moyen terme**
  2. **Wifi Protected Access (WPA)**
     - **Double authentification du terminal sur la base du port physique (802.1x) puis par mot de passe ou carte à puce via un serveur RADIUS (EAP).**
     - **TKIP : Temporal Key Integrity Protocol (TKIP) : clé différente par station et par paquet avec renouvellement périodique;**
- **A long terme**
  3. **802.11i basé sur AES (Advanced Encryption Standard)**
     - **WPA + algo. de cryptage plus robuste et moins gourmand en resource**

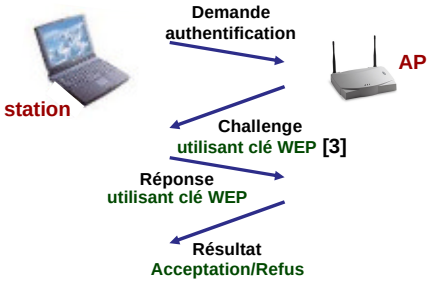
Les services de station -1-

- **authentification**
  - **processus suivant l'accès à une cellule et précédent une association**
  - **prévention de l'accès aux ressource du réseau**
  - **en deux modes :**

Open System Authentication

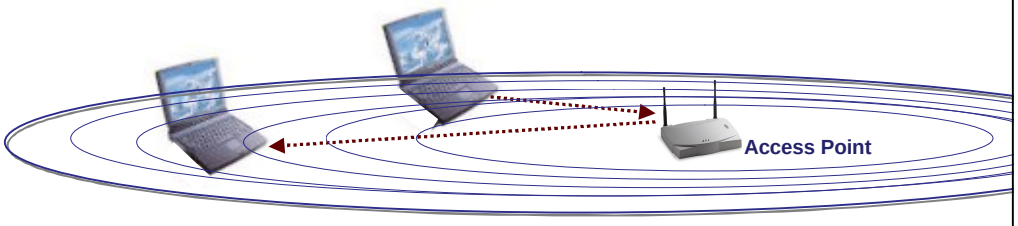


Shared Key Authentication



Topologies IEEE 802.11 -1-

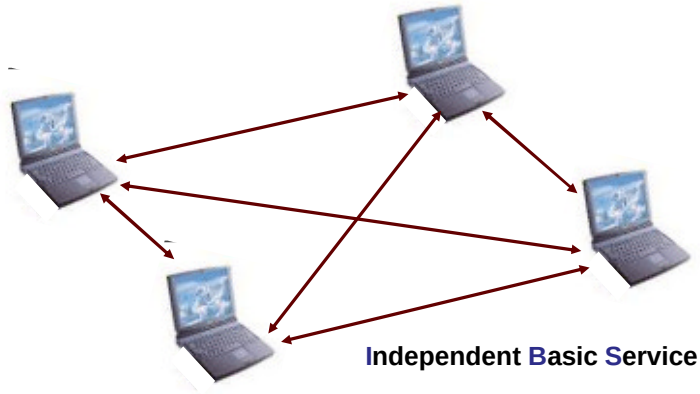
- **Architecture basée infrastructure**
  - **architecture cellulaire**
  - **architecture BSS (Basic Service Set)**
  - **chaque cellule (BSS) est contrôlée par une station de base appelée Point d'accès : AP (Access Point)**



Basic Service Set

Topologies IEEE 802.11 -2-

- Architecture ad hoc
  - aucune infrastructure
  - architecture IBSS (Independent Basic Service Set)



Independent Basic Service Set

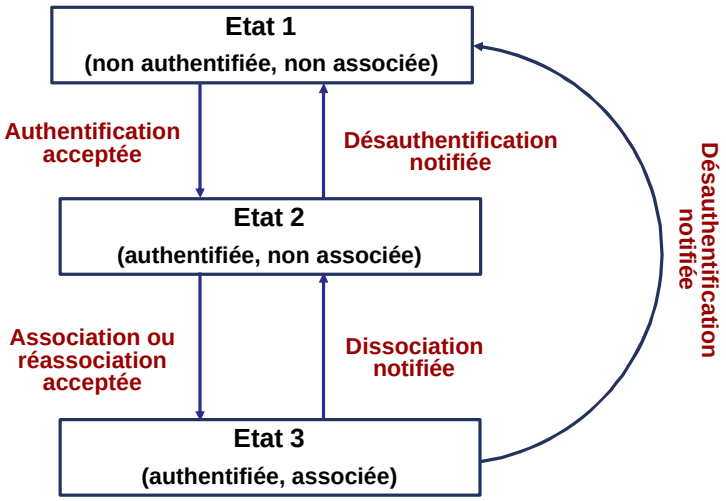
Au cœur de la couche MAC 802.11

- fonctions sous-couche MAC
  - accès au réseau
  - sécurité (authentification, confidentialité)
  - économie d'énergie
  - accès au médium
  - fragmentation des longues trames
  - Qualité de Services

Initialisation : Accès au Réseau

- **Allumer station : phase de découverte**
  - **Découvrir l'AP et/ou les autres stations**
  - **La station attend de recevoir une trame de balise (Beacon) émise toute les 0,1 sec.**
  - **A la réception de « Beacon » prendre les paramètres (SSID & autres)**
  - **SSID Service Set Identifier : nom du réseau (chaîne de 32 caractères max.)**
- **Présence détectée : rejoindre le réseau**
  - **Service Set Id (SSID) : nom du réseau de connexion**
  - **Synchronisation**
  - **Récupération des paramètres de la couche PHY**
- **Négocier la connexion**
  - **Authentification & Association**

Diagramme d'états d'une station



Accès au medium

Deux méthodes :

- **DCF (Distributed Coordination Function)**
  - **basé sur le mécanisme CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) et Acquittement positif**
  - **utilisé en mode Ad hoc et AP**
- **PCF (Point Coordination Function)**
  - **basé sur l'interrogation (Polling)**
  - **utilisé en mode AP uniquement**

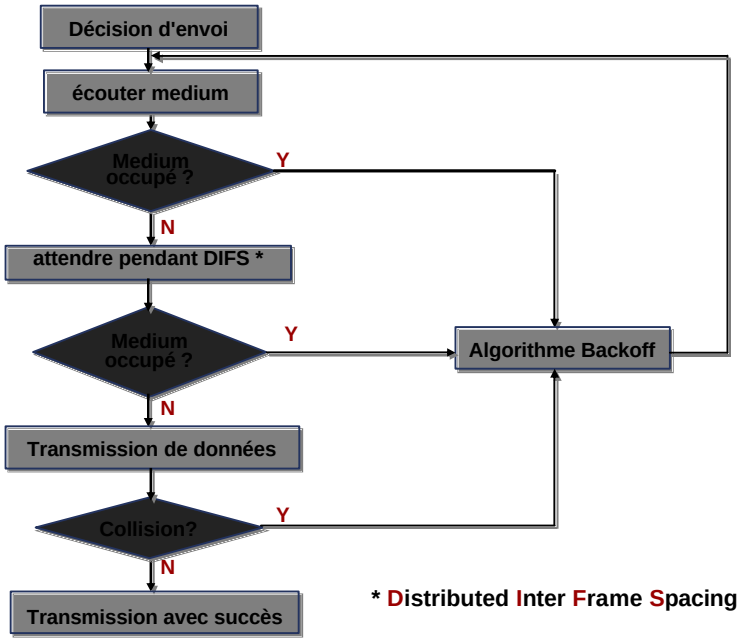
les deux mécanismes peuvent coexister dans une même cellule

CSMA/CA

Le CSMA/CA en mode DCF est basé sur :

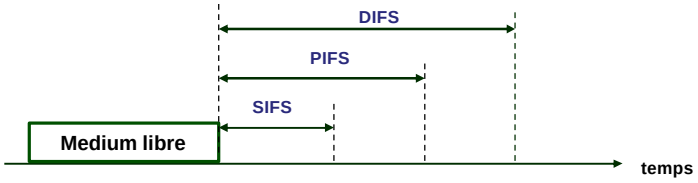
1. L'écoute du canal avant transmission
2. Si canal occupé alors tirage aléatoire d'un délai d'attente (algo. Backoff) puis attente durant une durée prédéfinie de 234 ms appelée DIFS DCF Inter Frame Space;
3. Si canal libre alors :
   1. Annonce de l'intention d'émettre par la source (trames RTS)
   2. Annonce de l'intention de recevoir par la destination ou le Point d'accès (trames CTS) : car problème des stations cachées.
4. Envoi des trames en rafales avec une temporisation entre 2 trames d'une durée de 28 ms (IFS : Inter Frame Sequence)
5. Acquittement positif des trames par le destinataire (trames ACK)

DCF - CSMA/CA



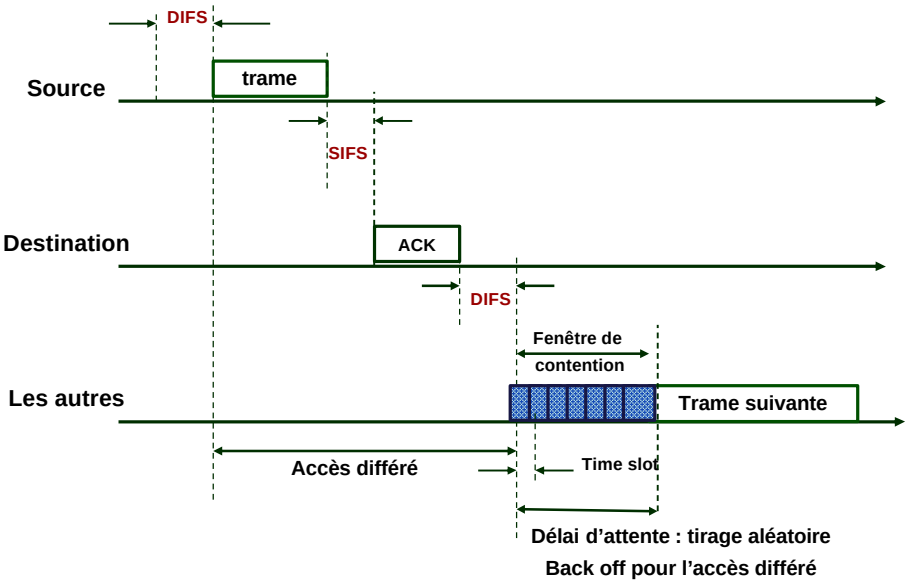
* Distributed Inter Frame Spacing

intervalles d'accès au medium



- IFS (Inter Frame Space)
  - SIFS (Short Inter Frame Space) : 28 µs
    - plus grande priorité (utilisé pour les trames prioritaires comme CTS, ACK
  - PIFS (PCF Inter Frame Space) : SIFS + 78 µs
    - utilisé par les stations opérants en mode PCF
    - priorité moyenne, pour des applications time-bounded
  - DIFS (DCF Inter Frame Space) : PIFS + 128 µs
    - utilisé par les stations opérants en mode DCF
    - priorité la plus basse, pour données best effort

DCF – algorithme backoff -1-



802.11b – Grandeurs Physiques

Tableau 1 – Récapitulatif des caractéristiques de la couche physique 802.11b

Variable	Valeur
Sensibilité des récepteurs (pour l'Europe)	– 80 dBm
Puissance maximale	20 dBm
Portée	30 à 60 m
SIFS	10 µs
Slot time	20 µs
Débit brut maximal	11 Mbit/s
Débit net approximatif	5 Mbit/s
Nombre maximal d'utilisateurs par AP	63
Nombre maximal d'utilisateurs par cellule	189

(1) dBm pour des puissances en milliwatts