

# Les Technologies sans fils

Plan :

- 1) Généralités
- 2) Les réseaux orientés téléphonies  
GSM, GPRS, UMTS, LTE
- 3) Etude d'une norme particulière: 802.11



# Généralités

**But : Communiquer avec différents systèmes sans utiliser de liaison filaire**

Plusieurs normes concurrentes :

- IrDA,
- liaison hertzienne, GSM, GPRS, UMTS, LTE (Long Term Evolution),...
- 802.11, 802.15, 802.16,...

Chaque norme correspond à une application bien spécifique.

WLAN : Wireless Local Area Network *a été défini par*

WECA : Wireless Ethernet Compatibility Alliance

( 3com, Apple, Compaq, Dell, Lucent Technologies, Nokia, ....)

## Utilisation de la bande ISM : Industriel, Scientifique et Médical

VLF	LF	MF	HF	VHF	UHF	SHF	EHF	IR
-----	----	----	----	-----	-----	-----	-----	----

9 kHz    30 kHz    300 kHz    3 MHz    30 MHz    300 MHz    3 GHz    30 GHz    300 GHz    THz

VLF : Very Low Frequencies -> navigation maritime

LF : Low Frequencies -> aéronautique

MF : Medium Frequencies -> 500Khz et 2182 Khz = S.O.S, entre 535 et 1705 khz= Radio AM

HF : High Frequencies -> **6,7 Mhz=ISM**, radio-diffusion sur onde courte

VHF : Very High frequencies ->entre 55 et 88 Mhz=Télé, entre 88 et 108 Mhz=radio FM, communication satellite LEO, trafic aérien

UHF : Ultra High Frequencies -> entre 470 et 806 Mhz=Télé, **900, 1800, 2400 Mhz=ISM**, trafic aérien, 1600 Mhz=GPS, communication satellite LEO et MEO, **2400 Mhz = micro-onde**

SHF : Super High Frequencies-> **5 et 5,7 Ghz = ISM**, communication satellite

EHF : Extremely High Frequencies -> recherche spatiale





# Généralités

- Vers 1960, Création du port RS232 pour relier **deux** systèmes
- Amélioration de ce protocole pour souris et clavier -> PS2
- Evolution logique vers le sans fil, -> **IrDA**
  - **Pb : permet seulement la communication entre deux systèmes**
- Passage à l'USB pour relier plusieurs périphériques
- Evolution logique vers le sans fil, -> Bluetooth v1.0, puis depuis 11/2004 Bluetooth v2.0
- UWB : Ultra Wide Band → successeur de usb sans fil (BP: de 3,1 à 10 Ghz)

## **Norme :**

802.15.1 : Bluetooth v1.0 ➡ **WPAN** : Wireless Personal Area Network

802.15.2 : Amélioration de la norme sur la QoS

802.15.3 : Augmentation du débit et de la portée  
( 54 Mbps et 100m, BP : 2,4 Ghz)

802.15.4 : Norme Zigbee ( 900 Mhz, 2,4 Ghz)



# Généralités

## Norme 802.16 :

- Réseau sans fil à large Bande
- Utilisation de la technologie BWA (Broadband Wireless Access)
- Débit jusqu'à 70Mb/s sur de grandes distances ( 20 km), BP de 2 à 11 Ghz
- Technique MIMO (Multiple Input/Multiple Output) -> plusieurs antennes en émission et en réception

 Consortium WiMax  
(*Worldwide Interoperability for Microwave Access*)

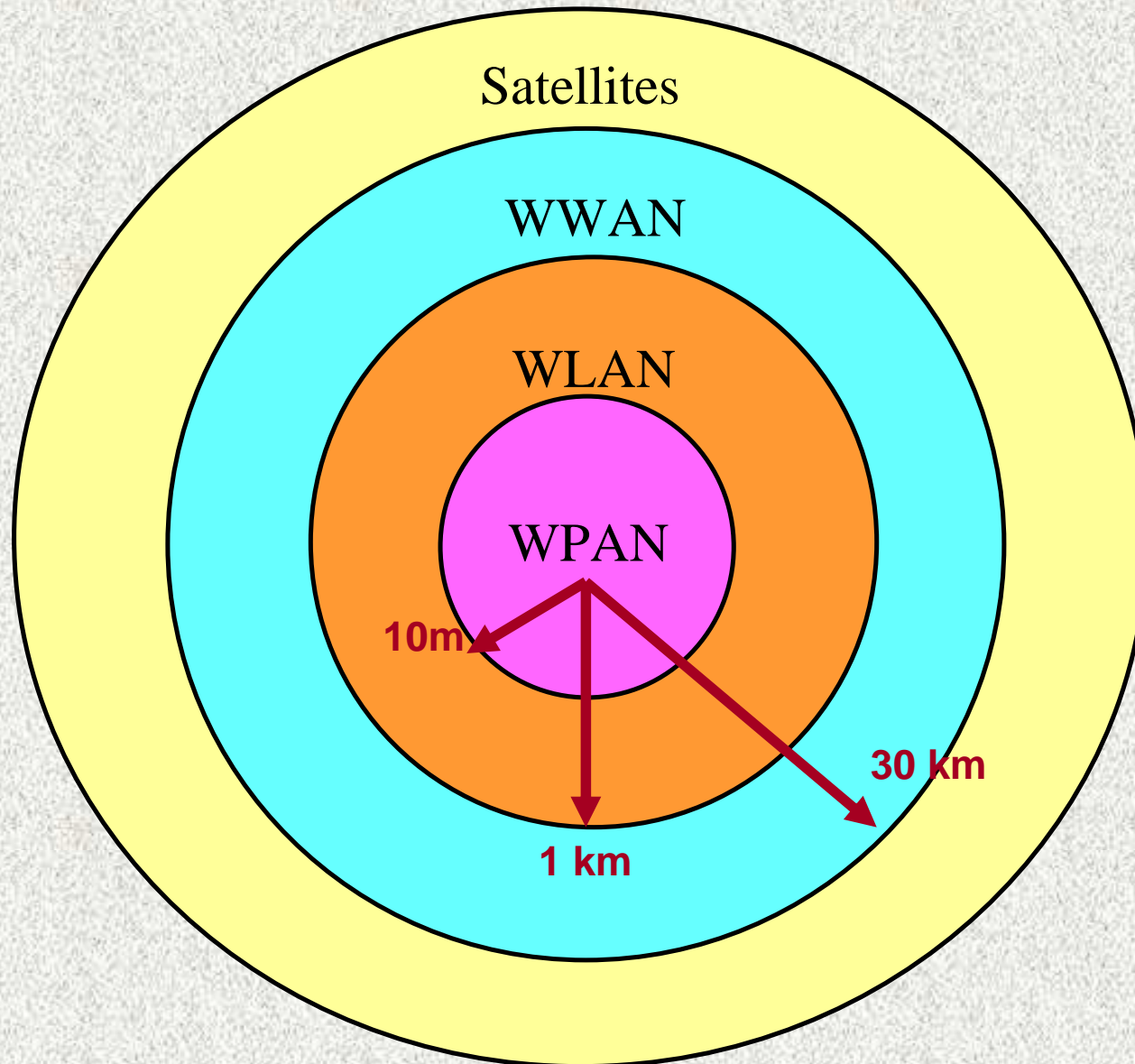
Définition de la norme 802.16a, b, i, ....

But : relier les villages ne pouvant bénéficier de l'ADSL  
BLR ( Boucle Local Radio)

Actuellement, 2 licences WiMax par région + 1 nationale

- deux choisis par l'ARCEP ( auvergne : Maxtel et Bolloré)
- une appartenant à Altitude Telecom ( racheté par Iliad (free))

# Généralités





# La norme 802.11

La norme **802.11** définit la couche 1 et 2 pour une liaison sans fil utilisant des ondes électromagnétiques :

- La couche physique
  - ◆ codage DSSS, FHSS, IrDA
- La couche Liaison de données
  - ◆ couche LLC et couche MAC

Cette norme permet d'avoir un débit de 1 ou 2Mb/s et elle utilise un accès au médium par compétition ( méthode CSMA/CA)  
(CA : Collision Avoidance)

**Mais, évolution de cette norme**

**Wi-Fi ( Wireless Fidelity)**

Nom de la norme	Nom	Description
802.11a	Wifi5	Débit : 54Mb/s, 8 canaux radio dans la bande de fréquence des 5 Ghz.
802.11b	Wifi	Débit : 11Mb/s, portée 300m, 3 canaux radio dans la bande de fréquence des 2,4 Ghz
802.11c	Pontage	Etablissement d'un pont pour la norme 802.11d
802.11d	International	Etablit les règles à respecter entre les différents pays pour transporter les données 802.11
802.11e	QoS	Définition d'une QoS
802.11f	Roaming	Interopérabilité entre les différents points d'accès pour permettre l'itinérance ( définition de l'IAPP)
802.11g	Wifi	Débit : 54MB/s, portée 300m, compatible avec 802.11b
802.11h	?	Norme proche de HyperLan 2, réseau européen
802.11i	WPA2	Amélioration de la sécurité pour les normes a, b et g.
802.11j	?	Norme pour la communauté japonaise
802.11n	Wifi	Débit : 320 Mb/s avec intégration de la norme i



- **2 Sortes d'équipement**

- *Une station sans fil*

- un ordinateur muni d'une carte Wifi  
(carte PCI, PCMCIA, adaptateur USB, carte compactflash, ...)

- *Un point d'accès ( Access Point) ou borne sans fil*

- joue le rôle de pont entre réseau filaire et sans fil
- équipé :
  - d'un émetteur/récepteur radio
  - d'une carte réseau filaire
  - d'un logiciel de pontage conforme à la norme 802.11d



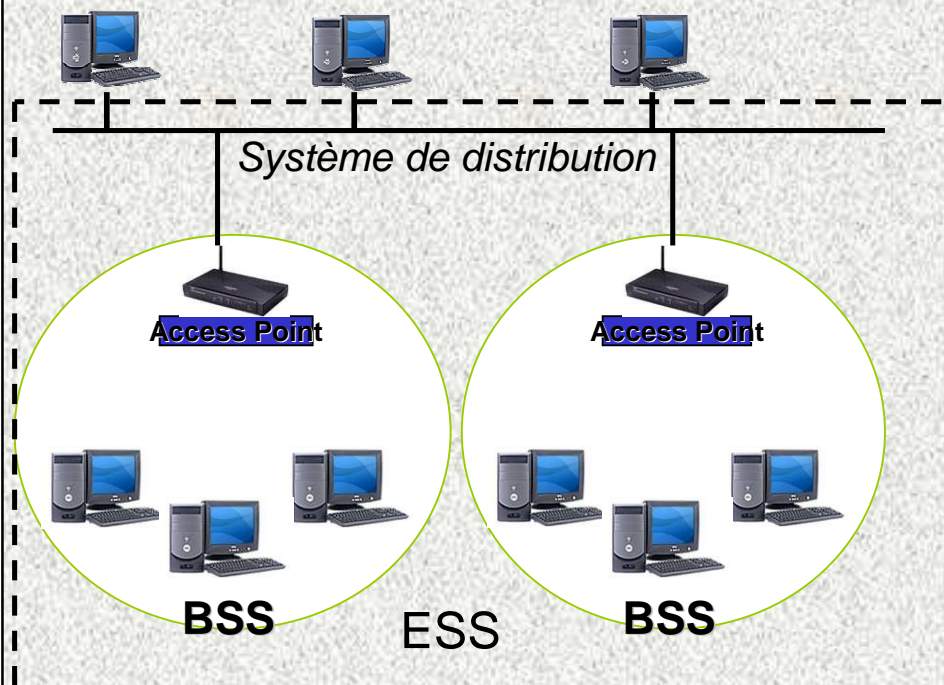
Access Point

## ◆ Mode Infrastructure

- Au minimum , 1 AP + postes sans fil

➡ BSS : Basic Service Set

- identifié par un BSSID ( abrégé en SSID -> Service Set Identifier)



- Plusieurs BSS forment un ESS ( Extended Service Set) relié par un DS ( Système de Distribution)

- identifié par un SSID

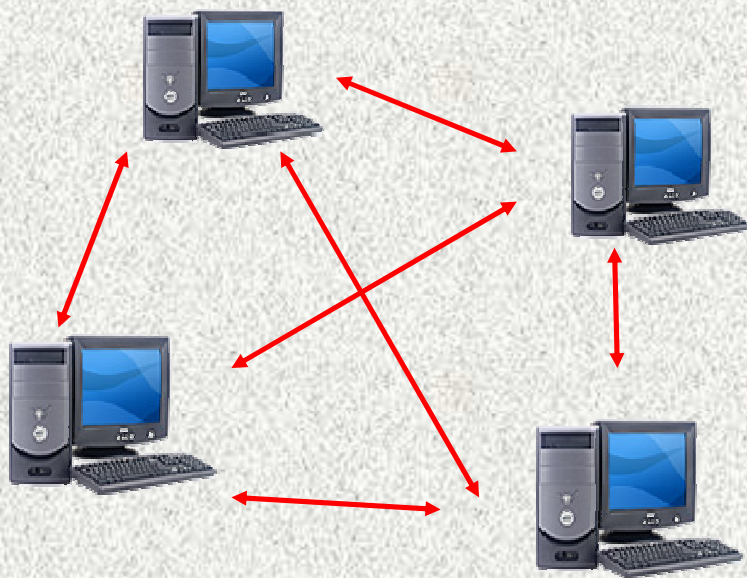
*Possibilité de roaming si même SSID*

## ◆ Mode Ad-Hoc

- Aucun AP, que des postes sans fil

➡ IBSS : Independant Basic Service Set

- identifié par un SSID



- Problème pour le routage

$$\left. \begin{array}{l} \text{si } A \dashrightarrow B \\ \text{si } B \dashrightarrow C \end{array} \right\} \text{ alors } A \nrightarrow C$$

*Tout le monde doit voir tout le monde  
ou  
Pc configuré comme routeur*



# Architecture en couches

## ◆ WiFi

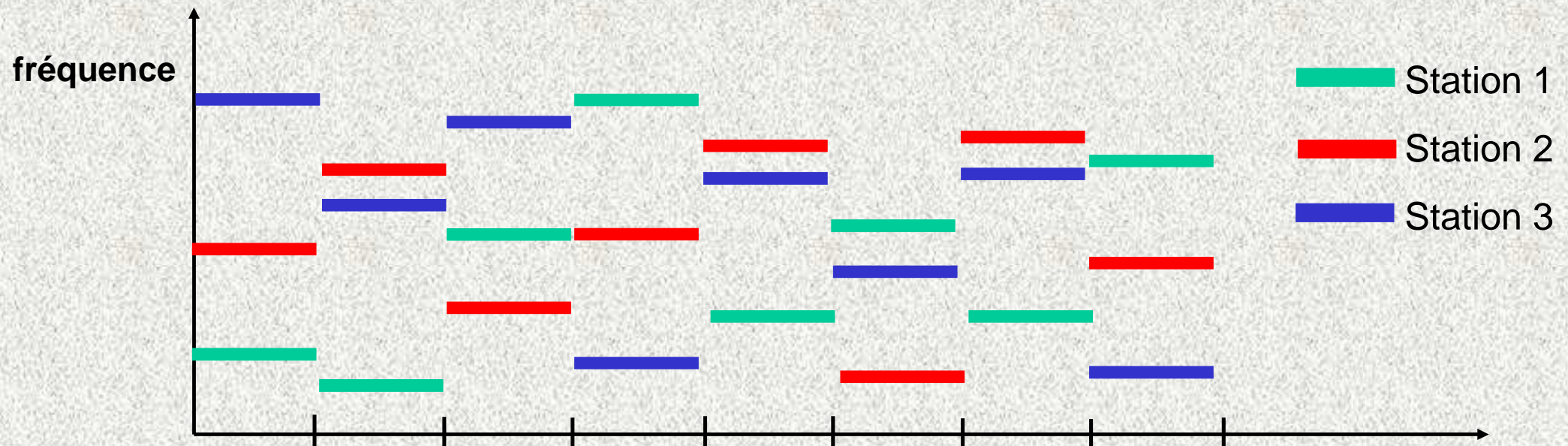
PLCP : Physical Layer Convergence Procedure

PMD : Physical Medium Dependant



## ◆ FHSS : Frequency Hoping Spread Spectrum

- Découpage de la bande de fréquence en 79 canaux de 1 Mhz, puis transmission en utilisant une combinaison de canaux connue de toutes les stations ( 78 combinaisons possibles)
- Emission sur un canal pendant 400ms, puis changement de canal,etc...
- Bande de fréquence entre 2,4 Ghz et 2,4835 GHz



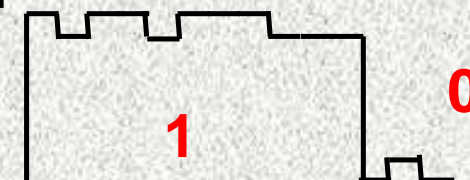
## ◆ DSSS : Direct Sequence Spread Spectrum

- Découpage de la bande de fréquence en 14 canaux de 22 Mhz, mais recouvrement des canaux -> utilisation des canaux 1, 6 et 11

Canal	1	2	3	4	5	6	7
Fréquence (Ghz)	2,412	2,417	2,422	2,427	2,432	2,437	2,442
Canal	8	9	10	11	12	13	14
Fréquence (Ghz)	2,447	2,452	2,457	2,462	2,467	2,472	2,483

Pour éviter les collisions, on utilise le « chipping », c'est à dire faire une petite modulation pour faire apparaître plusieurs bits (*séquence barker*, 11 bits) lorsque l'on émet un seul bit ➡ redondance de l'information


bit 1 = 10110111000, bit 0 = 01001000111






## ◆ Législation française

- Equipement fonctionnant sur 2400-2483,5 MHz autorisation de puissance :
  - 10 mW à l'intérieur
  - 2,5 mW à l'extérieur
- Equipement fonctionnant sur 2446,5-2483,5 Mhz autorisation de puissance de 100mW à l'intérieur et à l'extérieur (autorisation obligatoire ?)

Canal 10 : Fréquence 2,457 Ghz, mais BP de 20 Mhz d'où  
fréquence min -> 2, 447 Ghz  OK

Canal 9 : Fréquence 2,452 Ghz, mais BP de 20 Mhz d'où  
fréquence min -> 2, 442 Ghz  Pb

Donc, en France, utilisation des canaux 10 à 13 -> 1 seul AP  
aux USA, utilisation des canaux 1 à 11.

Interdiction du 802.11a en extérieur.

## ◆ OFDM : Orthogonal Frequency Division Multiplexing

- Basé sur la fréquence des 5 Ghz ou du 2,4 Ghz
  - Division du canal principal en sous canaux utilisés en parallèle
  - Un canal principal de 20 Mhz est divisé en 52 canaux de 300 Khz
  - Modulation différente pour chacun des canaux.
- 
- Très utilisé pour le 802.11a  
8 canaux de 20 Mhz entre 5,15 Ghz et 5,35 Ghz

## ◆ 802.11 : utilisation de modulation de phase

-> codage PSK : Phase Shift Keying

- Technique BPSK : Binary Phase Shift Keying valence = 2
- Technique QPSK : Quadrature PSK , valence = 4, d'ou débit \*2
- Technique CCK : Complementary Code Keying, basé sur séquence de Baker
  - > encodage de 4 bits simultanément -> débit = 5,5 Mb/s
  - > encodage de 8 bits simultanément -> débit = 11 Mb/s

Technologie	Fréquence	Modulation	Débit max
802.11	2,4 Ghz	BPSK	1 Mb/s
802.11	2,4 Ghz	QPSK	2 Mb/s
802.11b	2,4 Ghz	DSSS, CCK (4b)	5,5 Mb/s
802.11b	2,4 Ghz	DSSS, CCK (8b)	11 Mb/s
802.11a	5 Ghz	OFDM	54 Mb/s
802.11g	2,4 Ghz	OFDM	54 Mb/s



## ◆ La couche MAC

- Similaire à la couche Mac ethernet
- **Fonctionnalité**
  - Contrôle d'accès au support
  - Contrôle d'erreur par CRC
  - Fragmentation et réassemblage
  - Gestion de l'énergie
  - Gestion de la mobilité
- **Deux méthodes d'accès pour le 802.11a, b, g**
  - **DCF** ( Distributed Coordination Function ) : utilisation pour les données asynchrones, collisions possibles
  - **PCF** ( Point Coordination Function ) : utilisation pour les données synchrones, pas de collision.

# Distributed Coordination Function

## ◆ DCF

### • Basé sur un accès CSMA/CA

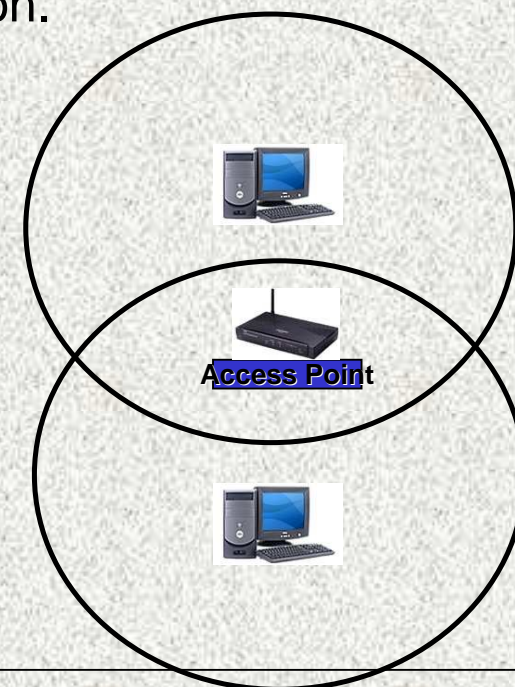
Pour émettre :

- On écoute le support ( ondes)
- Si libre pendant un temps donné ( *DIFS*, Distributed Inter Frame Space)
  - > transmission d'une trame Ready To Send (RTS) contenant les informations sur le volume de données et la vitesse de transmission.
  - > réception d'un Clear To Send ( CTS)
  - > envoi des données
  - > récupération d'un ACK pour chaque trame

Une station qui veut émettre doit attendre la libération du support.  
( NAV : Network Allocation Vector)

Pourquoi un ACK pour chaque trame ?

➡ 2 stations peuvent vouloir émettre en même temps sans se voir.

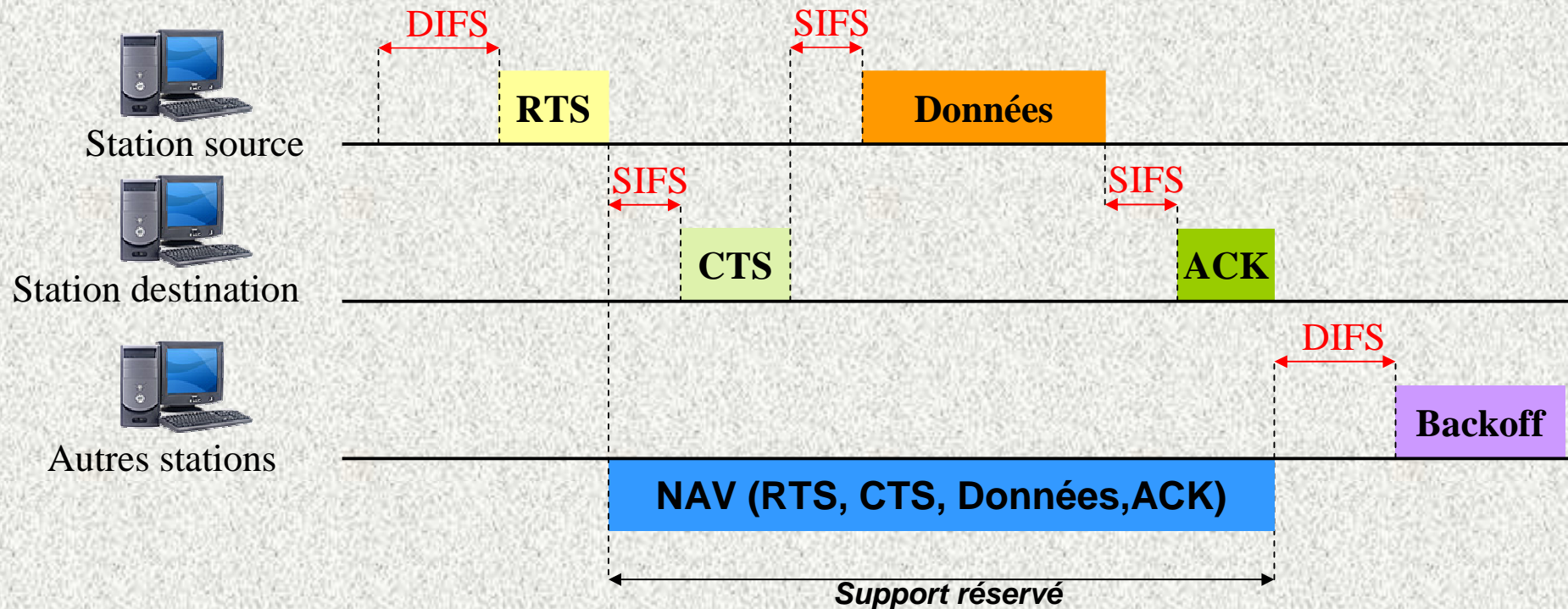


# Distributed Coordination Function

## ◆ DCF

### • Exemple de dialogue

**SIFS** : Short Inter Frame Space < **PIFS** : Prioritary < **DIFS** < **EIFS** (Extented)



**Backoff** : temps d'attente aléatoire pour que toutes les stations n'émettent pas en même temps.



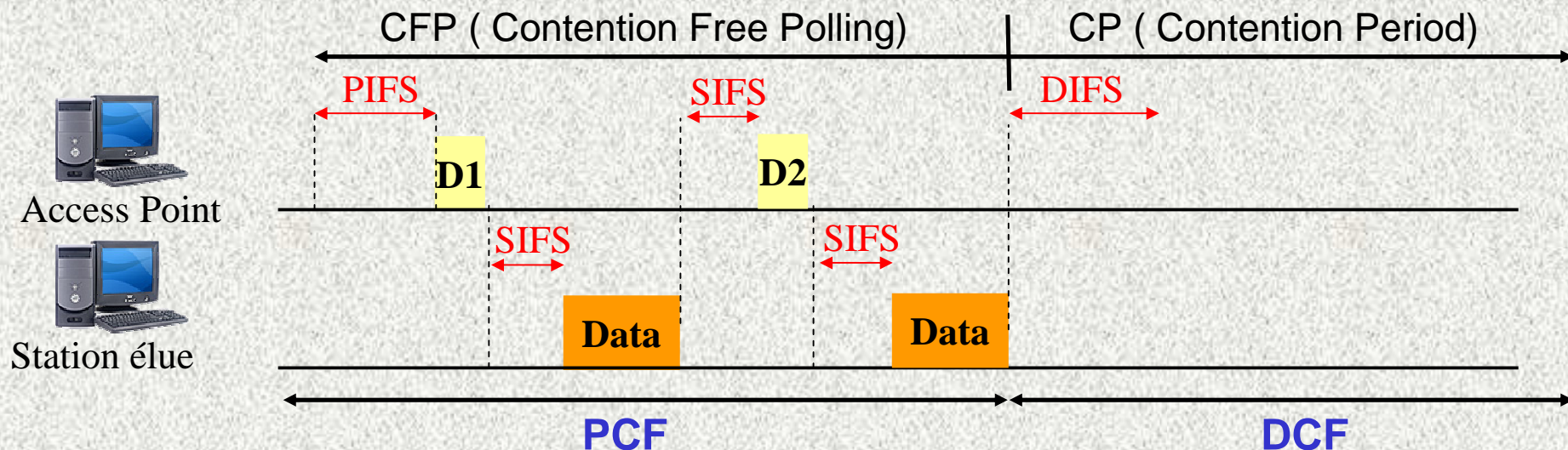
# Point Coordination Function

## ◆ PCF

- Permet le transfert de données temps-réel
  - > utilisation d'un AP qui prend le contrôle du support et choisit les stations ayant le droit d'émettre (mode infrastructure)
  - > utilisation d'un temps PIFS pour prendre la main.

( non implémenté actuellement !!!)

- Le point d'accès scrute les différentes machines en mode PCF, puis passe en mode DCF s'il reste du temps.
  - > reprend facilement la main car temps d'attente PIFS < DISF



# Les Trames WiFi (1)

## ◆ 3 types de trames

- Trames de *données*
- Trames de *contrôle* (RTS, CTS, ACK)
- Trames de *gestion*

## ◆ Toutes les trames sont composés des composants suivants :

Préambule	En- tête PLCP	Données MAC	CRC
-----------	---------------	-------------	-----

PLCP : Physical Layer Convergence Procedure  
-> renseigne sur la composition de la trame

Le préambule et le PLCP varie en fonction de l'interface physique utilisée  
(FHSS, DSSS, IrDA, OFDM)

# Les Trames WiFi (2)

## ◆ FHSS

- Préambule
  - 80 bits (Synch): alternance 0 et 1 pour la synchronisation
  - 16 bits (SFD) : début de trame -> 0000110010111101
- En-tête :
  - 12 bits (Length) : longueur de la trame
  - 4 bits (Payload Signalling Field) : débit utilisé
  - 16 bits : CRC

## ◆ DSSS

- Préambule
  - 128 bits (Synch): alternance 0 et 1 pour la synchronisation
  - 16 bits (SFD) : début de trame -> 11110011101010000
- En-tête :
  - 8 bits (Signal) : débit utilisé
  - 8 bits (Service): non utilisé-> que des 0
  - 16 bits (Length) : longueur de la trame
  - 16 bits : CRC



# Les Trames WiFi (3)

## ◆ IrDA

- Préambule
  - 73 bits (Synch): synchronisation
  - 4 bits (SFD) : début de trame
- En-tête :
  - 3 bits (Data rate) : débit utilisé
  - 32 bits : (Data Control Level Adjustment) : ajuste la vitesse
  - 16 bits (Length) : longueur de la trame
  - 16 bits : CRC

## ◆ OFDM

- Préambule
  - 12 symboles: synchronisation
- En-tête :
  - 4 bits (Rate) : débit utilisé
  - 1 bit (Reserved): non utilisé-> que des 0
  - 4 bits (Length) : longueur de la trame
  - 1 bit (Parity) : calcul de parité f
  - 10 bits : Tail+service, non utilisé -> que des 0

# Les Trames WiFi (4)

## ◆ Couche MAC pour les trames de données

Contrôle de trame 2 octets	Durée/ID 2 octets	Adresse 1 6 octets	Adresse 2 6 octets	Adresse 3 6 octets	Séquence 2 octets	Adresse 4 6 octets
Corps de la trame 0 à 2312 octets			CRC 4 octets			

## ◆ Contrôle de trame

Version de protocole (2 bits)	Type (2 bits)	Sous-Type (4 bits)	To DS (1 bit)	From DS (1 bit)	More Frag (1 bit)	Retry (1 bit)	Power Mgt (1 bit)	More Data (1 bit)	WEP (1 bit)	Order (1 bit)
----------------------------------	------------------	-----------------------	------------------	--------------------	----------------------	------------------	----------------------	----------------------	----------------	------------------

Version : actuellement, 00

Type : 3 types, plusieurs sous-types (00 : gestion, 01:contrôle, 10 : données)

To DS ou From DS : trame vers ou en provenance du système de distribution

More fragment : 1, trame fragmenté et pas dernier fragment, 0 sinon

Retry : 1 , retransmission

Power management : 1 , économie d'énergie, 0 actif

More Data : 1 si d'autres données à faire parvenir à la station

WEP : trame chiffrée ou non

order : Trame ordonné ou non

# Les Trames WiFi (5)

## ◆ Couche MAC pour les trames de données

Champ « *durée/ID* » : identifiant pour des trames polling de contrôle, ou durée pour calculer le NAV

Champ « *Adresse* » : même format que les adresses Mac ( 6 octets)

- DA : Destination Adresse : destination de la trame : individuelle ou groupe
- SA : Source Adresse : source de la trame : individuelle
- RA : Receiver Adresse : destination des données : individuelle ou groupe
- TA : Transmitter Adresse : source des données : individuelle
- BSSID : soit adresse MAC de l'AP, soit IBSS.

To DS	From DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	DA	SA	BSSID	Aucune
0	1	DA	BSSID	SA	Aucune
1	0	BSSID	SA	DA	Aucune
1	1	RA	TA	DA	SA

Champ « *contrôle de séquence* » : numérotation des trames



# Les Trames WiFi (6)

## ◆ Couche MAC pour les trames de contrôle

### Trame RTS

Contrôle de trame 2 octets	Durée 2 octets	RA 6 octets	TA 6 octets	FCS 2 octets
-------------------------------	-------------------	----------------	----------------	-----------------

### Trame CTS

Contrôle de trame 2 octets	Durée 2 octets	RA 6 octets	FCS 2 octets
-------------------------------	-------------------	----------------	-----------------

### Trame ACK

Contrôle de trame 2 octets	Durée 2 octets	RA 6 octets	FCS 2 octets
-------------------------------	-------------------	----------------	-----------------

## ◆ Quelques mot-clés pour la sécurité

- authentification
- confidentialité
- intégrité
- disponibilité
- non répudiation

## ◆ Les types d'attaque :

- Ecoute passive ou active → permet l'interception de données (WAR-CHALKING)  
→ facile à réaliser car les données sont émises dans un rayon, difficilement détectable
- Intrusion réseau (intrusion, usurpation) → par les employés, par virus,...
- Le brouillage radio (facilement détectable, mais très efficace)
- Les dénis de services

## ◆ Les contres mesures

- Limiter la puissance d'émission des bornes si possible  
éviter d'arroser le quartier
- Désactivation des services d'administration disponible (passwd admin)  
ou fermeture de port pour limiter les accès  
changement des mots de passes par défaut
- Changement de SSID par défaut (attribution d'un SSID)  
mais transmis en général par AP ou en méthode Ad-Hoc → Pb
- Désactivation du Broadcast du SSID  
mais visible dans les trames lors de l'association
- Filtrer les adresses MAC : utilisation des ACL (Access LISTS) des clients RLAN au  
niveau des bornes d'accès  
mais possibilité de « voler » une adresse MAC ( MAC Spoofing)
- Crypter les données



## ◆ Couche MAC pour la sécurité

### Le cryptage

- Utiliser un codage pour les données

- l'implémentation WEP (Wired Equivalent Privacy) (clé sur 40 bits / 104bits) donnée par les utilisateurs auquel est rajouté un vecteur d'initialisation (24 bits).

Fonctionnement : chiffrement RC4 en utilisant clé + vecteurs d'initialisation (IV)

message envoyé = (M.c(M)) xor RC4(IV . K)

$$\left\{ \begin{array}{l} c(M) = \text{checksum de M et K} = \text{clé} \\ \text{le RC4 donne des séquences pseudo-aléatoires} \end{array} \right.$$

Le vecteur d'initialisation change à chaque trame envoyé, on lui rajoute 1

( assez facilement crackable si on connaît le 1er octet de M et IV)

Pb : faiblesse d'implémentation dans IV commencent à 0 puis  
incrémentés de 1 à chaque envoi, vecteurs faibles ....

Actuellement, quelques dizaines de minutes pour cracker clé WEP

Si utilisation de WEP, alors codage supplémentaire : ssl, Ipsec, ssh,...

## ◆ Couche MAC pour la sécurité

### Le cryptage (suite)

- Utiliser la norme 802.1x ( WPA : Wifi protected Access ou WPA2)

=> concerne spécifiquement l'authentification

- 3 acteurs :
  - > le client (demandeur ou supplicant)
  - > le point d'accès relais  
(NAS : Network Access Server)
  - > le serveur d'authentification = serveur RADIUS

codage en utilisant les trames **EAP** : Extensible Authentication Protocol

- Pour le chiffrement : remplacement de WEP par TKIP

Temporal Key Integrity Protocol (changement de clé souvent)  
( cela ne sert à rien de décrypter une clé si elle n'est plus utilisée)