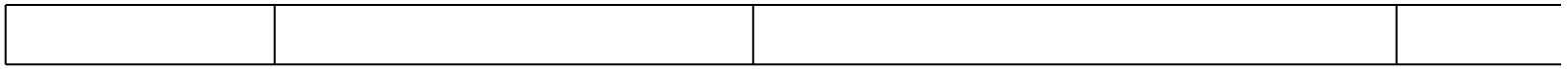
Internet Ambiant

Le protocole 802.11

Internet ambiant

- Internet ambiant => internet partout
- Plusieurs types de protocoles suivant le type de réseaux
- Ex: japon internet dans metro, trains, rue, projets pour la voiture



PAN WLAN WMAN

- PAN (personnal area network)
  - 802.15
  - =>802.15.1 bluetooth
  - =>802.15.4 zigbbe (connexion jouets)
- WLAN (wireless local area network)
  - 802.11(a,b,g,n…)=wifi, hyperlan2 (sans fil européen dans un carton)
- WMAN(wireless metropolitan area network)
  - 802.16 a b (pl km) =Wimax
  - 802.20 (reprends de bases de umts)

Exemples de PAN

- **bluetooth**

peu de débit MAIS nécessite peu de puissance, V5.0 en 2017 ! (low energy technology)

- Caractéristiques
  - 4Mbps sur 200m
- Fonctionnement
  - Technique FHSS (frequency hopping spread spectrum) voir Wifi, technique utilisée pour éviter les interférences
- Topologie par principe de Maitre/esclave
  - 1 maitre peut avoir au plus 7 esclaves => forment un piconet
  - 10 piconet peuvent coexister simultanément
  - En réalité, communication par paire et commutation rapide
  - 2 piconets peuvent être reliées pour former un scatternet

Exemples de PAN

- **bluetooth**

  - Etablissement de la connexion
    - Mode passif
    - Découverte des points d'accès (maitre envoi 1 requête à tous les périphériques)
    - Synchronisation
    - Découverte des services du point d'accès
    - Création d'un canal
    - Parrainage avec code PIN (mode sécurisé, s'il existe)
    - Utilisation du réseau
    - Possibilité d'utiliser un canal supplémentaire RFCOMM = port série virtuel, par ex utilisé par des périphériques GPS

  - Profils Bluetooth

    Profil = type de service, ex: Advanced Audio Distribution Profile (A2DP), File Transfert Profile (FTP), Headset Profile (oreillette),…

R sans fils pour l'IOT

Wireless Protocols for IoT	Frequency	Range (non-urban environment)	Data Rate	Power Draw	Topology	Requires Hub or Gateway?	Proprietary or Open?	Chipset Cost	Managed By	Security	Intended Use	Our Thoughts
ZigBee	2.4GHz, 915MHz (US), 868 MHz (EU)	100-325 ft	250 kbps (2.4) 40kbps (915) 20kbps (868)	low	Mesh	Yes	Open	$$	ZigBee Alliance (Comcast, Kroger, Samsung, TI)	Encrypted	Single Building	Zigbee is fractured, has multiple standards and one Zigbee product may not work with another Zigbee product. Zigbee can only be managed by one controller. Despite these shortcomings, ZigBee is already installed across the globe and ZigBee chips are readily available to develop on. For home-targeted products that need to be rolled out quickly, ZigBee is a good choice. ZigBee has the same downside as other mesh networks: many devices are required for reliable operation, and latency is relatively high. The upside is that ZigBee is already widely available and adopted, and works well if all of your ZigBee devices use the same standard. We think it's a good choice for low-cost products targeted at the home.
Z-Wave	915MHz (US) 868MHz (EU)	100-325 ft	40kbps (915) 20kbps (868)	low	Mesh	Yes	Proprietary	$$	Z-Wave Alliance	Encrypted	Single Building	Z-Wave is less fractured than ZigBee and probably has a better market share of Home Depot/Best Buy products in the U.S. Z-Wave uses a lower frequency than US ZigBee, which means it should have better range and less power draw. Unfortunately, Z-Wave chips are generally more expensive because they are only made by one manufacturer. Z-Wave is mesh, so many devices are required for reliable operation and latency is relatively high. Despite these shortcomings, Z-Wave is widely adopted and reliable if setup correctly. We think it's a good choice for products targeted at the home.
Bluetooth 4.0+	2.4GHz	200 ft	25Mbps	medium	PAN	Yes	Open	$	Bluetooth Special Interest Group (3k members)	Encrypted	Personal	Bluetooth is tempting to use for IoT products because it is built into every smartphone already. Bluetooth can have high data rates and low power consumption. The downside of Bluetooth for IoT is the PAN network model. It's challenging to have multiple devices on the network. There is generally a limit of 8 devices. Bluetooth 4.0+ is is a good choice for products that can be managed from just a smartphone.

Source: http://glowlabs.co/wireless-protocols/

Bluetooth 5	2.4GHz	800 ft	50Mbps	medium	PAN	Yes	Open	$	Bluetooth Special Interest Group (3k members)	Encrypted	Personal	The latest Bluetooth standard should have 4x the range and 2x the data rate of Bluetooth 4.0+. It still uses the PAN network model so it shares many of the same challenges as Bluetooth 4.0+. If you're going to start building a Bluetooth product, you should include the latest standard Bluetooth chip which will be shipping in all smartphones soon.
Bluetooth Low Energy (BLE)	2.4GHz	200 ft	10kB/s	low	PAN	Yes	Open	$	Bluetooth Special Interest Group (3k members)	Encrypted	Personal	BLE is essentially Bluetooth except it goes into sleep mode after connecting for a few mS. The low power consumption means the BLE is a better protocol for IoT, except it still uses the very limited PAN network topology. There is an upcoming BLE Mesh standard which SHOULD fix the issues of the PAN network model. If it does, BLE will be a very powerful IoT communication protocol. BLE is already a great technology choice for wearable products.
Wi-Fi	2.4GHZ/5GHz	115-230	7Gbps	high	Star	No	Open	$$	IEEE	Optional	Single Building	Wi-Fi is readily available in most commercial buildings and homes. This is a massive advantage for IoT products targeting those markets. Because of the pre-existing Wi-Fi networks, Wi-Fi products do not require a hub that's separate from the router. They don't need unreliable mesh networks to extend range either. They have instant access to the cloud. The downside of Wi-Fi is that it can be difficult for the consumer to get it connected to their router and it has a very high power draw. Wi-Fi is a great technology choice for standalone products targeted at the home or business. It can be used for battery-powered products if power is managed appropriately.
Wi-Fi-ah (HaLow)	900MHz	3000 ft	347Mbps	low	Star	No	Open	???	IEEE	???	Single Building	HaLow requires a special Wi-Fi router that's available on the market now but not installed in most homes. HaLow devices will have instant internet access like traditional Wi-Fi devices assuming the router is HaLow compatible. Halow has better wall penetration and range than Wi-Fi because it uses the lower 900MHz frequency band. This also means lower power draw for battery operated devices. If all routers start shipping with HaLow built in, this will be a very strong wireless protocol for homes and commercial buildings. Watch the adoption rate of HaLow and plan your

Thread	2.4GHz	100 ft	250kbps	low	Mesh	Yes	Open	$$	Thread Group (Google, Samsung, etc.)	Encrypted	Single Building	Thread is backed by Google, so you know there are some excellent engineers behind it. It's built on the 6LoWPAN stack which uses the same 802.15.4 radio as ZigBee and could become a dominant player in the Home Automation space. It's seems to be built so that Nest becomes the ZigBee-like hub of the house. Nest uses it's Wi-Fi connection to get low-power thread devices online. It's a great idea in theory, but has yet to become widely adopted. There's discussion of building Thread compatibility with ZigBee devices. Thread is a great technology for home-targeted products that target customers who already have a Nest.
DigiMesh	2.4GHz/900 MHz (US)/868 MHz (EU)	~20 miles	250 kbps (2.4) 40kbps (915) 20kbps (868)	low	Mesh	Yes	Proprietary	$$$	DigiMesh	Encrypted	Single Building or WAN	DigiMesh is essentially modified ZigBee focused on long range point to point communication. It looks like a good technology, but nobody that I found has actually built products on it. This may be because the cost per chip is very high. For products targeted at large commercial buildings without per-device cost constraints, DigiMesh is a good choice.
MiWi	2.4GHz or subGHz	800 ft	250kbps	low	Mesh or Star	Yes	Proprietary	$	MiWi	Encrypted	Single Building or WAN	MiWi is similar to DigiMesh in that it's a modified and proprietary form of ZigBee. It requires less power, lower memory, and is good for very low-cost products and systems. It's not widely adopted yet but could be good for products that will require a custom hub anyway. MiWi also has low memory constraints, which makes it a good choice for products that have to have a very low per-unit BOM cost.
EnOcean	900Mhz (US) 868 MHz (EU) 315 MHz	30-100 ft	125kbps	"Battery Free"	Mesh	Yes	Proprietary	$$	EnOcean	Encrypted	Single Building	Battery-free operation promises a long device life. It's a very interesting technology that we haven't had a chance to play with, but we follow the company closely. EnOcean can be prototyped with a raspberry pi which lowers development costs. EnOcean is a good technology choice for products targeted at the commercial building that should have low maintenance costs.
6LoWPAN	2.4GHz	380 ft	250kbps	low	Mesh	Yes	Open	$	IEEE	Optional	Single Building	6LoWPAN is a promising alternative to other mesh network technologies. Because it's based on IPV6 addressing, it's relatively simple for 6LoWPAN devices to communicate with other IoT networks by

Weightless (W, N, P)	white-spaces, 915MHz, 868MHz, 780MHz, 470 MHz, 433 MHz, 169 MHz	1.2 miles (P), 3 miles (W, N)	200bps-100kbps	low (N), medium (W, P)	Star	Yes	Open	$$	Weightless Special Interest Group	Encrypted	WAN	Weightles-W was rejected by the FCC and other governing bodies, but N and P look like solid WAN technologies. Weightless is a SIG with tons of members and competeing ine the LPWAN space. Weightless N is one-way communication which is very limiting. Weightless-P looks like a great LPWAN technology, but it hasn't been deployed yet. With royalty free deployment, Weightless-P and Weightless-N look like good technologies for LPWAN products.
mcThings	2.4GHz	650 ft	50kbps	low	Star	Yes	Proprietary	$$$	mcThings	???	Single Building	mcThings is great for deploying a custom set of sensors in a few buildings. The cost per unit is high, but the technology is very power efficient and requires little maintenance. You can easily expand a mcThings network with bridges, and battery life for basic sensors can be up to 10 years. We recommend mcThings for sensor-based products targeting a few businesses buildings.
LoRa	150MHz-1GHz (lots of options)	up to 20 miles	50kbps	low	Star	Kind of	Open	$$$	LoRa Alliance	Encrypted	WAN	LoRaWAN is an alliance focused on creating a LPWAN technology for IoT devices. LoRa uses spread-spectrum technology that lets the LoRa chip decide the best spectrum to use for data rates, interference, and battery life. It's strongly adopted and deployed, with multiple vendors selling proven LoRa hardware. Because it's relatively inexpensive to cover a new area with LoRa, it's a good technology choice for LPWAN IoT products that need to be placed in areas without cell service.
SigFox	900Mhz (US) 868 MHz (EU)	~20 miles	100bps	low	Star	Yes	Proprietary	$$$	SigFox	Encrypted	WAN	The original player in the LPWAN space, SigFox had the vision to see LPWAN coming and has already deployed their network over most of Europe. SigFox is a proprietary technology, so your price per chip is relatively high. SigFox has great coverage right now, but they are threatened by the onset of LTE Cat M1 and NB-IoT. SigFox is a good choice for LPWAN products that need to be deployed in Europe right now.
LTE Cat-M1	1.4MHz	~20 miles	1Mbps	low	Star	No	Open	???	3GPP, LTE-M TaskForce	???	WAN	LTE M1 is not available yet, but it's a very exciting LPWAN technology. M1 should be deployable on existing LTE networks without hardware upgrades.

R sans fils pour l'IOT

NarrowBand-IoT (Cat M2)	Below 1GHz	~20 miles	100kbps	low	Star	No	Open	???	3GPP, Ericsson, Huawei	Encrypted	WAN	NB-IoT is similar to LTE Cat M1, except it is GSM-based. NB-IoT till do better globally (where LTE networks are not prevalent) and well on T-Mobile & Sprint in the US. All these IoT technologies sleep but NB-IoT also usesless power than the competitors when the radio is on due to a relatively simple waveform. NB-IOT should also have a cheaper chip than it's LTE-M1 counterpart. Not officially rolled out yet, but it's being tested in a few areas and should be watched closely. It could be a good choice for products that target massive areas like nations, states, or cities.
3G and 4G Cellular (US)	700 MHz, 800 MHz, 850MHz, 1700MHz, 1900MHz, 2100MHz, 2300MHz, 2500MHz	~20 miles	200kbps (3G) 10Mbps (4G)	high	Star	No	Open	$$	3GPP	Encrypted	WAN	Cellular technology is not designed for IoT, but it's already rolled out across most of the globe. For IoT devices that do not require battery power and need to be launched immediately, cellular is a good choice. For IoT products that can wait to launch, it's worth waiting to see who comes out on top in the cellular LPWAN war.

Mais aussi 802.3 (wifi)ag pour l'iot (moins de consommation, temps de pause)

WLAN IEEE 802.11

Plusieurs normes:

Norme	Dthéorique	Dutile
802.11a	54Mbits/s	18
802.11b	11Mbits/s	5
802.11b 2x	22Mbits/s	7
802.11g	54 Mbits/s	14
802.11g 2x	108 Mbits/s	
802.11n	540max Mbps	?
802.11ac	6gbps	
802.11 6e	11gbps	

- **802.11n (540 Mbits/s) draft 2.0 03/2007, draft 3.0 fin 2007, norme sept 2009**
- **Mais aussi:**
- **802.11ah (pour l'IOT) mai 17**
- **802.11ax (Wifi 6) 2019, (11Gbps)**

Qualité de service wifi

•Plus on s'éloigne plus le débit est faible (300m pour le 802.11b, moins pour les normes g, a ,en réalité, 20-30m en intérieur
•)

•Chaque station émet avec son propre débit
=>si un utilisateur est à 1 Mbit/s tout le système tombe à 1 Mbit/s (car 9/10 temps pour station à 1Mbits/s et 1/10 pour la plus rapide) si on tombe dans l'utile => 500 kbits/s !

=>système se dégrade, difficile à manipuler

solutions ?
=>déconnection des plus faibles,
=>plus de points d'accès
=>802.11e priorité des paquets => classe de service mais difficile si grands nb d'utilisateurs qui arrive et qui partent
=>802.11n pour qos (quality of service)

WMAN

802.16 WIMAX (famille 4G) proposé par Wimax Forum

- protocole **OFDMA** (*Orthogonal Frequency Division Multiple Access*)
- Bande 700Mhz, 2,3Ghz , 2,5Ghz
- longue portée dizaine de km (45km suivant les tests actuels)
- débit allant jusqu'à 1 Gbps (802.16-2204:70Mbps sur 10km, 802.16e 30Mbps sur 3.5km, 802.16^{e} 1Gbps en fixet et 100Mbps en mobile)

- temps découpé en tranches par utilisateurs => Wll (wirelless local loop)
  trames (slots) pour chaque utilisateur
- pb pluie etc obstacle
- Différents standard 16.1, 16.2, 16.3
  ex: antenne centrale vers village, etc

WMAN

3GPP LTE, Proposé consortium 3GPP

- =4G (4ieme génération après UMTS(3G) et 3G+(HSPA débit 14,4Mbps down)
  - Bande passante 100Mhz
  - Offre de débit descendant 1Gbps
  - 2 candidats possibles: Wimax et LTE

- LTE?
  - Proposé par consortium 3GPP
  - Long term evolution
  - 3G mise à jour,
  - version 10 (LTE advanced) respectera norme 4G-> appelé 4G+

  - Version 8:
    - Norme 2008
    - 5 classes de terminaux, Bp de 1,4Mhz à 20Mhz
    - OFDMA, MIMO 2x2, 4x4
    - BP en France (dec 2011): 800Mhz, 2600Mhz

Catégories de terminaux LTE

Catégories des terminaux LTE et LTE Adv (3GPP rel.11)[11]										
Catégorie		1	2	3	4	5	6[A 1]	7	8[A 2]	9	10
Débit crête (Mbit/s)	Descendant	10	50	100	150	300	300	300	3000	450	450
	Montant	5	25	50	50	75	50	100	1500	50	100
Caractéristiques fonctionnelles minimales[A 3]										
Largeur de la bande de fréquence de chaque porteuse		1,4 à 20 MHz								
Nombre minimal de porteuses radio agrégées dans le sens descendant		1					1, 2 ou 3		5	2, 3 ou +	
Nombre de porteuses radio agrégées dans le sens montant		1					1	2	5	1	2
Modulations	Descendante	QPSK, 16QAM, 64QAM									
	Montante	QPSK, 16QAM				QPSK, 16QAM, 64QAM	QPSK, 16QAM		QPSK, 16QAM, 64QAM	QPSK, 16QAM	
Antennes										
MIMO 2x2		Non	Oui								
MIMO 4x4		Non				Oui	Oui/Non		Oui	Oui/Non	
MIMO 8x8		Non							Oui	Non	

=> Débit dépend~: de la modulation, du nombre d'antennes, du multiplexage

WMAN

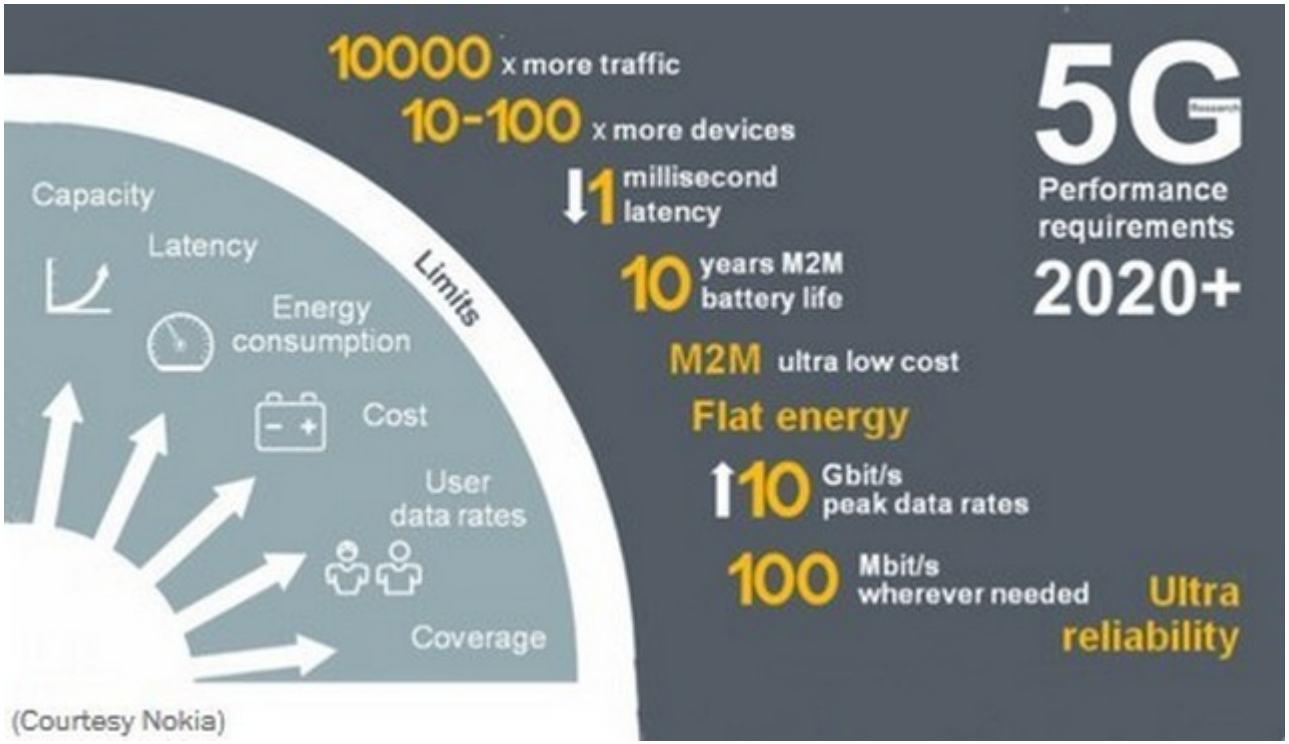
5G (nom: IMT2020)

mi-2018 de "non-standelone 5G NR
appareils compatibles avec la future 5G. Ils communiqueront via les réseaux 4G et LTE en attendant le déploiement de l'infrastructure 5G

Débit:
capables de transférer 20 gigabits/s de données, depuis une station de base jusqu'à un appareil connecté au réseau, et 10 gigabits/s dans le sens inverse, soit environ 100 fois plus que les réseaux 4G.
temps de latence devrait être inférieur à une milliseconde, contre 25 à 40 millisecondes pour la 4G.

Accessible pour l'usager d'ici 2020

WMAN



Projets pour l'IOT, drones (parrot), etc.

Le protocole 802.11

Introduction

•Norme *IEEE 802.11* (*ISO/IEC 8802-11*) est un standard international décrivant les caractéristiques d'un réseau local sans fil (*WLAN*).

•**Objectifs:**

Réseau local sans fil, itinérance automatique
Faible consommation de puissance
Facilité d'utilisation et … d'installation
Transparence pour les couches sup (≥ 3) et les applis
Possibilité de localisation

Introduction

Avantages

Très flexibles dans la zone de réception
Réseaux de type ad-hoc (pas de planification nécessaire)
pas d'infrastructure !
Presque pas de difficultés de câblage (e.g. bâtiments historiques, …)
Plus robuste en situation de désastre … ou déconnexion de câble !
2 types de réseaux: ad-hoc ou infrastructure

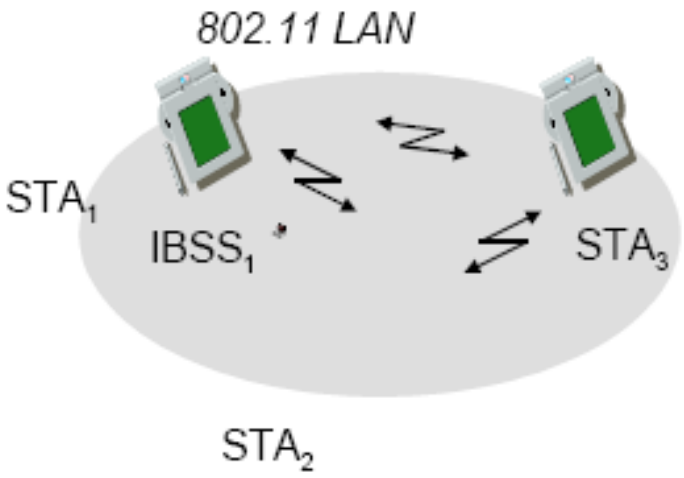
Désavantages

Deff relativement faible
Puissance électrique nécessaire importante
Beaucoup de solutions propriétaires, établissement lent des normes (IEEE 802.11(US), et Hiperlan (Europe))
Beaucoup de lois nationales,
les législations internationales sont lentes et difficiles

Réseau de type Ad-hoc

En mode **ad hoc,** les stations se connectent les unes aux autres afin de constituer un réseau point à point (*peer to peer* en anglais), cad un réseau dans lequel chaque machine joue en même temps de rôle de client et le rôle de point d'accès.

L'ensemble formé par les différentes stations est appelé *ensemble de services de base indépendants* (**independant basic service set**, *IBSS*). L'IBSS est identifié par un *SSID*, (*Service Set Identifier*) et représente le nom du réseau.



Réseau de type infrastructure

•chaque station **STA** se connecte à un point d'accès.

•L'ensemble formé par le point d'accès et les stations situés dans sa zone de couverture est appelé *ensemble de services de base* (en anglais *basic service set*, noté **BSS**) et constitue une cellule.

•Chaque *BSS* est identifié par un *BSSID*, un identifiant de 6 octets (48 bits). Dans le mode *infrastructure*, le *BSSID* correspond à l'adresse MAC du point d'accès.

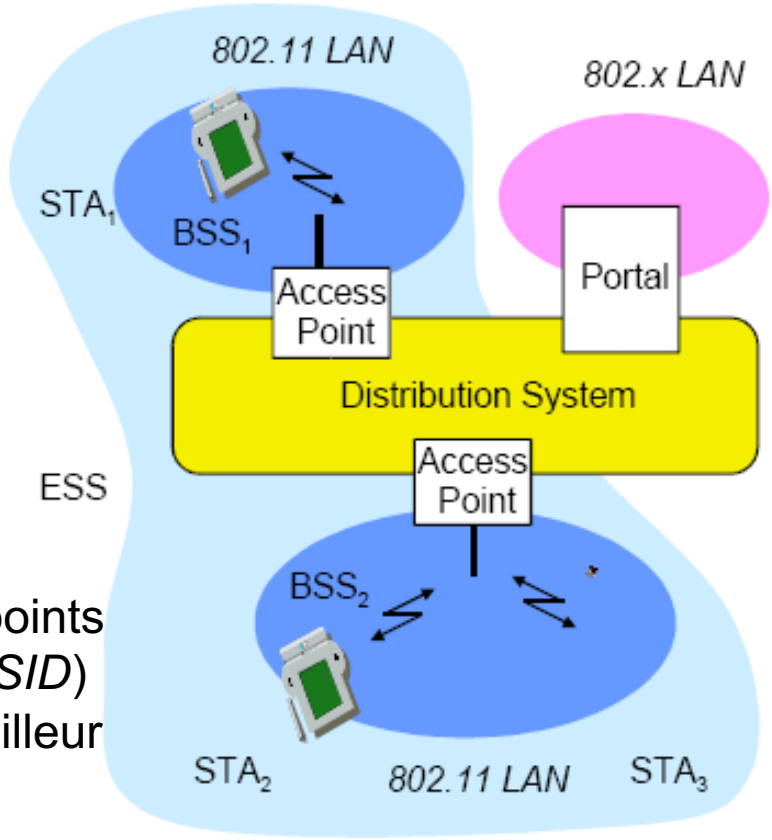
•Il est possible de relier plusieurs points d'accès entre eux par une liaison
•appelée *système de distribution* (DS, *Distribution System*) pour constituer
•un *ensemble de WLAN appelés ESS* (*extended service set*).

•Le système de distribution (*DS*) peut être aussi bien un réseau filaire, qu'un câble entre deux points d'accès ou bien même un réseau sans fil !

Réseau de type infrastructure

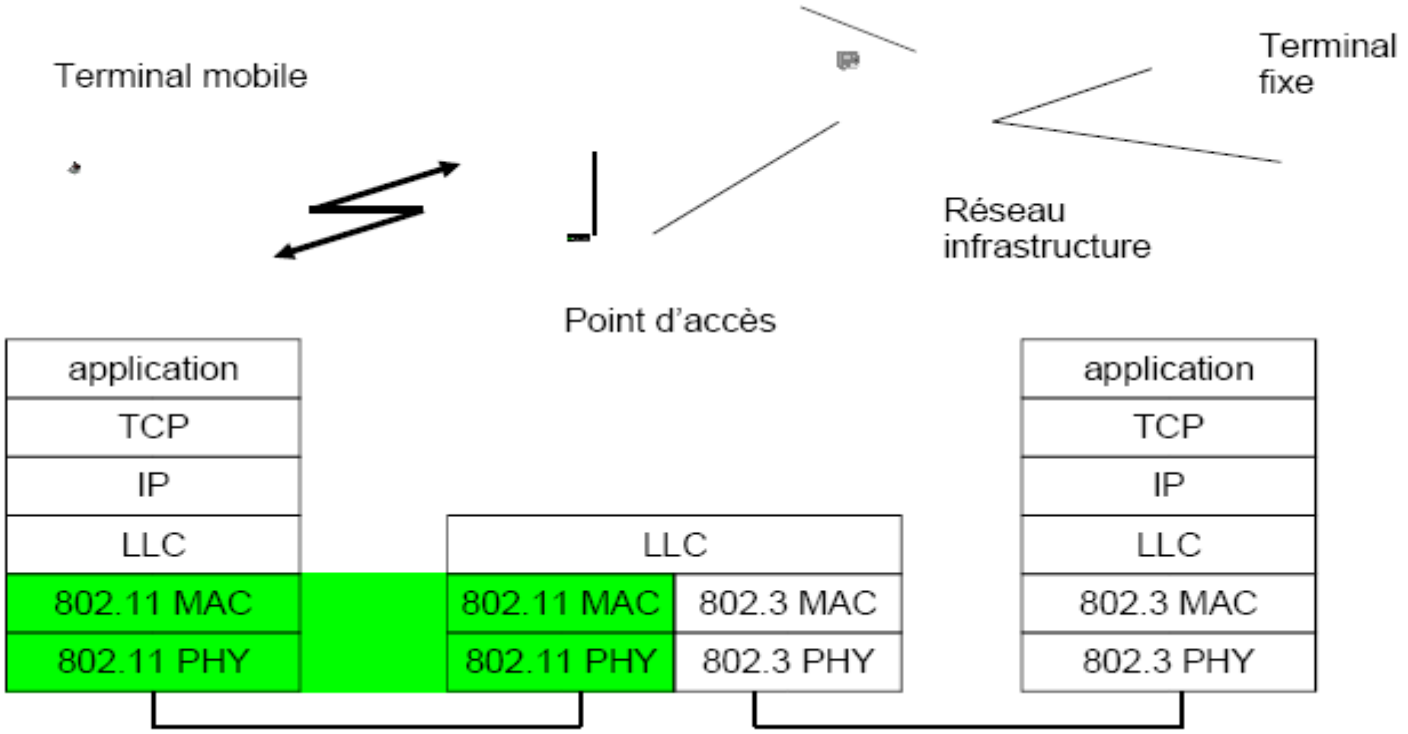
Un *ESS* est repéré par un **ESSID** (*Service Set Identifier*), servant de nom pour le réseau.
L'*ESSID* est souvent abrégé en **SSID**

Lorsqu'un utilisateur nomade passe d'un *BSS* à un autre lors de son déplacement au sein de l'*ESS*, l'adaptateur réseau sans fil est capable de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès.



Une station se trouvant à la portée de plusieurs points d'accès (possèdant bien évidemment le même *SSID*) pourra ainsi **choisir** le point d'accès offrant le meilleur compromis de débit et de charge.

Couches du 802.11



PHY->techniques de transmissions sur ondes radio (modulation)

4 techniques: FHSS, DSSS, IR(infrarouge), OFDM (802.11a, g)

Couche liaison=LLC+MAC -> accès au support

Couches PHY
techniques de transmission

La technique FHSS (*Frequency Hopping Spread Spectrum)*

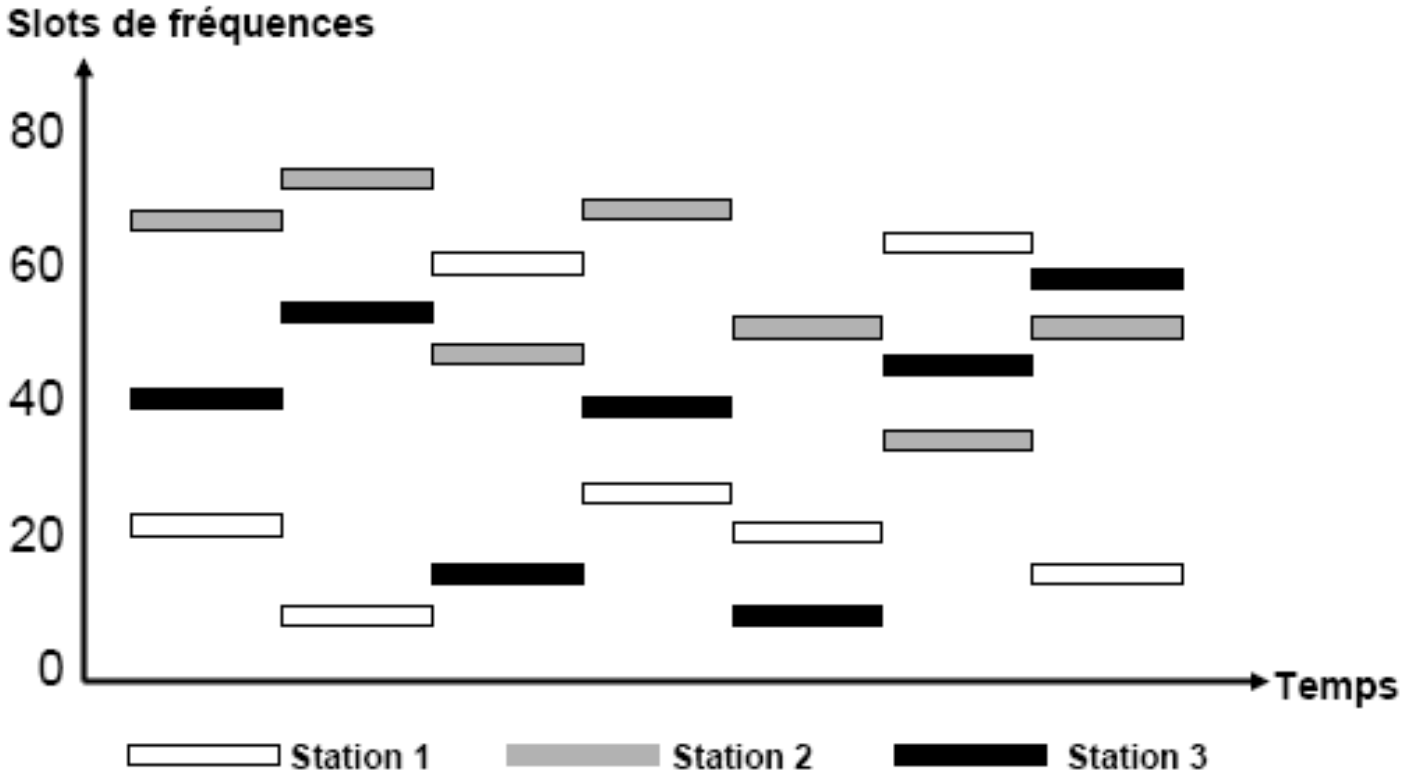
consiste à découper la large bande de fréquence en un minimum de 75 canaux (*hops* ou *sauts* d'une largeur de 1MHz)

transmission en utilisant une combinaison de canaux connue de toutes les stations de la cellule : l'émetteur et le récepteur s'accordent sur une succession de sauts entre canaux pour envoyer les données

Utilisée à l'origine par les militaires

Offre peu de débit (pas utilisée avec 802.11a,b, g)

Couches PHY
techniques de transmission

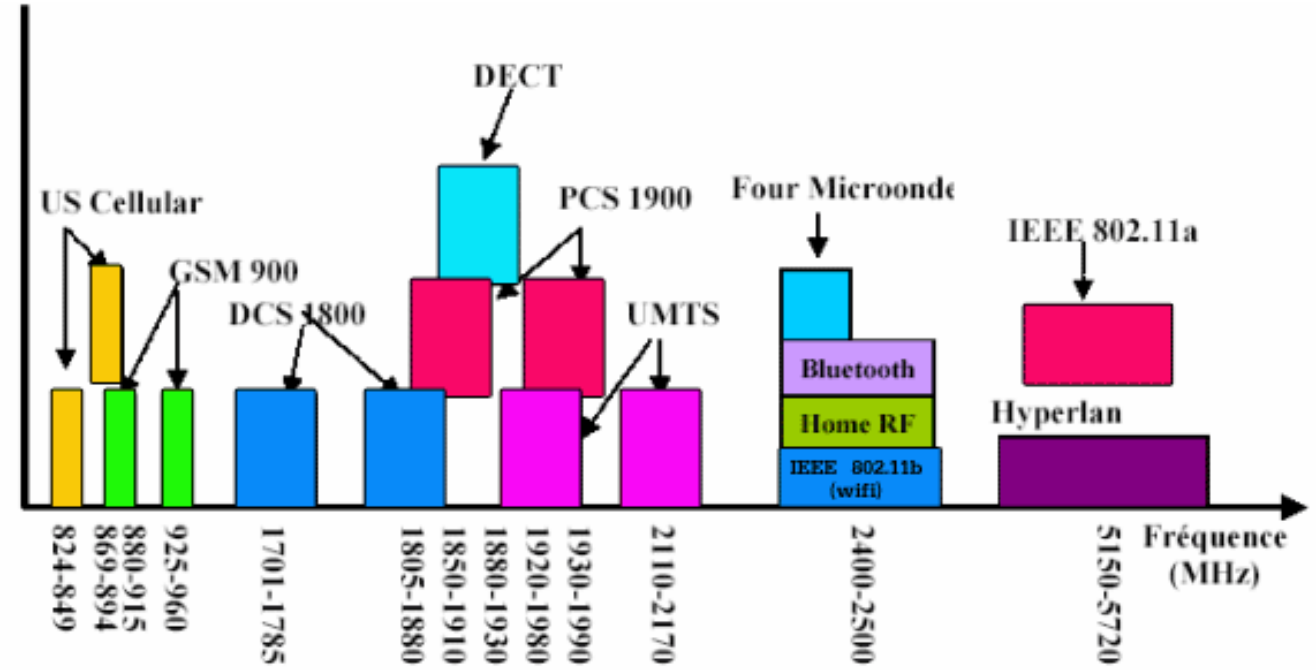


Couches PHY

techniques de transmission

Technique la plus répandue aujourd'hui

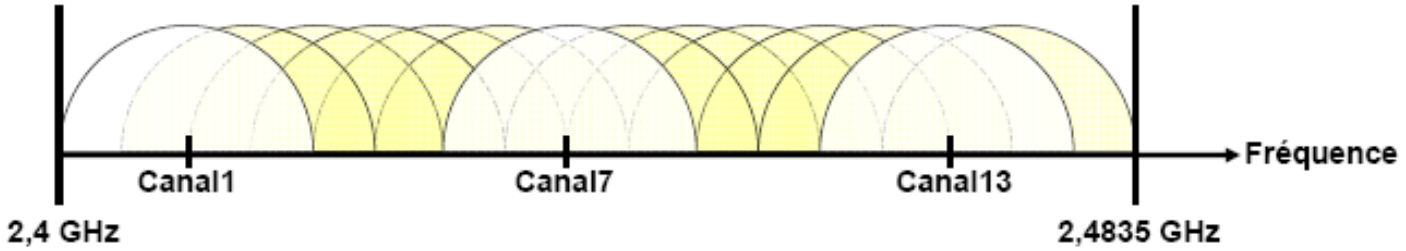
Découpage de la bande passante en 14 canaux de 20Mhz
=>802.11b g,bande de fréquence *2.400-2.4835 GHz*



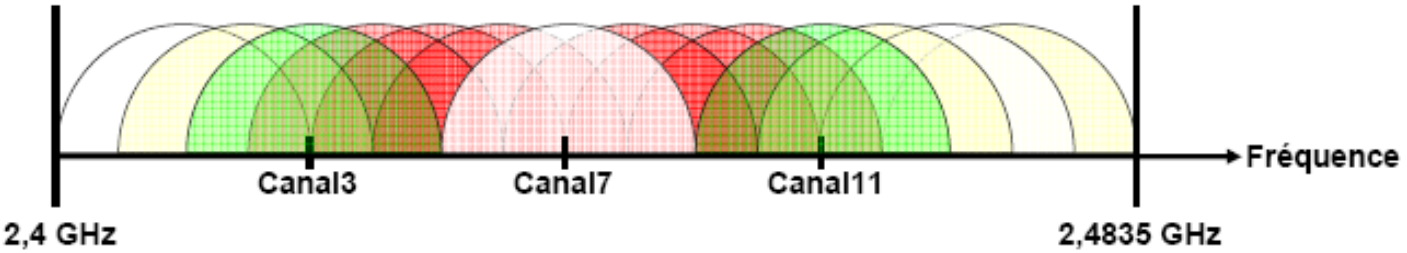
Couches PHY

techniques de transmission

Canaux:



Canaux proches inexploitables simultanément



Couches PHY
techniques de transmission

La technique DSSS (*Direct Sequence Spread Spectrum)*

1 seul canal utilisé simultanément

consiste à transmettre pour chaque bit une séquence appelée *Barker*.

802.11 définit une séquence de 11 bits (*10110111000*) pour représenter un 1 et son complément (*01001000111*) pour coder un 0.
On appelle *chip* ou *chipping code* chaque bit encodé à l'aide de la séquence.

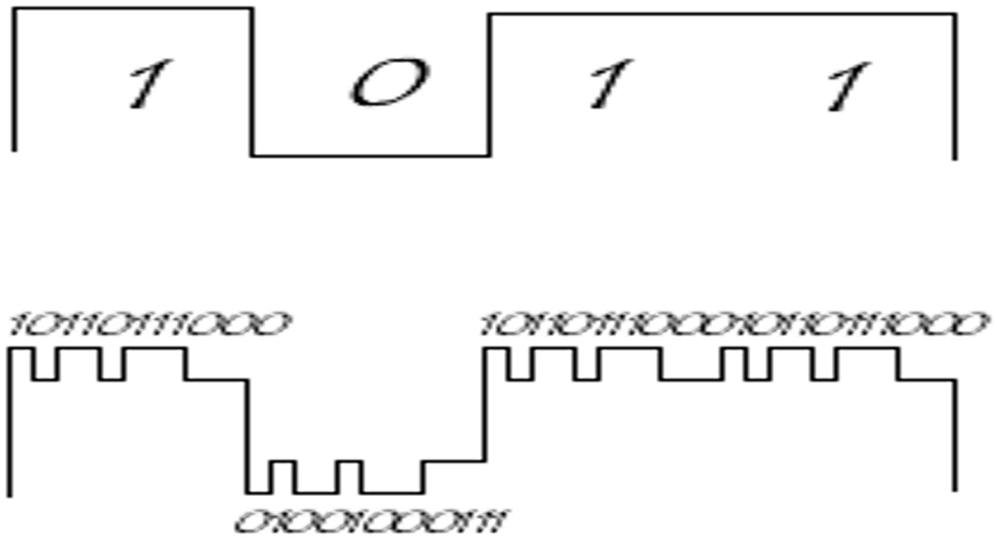
=>Débit 1, 2 Mbits/s

Ce codage est nécessaire pour retrouver les données malgré les parasites (bruit)

Couches PHY

techniques de transmission

Exemple de chipping code



Techniques de transmission pour 802.11 haut débit (a,b,g)

Techniques de transmission plus évoluées (basées sur DSSS):

- Technique CCK (Complementary Code Keying)

Au lieu de 2 séquences barker, on utilise la technique CCK

$\Rightarrow$ 64 mots de 8bits (toujours une distinction correcte)

$\Rightarrow$ Codage de 4 bits par signal (débit de 5,5) ou de 8bits (11Mbits/s)

Techniques de transmission pour 802.11 haut débit (a,b,g)

Débit à 1 ou 2 Mbit/s
Codage de 1 bit par un barker de 11 bits
Modulation définie (nb bits émis / signal : 1 bit par signal

Débit à 5,5 Mbits/s
Codage de 1 bit par une séquence de 8 bits
Modulation définie (nb bits émis / signal) : 4 bits par signal

Débit à 11 Mbits/s
Codage de 1 bit par une séquence de 8 bits
Modulation définie (nb bits émis / signal) : 8 bits par signal

Techniques de transmission pour 802.11 haut débit (a,b,g)

Débit à 54 Mbits/s ?

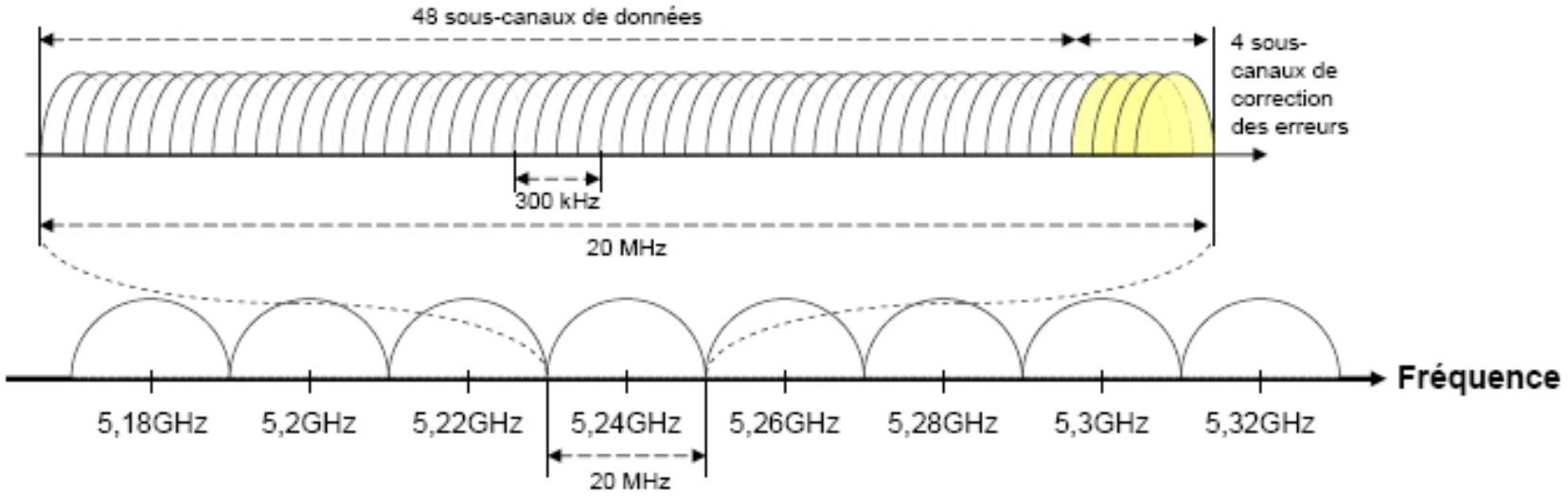
Utilisation d'une autre technique de remplacement à DSSS
La technique OFDM (*Orthogonal Frequency Division Multiplexing)*

Technique utilisée par les normes 802.11 a et g

Chaque canal fait 20 MHz, et est subdivisé en 52 sous canaux de 300khz (4 sont utilisés pour la correction d'erreurs).

le codage de l'information sur chaque sous-canaux est beaucoup plus lent,
Mais * 52, on obtient un débit th de 54Mbit/s

Techniques de transmission pour 802.11 haut débit (a,b,g)



Techniques de transmission pour 802.11 haut débit (n)

Débit à 108 -> 300 Mbits/s ?

•Utilisation d'une technique supplémentaire MIMO *(Multiple input, multiple output)*

Technique de modulation utilisant plusieurs antennes et divisant les données en autant de flux que d'antennes émettrices, transmis sur une même fréquence. Chaque antenne réceptrice reçoit une combinaison linéaire de ces flux, qui sont reconstitués par des fonctions de traitement de signal, et recollés pour constituer les données.

•Regroupement de canaux pour augmenter la bp

•Utilisation de canaux de 20Mhz, 40 Mhz …

Canaux 20Mhz + MIMO (2 antennes) -> Débit=140Mbits/s
Canaux 40Mhz + MIMO (2 antennes) -> Débit=315Mbits/s
Canaux 40Mhz + MIMO (3 4 antennes) -> Débit=540Mbits/s

Techniques de transmission pour 802.11 haut débit (n)

Débit à 108 -> 300 Mbits/s ?

Agrégation de paquets de données

Débit th max: 600 Mbit/s, débit moyen 144Mbits/s ?

Couverture: Intérieur ~50 m extérieur ~125 m

Ajout de qualité de service (QOS) : 802.11e

Toujours compatible avec 802.11b g (même trame, etc etc)

Techniques de transmission pour 802.11 ac

Norme de janvier 2014

Bande de fréquence entre 5 et 6 Ghz
Capacité max: 6,77Gbps

Techniques : MIMO, OFDMA, utilisation de plusieurs canaux jusqu'à 80Mhz
Rétrocompatible avec le 802.11n (5Ghz)

1 antenne, une carte => 867Mbps
Canaux passés de 40Mhz à 80 Mhz à 160Mhz

Techniques de transmission pour 802.11 ac

Capacité max: 6,77Gbps
1 antenne, une carte => 867Mbps
Canaux passés de 40Mhz à 80 Mhz à 160Mhz

Scenario	Typical Client Form Factor	PHY Link Rate	Aggregate Capacity
1-antenna AP, 1-antenna STA, 80 MHz	Handheld	433 Mbit/s	433 Mbit/s
2-antenna AP, 2-antenna STA, 80 MHz	Tablet, Laptop	867 Mbit/s	867 Mbit/s
1-antenna AP, 1-antenna STA, 160 MHz	Handheld	867 Mbit/s	867 Mbit/s
2-antenna AP, 2-antenna STA, 160 MHz	Tablet, Laptop	1.69 Gbit/s	1.69 Gbit/s
4-antenna AP, four 1-antenna STAs, 160 MHz (MU-MIMO)	Handheld	867 Mbit/s to each STA	3.39 Gbit/s
8-antenna AP, 160 MHz (MU-MIMO) -- one 4-antenna STA -- one 2-antenna STA -- two 1-antenna STAs	Digital TV, Set-top Box, Tablet, Laptop, PC, Handheld	3.39 Gbit/s to 4-antenna STA 1.69 Gbit/s to 2-antenna STA 867 Mbit/s to each 1-antenna STA	6.77 Gbit/s
8-antenna AP, four 2-antenna STAs, 160 MHz (MU-MIMO)	Digital TV, Tablet, Laptop, PC	1.69 Gbit/s to each STA	6.77 Gbit/s

Techniques de transmission pour 802.11 6, 6E

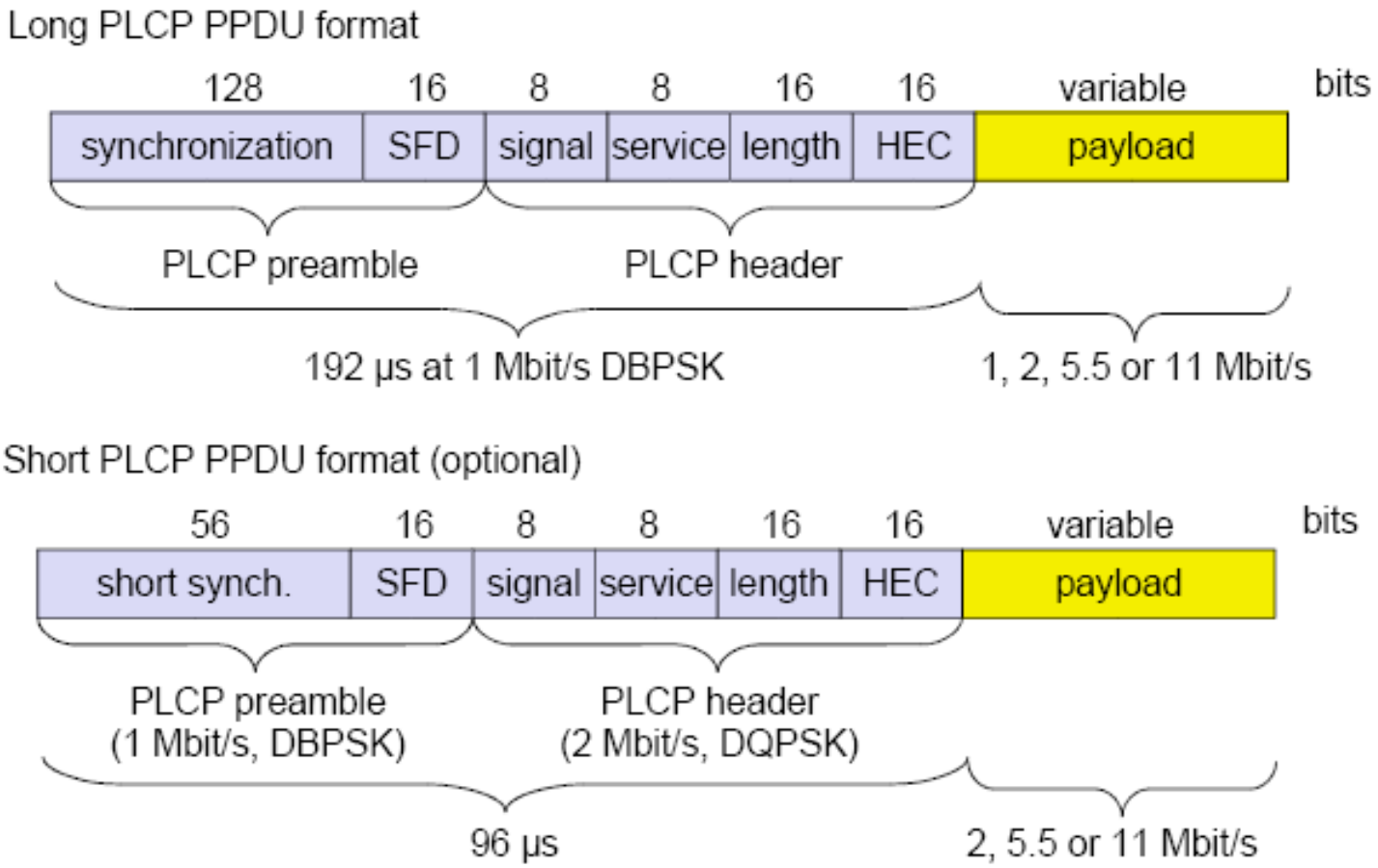
Aussi appelé Wifi 6 (les normes passées Wifi 5)

- Bandes de fréquences 2,4 et 5 GHz.
- débit maximal de 11 Gbit/s avec canaux de 160 MHz
- Même bande passante que le 802.11ac (20, 40 80 MHz et 80+80 MHz ou 160 MHz)
- MU-MIMO: nombre d'antennes présentes sur les émetteurs et les récepteurs passe de 4x4 actuellement à 8x8.

Wifi 6E (2021 ?)

- Utilise les mêmes fréquences et 14 additionnel canaux de 80 MHz ou 7 de 160 MHz dans les 6 GHz
- Fréquences plus libres actuellement, adition de fréquences -> prise en charge de plus d'utilisateurs à la fois

format de trames PHY



format de trames PHY

Synchronisation avec 0101010101…

SFD: Start frame delimiter

PLW (PLCP_PDU Length Word) = Longueur du payload, inclus. 32 bits CRC du
payload, PLW < 4096

PSF (PLCP Signaling Field): indique début des données (CRC+données)

HEC (Header Error Check): CRC avec x16+x12+x5+1

Signal : indique la modulation de signal utilisée et le débit (débit /100Kbps)

Service : non utilisé

Couche Liaison

Méthode d'accès:

Plusieurs méthodes toutes basées sur CSMA/CA: DFWMAC-DCF(CSMA/CA), DFWMAC /w RTS/CTS, DFWMAC PCF (points d'accès interrogent terminaux selon un liste)

Rappel : Ethernet CSMA/CD (collision detection) =>impossible dans la mesure où deux stations communiquant avec un récepteur ne s'entendent pas forcément mutuellement en raison de leur rayon de portée

La norme 802.11 utilise un protocole proche appelé **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 réception réciproques entre l'émetteur et le récepteur :

Couche Liaison

Emission de trames:

1er cas (sans options) CSMA/CA

station qui veut émettre, écoute le canal (clear channel assessment) pendant temps > DIFS

envoi des données (trame) si libre sinon backoff aléatoire

le récepteur acquitte (si CRC ok)

sinon (pas de ack) la trame est automatiquement renvoyée

⇒PB on peut montrer que des terminaux peuvent ne pas apparaître (cachés ou qu'ils sont exposés (peuvent émettre mais ne le font pas)

⇒Utilisation du protocole dérivé MACA (Multiple Access with Collision Avoidance)

Couche Liaison

Mise en œuvre de DFWMAC /w RTS/CTS :

1. La station voulant émettre écoute le réseau pendant temps > DIFS
Si le réseau est encombré, backoff. Dans le cas contraire, si le média est libre pendant un temps > IFS alors la station peut émettre.

2. La station transmet un message appelé *Ready To Send* (*RTS*) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission.

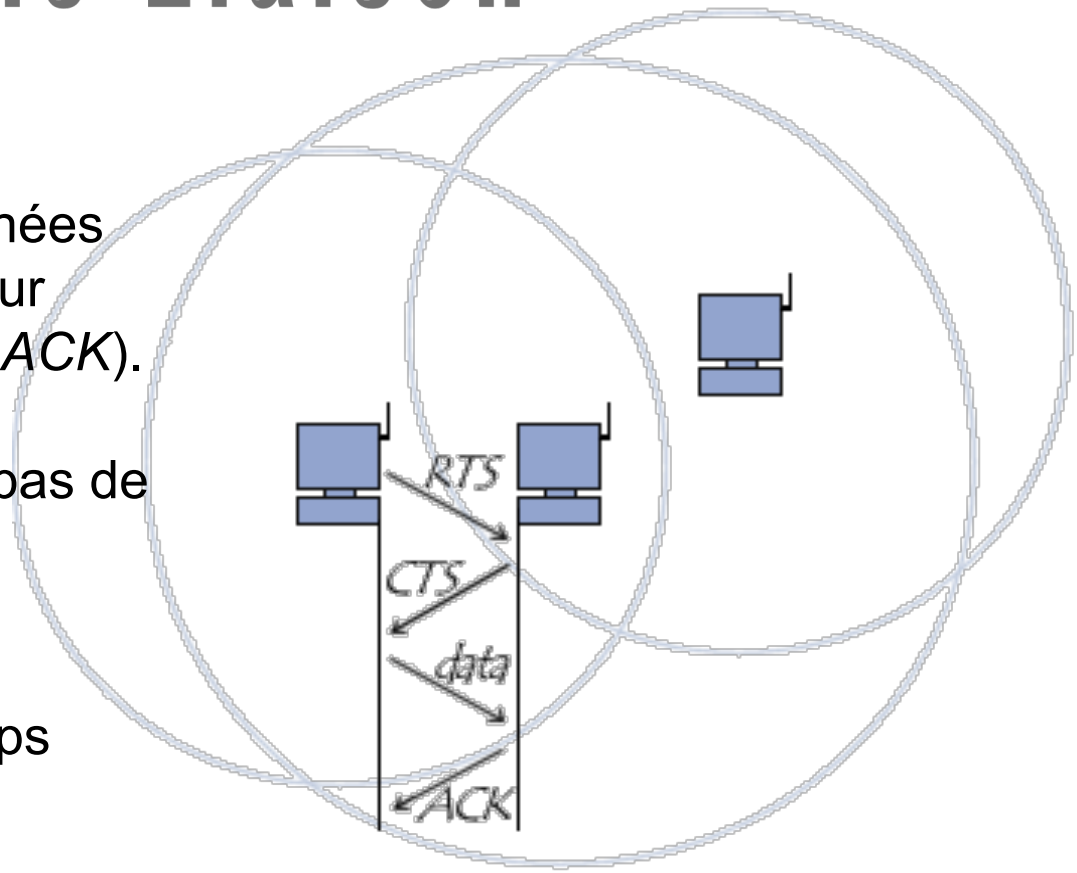
3. Le récepteur (généralement un point d'accès) répond un *Clear To Send* (*CTS*, *Le champ est libre pour émettre*), puis la station commence l'émission des données.

Couche Liaison

4. A réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (*ACK*).

Retransmission automatique si pas de ack

Toutes les stations avoisinantes patientent alors pendant un temps qu'elles considèrent être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.



IFS et priorités

Le temps IFS permet la gestion des priorités !!

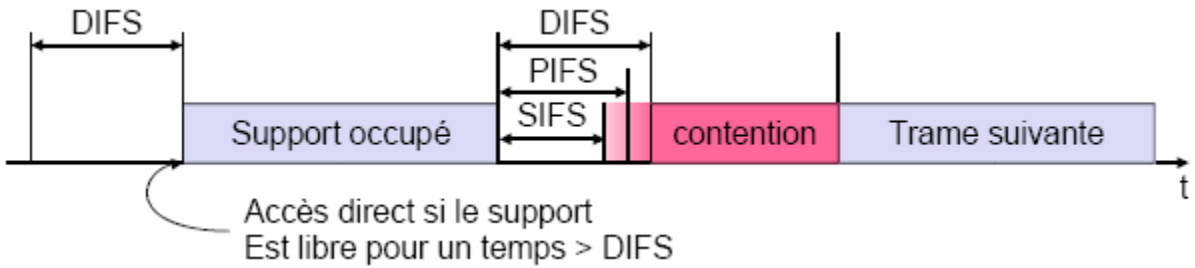
Le plus petit temps IFS=SIFS

Priorités des trames ACK et CTS: sont émises si le support (media) est libre pendant un temps SIFS

Priorité pour le temps réel IFS= PIFS: trames sont émises si le support (media) est libre pendant un temps PIFS > SIFS

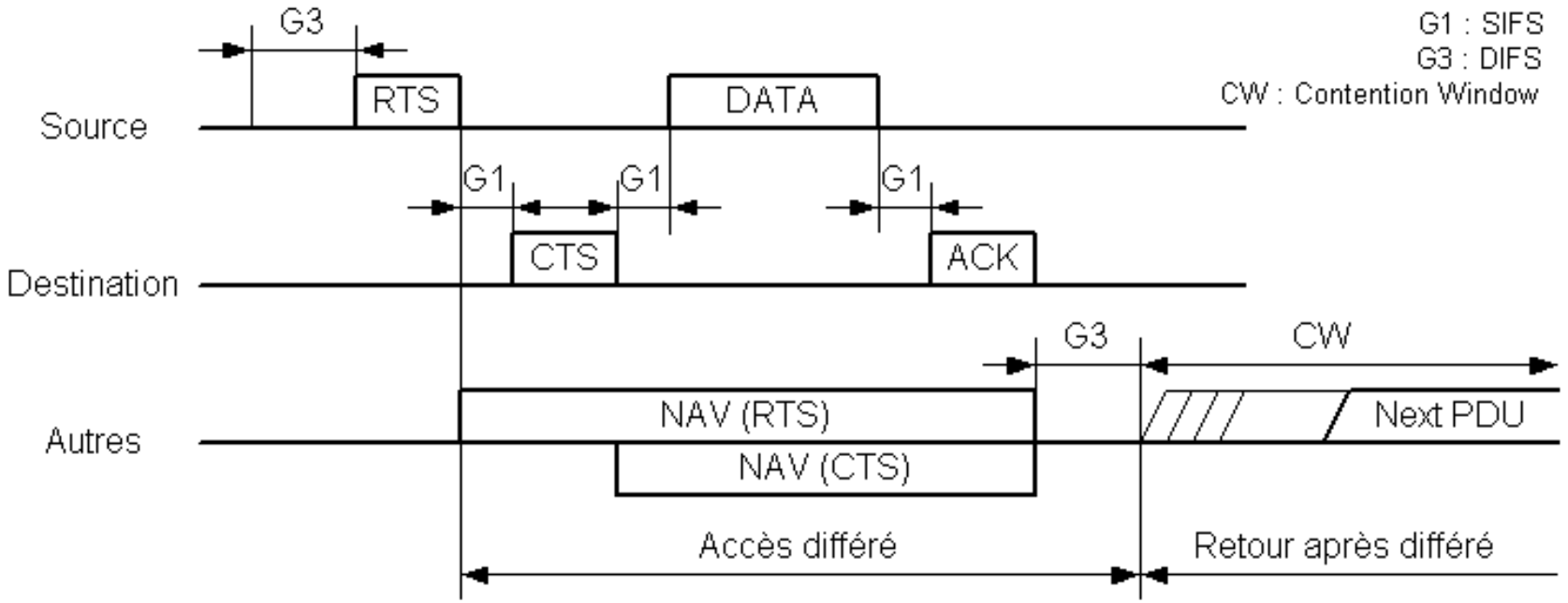
Priorité la plus basse: IFS =DIFS: trames de données sont émises si le support (media) est libre pendant un temps DIFS > PIFS > SIFS

=> Les trames ACK et CTS et celles du temps réel sont émises avant les trames de données



IFS et priorités

Un exemple de transfert complet



Autres services de la couche MAC

•**Somme de contrôle:**
La couche MAC du protocole 802.11 offre un mécanisme de contrôle d'erreur permettant de vérifier l'intégrité des trames

•**Fragmentation des trames:**
le taux d'erreur de transmission sur les réseaux sans fil augmente généralement avec des paquets de taille importante, c'est la raison pour laquelle la norme 802.11 offre un mécanisme de fragmentation, permettant de découper une trame en plusieurs morceaux (fragments).

•**Cryptage :**
WEP

•**Roaming:**
Passage d'une cellule à une autre

Autres services de la couche MAC

- **Synchronisation des stations:**

Les stations doivent rester synchronisées (nécessaire pour garder la synchronisation au cours des sauts, ou pour d'autres fonctions comme l'économie d'énergie.)

Synchronisation sur le Point d'Accès en utilisant le mécanisme suivant :

- Point d'Accès transmet périodiquement des trames appelées « trames balise »(beacon frame). Ces trames contiennent la valeur de l'horloge du Point d'accès.

- Les stations réceptrices vérifient la valeur de leur horloge au moment de la réception, et la corrige pour rester synchronisées avec l'horloge du Point d'Accès. Ceci évite des dérives d'horloge qui pourraient causer la perte de la synchronisation au bout de quelques heures de fonctionnement.

Autres services de la couche MAC

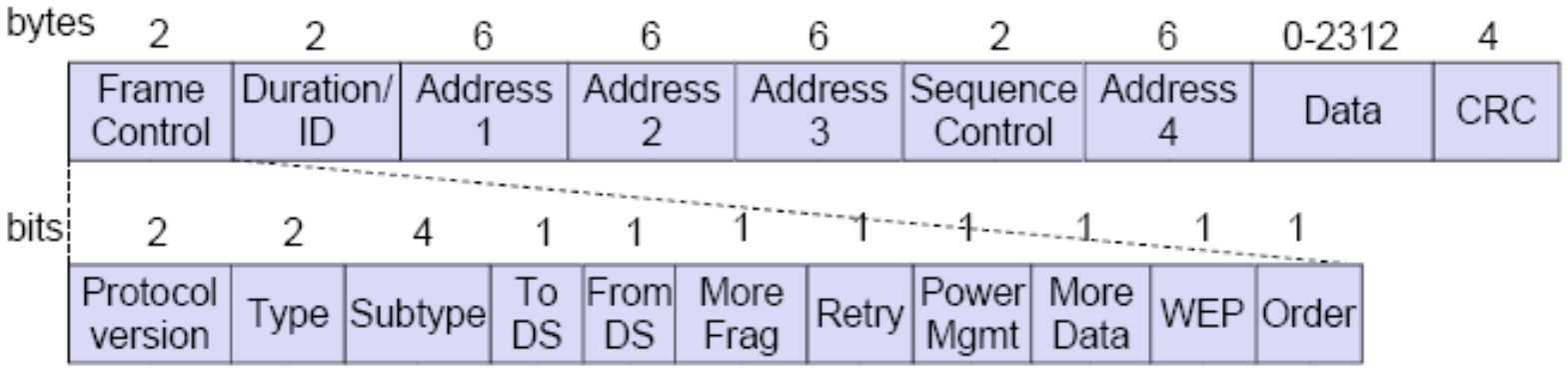
Gestion d'energie:

éteindre la radio si possible : état d'une station éveil ou sommeil

Point d'Accès maintient un enregistrement à jour des stations en mode d'économie d'énergie, et garde les paquets adressés à ces stations jusqu'à ce que les stations les demandent avec une Polling Request,
ou jusqu'à ce qu'elles changent de mode de fonctionnement.

Points d'Accès transmettent aussi périodiquement (dans les trames balise) des informations spécifiant quelles stations ont des trames stockées.
Ces stations peuvent ainsi se réveiller pour demander à récupérer ces trames.

format de trames MAC



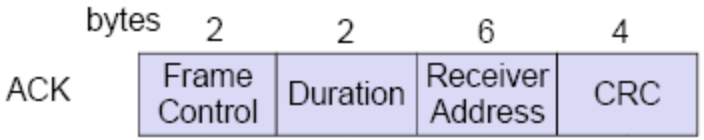
Version de protocole : 2 bits, pour prise en compte des évolutions
Type et **Sous-type** : 2 et 4 bits, définissent le type et le sous-type des trames (data, rts, …)
To DS : bit= 1 lorsque trame destinée au système de distribution (*DS*), 0 sinon.
Toute trame envoyée à un point d'accès possède ainsi un champ *To DS* positionné à 1.
From DS : bit=1 lorsque trame provient du système de distribution (*DS*), 0 sinon.
lorsque les deux champs *To* et *From=0* il s'agit d'une communication en mode *ad hoc*

format de trames MAC

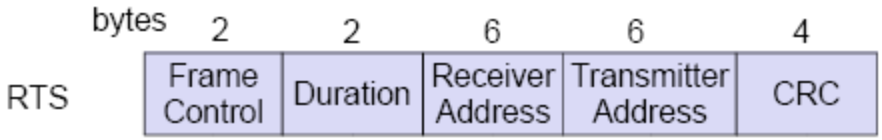
More Fragments : indique (lorsqu'il vaut 1) qu'il reste des fragments à transmettre
Retry : spécifie que fragment en cours est une retransmission d'un fragment précédemment envoyé
Power Management (*gestion d'énergie*) : si à 1, indique que la station ayant envoyé ce fragment entre en mode de gestion d'énergie
More Data (*gestion d'énergie*) : utilisé par le point d'accès pour spécifier à une station que des trames supplémentaires sont stockées en attente.
WEP : indique que l'algorithme de chiffrement WEP a été utilisé pour chiffrer le corps de la trame.
Order (*ordre*) : indique que la trame a été envoyée en utilisant la classe de service strictement ordonnée
Durée / ID : Ce champ indique la 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 : permet de distinguer les divers fragments d'une même trame. composé de deux sous-champs permettant de réordonner les fragments :
Le *numéro de fragment* + Le *numéro de séquence*
CRC : une somme de contrôle servant à vérifier l'intégrité de la trame.

format de trames MAC

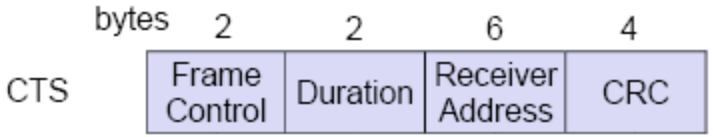
Acquittement



Request To Send



Clear To Send



Comment une station rejoint un AP ?

- Accès à un BSS existant

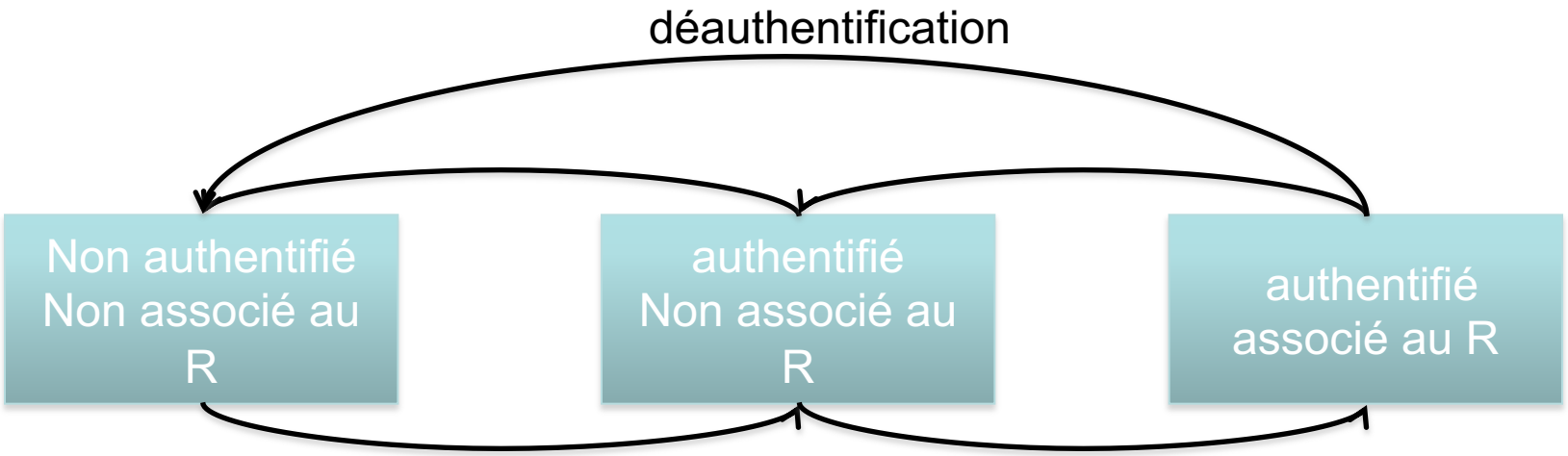
1. Ecoute active = recherche d'un point d'accès en transmettant une trame de demande d'enquète (Probe request frame) et attend la réponse d'éventuelles AP
   Ecoute passive = station attend de recevoir une trame balise (beacon frame)

2. Processus d'authentification

3. Processus d'association = échange d'info sur la cellule

Autres services de la couche MAC

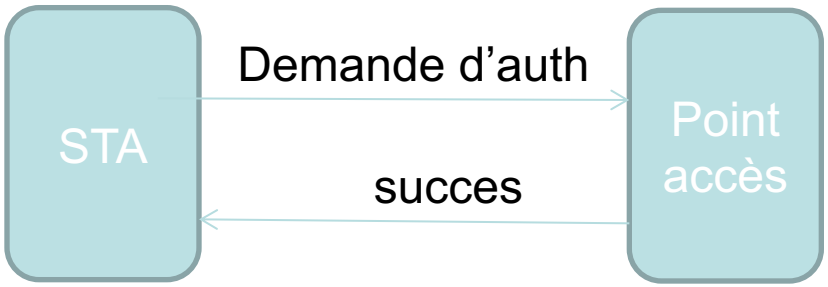
association



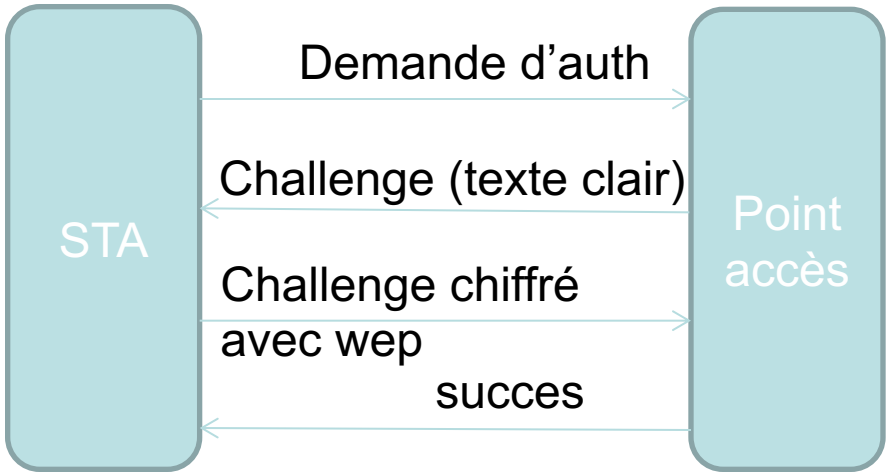
Autres services de la couche MAC

Deux modes d'authentification :
- ouvert (*open system)*
- partagé *(shared key)*

Open system



Shared key



Utiliser open system! Shared key moins sécurisé (possibilité de récupérer la clé wep avec les challenges)

Sécurité

•*Le groupe WIFI alliance* réunit les acteurs (commerciaux, chercheurs, …)pour promouvoir wifi => améliorer interopérabilité + sécurité

•Système de base : WEP (wireless encryption protocol)

Encryptage des données avec un algorithme de type RC4 utilisant une clée

Clée peut être cassée en récupérant 1e6 trames + algo de décryptage

•**Solution?**

=>wpa, wpa2, wpa3
=>carte à puce, coûteux, authentification par carte sim
=> Serveur d'authentification (radius)
=>vpn (virtual private network)
=> + filtrage des adresses, pas de nom par défaut !

Sécurité

WPA

- basé sur 802.11i, surcouche du WIFI (dans la couche réseau ?) (le wep reste présent)

- technologie TKIP : renouveler clé de manière régulière , perf moins bonne mais compatible avec WEP
  peut aussi être utilisé en mode pre shared key PSK (moins sécurisé, utilisation d'une phrase secrète partagée)

- Intégrité des données (CRC) amélioré

WPA2

utilise toute la norme 802.11i
cryptage AES plutôt que RC4
gestion des clées par le protocole CCMP, plus sur que TKIP

Sécurité

WPA 3
WPA2 cassé par une attaque faite au moment de la connection. WPA3 corrige cette faille

Méthode d'authentification appelée Simultaneous Authentication of Equals (SAE)
802.1x

« With SAE, the encryption password is changed each time a connection is established, so even if an attacker did trick their way into the network, they could only steal the passwords to decrypt data transmitted after that time. » *ieee spectrum*

Chiffrage à 192bits au lieu de 128 pour WPA 3 enterprise

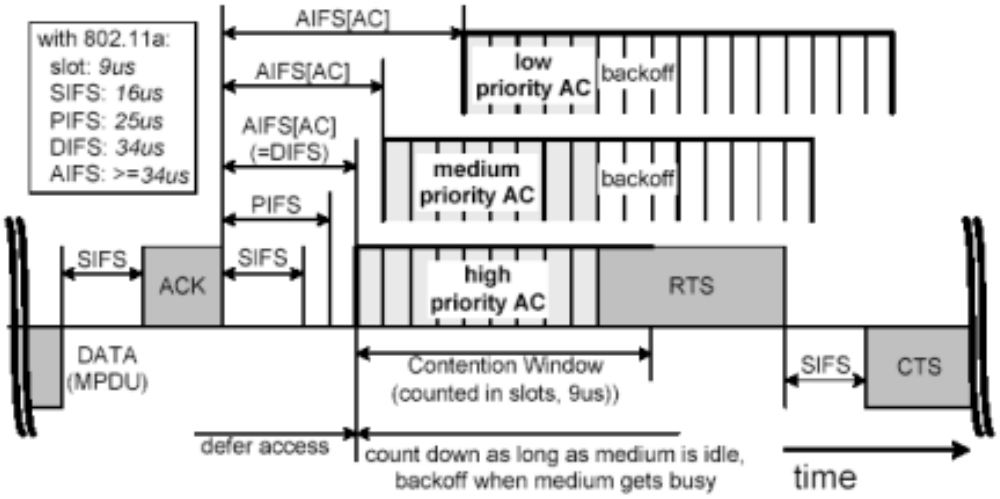
802.11e pour la QOS

•En resumant:

IEEE 802.11e a pour but d'améliorer la QoS (Quality of Service) en ajoutant deux nouvelles méthodes d'accès, EDCF (Extended DCF) et HCF (Hybrid Coordination Fonction).

HCF : méthode qui utilise le point d'accès pour gérer le trafic en définissant des périodes avec et sans contention

EDCF: 8 niveaux de priorité qui dépendent du temps IFS



802.11 mc

Version de maintenance/revision pour le standard IEEE 802.11 WLAN

Apport du « GPS local »

*More commonly known as **Wi-Fi Round-Trip-Time (WiFi RTT)**, allows computing devices to measure the distance to nearby Wi-Fi access points (APs) and determine their indoor location with a precision of 1-2 metres.*

With a single Wi-Fi access point, only a distance measurement is available. With three or more nearby APs, an app can trilaterate a device's location with an accuracy of one to two meters. Not all devices have the necessary hardware support yet for this feature.

Utilisé avec Android P

Ce que l'on n'a pas vu...

- Gestion du roaming (entre AP)
  - Scanning
  - Demande de réassociation
  - Réponse d'association
  - Acceptation de demande

- Gestion de puissance (éteindre la radio si possible, station active ou en sommeil)

- Synchronisation
  - découverte de Lan
  - maintien du Lan

- Gestion de MIB

⇒Utilisation de balises (petits paquets spéciaux) =beacon frame

Des antennes parmi tant d'autres

Les antennes ricorés permettent une émission du signal jusqu'à 6 km (environ 10 bd)! En 802.11b => permet la création de réseaux san fil citoyens (gratuit)

Ex: paris, chamalière ?

Les meilleures antennes peuvent aller jusqu'à 30 km