Introduction aux réseaux Wi-Fi

NET 4104 - Cours - Internet sans fil : concepts, technologies et architectures

Rémy Grünblatt – remy@grunblatt.org

février 2022

Avant de commencer...

- Première fois que cette présentation est donnée !
- Feedback apprécié, anonymement ou non, par mail (mettre "[NET4104]" dans le sujet):
  - remy@grunblatt.org
  - remy.grunblatt@telecom-sudparis.eu
- Posez moi des questions pendant le cours !

$\rightarrow$ **Panorama autour des réseaux Wi-Fi**

Avant de commencer...

Introduction et rappels autour des ondes électro-magnétiques

Équations de Maxwell

Maxwell-Faraday:

$$\overrightarrow{rot}\ \vec{E} = -\frac{\partial \vec{B}}{\partial t}$$

Maxwell-Ampère:

$$\overrightarrow{rot}\ \vec{B} = \mu_0 \vec{j} + \mu_0 \varepsilon_0 \frac{\partial \vec{E}}{\partial t}$$

Équations de Maxwell

Maxwell-Faraday:

$$\overrightarrow{rot}\ \vec{E} = -\frac{\partial \vec{B}}{\partial t}$$

Maxwell-Ampère:

$$\overrightarrow{rot}\ \vec{B} = \mu_0 \vec{j} + \mu_0 \varepsilon_0 \frac{\partial \vec{E}}{\partial t}$$

Courant variable $\vec{j}(t)$ $\Rightarrow$ Champ magnétique variable $\vec{B}(t)$

$\Rightarrow$ Champ électrique variable $\vec{E}(t)$

$\Rightarrow \ldots$

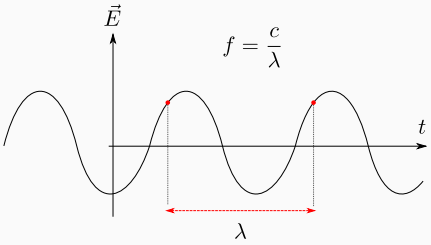
$\rightarrow$ propagation d'une onde électromagnétique

Linéarité !

Caractéristiques des ondes électro-magnétiques

Caractéristiques importantes :

- Amplitude
- Longueur d'onde (λ, en m)
- Fréquence (f, en Hz)



On peut décomposer un signal « classique » (périodique) en une somme de sinusoïdes (Fourier) :

$$f(x) = \sum_{n=-\infty}^{+\infty} c_n(f) \mathrm{e}^{\mathrm{i}2\pi \frac{n}{T} x}$$

$$\text{avec } c_n(f) = \frac{1}{T} \int_T f(t) \mathrm{e}^{-\mathrm{i}2\pi \frac{n}{T} t} \mathrm{d}t$$

(et réciproquement)

Organisation du spectre

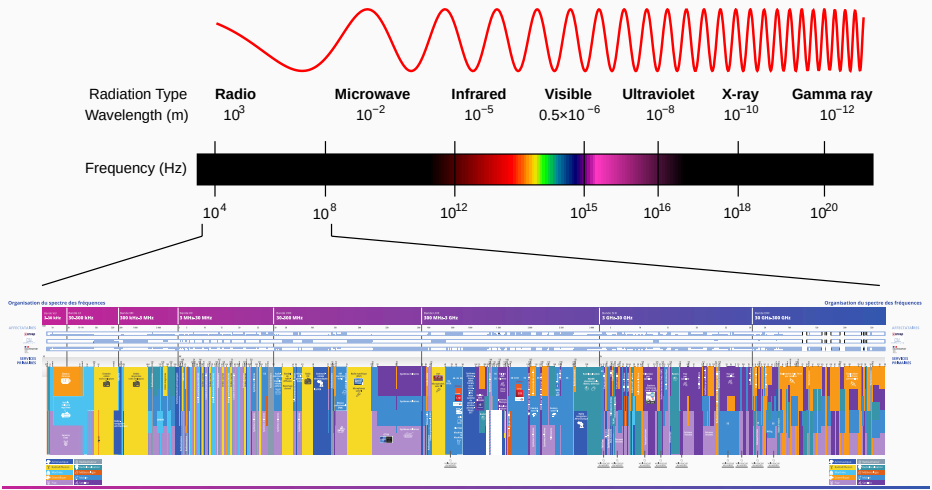


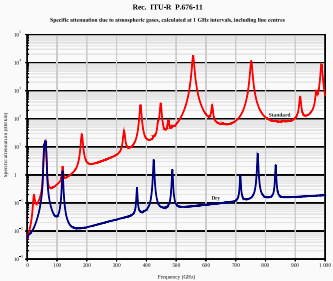
Illustration : CC-BY-SA 3.0 – Inductiveload, NASA @ Wikimedia (haut) et ANFR (bas)

Propagation des ondes électro-magnétiques

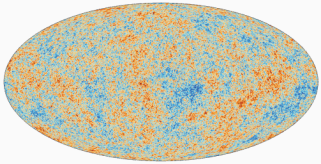
Les ondes électro-magnétiques :

- sont omniprésentes
- se propagent dans la majorités des medias
- subissent des réflections, réfractions, diffractions
- intéragissent avec le milieu différemment selon leurs fréquences

JrPol – CC-BY-SA 4.0



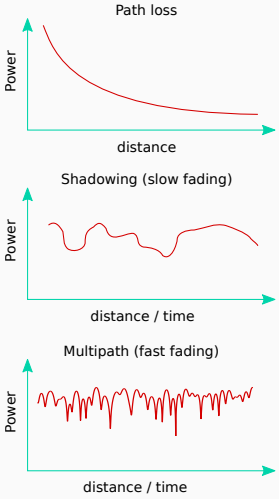
Röntgen – First X-Ray

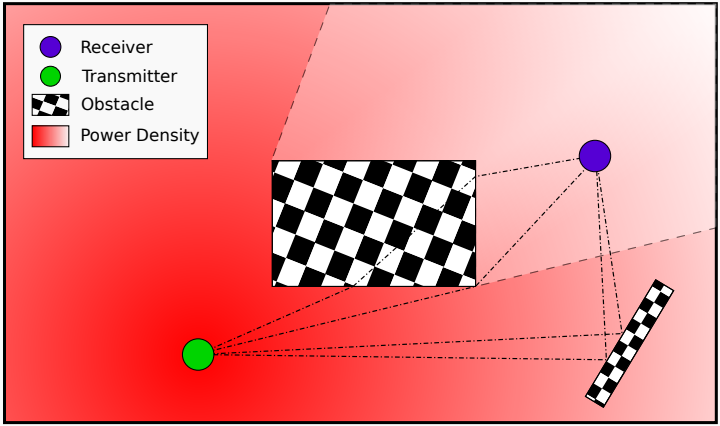


ESA - Cosmic Microwave Background

Source: NASA/IPAC – Public Domain

Modélisation de canal





Bilan de liaison

$$P_{reçue} = P_{transmise} + Gains - Pertes$$

- *Gains* : Gains d'antennes en émission et réception
- *Pertes* : Pertes liées aux câbles, à la propagation (path loss, shadowing, fast-fading)

Outils théoriques

Relation de Shannon-Hartley

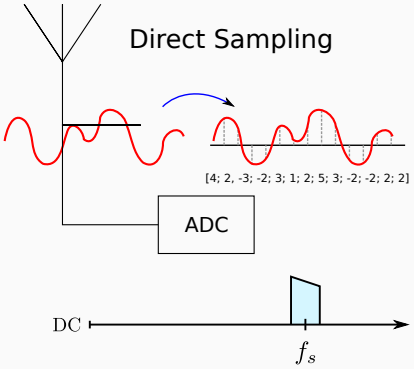
$$C = B \log_2 \left(1 + \frac{S}{N}\right)$$

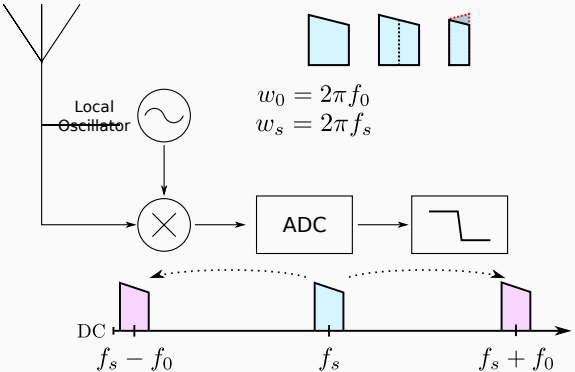
- C : Capacité en bps
- B : Largeur de canal en Hz
- N : Puissance moyenne du bruit
- S : Puissance moyenne du signal

Théorème de Nyquist-Shannon

Pour sampler un signal, il faut une fréquence d'échantillonnage supérieure à deux fois la fréquence maximale du signal.

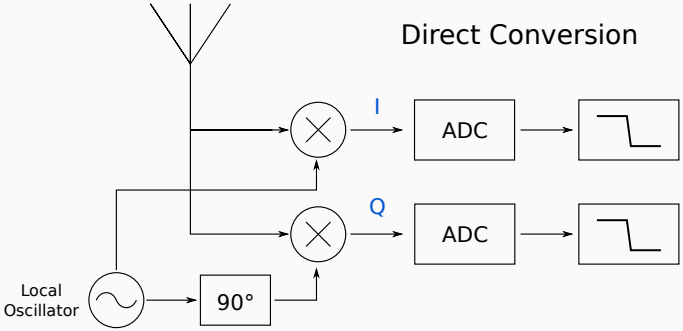
Sampling et Décodage Numérique

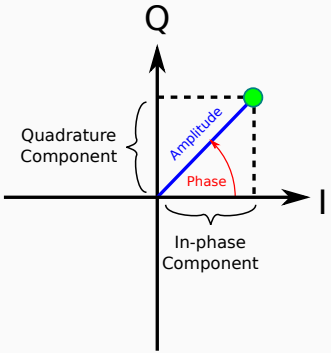




$$cos(w_0 t) * cos(w_s t) = \frac{1}{2} cos((w_0 - w_s)t) + \frac{1}{2} cos((w_0 + w_s)t)$$

Sampling et Décodage Numérique : I et Qs





Fonctionnement des réseaux Wi-Fi / 802.11

Petit Historique

fixed station

portable station

moving station

ALOHANet

1971

1997

IEEE 802.11

1999

802.11a
802.11b

Apple iBook

First laptop with Wireless Lan

2003

802.11g

2007

Apple iPhone

Wi-Fi enabled smartphone

2009

802.11n

2010

802.11p (V2V)

2013

802.11ac

2021

802.11ax

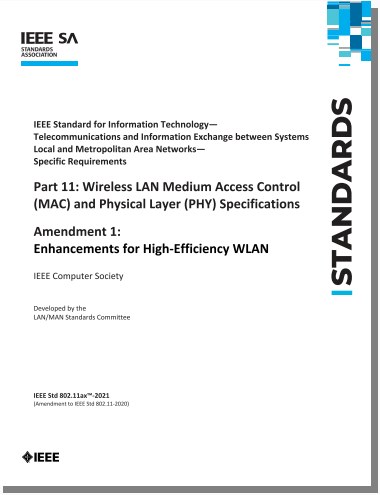
Intel Centrino

Marketing to the general public

AR.Drone

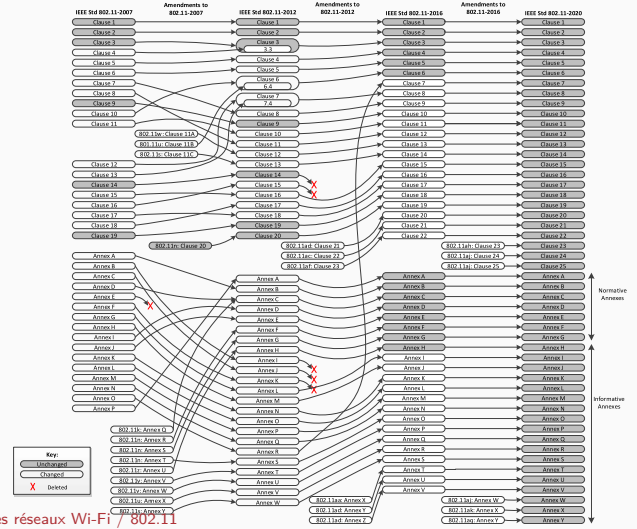
Wi-Fi Quadcopter

Les standards 802.11...



. . . évoluent dans le temps. . .

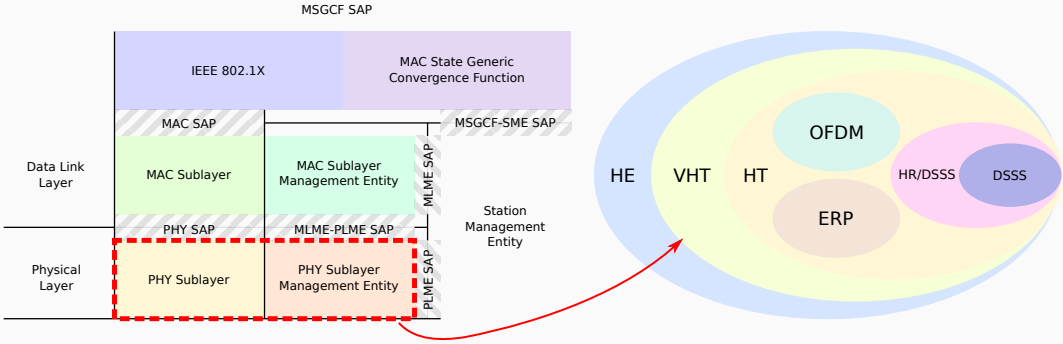
2020 – Figure 1—The evolution of numbering in IEEE Std 802.11



. . . et s'organisent autour de plusieurs couches physiques

2020 – 4.9 Reference model

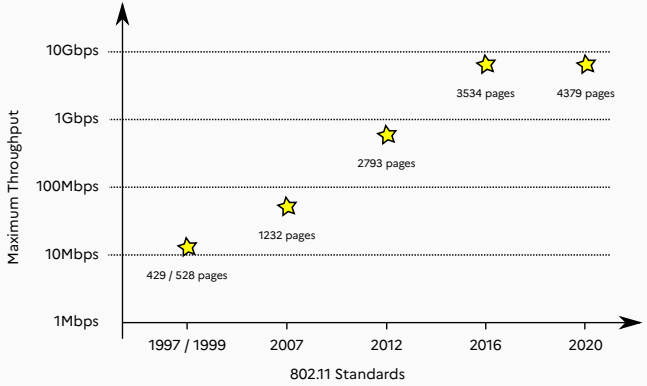
Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications



Les standards 802.11

Name	Year	Document
802.11ax	2021	Amendment
802.11	2020	Standard
802.11	2016	Standard *
802.11ac	2013	Amendment *
802.11	2012	Standard *
802.11n	2009	Amendment *
802.11	2007	Standard *
802.11g	2003	Amendment *
802.11b	1999	Amendment *
802.11a	1999	Amendment *
802.11	1999	Standard *
802.11	1997	Standard *

* : Superseded



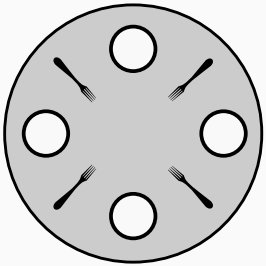
Couche MAC

Qu'est ce que c'est ?

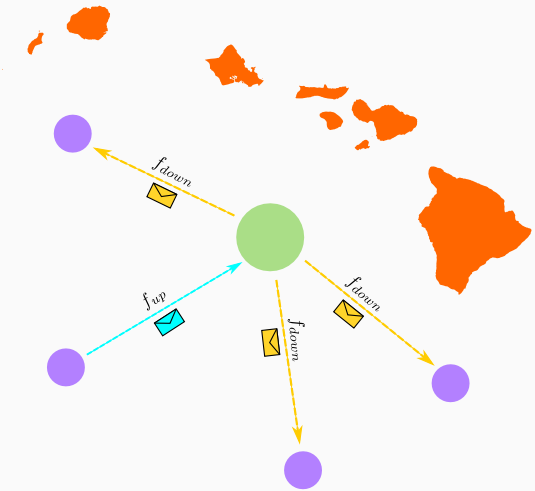
MAC : Medium Access Control

Qu'est ce que c'est ?

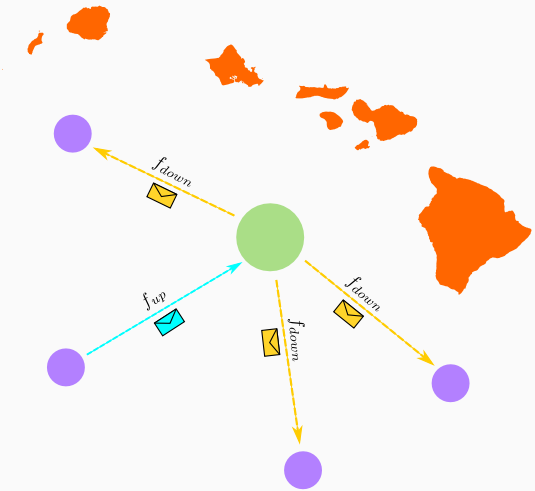
MAC : Medium Access Control



Précurseur: Aloha Net



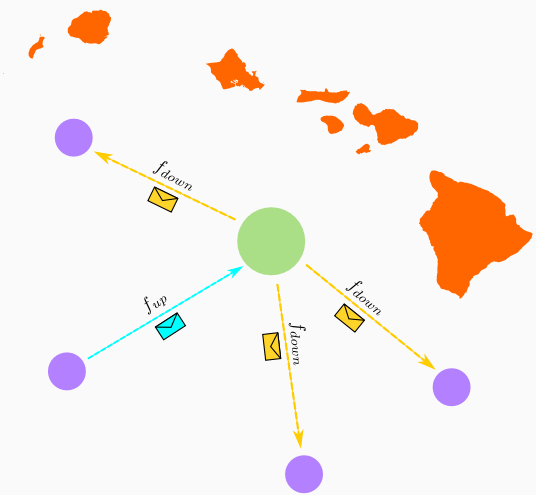
Précurseur: Aloha Net



Principe de base :

- Une fréquence montante, utilisé par les « stations » pour communiquer vers un nœud spécial (qui sert de « hub »)
- Une fréquence descendante, qui sert au « hub » pour communiquer avec les « stations »

Précurseur: Aloha Net



Principe de base :

- Une fréquence montante, utilisé par les « stations » pour communiquer vers un nœud spécial (qui sert de « hub »)
- Une fréquence descendante, qui sert au « hub » pour communiquer avec les « stations »

Accès au medium :

- Quand une station souhaite transmettre, elle transmet
- Le hub répond avec un message court (acquittement) pour confirmer la bonne réception des données
- Si la station n'entend pas d'acquittement, elle retransmet après une période de temps aléatoire

Principe de base : CSMA/CA et DCF

2020 – 10.3 DCF

→ Carrier Sense Multiple Access / Collision Avoidance

Algorithme distribué de partage d'accès au medium et d'évitement de collision

Principe de base : CSMA/CA et DCF

2020 – 10.3 DCF

→ Carrier Sense Multiple Access / Collision Avoidance

Algorithme distribué de partage d'accès au medium et d'évitement de collision

- **Carrier Sense** : écoute du medium avant d'émettre pour éviter les collisions
  1. Si le medium est libre, on émet
  2. Si le medium est occupé, *backoff* aléatoire avant d'émettre
- **Fréquence unique** partagée par les stations (montante *et* descendante)
- **Acquittement positif** (si bien reçu, j'acquitte)
- **Ré-émission** des trames non acquittées

Limites de CSMA/CA

2020 – 3. Definitions, acronyms, and abbreviations

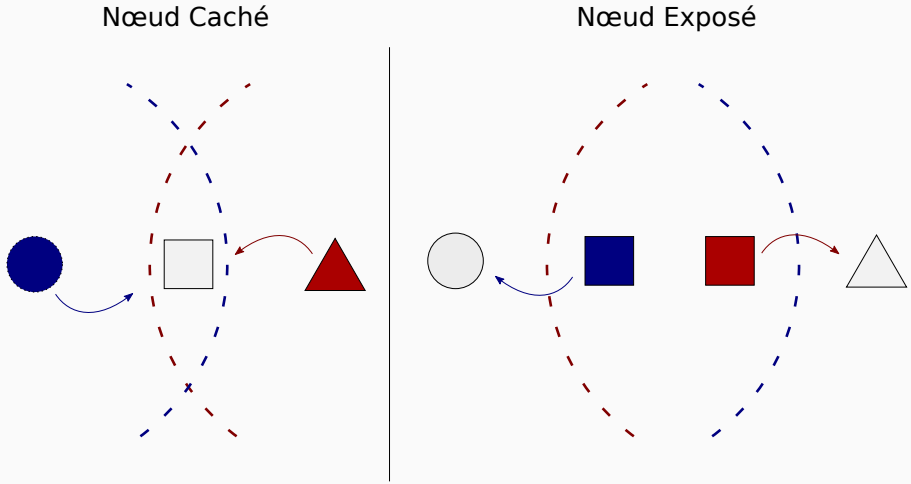


Illustration avec trois stations

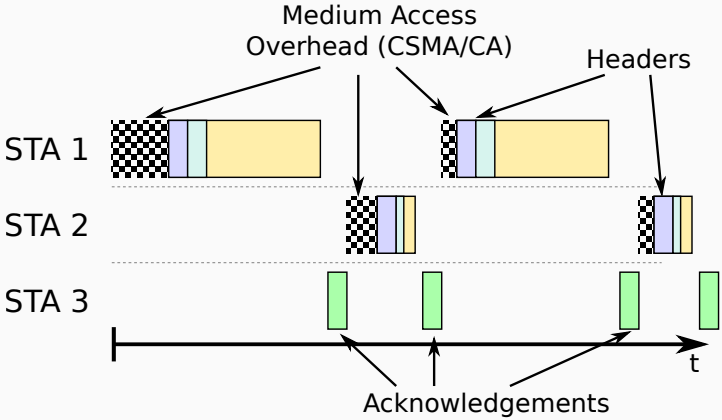
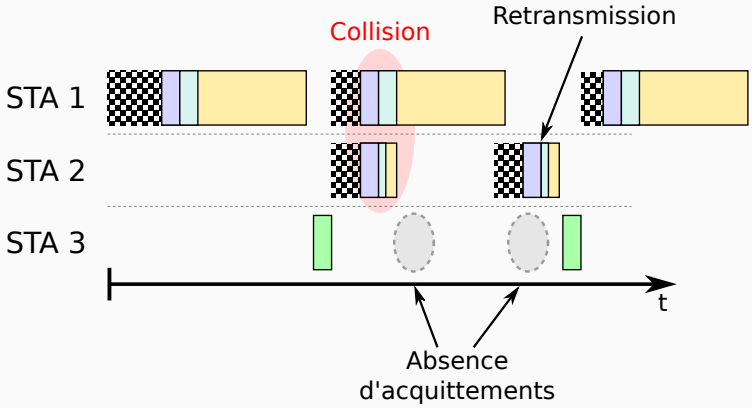


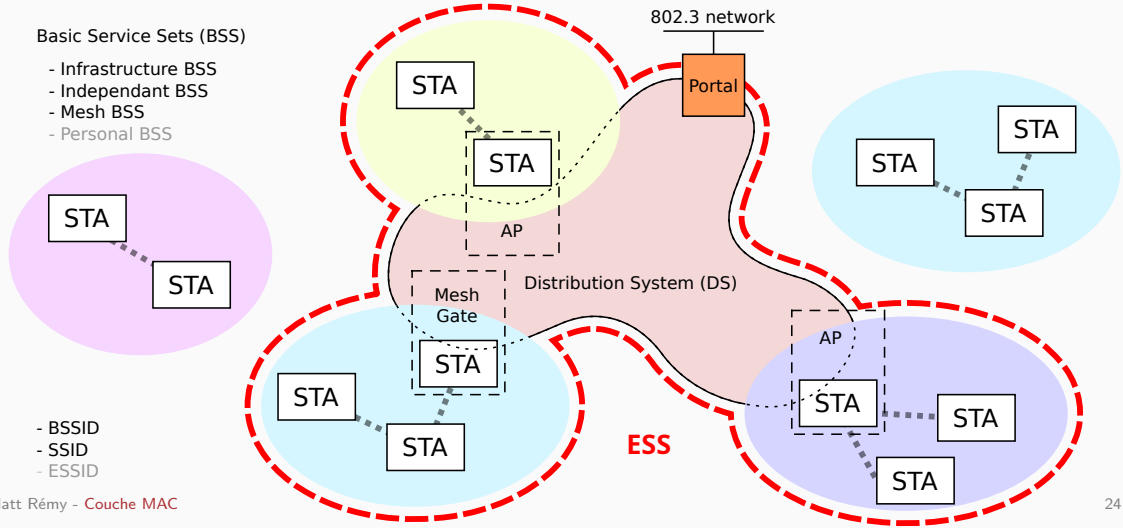
Illustration avec trois stations: collision



Architectures des réseaux Wi-Fi

Basic Service Sets (BSS)

- Infrastructure BSS
- Independant BSS
- Mesh BSS
- Personal BSS



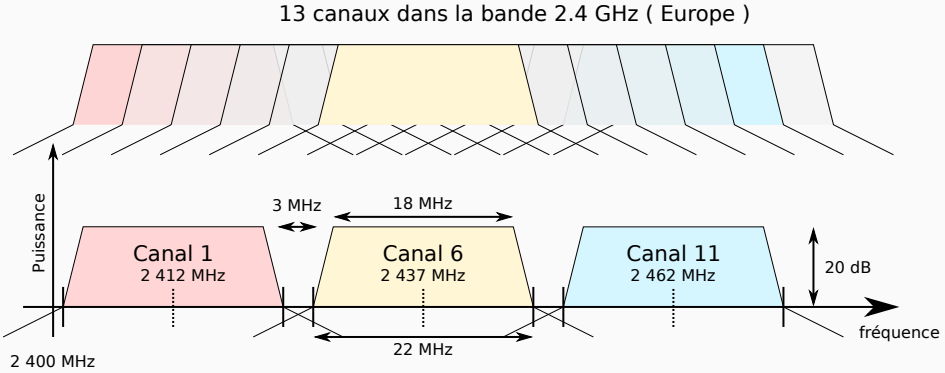
- BSSID
- SSID
- ESSID

Couche Physique

Bandes de fréquences

Canaux dans la bande 2.4 GHz (20 MHz)

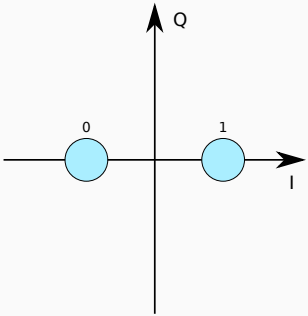
2020 – 17.3.8.4.1 Operating frequency range



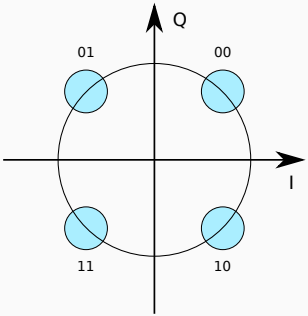
Modulations

2020 – 17.3.5.8 Subcarrier modulation mapping

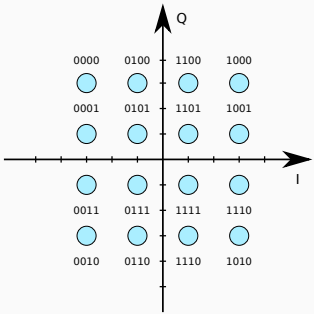
BPSK



QPSK



16-QAM



64-QAM

(...)

256-QAM

(...)

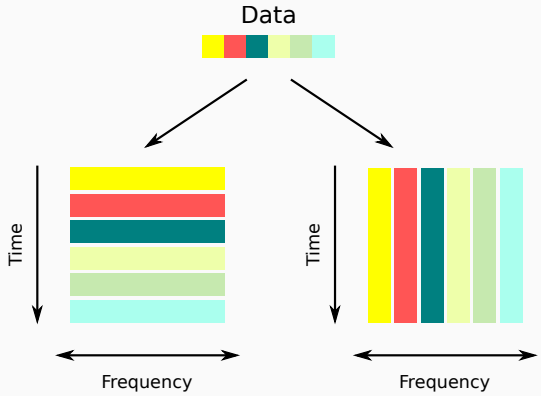
1024-QAM

(...)

OFDM

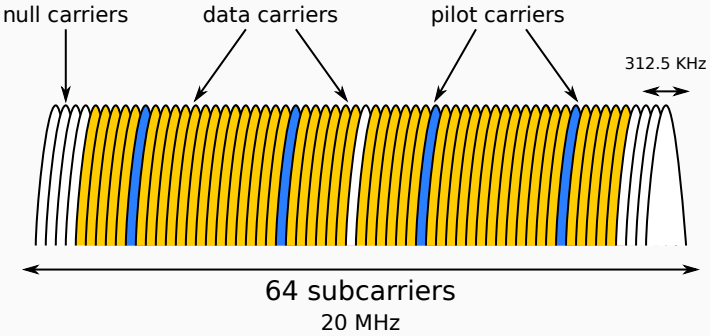
2020 – 17. Orthogonal frequency division multiplexing (OFDM) PHY specification

OFDM: Orthogonal Frequency Division Multiplexing



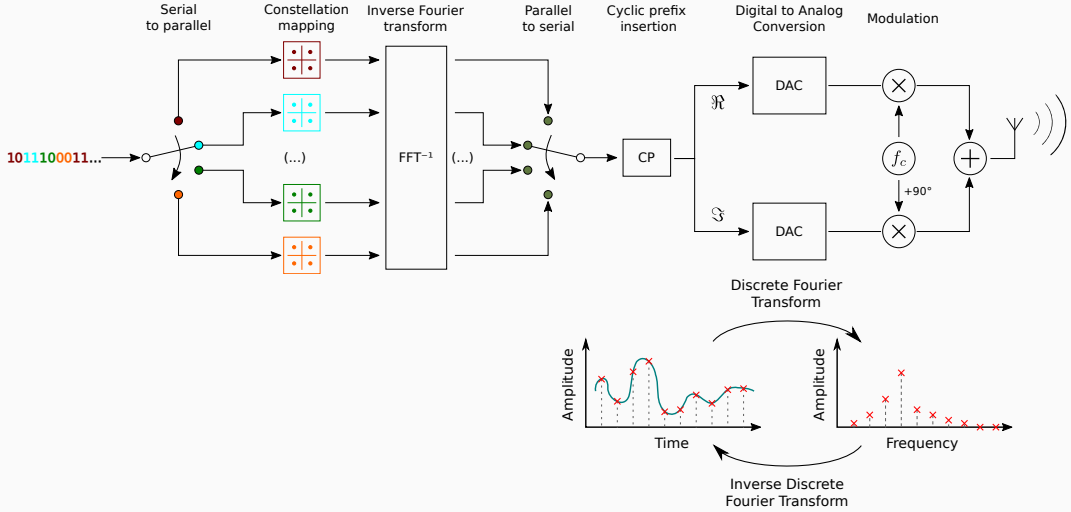
Principe: Transformer un flux « haut débit » en plusieurs flux « bas débits » transmis sur plusieurs fréquences (multiplexage) orthogonales

Décomposition du canal (20 MHz)



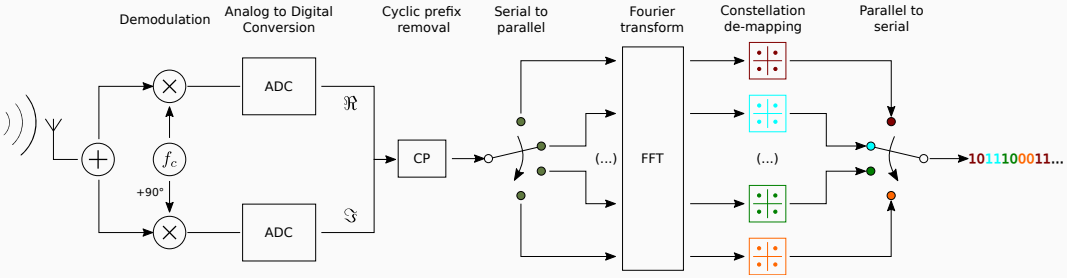
Chaîne de transmission (OFDM)

2020 – Figure 17-12—Transmitter and receiver block diagram for the OFDM PHY



Chaîne de réception (OFDM)

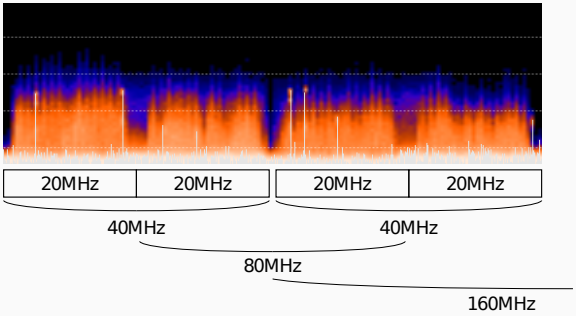
👁 **2020 – Figure 17-12—Transmitter and receiver block diagram for the OFDM PHY**



Aggrégation de canaux

2020 – 19.3.7 Mathematical description of signals

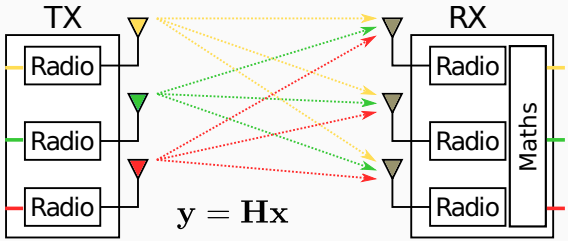
- 40 MHz : HT PHY
- 80 MHz, 160 MHz, 80 + 80 MHz : VHT PHY



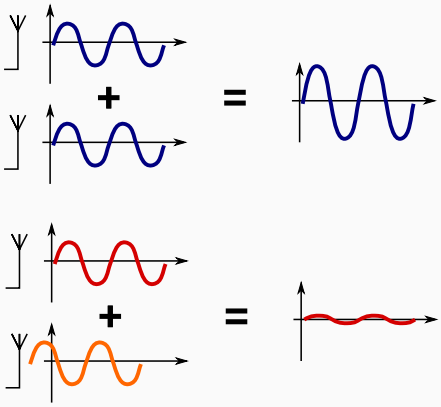
Utilisation de plusieurs antennes: MIMO

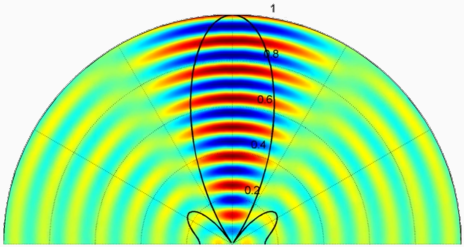
2020 – 19.3 HT PHY

MIMO: Multiple Input, Multiple Output



Utilisation de plusieurs antennes: BeamForming

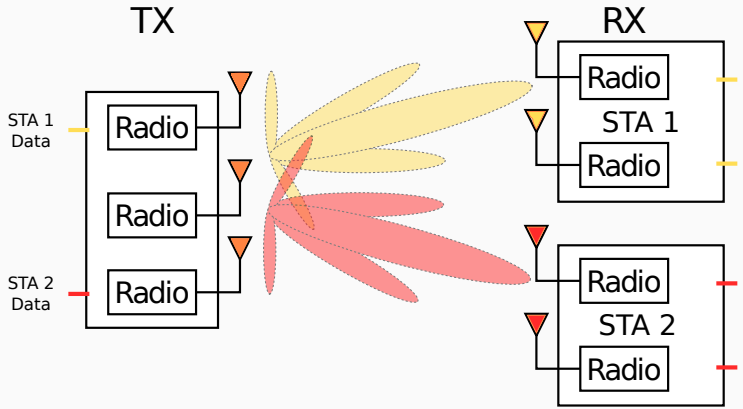




MU-MIMO

2020 – 21.3.11.1 General

Multi-User MIMO = Beamforming + MIMO !



Capacité = f(Paramètres de transmission)

Guard Interval :

- SGI : 0.4 μs
- LGI : 0.8 μs

Largeur de transmission :

- 20 MHz
- 40 MHz
- 80 MHz
- 160 MHz

Nombre de flux spatiaux :

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8

MCS Index :

MCS Index	Modulation	Taux d'encodage
0	BPSK	1/2
1	QPSK	1/2
2	QPSK	3/4
3	16-QAM	1/2
...		

Capacité = f(Paramètres de transmission)

Guard Interval :

- SGI : 0.4 μs
- LGI : 0.8 μs

Largeur de transmission :

- 20 MHz
- 40 MHz
- 80 MHz
- 160 MHz

Nombre de flux spatiaux :

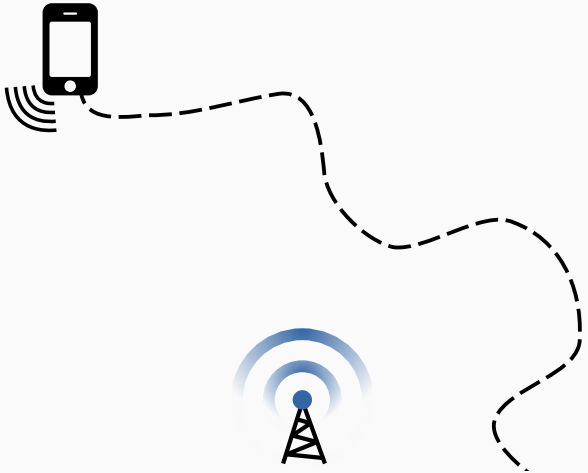
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8

MCS Index :

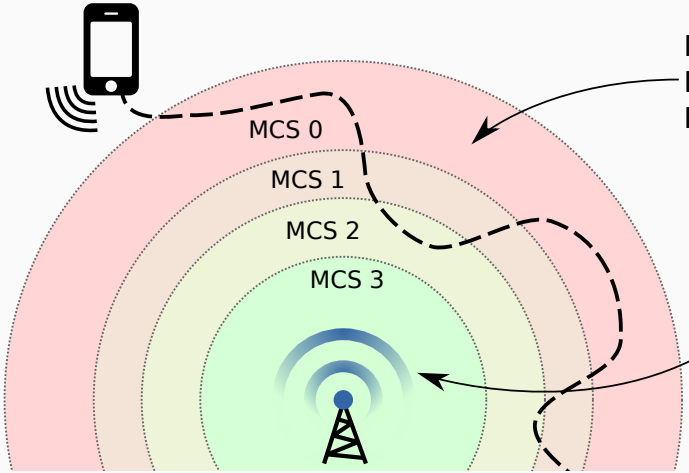
MCS Index	Modulation	Taux d'encodage
0	BPSK	1/2
1	QPSK	1/2
2	QPSK	3/4
3	16-QAM	1/2
...		

- 40 Mhz + LGI + 1 flux + MCS 3 $\rightarrow$ 54 Mbps
- 20 Mhz + SGI + 2 flux + MCS 7 $\rightarrow$ 144.4 Mbps

Adaptation de débit à la mobilité



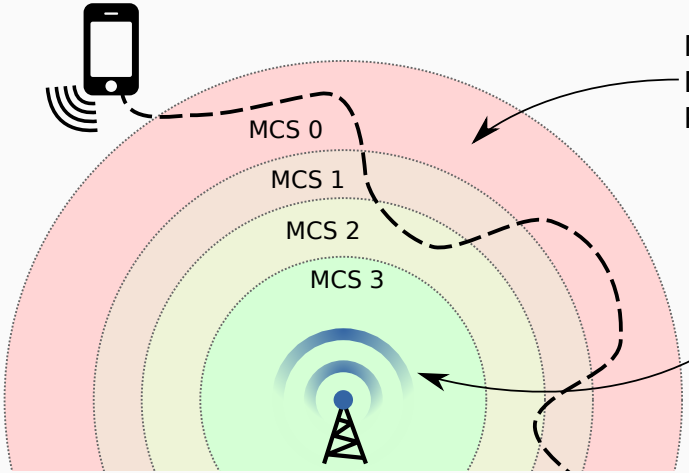
Adaptation de débit à la mobilité



Modulation plus robuste
Débit plus faible
Portée plus élevée

Modulation moins robuste
Débit plus élevé
Portée plus limitée

Adaptation de débit à la mobilité



Modulation plus robuste
Débit plus faible
Portée plus élevée

Modulation moins robuste
Débit plus élevé
Portée plus limitée

→ **Algorithmes d'adaptation de débit**

Anomalie de performances

Que se passe-t-il quand deux nœuds, l'un émettant à 2Mbps et l'un émettant à 200Mbps se partagent le medium ?

Anomalie de performances

Que se passe-t-il quand deux nœuds, l'un émettant à 2Mbps et l'un émettant à 200Mbps se partagent le medium ?

Suppositions / Approximations :

- Trames de 1500 octets envoyées en continu
- Équité dans l'accès au medium : une trame sur deux par nœud
- Approximation grossière des temps d'émission / Accès au medium instantané

Anomalie de performances

Que se passe-t-il quand deux nœuds, l'un émettant à 2Mbps et l'un émettant à 200Mbps se partagent le medium ?

Suppositions / Approximations :

- Trames de 1500 octets envoyées en continu
- Équité dans l'accès au medium : une trame sur deux par nœud
- Approximation grossière des temps d'émission / Accès au medium instantané

Quel est le débit effectif pour chaque nœud ?

Anomalie de performances

Que se passe-t-il quand deux nœuds, l'un émettant à 2Mbps et l'un émettant à 200Mbps se partagent le medium ?

Suppositions / Approximations :

- Trames de 1500 octets envoyées en continu
- Équité dans l'accès au medium : une trame sur deux par nœud
- Approximation grossière des temps d'émission / Accès au medium instantané

Quel est le débit effectif pour chaque nœud ?

Quelle solutions potentielles ?

Anomalie de performances

Que se passe-t-il quand deux nœuds, l'un émettant à 2Mbps et l'un émettant à 200Mbps se partagent le medium ?

Suppositions / Approximations :

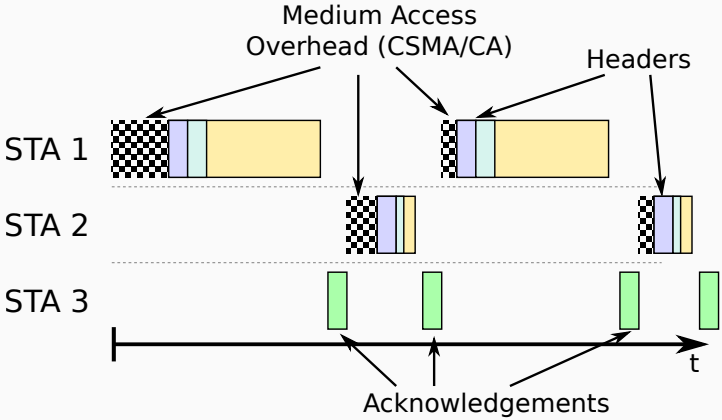
- Trames de 1500 octets envoyées en continu
- Équité dans l'accès au medium : une trame sur deux par nœud
- Approximation grossière des temps d'émission / Accès au medium instantané

Quel est le débit effectif pour chaque nœud ?

Quelle solutions potentielles ?

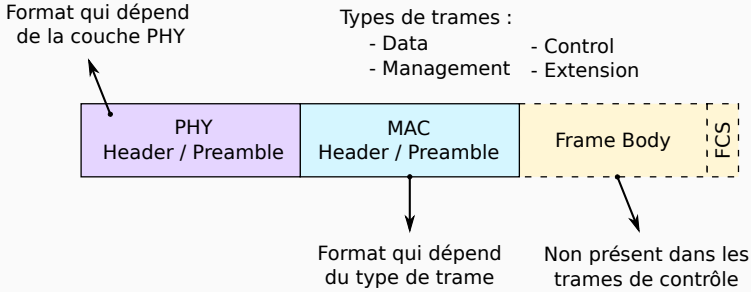
→ Aggrégation de trames

Retour sur CSMA/CA / Framing



Framing

2020 – 9.3 Format of individual frame types



Management Frames

- Beacon
- Association Request / Response
- Authentication / Deauthentication

Control Frames

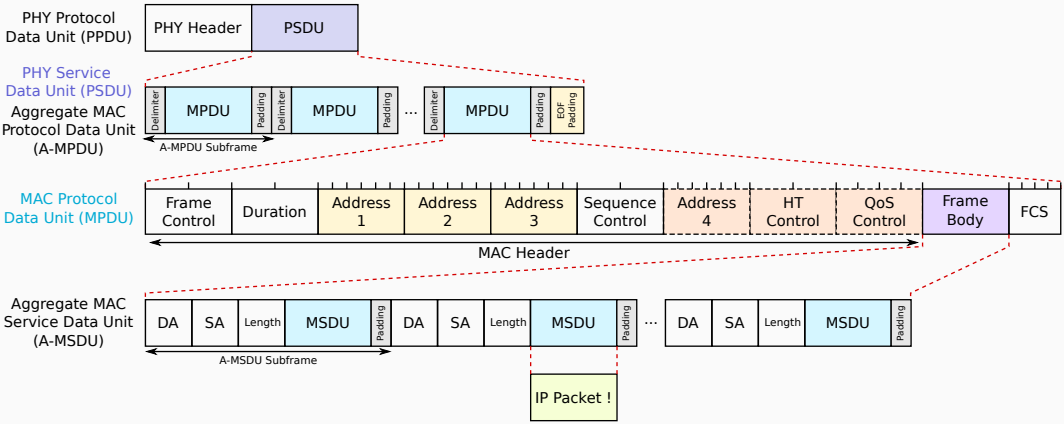
- RTS / CTS
- Ack / Block Ack

Data Frames

- MSDU
- A-MSDU

Framing et aggrégation de trames

2020 – 9.3 Format of individual frame types



Les adresses SA, TA, RA et DA

- SA: Source Address
- TA: Transmitter Address
- RA: Receiver Address
- DA: Destination Address

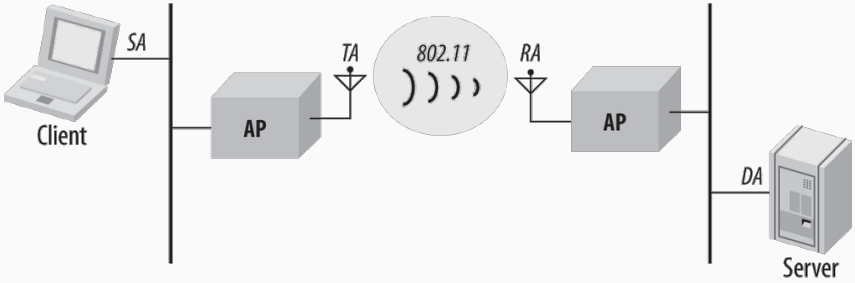


Image : Matthew Gast - 802.11 Wireless Networks: The Definitive Guide

Sécurité des réseaux sans fils

The CIA triad

Confidentialité

The CIA triad

Confidentialité

- Simple de savoir quelle station transmet ✗
- Simple d'écouter le medium ✗
- Failles régulières sur les protocoles de sécurisation ✗

The CIA triad

Confidentialité

- Simple de savoir quelle station transmet ✗
- Simple d'écouter le medium ✗
- Failles régulières sur les protocoles de sécurisation ✗

Disponibilité

The CIA triad

Confidentialité

- Simple de savoir quelle station transmet ✗
- Simple d'écouter le medium ✗
- Failles régulières sur les protocoles de sécurisation ✗

Disponibilité

- Simple à brouiller ✗

The CIA triad

Confidentialité

- Simple de savoir quelle station transmet ✗
- Simple d'écouter le medium ✗
- Failles régulières sur les protocoles de sécurisation ✗

Disponibilité

- Simple à brouiller ✗

Intégrité

The CIA triad

Confidentialité

- Simple de savoir quelle station transmet ✗
- Simple d'écouter le medium ✗
- Failles régulières sur les protocoles de sécurisation ✗

Disponibilité

- Simple à brouiller ✗

Intégrité

- Failles régulières sur les protocoles de sécurisation ✗

The CIA triad

Confidentialité

- Simple de savoir quelle station transmet ✗
- Simple d'écouter le medium ✗
- Failles régulières sur les protocoles de sécurisation ✗

Disponibilité

- Simple à brouiller ✗

Intégrité

- Failles régulières sur les protocoles de sécurisation ✗

Mais beaucoup d'efforts et d'améliorations au cours du temps ! ✓

Standards de sécurisation

Protocoles de sécurisation :

- 1997 : OPEN
- 1997 : WEP (déprécié)
- 2003 : WPA (déprécié)
- 2004 : WPA 2
- 2018 : WPA 3

Mode de fonctionnement :

- Personnel
- Entreprise

Type d'attaques :

- Man-in-the-Middle
- Key-recovery
- Traffic Decryption
- Denial of Service

- Publications de Mathy Vanhoef : KRACK, DragonBlood, ...
- *A Comprehensive Taxonomy of Wi-Fi Attacks – 2020 – Mark Vink*

Architectures de réseaux - Des besoins différents

Hot-Spot

- Open Membership
- Clients indifférenciés

→ OPEN / Portail Captif

Réseau Personnel

- Managed Membership
- Clients indifférenciés

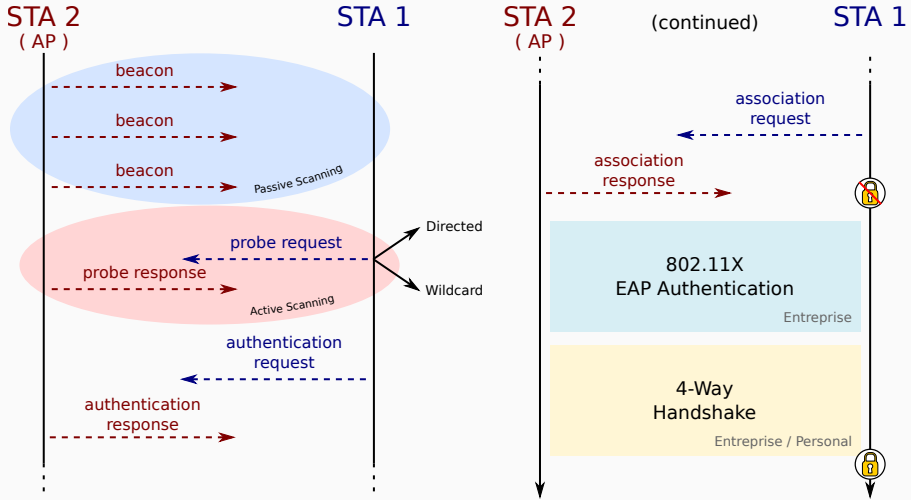
→ Pre-Shared Key (PSK)

Réseau Entreprise

- Managed Membership
- Clients différenciés

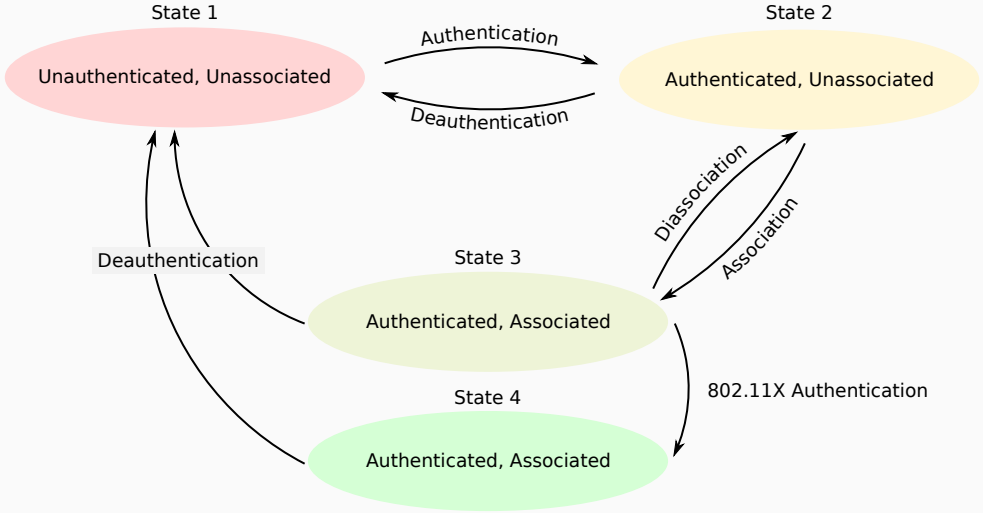
→ 802.11X (Radius)

Anatomie d'une connexion à un réseau Wi-Fi



Machine à états authentification / association

2020 – 11.3 STA authentication and association



Authentication et Association

Authentication **Ne veut pas dire sécurisation !**

- Shared Key Authentication — WEP
- Open System Authentication — WPA 1 et WPA 2
- Simultaneous Authentication of Equals (SAE) — WPA3
- Fast Transition Authentication (FT) / Fast Initial Link Setup (FILS)

Cette étape ne sert globalement pas à grand chose... (mis à part pour SAE)

Authentication et Association

Authentication **Ne veut pas dire sécurisation !**

- Shared Key Authentication — WEP
- Open System Authentication — WPA 1 et WPA 2
- Simultaneous Authentication of Equals (SAE) — WPA3
- Fast Transition Authentication (FT) / Fast Initial Link Setup (FILS)

Cette étape ne sert globalement pas à grand chose... (mis à part pour SAE)

Association **Ne veut pas dire sécurisation !**

- Association de la STA à un point d'accès (AP) spécifique.

Authentication et Association

Authentication **Ne veut pas dire sécurisation !**

- Shared Key Authentication — WEP
- Open System Authentication — WPA 1 et WPA 2
- Simultaneous Authentication of Equals (SAE) — WPA3
- Fast Transition Authentication (FT) / Fast Initial Link Setup (FILS)

Cette étape ne sert globalement pas à grand chose... (mis à part pour SAE)

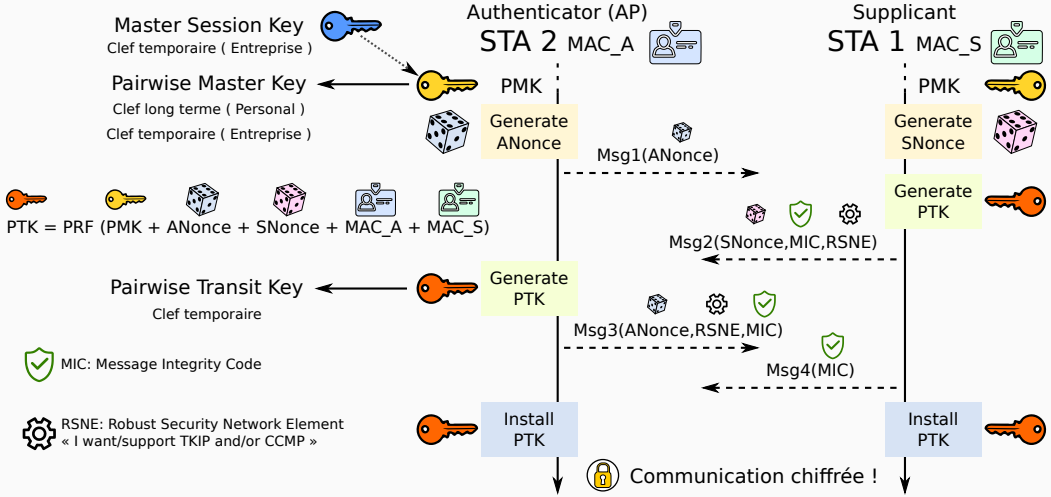
Association **Ne veut pas dire sécurisation !**

- Association de la STA à un point d'accès (AP) spécifique.

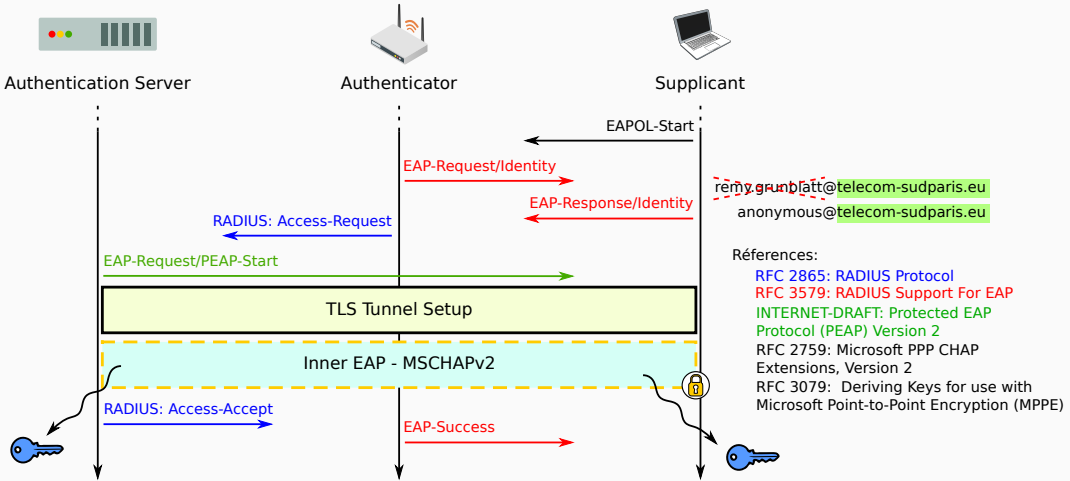
Une STA peut avoir **plusieurs** authentifications en même temps, mais ne peut avoir qu'**une** association à la fois !

The 4-way handshake

2020 – 12.7.6 4-way handshake

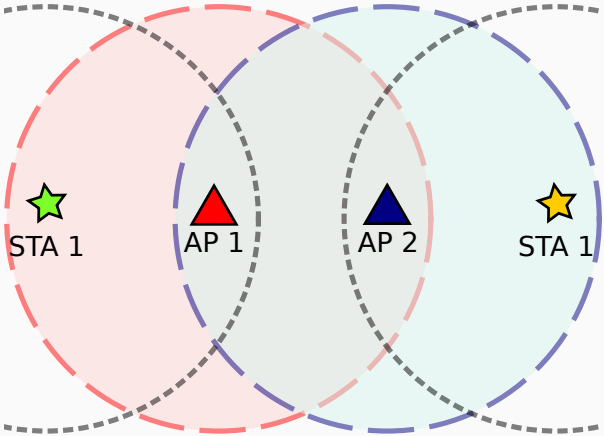


802.1X

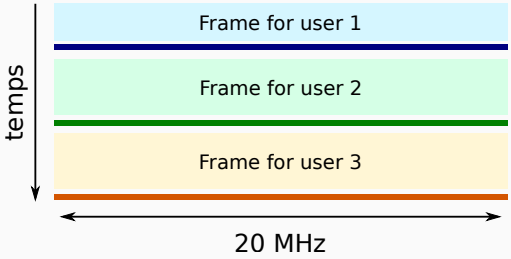

Authentication Server
Authenticator
Supplicant
EAPOL-Start
EAP-Request/Identity
remy.grunblatt@telecom-sudparis.eu
EAP-Response/Identity
anonymous@telecom-sudparis.eu
RADIUS: Access-Request
EAP-Request/PEAP-Start
TLS Tunnel Setup
Inner EAP - MSCHAPv2
RADIUS: Access-Accept
EAP-Success
Réferences:
RFC 2865: RADIUS Protocol
RFC 3579: RADIUS Support For EAP
INTERNET-DRAFT: Protected EAP Protocol (PEAP) Version 2
RFC 2759: Microsoft PPP CHAP Extensions, Version 2
RFC 3079: Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)

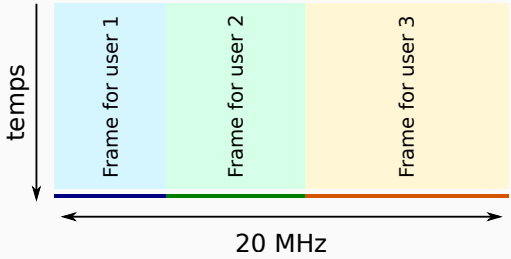
Avancées proposées par 802.11ax (Wi-Fi 6)

Coloration de BSS



OFDM → OFDMA


temps
Frame for user 1
Frame for user 2
Frame for user 3
20 MHz


temps
Frame for user 1
Frame for user 2
Frame for user 3
20 MHz