NET 4104 - Internet sans fil

Concepts, technologies et architectures

Rémy Grünblatt – remy@grunblatt.org

Février 2023

Séance	Date	Début	Fin	Salle
Séance 1	6 février 2023	14h30	17h45	B101
Séance 2	7 février 2023	14h30	17h45	B101
Séance 3	14 février 2023	14h30	17h45	B101
Séance 4	16 février 2023	10h00	13h15	B101
Séance 5	21 février 2023	14h30	17h45	B101
Séance 6	24 février 2023	10h00	13h15	J004
Séance 7	7 mars 2023	10h00	13h15	E'0021
Séance 8	9 mars 2023	10h00	13h15	B109
Séance 9	10 mars 2023	10h00	13h15	B109

Séance	Date	Début	Fin	Salle
Séance 1	7 février 2023	10h00	13h15	B101
Séance 2	8 février 2023	10h00	13h15	B101
Séance 3	14 février 2023	10h00	13h15	B101
Séance 4	15 février 2023	10h00	13h15	B101
Séance 5	21 février 2023	10h00	13h15	B101
Séance 6	7 mars 2023	14h30	17h45	E'0022
Séance 7	8 mars 2023	10h00	13h15	B109
Séance 8	15 mars 2023	10h00	13h15	B109
Séance 9	17 mars 2023	10h00	13h15	E'0021

- Plusieurs intervenants :
  - Badii Jouaber – Coordinateur
  - Michel Marot
  - Rémy Grünblatt – Coordinateur
  - Bruno Di Gennaro
- Refonte partielle du cours en 2023 ; C'est la première fois que ce cours est donné
- Retours appréciés, 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 !

→ **Panorama autour de l'Internet sans fil**

Avant de commencer...

Ressources utilisées pour la préparation de ce cours

- PySDR: A Guide to SDR and DSP using Python – Dr. Marc Lichtman
- Electromagnetics - Volume 1 et Volume 2 – Steven W. Ellingson

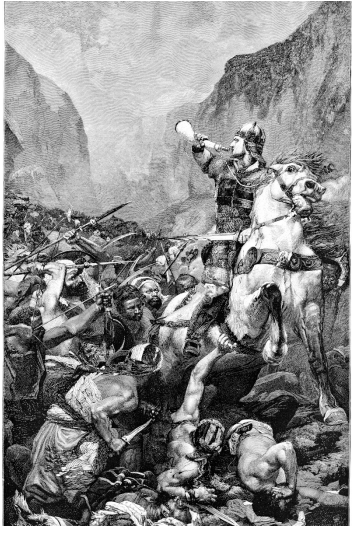
Pourquoi et comment communiquer sans fils ?

Qu'est ce qui est apparu en premier ?

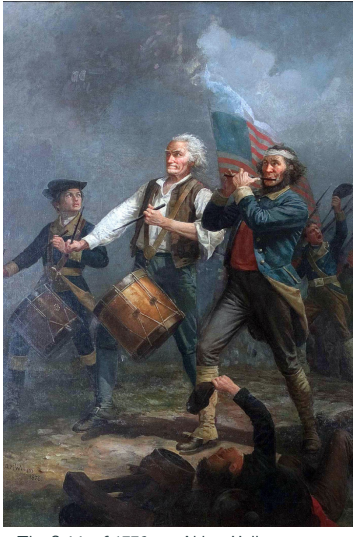
- Les communications filaires (électriques) ?
- Les communications sans fils (électro-magnétiques) ?

Pourquoi et comment communiquer sans fils ?

« The Moose Call » – Roland W. Reed



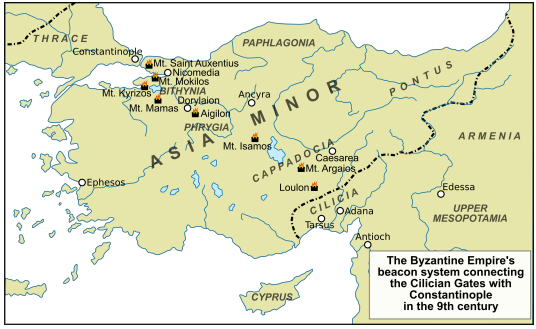
« Roland à la bataille de Roncevaux » – A. Closs



« The Spirit of 1776 » – Abbot Hall

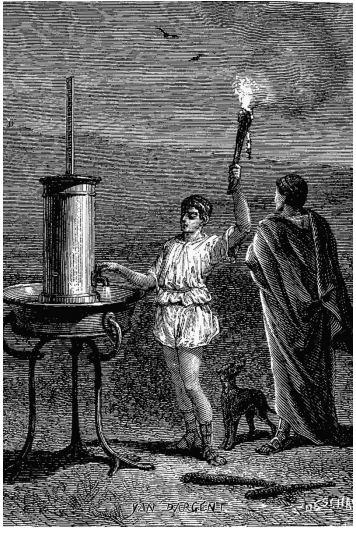
Pourquoi et comment communiquer sans fils ?

Smoke Signals – Frederic Sackrider Remington

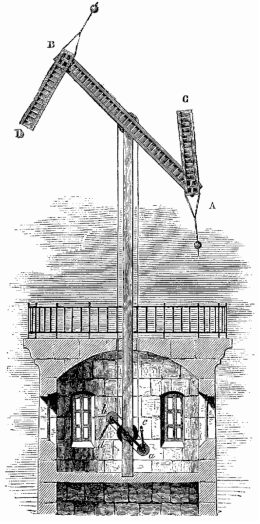


Byzantine Beacon System – Constantine Plakidas – CC-BY-SA 3.0

Pourquoi et comment communiquer sans fils ?



Télégraphe d'Aenas



Télégraphe de Chappe

Sémaphores navals

Pourquoi et comment communiquer sans fils ?

. . . avec des ondes électro-magnétiques !

Pourquoi et comment communiquer sans fils ?

. . . avec des ondes électro-magnétiques !

- $\rightarrow$ Communication à la vitesse de la lumière
- $\rightarrow$ Peu ou pas d'infrastructures à mettre en place
- $\rightarrow$ Plus résilient. . . ? Plus sécurisé. . . ?

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:

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

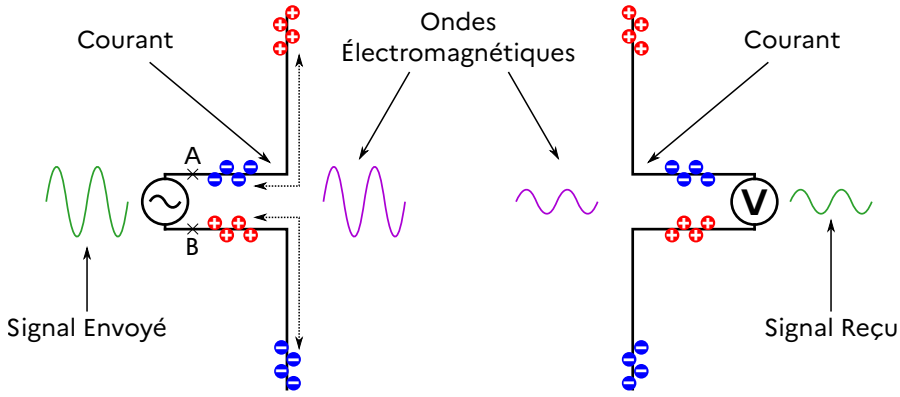
Courant variable $\vec{j}(t)$ $\Rightarrow$ Champ magnétique variable $\vec{B}(t)$

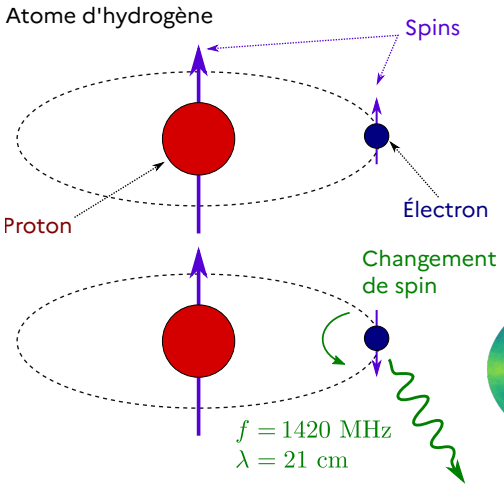
$\Rightarrow$ Champ électrique variable $\vec{E}(t)$

$\Rightarrow \ldots$

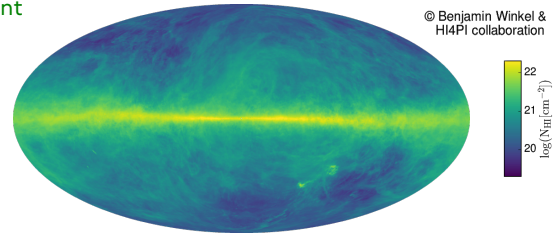
$\rightarrow$ propagation d'une onde électromagnétique

Propriété importante: la linéarité !


Courant
Ondes
Électromagnétiques
Courant
A
B
V
Signal Envoyé
Signal Reçu

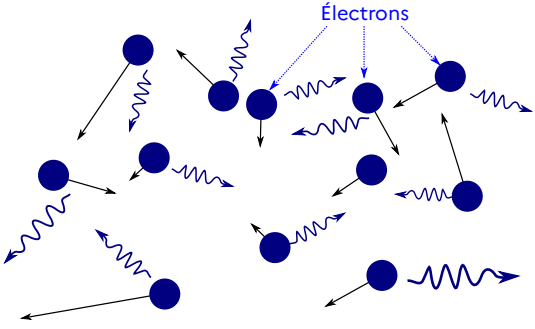

Atome d'hydrogène
Spins
Proton
Électron
Changement
de spin
$f = 1420$ MHz
$\lambda = 21$ cm


CC-BY-SA 4.0 -- Mihaisiscanu

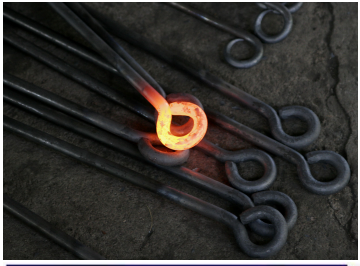

© Benjamin Winkel &
HI4PI collaboration
22
21
20
$\log(N_{HI}[cm^{-2}])$

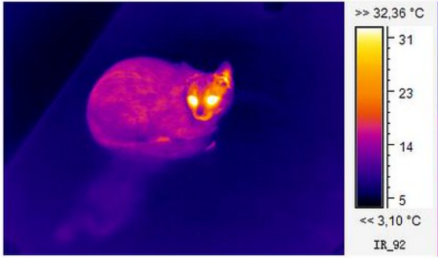
Parenthèse : Bruit et Linéarité

Agitation thermique
des porteurs de charges :



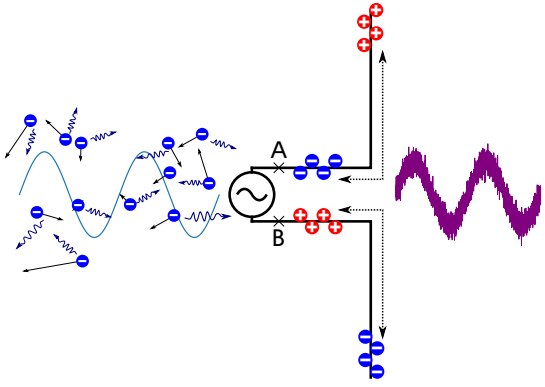
CC-BY NC – Fir0002/Flagstaffotos

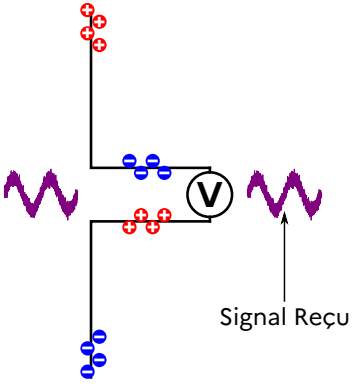




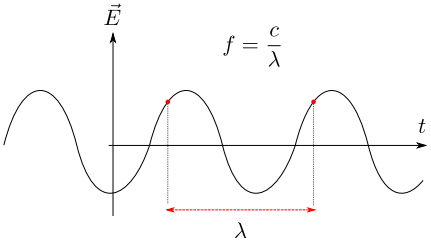
CC-BY – yellowcloud

Parenthèse : Bruit et Linéarité





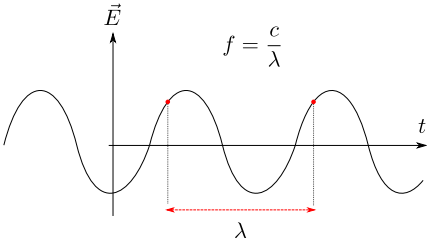
Caractéristiques des ondes électro-magnétiques



Caractéristiques importantes :

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

Caractéristiques des ondes électro-magnétiques



Caractéristiques importantes :

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

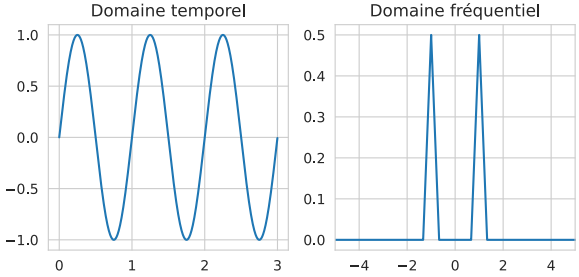
On peut décomposer un signal périodique « qui a une bonne tête » (périodique) en une somme d'exponentielles complexes (Fourier) :

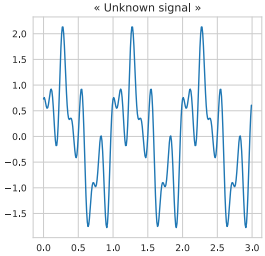
$$f(x) = \sum_{n=-\infty}^{+\infty} c_n(f) \mathrm{e}^{2\mathrm{i}\pi \frac{n}{T} x}$$

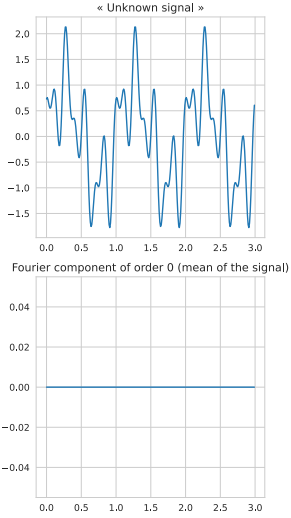
$$\text{avec } c_n(f) = \frac{1}{T} \int_T f(t) \mathrm{e}^{-2\mathrm{i}\pi \frac{n}{T} t} \mathrm{d}t$$

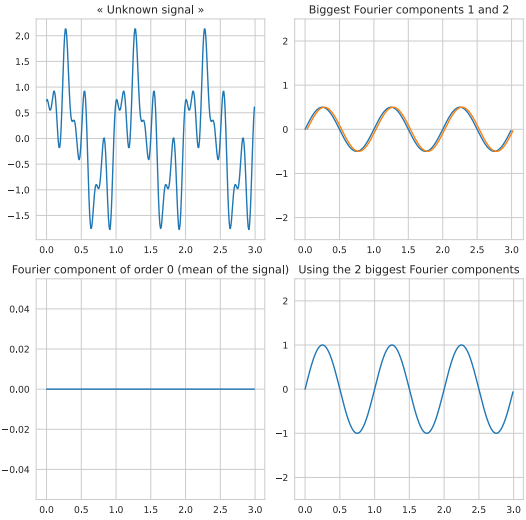
(et réciproquement)

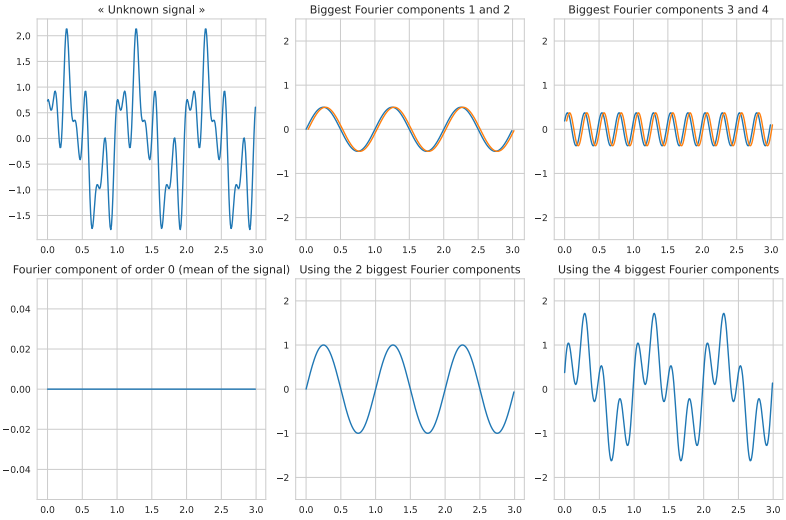
La transformée de Fourier permet de passer du domaine temporel au domaine fréquentiel, et la transformée de Fourier inverse permet de passer du domaine fréquentiel au domaine temporel :

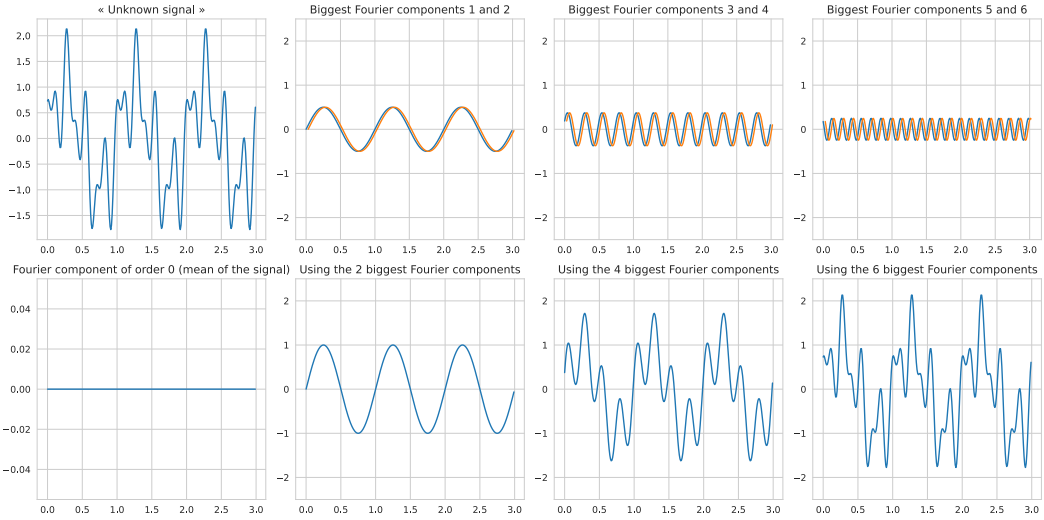


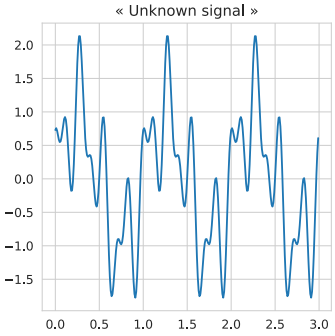

« Unknown signal »
2.0
1.5
1.0
0.5
0.0
−0.5
−1.0
−1.5
0.0
0.5
1.0
1.5
2.0
2.5
3.0

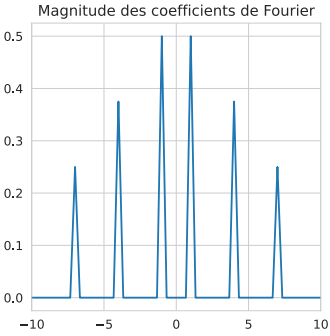

« Unknown signal »
2.0
1.5
1.0
0.5
0.0
−0.5
−1.0
−1.5
0.0
0.5
1.0
1.5
2.0
2.5
3.0
Fourier component of order 0 (mean of the signal)
0.04
0.02
0.00
−0.02
−0.04
0.0
0.5
1.0
1.5
2.0
2.5
3.0

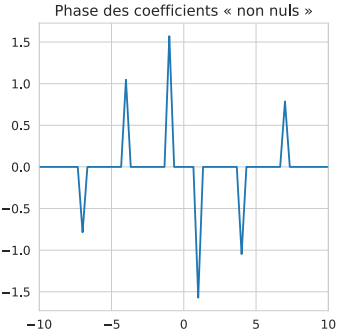

« Unknown signal »
Biggest Fourier components 1 and 2
Fourier component of order 0 (mean of the signal)
Using the 2 biggest Fourier components

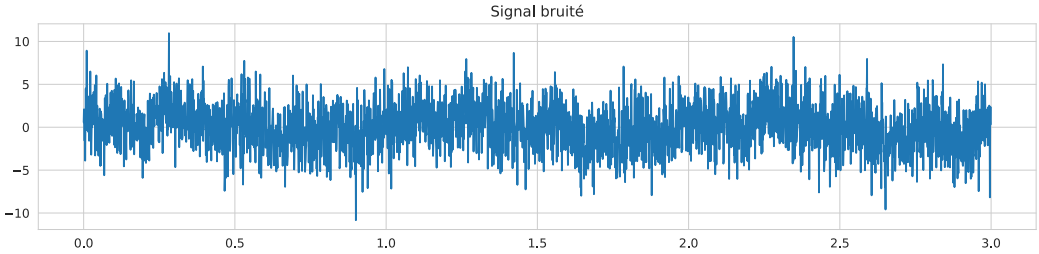

« Unknown signal »
Biggest Fourier components 1 and 2
Biggest Fourier components 3 and 4
Fourier component of order 0 (mean of the signal)
Using the 2 biggest Fourier components
Using the 4 biggest Fourier components

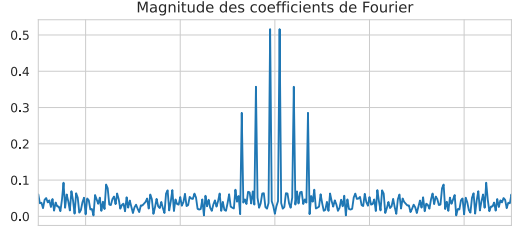

« Unknown signal »
Biggest Fourier components 1 and 2
Biggest Fourier components 3 and 4
Biggest Fourier components 5 and 6
Fourier component of order 0 (mean of the signal)
Using the 2 biggest Fourier components
Using the 4 biggest Fourier components
Using the 6 biggest Fourier components

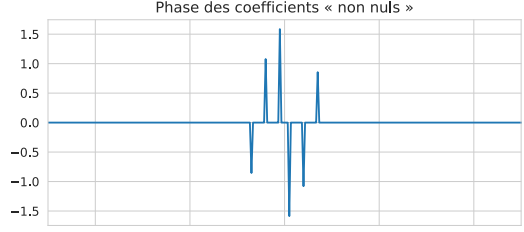

« Unknown signal »
2.0
1.5
1.0
0.5
0.0
−0.5
−1.0
−1.5
0.0
0.5
1.0
1.5
2.0
2.5
3.0


Magnitude des coefficients de Fourier
0.5
0.4
0.3
0.2
0.1
0.0
−10
−5
0
5
10


Phase des coefficients « non nuls »
1.5
1.0
0.5
0.0
−0.5
−1.0
−1.5
−10
−5
0
5
10


Signal bruité
10
5
0
−5
−10
0.0
0.5
1.0
1.5
2.0
2.5
3.0


Magnitude des coefficients de Fourier
0.5
0.4
0.3
0.2
0.1
0.0
−40
−20
0
20
40

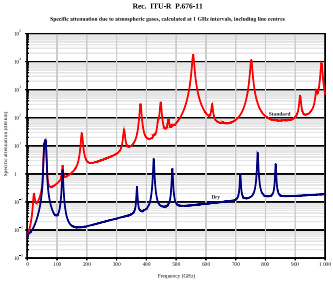

Phase des coefficients « non nuls »
1.5
1.0
0.5
0.0
−0.5
−1.0
−1.5
−40
−20
0
20
40

Propagation des ondes électro-magnétiques

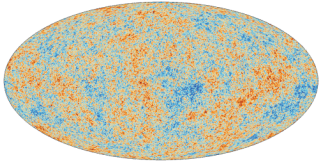
Les ondes électro-magnétiques :

- 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

$$P_r = P_t \, G_t \, G_r \left(\frac{\lambda}{4\pi R} \right)^2$$

$$P_r = P_t \, G_t \, G_r \left(\frac{\lambda}{4\pi R} \right)^2$$

- P_r : Puissance reçue, en Watts (W) ;
- P_t : Puissance transmise, en Watts (W) ;
- G_r : Gain de l'antenne de transmission (sans unité) ;
- G_t : Gain de l'antenne de réception (sans unité) ;
- λ : Longueur d'onde de la transmission, en mètres (m) ;
- R : Distance entre l'émetteur et le récepteur, en mètres (m) ;

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi R} \right)^2$$

- P_r : Puissance reçue, en Watts (W) ;
- P_t : Puissance transmise, en Watts (W) ;
- G_r : Gain de l'antenne de transmission (sans unité) ;
- G_t : Gain de l'antenne de réception (sans unité) ;
- λ : Longueur d'onde de la transmission, en mètres (m) ;
- R : Distance entre l'émetteur et le récepteur, en mètres (m) ;

. . . aussi connu sous le nom de Canal de Friis, ou « Free Space Path Loss »

Rappels sur le logarithme :

- $\log_{10}(a * b) = \log_{10}(a) + \log_{10}(b)$
- $\log_{10}\left(\frac{a}{b}\right) = \log_{10}(a) - \log_{10}(b)$
- $\log_{10}(10^x) = x$
- $\log_{10}(x^n) = n * \log_{10}(x)$

Rappels sur le logarithme :

- $\log_{10}(a * b) = \log_{10}(a) + \log_{10}(b)$
- $\log_{10}\left(\frac{a}{b}\right) = \log_{10}(a) - \log_{10}(b)$
- $\log_{10}(10^x) = x$
- $\log_{10}(x^n) = n * \log_{10}(x)$

Rappels sur les bels et décibels :

- Un bel (B) représente un rapport entre deux quantités sur une échelle logarithmique
- Un décibel (dB) est un dixième de bel
- Un décibel n'a pas d'unité : c'est un rapport !

Pour des **puissances** exprimées en Watt (W), le rapport R entre P et P_0 **en bel (B)** est donné par :

$$R = \log_{10}\left(\frac{P}{P_0}\right)$$

Pour des **puissances** exprimées en Watt (W), le rapport R entre P et P_0 **en bel (B)** est donné par :

$$R = \log_{10}\left(\frac{P}{P_0}\right)$$

Pour des **puissances** exprimées en Watt (W), le rapport R entre P et P_0 **en décibel (dB)** est donné par :

$$R = 10 * \log_{10}\left(\frac{P}{P_0}\right)$$

Un dBm est une unité de **puissance** exprimant la relation entre la puissance mesurée par rapport à 1 milli-watt (mW) en dB.

Un dBm est une unité de **puissance** exprimant la relation entre la puissance mesurée par rapport à 1 milli-watt (mW) en dB.

Pour exprimer une puissance P, **exprimée en mW**, comme une valeur x **exprimée en dBm** , on utilise la formule suivante :

$$x = 10 * \log_{10}\left(\frac{P}{1\text{mW}}\right)$$

Un dBm est une unité de **puissance** exprimant la relation entre la puissance mesurée par rapport à 1 milli-watt (mW) en dB.

Pour exprimer une puissance P, **exprimée en mW**, comme une valeur x **exprimée en dBm** , on utilise la formule suivante :

$$x = 10 * \log_{10}\left(\frac{P}{1\text{mW}}\right)$$

Pour exprimer une puissance P, **exprimée en dBm**, comme une valeur x **exprimée en** mW , on utilise la formule suivante :

$$x = 1\text{mW} * 10^{\frac{P}{10}}$$

L'équation $P_r = P_t\, G_t\, G_r \left(\frac{\lambda}{4\pi R}\right)^2$ peut aussi s'écrire sous la forme logarithmique :

$$P_r^{[dB]} = P_t^{[dB]} + G_t^{[dBi]} + G_r^{[dBi]} + 20\log_{10}\left(\frac{\lambda}{4\pi R}\right)$$

- P_r et P_t : Puissance de réception et de transmission, en dB
- *Gains* : Gains d'antennes en émission et réception, en dBi (décibel relatifs à l'antenne isotrope)
- *Pertes* : Pertes liées aux câbles, à la propagation (path loss , shadowing, fast-fading), en dB (décibel)

L'équation $P_r = P_t\, G_t\, G_r \left(\frac{\lambda}{4\pi R}\right)^2$ peut aussi s'écrire sous la forme logarithmique :

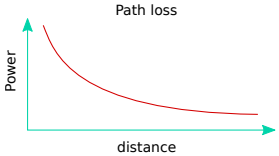
$$P_r^{[dB]} = P_t^{[dB]} + G_t^{[dBi]} + G_r^{[dBi]} + 20\log_{10}\left(\frac{\lambda}{4\pi R}\right)$$

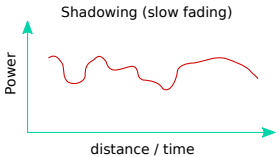
- P_r et P_t : Puissance de réception et de transmission, en dB
- *Gains* : Gains d'antennes en émission et réception, en dBi (décibel relatifs à l'antenne isotrope)
- *Pertes* : Pertes liées aux câbles, à la propagation (path loss , shadowing, fast-fading), en dB (décibel)

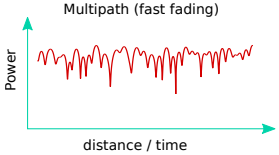
Il existe des modèles plus complexes ! (modèle à deux raies, ...)

D'une manière plus générale, un bilan de liaison s'écrit (exprimé logarithmiquement) :

$$P_r = P_t + \text{Gains} - \text{Pertes}$$


Path loss
Power
distance


Shadowing (slow fading)
Power
distance / time


Multipath (fast fading)
Power
distance / time

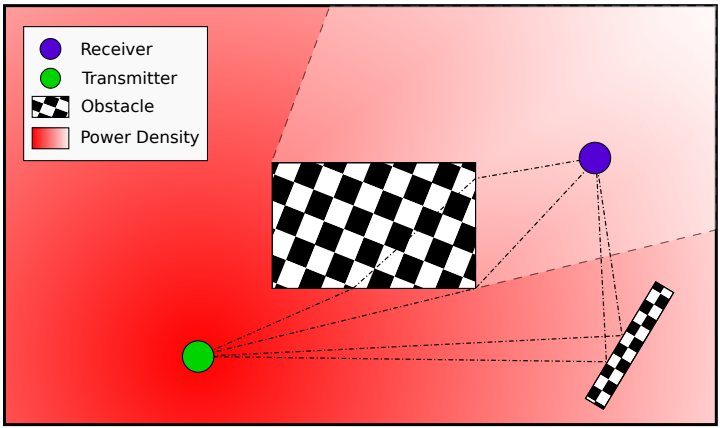

Receiver
Transmitter
Obstacle
Power Density

Illustration calculatoire

- En france, une borne Wi-Fi émet à 20 dBm / 100 mW maximum
- On utilise le canal centré sur f=2412 MHz
- On suppose les antennes utilisées comme n'ayant pas de gains
- On suppose qu'un récepteur a besoin de -65 dBm / 316 pW pour décoder 54 Mbps (64-QAM 2/3)

Quelle est la portée maximale de la borne en supposant un canal de Friis ?

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, en W
- S : Puissance moyenne du signal, en W

Outils théoriques – Relation de Shannon-Hartley

- Un canal Wi-Fi, dans sa configuration la plus courante, fait 20 MHz de large
- On reçoit les signaux à une puissance de -78 dBm
- On mesure le niveau du bruit à -96 dBm

Quelle est la capacité de ce canal, en Mbps ?

Outils théoriques – Relation de Shannon-Hartley

- Un canal Wi-Fi, dans sa configuration la plus courante, fait 20 MHz de large
- On reçoit les signaux à une puissance de -78 dBm
- On mesure le niveau du bruit à -96 dBm

Quelle est la capacité de ce canal, en Mbps ?

Même question pour un canal bluetooth (1 MHz de large)

Outils théoriques – Théorème de Nyquist-Shannon

Sampler : passer d'un signal continu à un signal discret

Outils théoriques – Théorème de Nyquist-Shannon

Sampler : passer d'un signal continu à un signal discret

Pour capturer toute l'information qu'un signal contient, il faut « sampler » (échantillonner) avec une fréquence d'échantillonnage supérieure à deux fois la fréquence maximale du signal.

Outils théoriques – Théorème de Nyquist-Shannon

Sampler : passer d'un signal continu à un signal discret

Pour capturer toute l'information qu'un signal contient, il faut « sampler » (échantillonner) avec une fréquence d'échantillonnage supérieure à deux fois la fréquence maximale du signal.

$\rightarrow$ script pour illustrer

Outils théoriques – Théorème de Nyquist-Shannon

Sampler : passer d'un signal continu à un signal discret

Pour capturer toute l'information qu'un signal contient, il faut « sampler » (échantillonner) avec une fréquence d'échantillonnage supérieure à deux fois la fréquence maximale du signal.

$\rightarrow$ script pour illustrer

Des signaux audio sont généralement samplés à une fréquence de 44.1kHz. Pourquoi ?

Comment encoder de l'information dans un signal ?

Comment encoder de l'information dans un signal ?

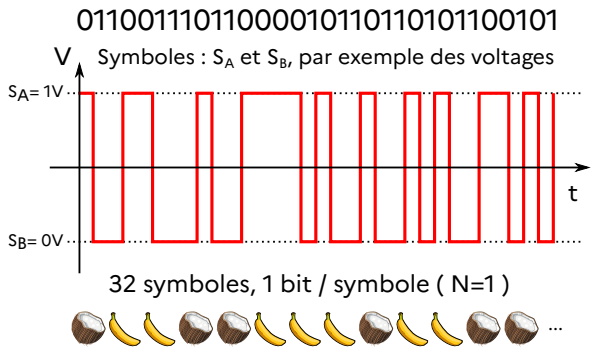
On utilise des symboles !

1 symbole = N bits d'information, avec N *variable* :

Comment encoder de l'information dans un signal ?

On utilise des symboles !

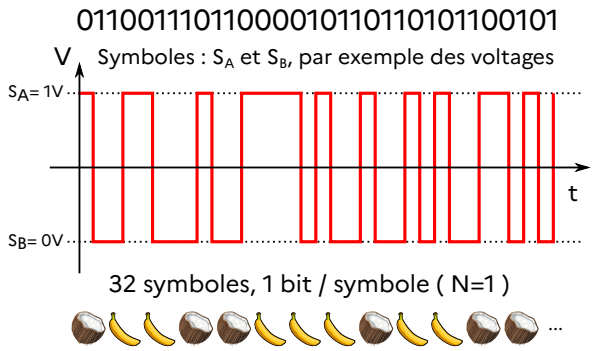
1 symbole = N bits d'information, avec N *variable* :

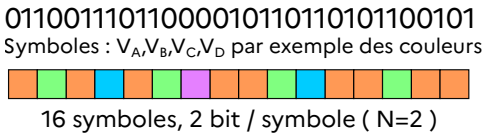


Comment encoder de l'information dans un signal ?

On utilise des symboles !

1 symbole = N bits d'information, avec N *variable* :



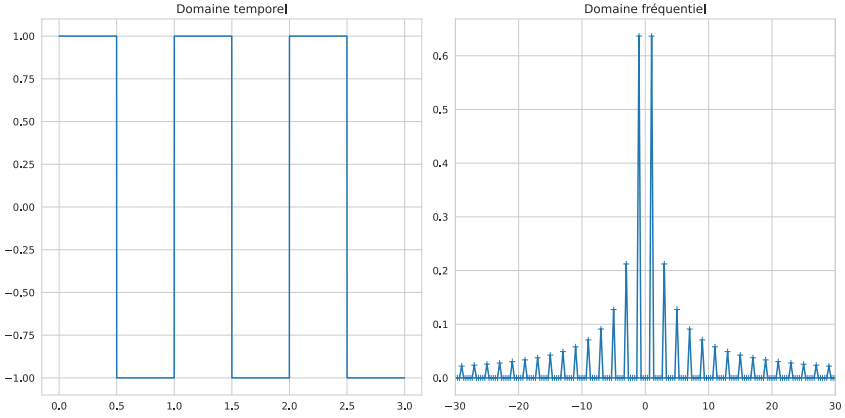


Comment encoder de l'information dans un signal ?

Pourquoi ne pas simplement envoyer les symboles « bruts » dans une antenne ?

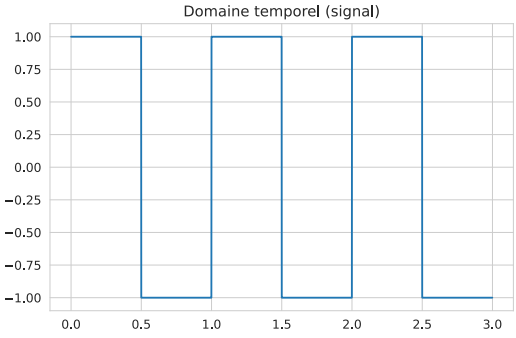
Comment encoder de l'information dans un signal ?

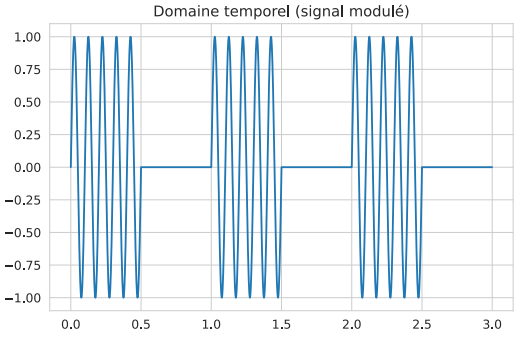
Pourquoi ne pas simplement envoyer les symboles « bruts » dans une antenne ?



Comment encoder de l'information dans un signal ?

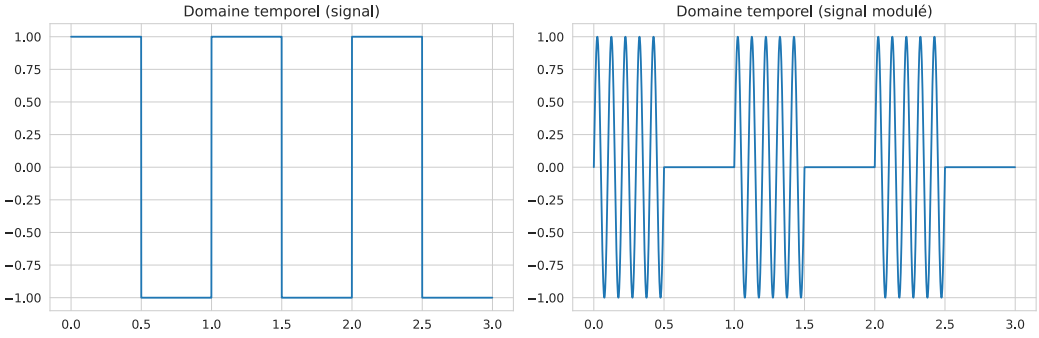
Solution : moduler les signaux à envoyer par des « porteuses » :





Comment encoder de l'information dans un signal ?

Solution : moduler les signaux à envoyer par des « porteuses » :



→ OOK : On Off Keying

Organisation du spectre

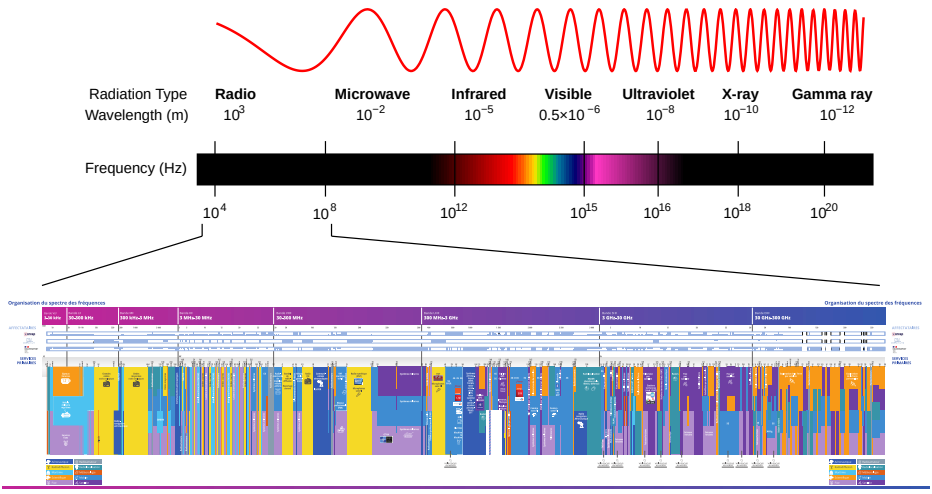
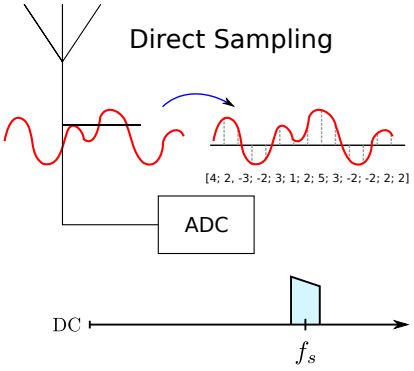
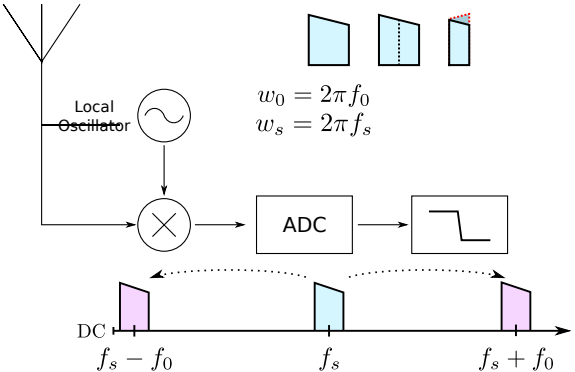


Illustration : CC-BY-SA 3.0 – Inductiveload, NASA @ Wikimedia (haut) et ANFR (bas)

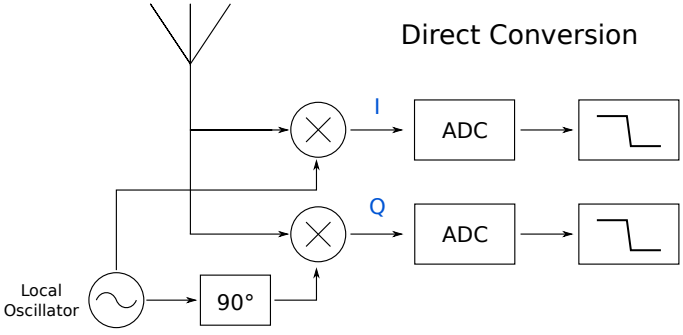
Sampling et Décodage Numérique

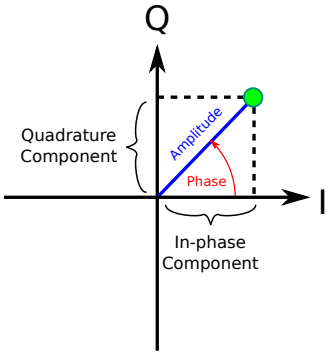




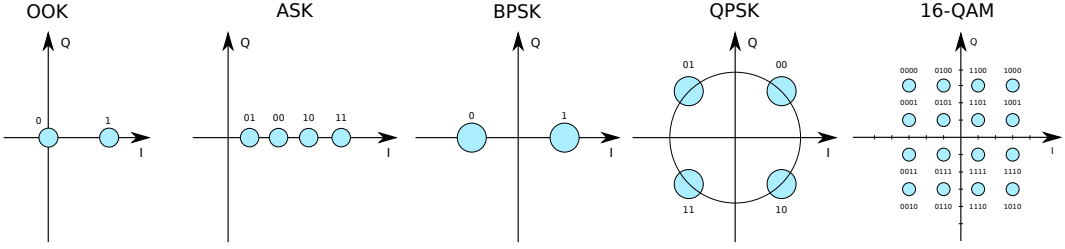
$$cos(w_0 t) * cos(w_s t) = \frac{1}{2} cos((w_0 - w_s)t) + \frac{1}{2} cos((w_0 + w_s)t)$$

Sampling et Décodage Numérique : I et Qs





Modulations complexes - Diagrammes de constellation



64-QAM

(...)

256-QAM

(...)

1024-QAM

(...)

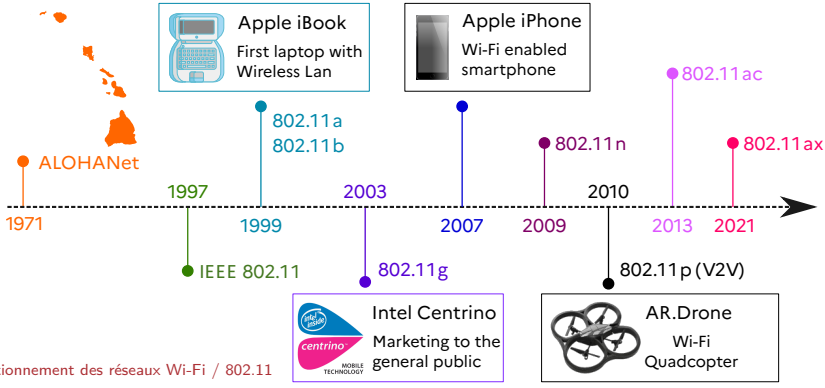
Fonctionnement des réseaux Wi-Fi / 802.11

Petit Historique

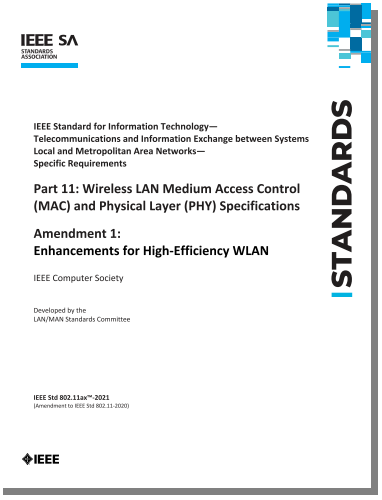
fixed station

portable station

moving station

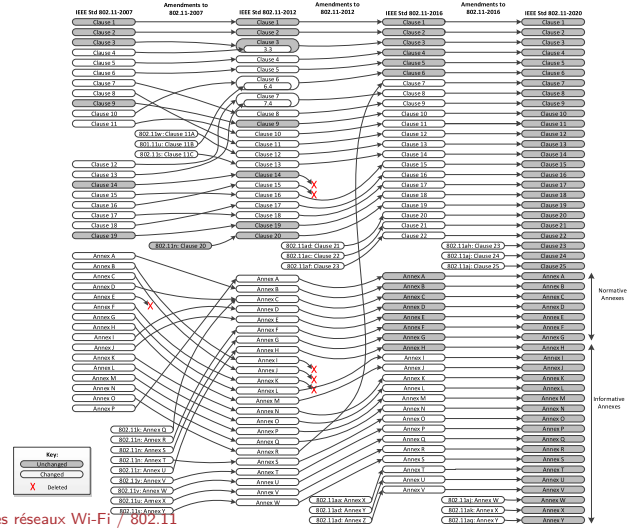


Les normes 802.11...



. . . évoluent dans le temps. . .

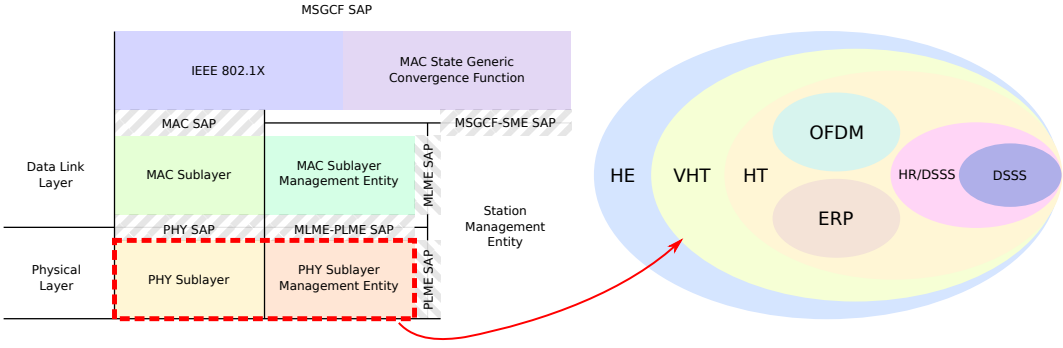
2020 – Figure 1—The evolution of numbering in IEEE Std 802.11



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

2020 – 4.9 Reference model

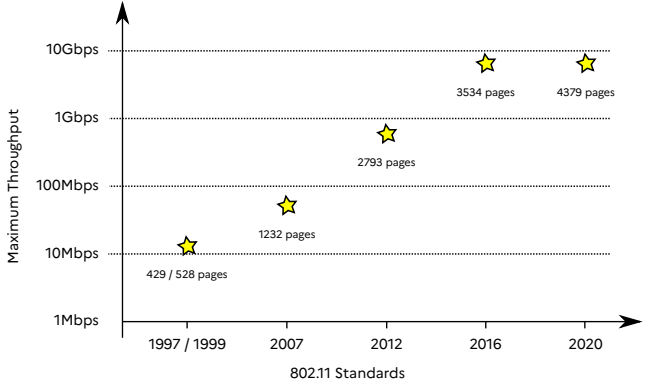
Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications



Les normes 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

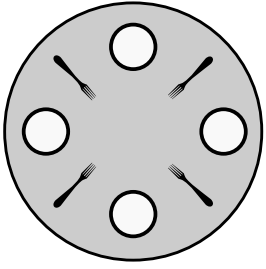


Couche MAC

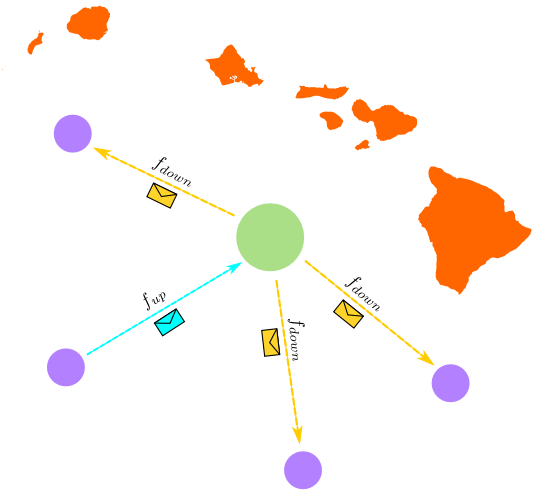
Qu'est ce que c'est ?

MAC : Medium Access Control

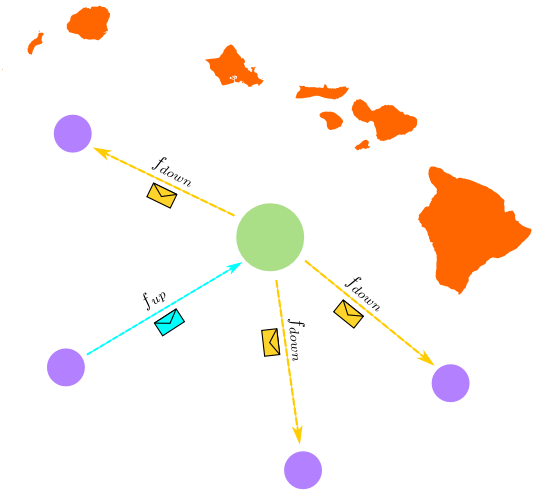
MAC : Medium Access Control



Précurseur: Aloha Net



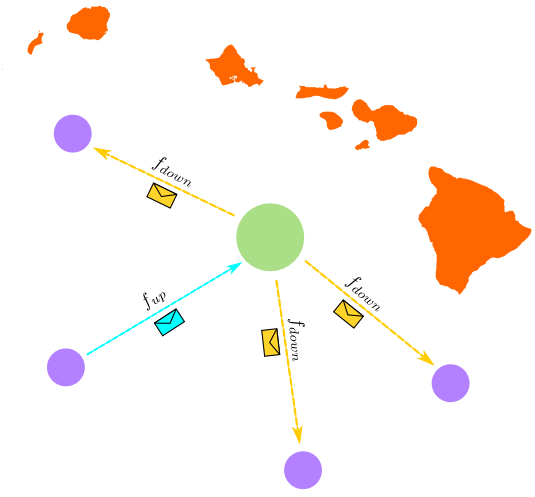
Précurseur: Aloha Net



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

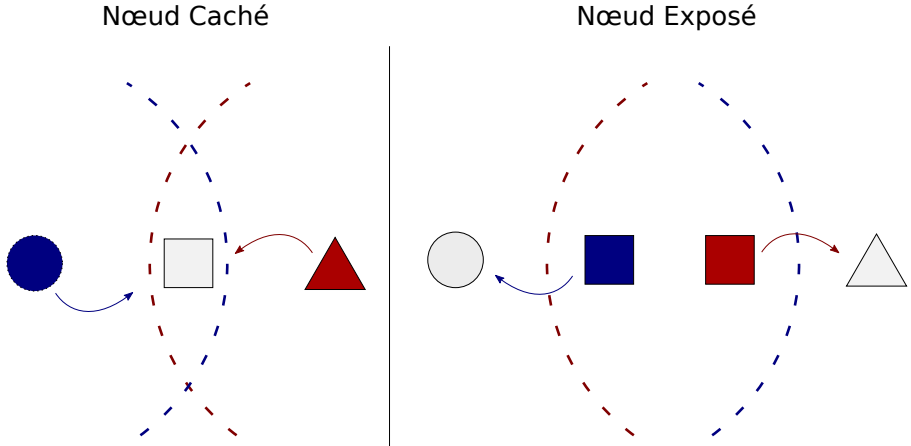


Illustration avec trois stations

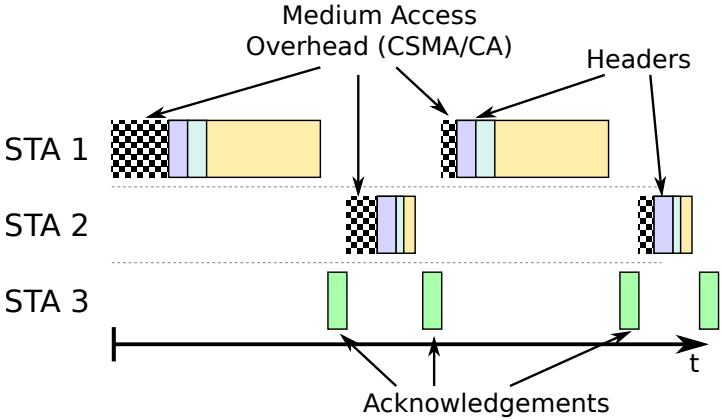
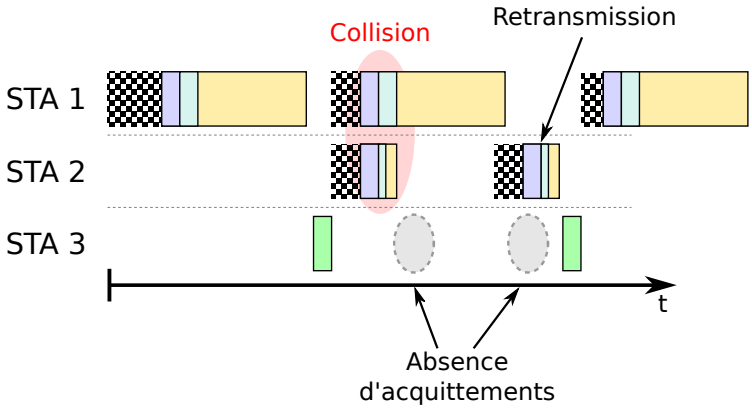


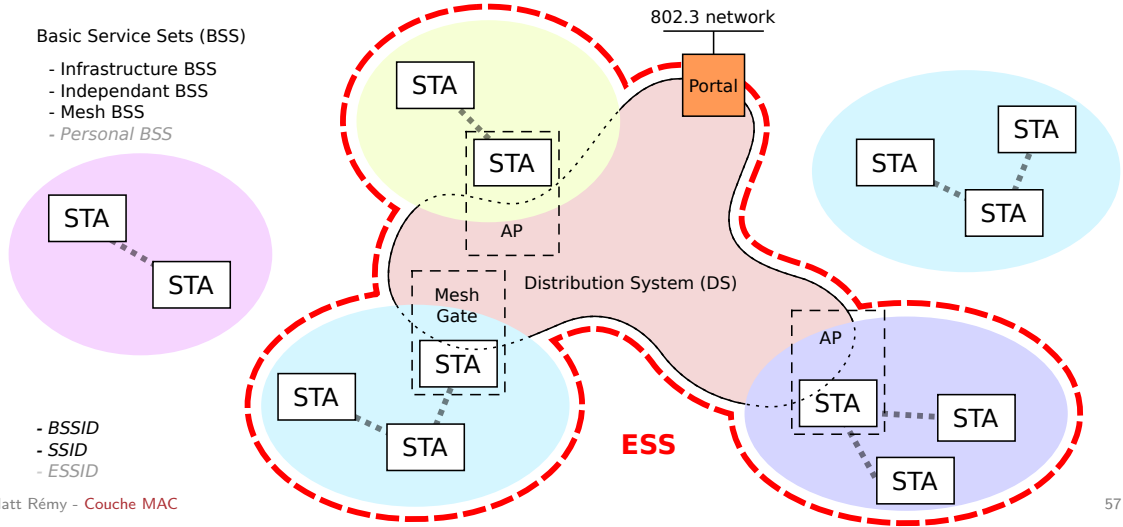
Illustration avec trois stations: collision



Architectures des réseaux Wi-Fi

Basic Service Sets (BSS)

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



- *BSSID*
- *SSID*
- *ESSID*

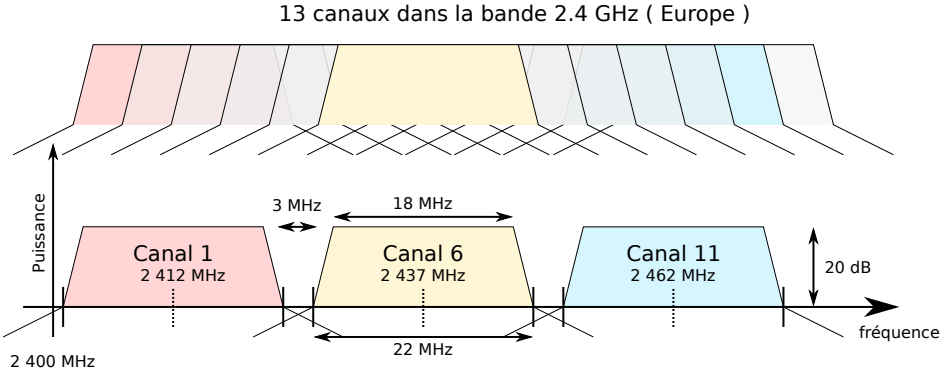
Couche Physique

Bandes de fréquences

900MHz	2.4GHz	3.65GHz	4.9 / 5GHz	5GHz	5.9GHz	6GHz	60GHz
801.11ah	801.11b 802.11g 802.11n 802.11ax	802.11y	801.11j	802.11a 802.11h 802.11j 802.11n 802.11ac 802.11ax	802.11p	802.11ax	802.11ad 802.11ay

Canaux dans la bande 2.4 GHz (20 MHz)

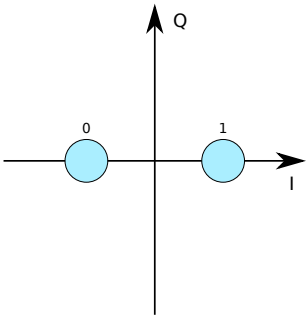
2020 – 17.3.8.4.1 Operating frequency range



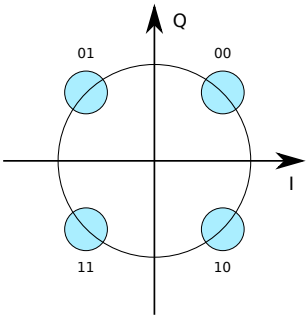
Modulations

2020 – 17.3.5.8 Subcarrier modulation mapping

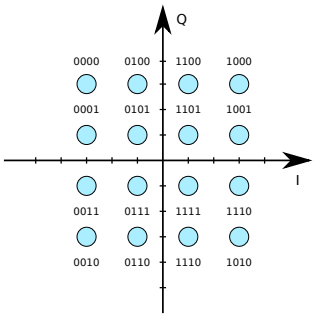
BPSK



QPSK



16-QAM



64-QAM

(...)

256-QAM

(...)

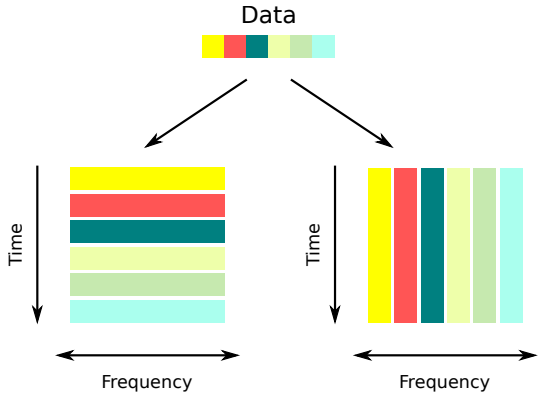
1024-QAM

(...)

OFDM

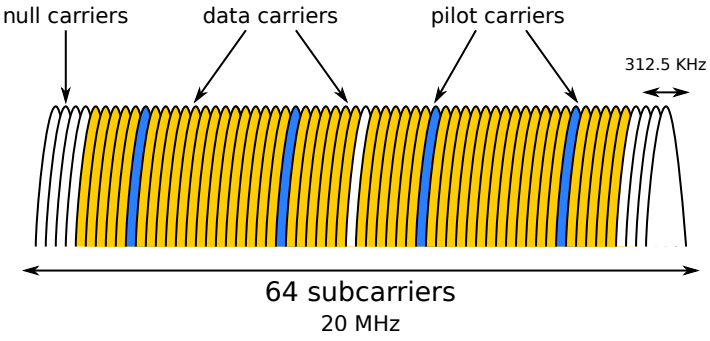
2020 – 17. Orthogonal frequency division multiplexing (OFDM) PHY specification

OFDM: Orthogonal Frequency Division Multiplexing



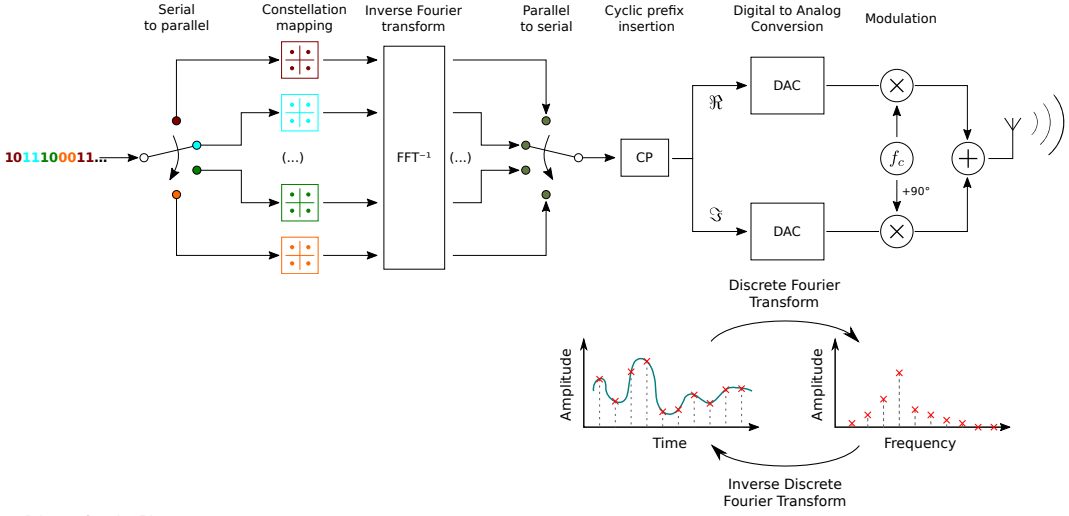
Principe: Transformer un flux « haut débit » en plusieurs flux « bas débits » transmis sur plusieurs fréquences (multiplexage) orthogonales

Décomposition du canal (20 MHz)



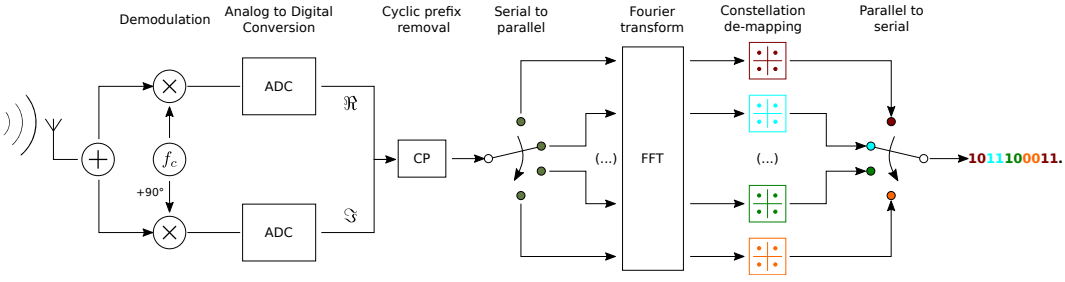
Chaîne de transmission (OFDM)

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



Chaîne de réception (OFDM)

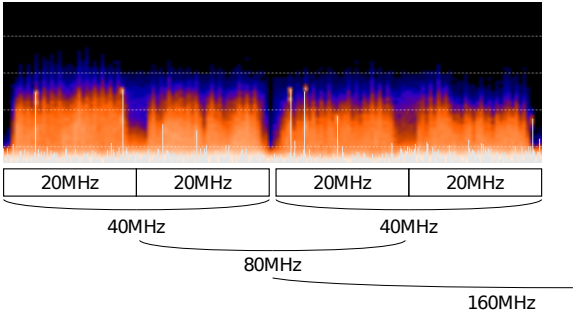
👁 **2020 – Figure 17-12—Transmitter and receiver block diagram for the OFDM PHY**



Aggrégation de canaux

2020 – 19.3.7 Mathematical description of signals

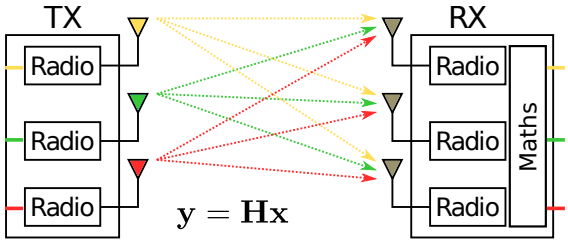
- 40 MHz : HT PHY
- 80 MHz, 160 MHz, 80 + 80 MHz : VHT PHY



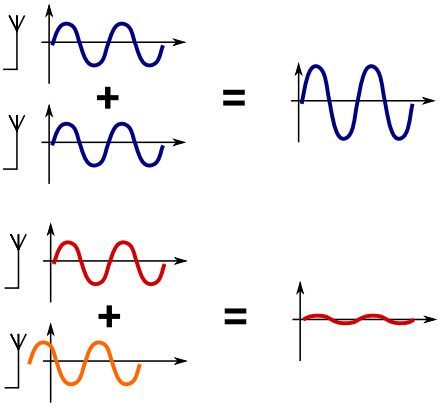
Utilisation de plusieurs antennes: MIMO

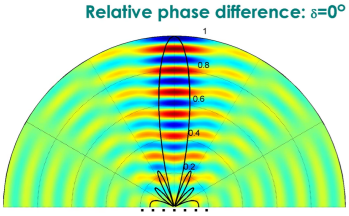
2020 – 19.3 HT PHY

MIMO: Multiple Input, Multiple Output



Utilisation de plusieurs antennes: BeamForming

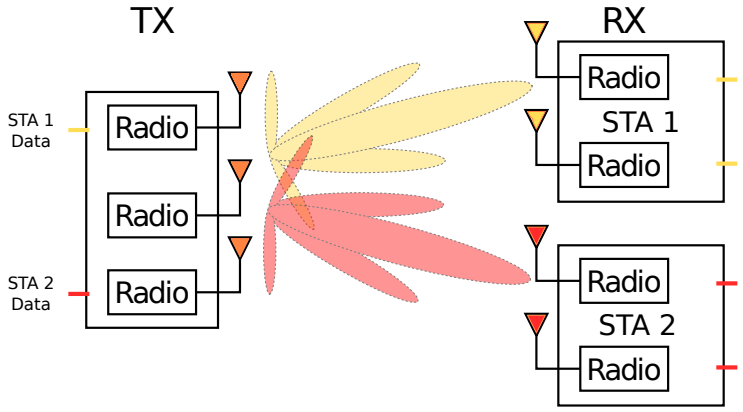




MU-MIMO

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 :

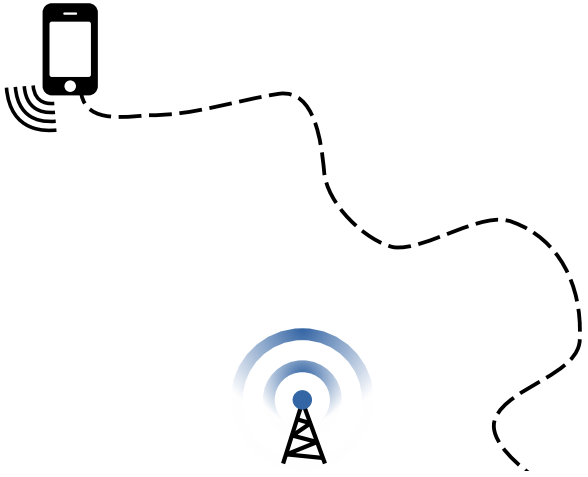
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8

MCS Index :

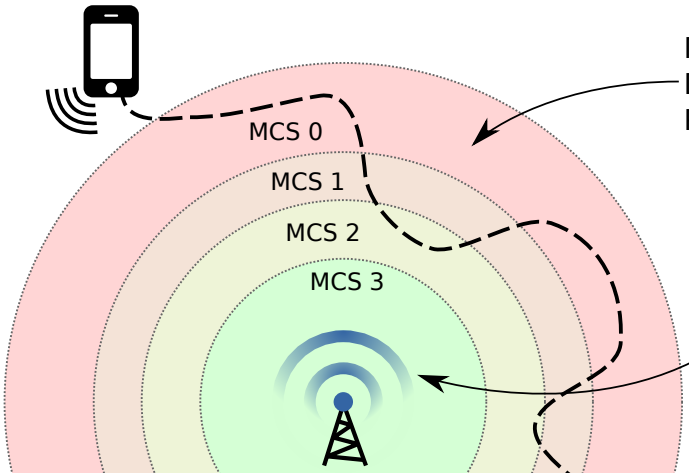
MCS Index	Modulation	Taux d'encodage
0	BPSK	1/2
1	QPSK	1/2
2	QPSK	3/4
3	16-QAM	1/2
...		

- 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



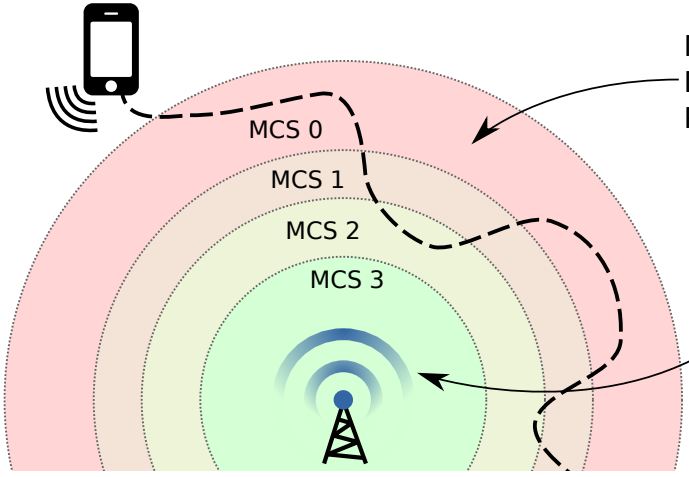
Adaptation de débit à la mobilité



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 :

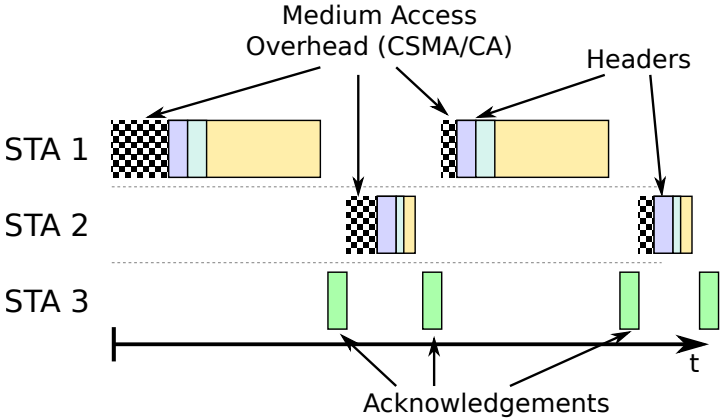
- Trames de 1500 octets envoyées en continu
- Équité dans l'accès au medium : une trame sur deux par nœud
- Approximation grossière des temps d'émission / Accès au medium instantané

Quel est le débit effectif pour chaque nœud ?

Quelle solutions potentielles ?

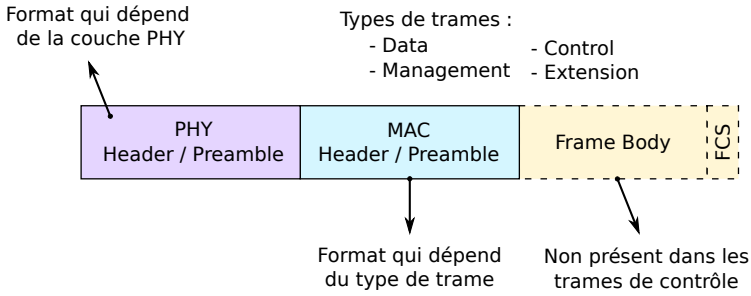
$\rightarrow$ Aggrégation de trames

Retour sur CSMA/CA / Framing



Framing

2020 – 9.3 Format of individual frame types



Management Frames

- Beacon
- Association Request / Response
- Authentication / Deauthentication

Control Frames

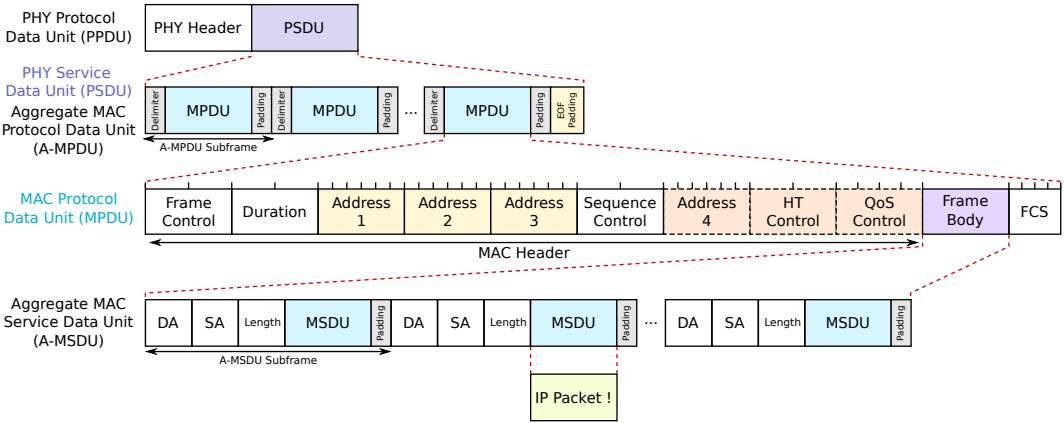
- RTS / CTS
- Ack / Block Ack

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

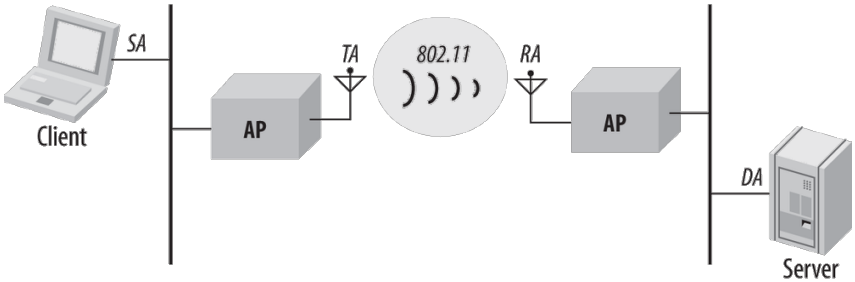


Image : Matthew Gast - 802.11 Wireless Networks: The Definitive Guide

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 ! ✓

Normes 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

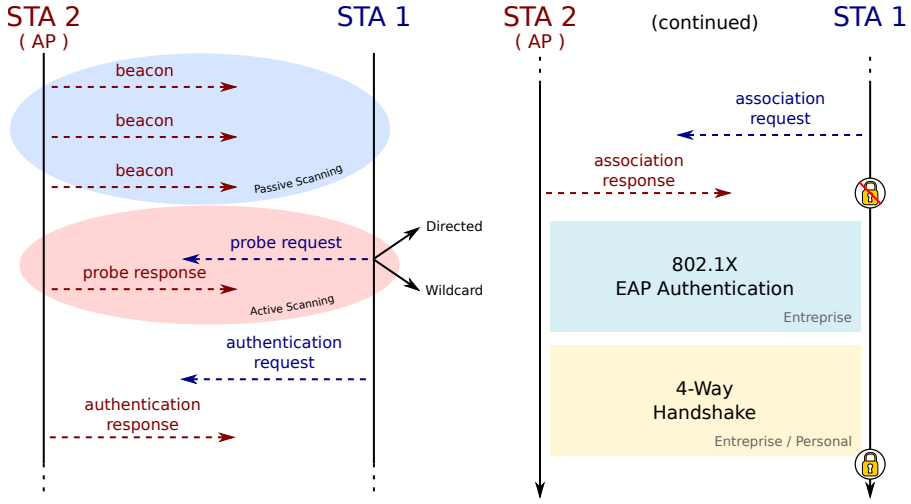
→ Pre-Shared Key (PSK)

Réseau Entreprise

- Managed Membership
- Clients différenciés

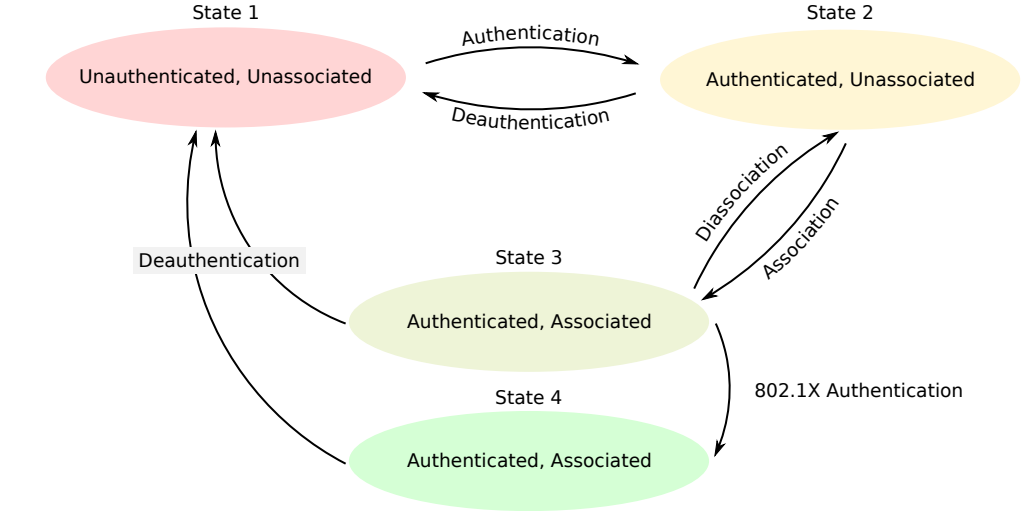
→ 802.1X (Radius)

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)

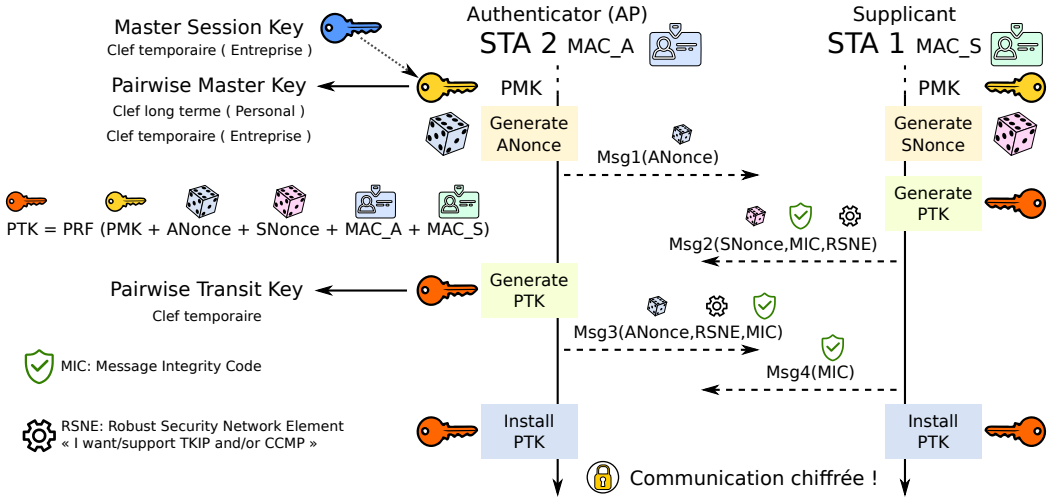
Association **Ne veut pas dire sécurisation !**

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

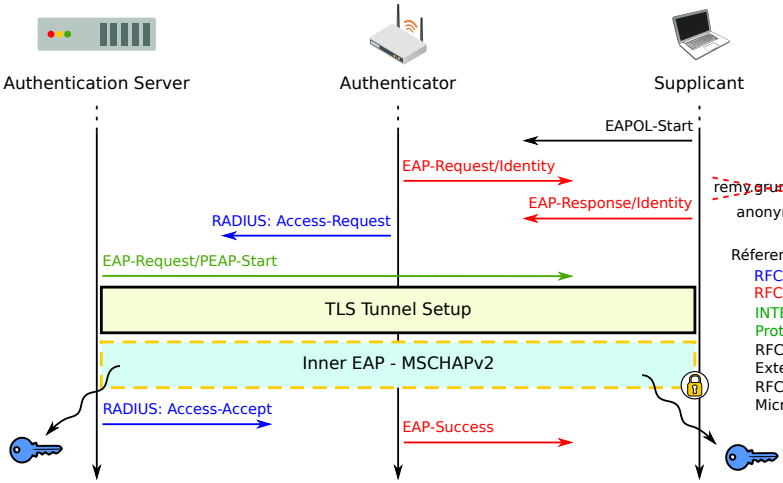
Une STA peut avoir **plusieurs** authentifications en même temps, mais ne peut avoir qu'**une** association à la fois !

The 4-way handshake

2020 – 12.7.6 4-way handshake



802.1X

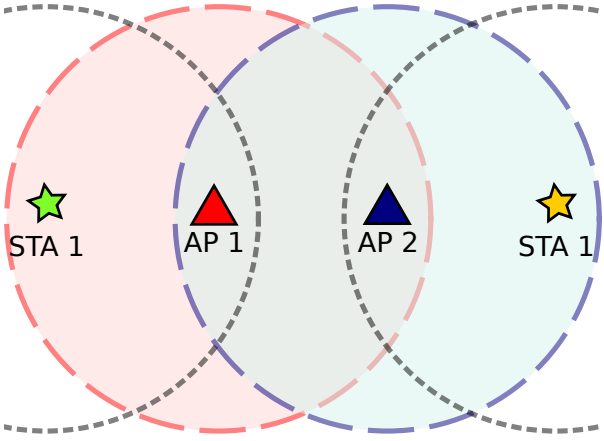


Réferences:

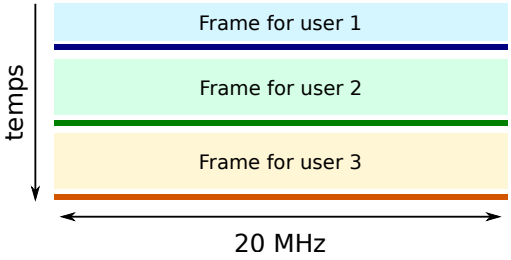
- RFC 2865: RADIUS Protocol
- RFC 3579: RADIUS Support For EAP
- INTERNET-DRAFT: Protected EAP Protocol (PEAP) Version 2
- RFC 2759: Microsoft PPP CHAP Extensions, Version 2
- RFC 3079: Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)

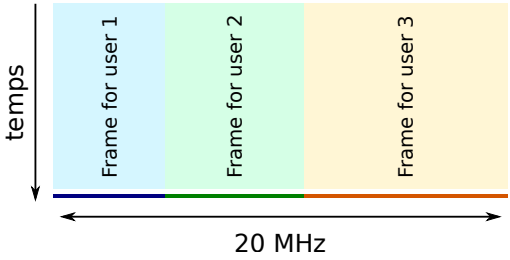
Avancées proposées par 802.11ax (Wi-Fi 6)

Coloration de BSS



OFDM → OFDMA


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

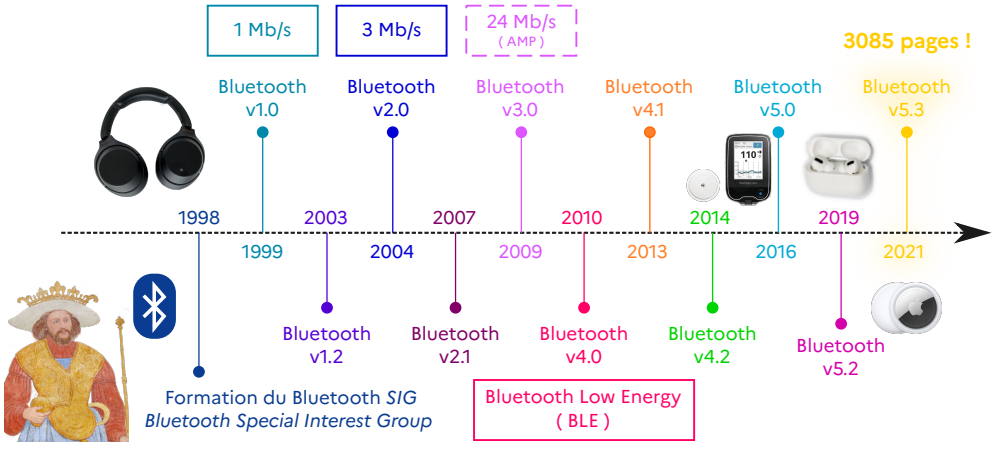

temps
Frame for user 1
Frame for user 2
Frame for user 3
20 MHz

WPAN : Bluetooth et Bluetooth Low Energy (BLE)

Références pour ce cours

- Spécification Bluetooth 5.3 – Bluetooth SIG
- Wireless and Communication in the Internet of Things – Pat Pannuto – CC-BY-SA 4.0
- Understanding Reliability in Bluetooth Technology – Martin Woolley
- Introduction to Bluetooth Low Energy – Adafruit

Un peu d'historique...



*« Bluetooth wireless technology is a **short-range** communications system intended to replace the cable(s) connecting portable and/or fixed **electronic devices** » – Norme Bluetooth 5.3*

*« Bluetooth wireless technology is a **short-range** communications system intended to replace the cable(s) connecting portable and/or fixed **electronic devices** » – Norme Bluetooth 5.3*

- Opération dans une bande sans licence (2.4 GHz)
- Coût limité

Bluetooth Classic – **BR/EDR** :

- 721.2 kb/s – Basic Rate (BR)
- 2/3 Mb/s – Enhanced Data Rate (EDR)
- Portée : 10 – 100m

Bluetooth Low Energy – **(B)LE** :

- 1 Mb/s
- Optionnel: 2 Mb/s
- Portée : 10 – 50m

- Bluetooth Classic : protocole historique, standard *de facto* pour l'audio
- BLE : focus sur la consommation d'énergie, portée réduite

- Bluetooth Classic : protocole historique, standard *de facto* pour l'audio
- BLE : focus sur la consommation d'énergie, portée réduite

En pratique :

- Cohabitation des deux protocoles sur les smartphones et ordinateurs
- IOT : BLE uniquement (ou 802.15.4 – Zigbee – un cousin éloigné du BLE)

- Bluetooth Classic : protocole historique, standard *de facto* pour l'audio
- BLE : focus sur la consommation d'énergie, portée réduite

En pratique :

- Cohabitation des deux protocoles sur les smartphones et ordinateurs
- IOT : BLE uniquement (ou 802.15.4 – Zigbee – un cousin éloigné du BLE)

Bande de fréquence : 2400 MHz $\rightarrow$ 2483.5 MHz

- Bluetooth Classic : protocole historique, standard *de facto* pour l'audio
- BLE : focus sur la consommation d'énergie, portée réduite

En pratique :

- Cohabitation des deux protocoles sur les smartphones et ordinateurs
- IOT : BLE uniquement (ou 802.15.4 – Zigbee – un cousin éloigné du BLE)

Bande de fréquence : 2400 MHz $\rightarrow$ 2483.5 MHz

Co-existence avec le Wi-Fi (et d'autres technologies) nécessaire ...

- Bluetooth Classic : protocole historique, standard *de facto* pour l'audio
- BLE : focus sur la consommation d'énergie, portée réduite

En pratique :

- Cohabitation des deux protocoles sur les smartphones et ordinateurs
- IOT : BLE uniquement (ou 802.15.4 – Zigbee – un cousin éloigné du BLE)

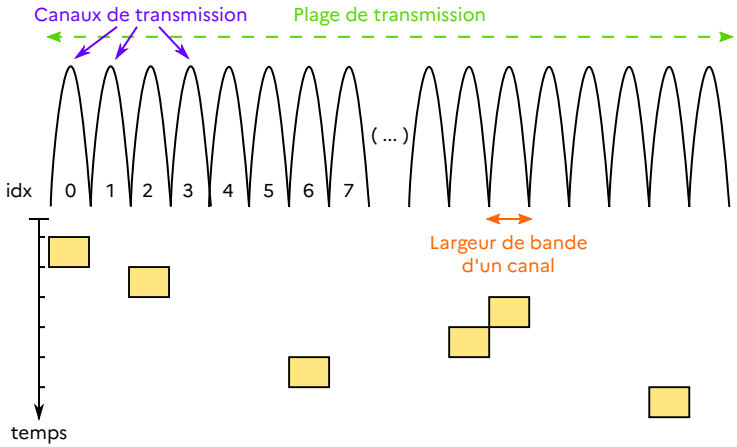
Bande de fréquence : 2400 MHz $\rightarrow$ 2483.5 MHz

Co-existence avec le Wi-Fi (et d'autres technologies) nécessaire ...

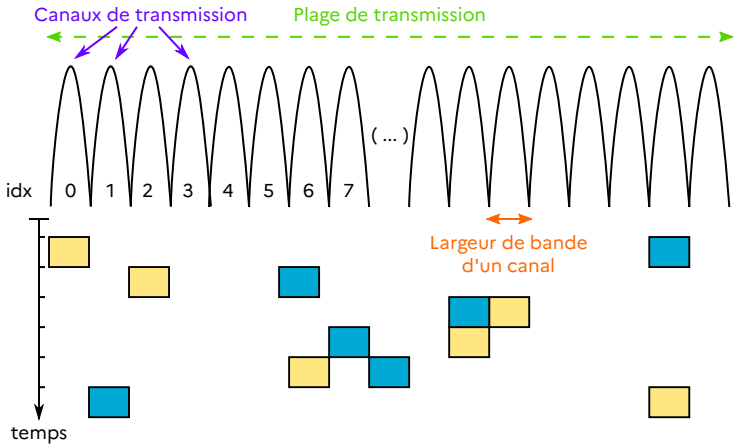
... au niveau de la couche MAC ou de la couche PHY ?

Frequency Hopping Spread Spectrum – Étalement de spectre par saut de fréquence

Frequency Hopping Spread Spectrum – Étalement de spectre par saut de fréquence



Frequency Hopping Spread Spectrum – Étalement de spectre par saut de fréquence



Quelle est la probabilité de collision entre deux émissions sur deux réseaux bluetooth ?

Bluetooth Classic – **BR/EDR** :

- 79 canaux de 1 MHz

Bluetooth Low Energy – **(B)LE** :

- 40 canaux de 2 MHz

Quelle est la probabilité de collision entre deux émissions sur deux réseaux bluetooth ?

Bluetooth Classic – **BR/EDR** :

- 79 canaux de 1 MHz

Bluetooth Low Energy – **(B)LE** :

- 40 canaux de 2 MHz

Simplification / suppositions :

- Les deux réseaux possèdent des « slots » synchronisés
- La sélection du canal se fait aléatoirement
- Il n'y a pas de paquets multi-slots
- Des paquets sont échangés en permanence

Quelle est la probabilité de collision entre deux émissions sur deux réseaux bluetooth ?

Bluetooth Classic – **BR/EDR** :

- 79 canaux de 1 MHz

Bluetooth Low Energy – **(B)LE** :

- 40 canaux de 2 MHz

Simplification / suppositions :

- Les deux réseaux possèdent des « slots » synchronisés
- La sélection du canal se fait aléatoirement
- Il n'y a pas de paquets multi-slots
- Des paquets sont échangés en permanence

Combien de réseaux peuvent cohabiter si l'on souhaite moins de 50 % de chance de collision ?

Quelle est la probabilité de collision entre deux émissions sur deux réseaux bluetooth ?

- Bluetooth Classic – **BR/EDR** :
  - 79 canaux de 1 MHz
- Bluetooth Low Energy – **(B)LE** :
  - 40 canaux de 2 MHz

Simplification / suppositions :

- Les deux réseaux possèdent des « slots » synchronisés
- La sélection du canal se fait aléatoirement
- Il n'y a pas de paquets multi-slots
- Des paquets sont échangés en permanence

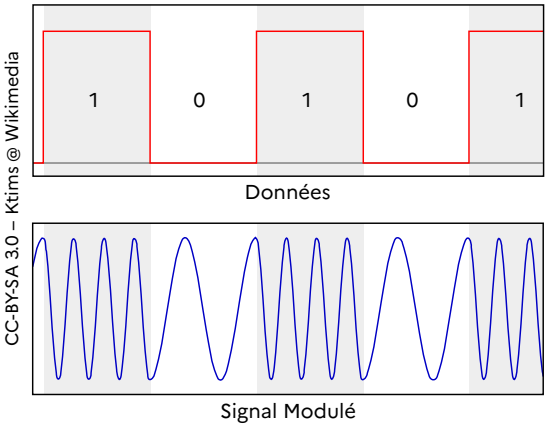
Combien de réseaux peuvent cohabiter si l'on souhaite moins de 50 % de chance de collision ?

Quel est le « goodput » théorique maximum pour l'ensemble de ces réseaux si l'on suppose un SNR de +30dB ?

La norme bluetooth impose :

- une sensibilité de -70 dBm (BER 0.1) minimum
- une puissance maximum de transmission de 20 dBm

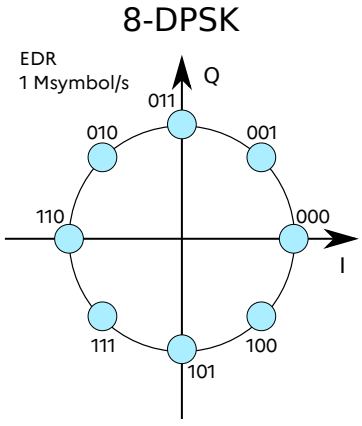
En supposant un canal de Friis, un gain d'antenne de -5 dBi en émission et réception, quelle est la portée maximale du Bluetooth ?

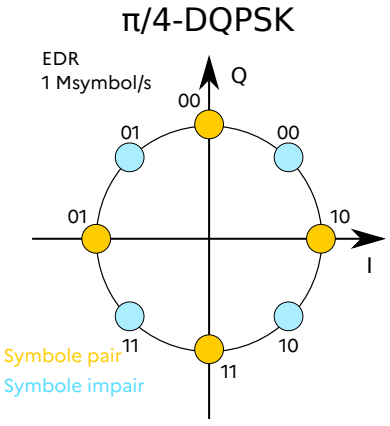


GFSK : Gaussian Frequency Shift Keying

GFSK vs FSK : Dans la modulation GFSK, on « adoucit » les transitions entre les deux fréquences en utilisant un filtre Gaussien, au lieu de « sauter » brusquement d'une fréquence à l'autre.

BR : 1Msymbol/s
BLE : 1Msymbol/s ou 2Msymbol/s


8-DPSK
EDR
1 Msymbol/s
Q
I
011
010
001
110
000
111
100
101


π/4-DQPSK
EDR
1 Msymbol/s
Q
I
00
01
00
01
10
11
10
11
Symbole pair
Symbole impair

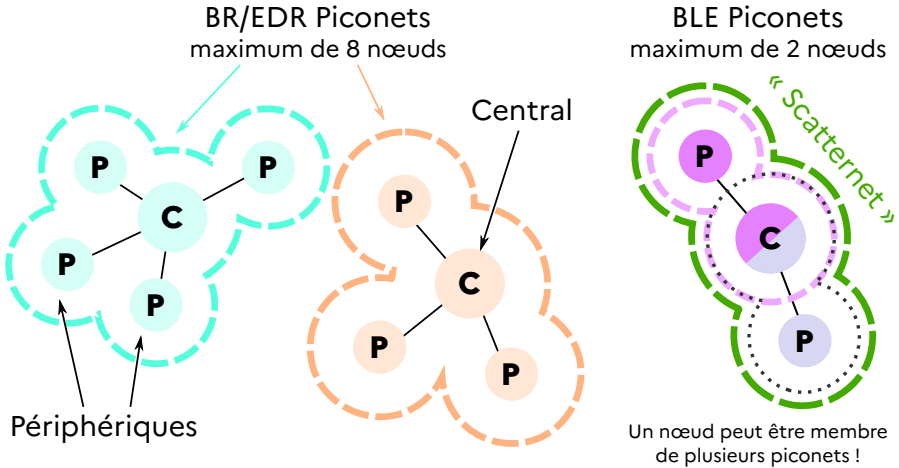
Focus sur Bluetooth Low Energy

Advertising (« Annonces »)

- Mécanisme de découverte
- Deux types de nœuds : Advertiser / Scanner
- Communication uni-directionnelle
- Communication éphémère
- Utilisation d'Aloha pour accéder au medium

Connection (« Connexions »)

- Mécanisme d'intéraction
- Deux types de nœuds : Périphérique / Central
- Communication bi-directionnelle
- Communication maintenue dans le temps
- Utilisation de TDMA pour accéder au medium



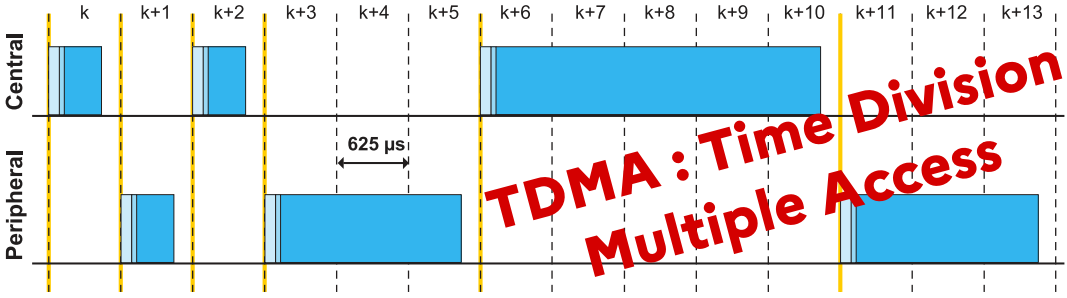
« Piconets shall not be frequency synchronized and each piconet has its own hopping sequence »

- Chaque nœud bluetooth possède une horloge qui génère des « ticks » toutes les 312.5μs ($f = 3.2$ kHz)

- Chaque nœud bluetooth possède une horloge qui génère des « ticks » toutes les 312.5μs ($f = 3.2$ kHz)
- Chaque « slot » sur chaque canal dure 625μs ($f = 1.6$ kHz)

- Chaque nœud bluetooth possède une horloge qui génère des « ticks » toutes les 312.5μs ($f = 3.2$ kHz)
- Chaque « slot » sur chaque canal dure 625μs ($f = 1.6$ kHz)
- Les « périphériques » s'alignent sur l'horloge de leur « central » et utilisent la séquence de sauts de ce nœud après un échange initial $^{(*)}$

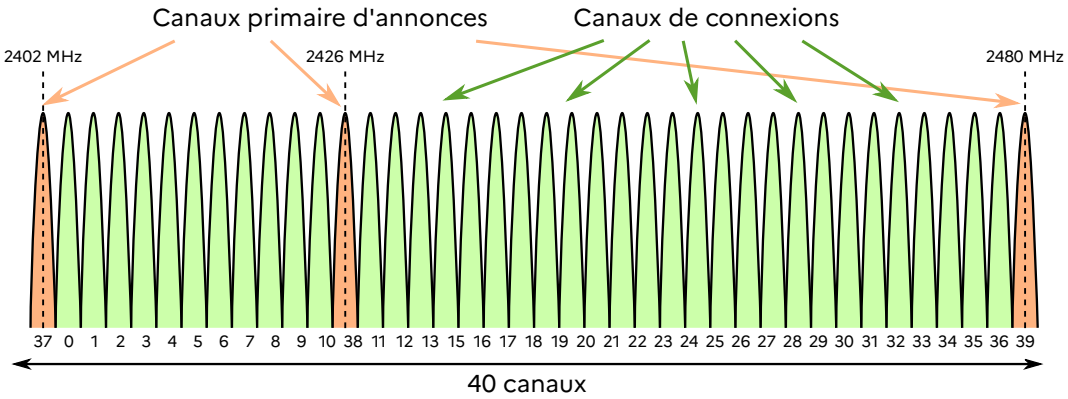
- Chaque nœud bluetooth possède une horloge qui génère des « ticks » toutes les 312.5μs ($f = 3.2$ kHz)
- Chaque « slot » sur chaque canal dure 625μs ($f = 1.6$ kHz)
- Les « périphériques » s'alignent sur l'horloge de leur « central » et utilisent la séquence de sauts de ce nœud après un échange initial $^{(*)}$

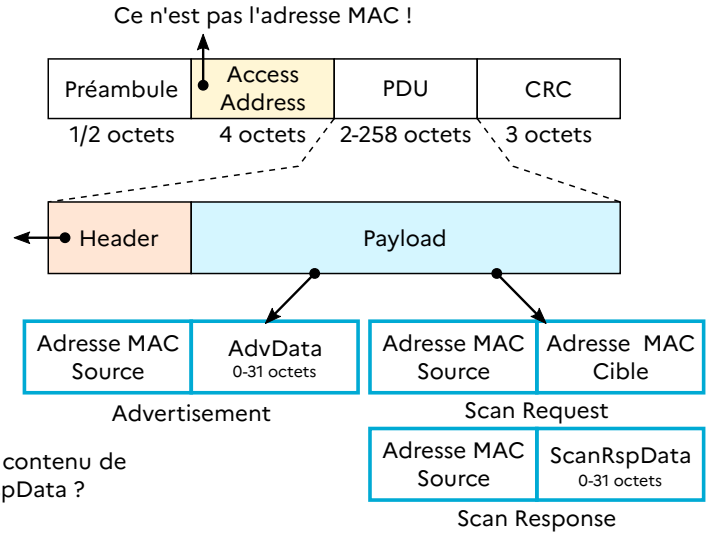


$^{(*)}$: il existe six méthodes différentes de sauter entre tous les canaux...

$^{(*)}$: il existe six méthodes différentes de sauter entre tous les canaux...

- Notion de « Time-Division Duplex » (*TDD*) : le bluetooth est (comme le Wi-Fi) half-duplex, mais donne l'impression d'une connexion full-duplex en partageant les slots entre *RX* et *TX*


Canaux primaire d'annonces
Canaux de connexions
2402 MHz
2426 MHz
2480 MHz
37 0 1 2 3 4 5 6 7 8 9 10 38 11 12 13 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 39
40 canaux


Ce n'est pas l'adresse MAC !
Préambule
Access Address
PDU
CRC
1/2 octets
4 octets
2-258 octets
3 octets
Header
Payload
Définit si le paquet est une annonce, une requête de scan ou une réponse de scan. En cas d'annonce, définit si le nœud accepte les connections et les requêtes de scan.
Définit si l'adresse MAC est une adresse « publique » ou « privée »
Adresse MAC Source
AdvData
0-31 octets
Advertisement
Adresse MAC Source
Adresse MAC Cible
Scan Request
Adresse MAC Source
ScanRspData
0-31 octets
Scan Response
Comment formater le contenu de AdvData ou de ScanRspData ?

Solution : suite de TLVs !

Solution : suite de TLVs !

TLV : Type – Length – Value

Solution : suite de TLVs !

TLV : Type – Length – Value

- Pas forcément dans cette ordre, pour le BLE l'ordre est LTV
- Liste des TLVs normalisés dans BLE : Core Specification Supplement 11
- Codes assignés aux TLVs normalisés : Assigned Number

Solution : suite de TLVs !

TLV : Type – Length – Value

- Pas forcément dans cette ordre, pour le BLE l'ordre est LTV
- Liste des TLVs normalisés dans BLE : Core Specification Supplement 11
- Codes assignés aux TLVs normalisés : Assigned Number

Exemples :

- Shortened Local Name : 0x08
- Complete Local Name : 0x09
- Device ID : 0x10
- ...

Sur quels canaux « annoncer » ou « écouter » ?

Sur quels canaux « annoncer » ou « écouter » ?

Question de l'efficacité énergétique : combien de temps émettre et combien de temps écouter ? (question du *duty-cycle*)

Sur quels canaux « annoncer » ou « écouter » ?

Question de l'efficacité énergétique : combien de temps émettre et combien de temps écouter ? (question du *duty-cycle*)

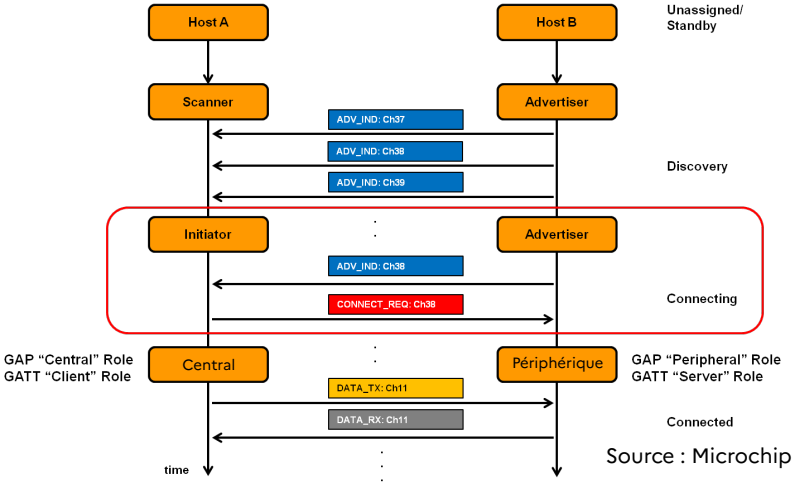
- Émission : canaux 37, 38 et 39, en round-robin, avec succession d'annonces et de fenêtre d'écoute pour pouvoir écouter des scan requests associées sur chaque canal, avec un délai aléatoire au début de l'émission
- Réception : canaux 37, 38, 39, en round-robin

Pourquoi un mode connecté ? Principalement, augmenter le débit !

Pourquoi un mode connecté ? Principalement, augmenter le débit !

Anatomie d'une connexion :

1. Initiation de la connexion :
   - Un annonceur envoie régulièrement des annonces
   - Un scanneur reçoit une annonce et décide de s'y connecter
   - Le scanneur envoie une requête de connexion à l'annonceur
2. Maintient de la connexion :
   - C envoie un paquet à chaque intervalle de connexion
   - P répond de manière immédiate avec un paquet
3. Terminaison de la connexion :
   - P/C envoie un paquet de déconnexion
   - Un timeout est atteint


Host A
Host B
Unassigned/
Standby
Scanner
Advertiser
ADV_IND: Ch37
ADV_IND: Ch38
ADV_IND: Ch39
Discovery
Initiator
Advertiser
ADV_IND: Ch38
CONNECT_REQ: Ch38
Connecting
GAP "Central" Role
GATT "Client" Role
Central
Périphérique
GAP "Peripheral" Role
GATT "Server" Role
DATA_TX: Ch11
DATA_RX: Ch11
Connected
time
Source : Microchip

GATT : Generic Attribute Profile

GATT : Generic Attribute Profile

- Organisation des données *exposées* par un nœud bluetooth sous une forme pré-définie
- Modèle « Client-Serveur » pour accéder à ces données en BLE

GATT : Generic Attribute Profile

- Organisation des données *exposées* par un nœud bluetooth sous une forme pré-définie
- Modèle « Client-Serveur » pour accéder à ces données en BLE

Trois niveaux d'organisation :

- **Profiles** : Schéma normalisé par le SIG, e.g. « Heart Rate », « Continuous Glucose Monitoring » ou « A/V Remote Control », combinant plusieurs services
- **Services** : Catégorisation des données liées aux profiles, e.g. « Device Information », « Heart Rate », chaque service combinant une ou plusieurs caractéristiques (UUID)
- **Caractéristiques** : Point de données « brut », e.g. « Pression », « Température », ... (UUID)

Permissions sur ces caractéristiques :

- « Readable » : pull (du client)
- « Writable » : push (vers le serveur)
- « Notify » / « Indication » : envoi par le serveur (no ack / ack)

Permissions sur ces caractéristiques :

- « Readable » : pull (du client)
- « Writable » : push (vers le serveur)
- « Notify » / « Indication » : envoi par le serveur (no ack / ack)

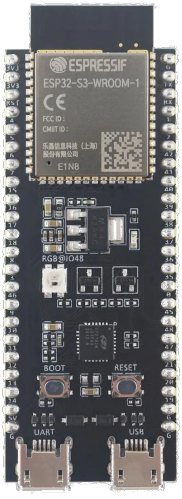
Exploration des données :

- Liste de profiles : Specs SIG
- Assignation d'UUID : Assigned Numbers

ESP-32-S3

Micro contrôleur qui sait faire du Wi-Fi et du BLE !

- Documentation ESP-IDF
- Compatibilité avec Micro-python
- Plein d'exemples d'utilisation du framework [esp-idf]
- Programmation principalement en C mais possible, de manière limitée, en python



Mini-projets autour de l'ESP32-S3, Wi-Fi et BLE

Idées en vrac :

- Vos idées !
- Faire un détecteur de présence en utilisant un objet BLE type montre connecté
- Faire un « chat » qui permet une communication multi-sauts en BLE
- Test de la fonctionnalité FTM (Fine Timing Measurements)
  → Détecter la distance entre modules en mesurant le *Time Of Flight* des ondes Wi-Fi
- Test de la fonctionnalité CSI (Channel State Information)
  → Détecter des changements dans l'environnement en mesurant les changements dans la propagation du canal

Mini-projets autour de l'ESP32-S3, Wi-Fi et BLE

Idées en vrac :

- Vos idées !
- Faire un détecteur de présence en utilisant un objet BLE type montre connecté
- Faire un « chat » qui permet une communication multi-sauts en BLE
- Test de la fonctionnalité FTM (Fine Timing Measurements)
  → Détecter la distance entre modules en mesurant le *Time Of Flight* des ondes Wi-Fi
- Test de la fonctionnalité CSI (Channel State Information)
  → Détecter des changements dans l'environnement en mesurant les changements dans la propagation du canal

1. Setup de l'environnement de développement, choix des projets
2. Début du projet, travail à la maison
3. Prochaine séance autour des projets !