Réseaux mobiles et réseaux sans fil

RSX116

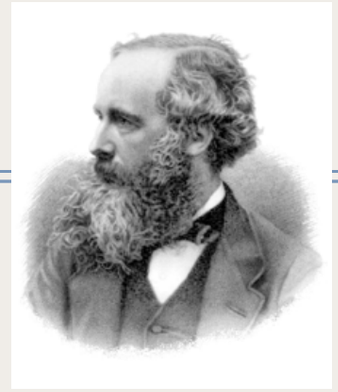
Réseaux sans fil : IEEE 802.11, IEEE 802.15, etc.

Documents liés aux cours : https://rsx116.seancetenante.com

François Lacomme <francois@seancetenante.com>

Réseaux sans fil ; présentation

La transmission sans fil



James Clerk Maxwell.

Heinrich Hertz

- Le spectre électromagnétique
  - 1863 - **Clerk Maxwell** - théorie ondulatoire
  - 1887 - **Heinrich Hertz** - vérification expérimentale de la théorie de Maxwell
- Principe :
  - une onde électromagnétique (o.e.m.) se propage entre un émetteur et un récepteur

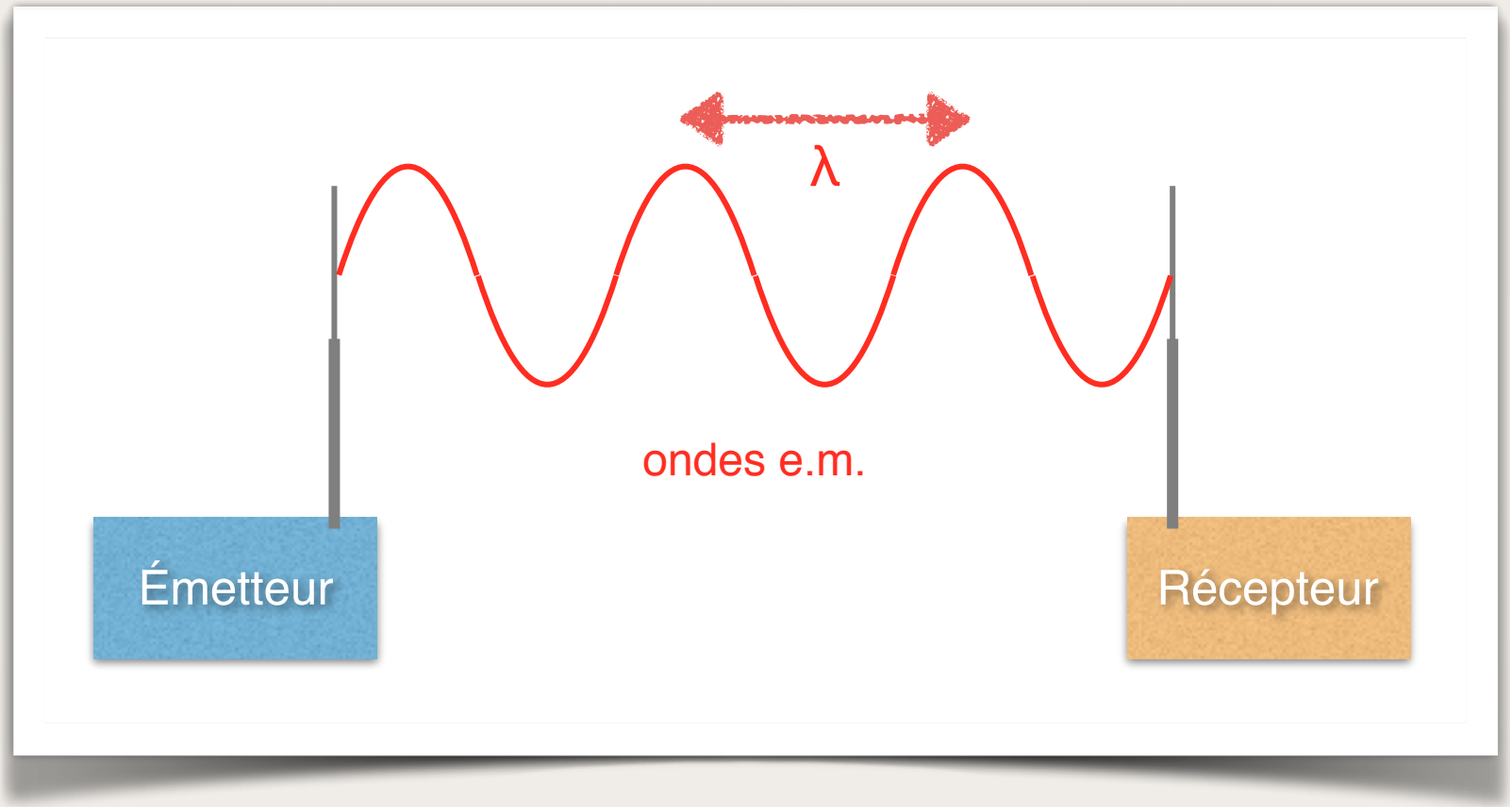


Fig 1.1. - Principe des ondes électromagnétiques

Réseaux sans fil ; présentation

La transmission sans fil

- Définitions
  - **Fréquence d'une onde** : nombre d'oscillation par seconde ; en **Hertz**
  - **Longueur d'onde λ**, en **mètre** : distance entre 2 maxima consécutifs d'une o.e.m.
  - **Vitesse de propagation** d'une o.e.m. :
    - dans le vide, $c = 3 \times 10^8$ m/s (soit 30 cm/ns)
    - dans le cuivre ou le verre, $v \approx 2 \times 10^8$ m/s, en fonction de la fréquence
  - Dans le vide, **$\lambda.f = c$**
  - Ex. $f = 1$ MHz $\Rightarrow \lambda = 300$ m
    $\lambda = 1$ cm $\Rightarrow f = 30$ GHz

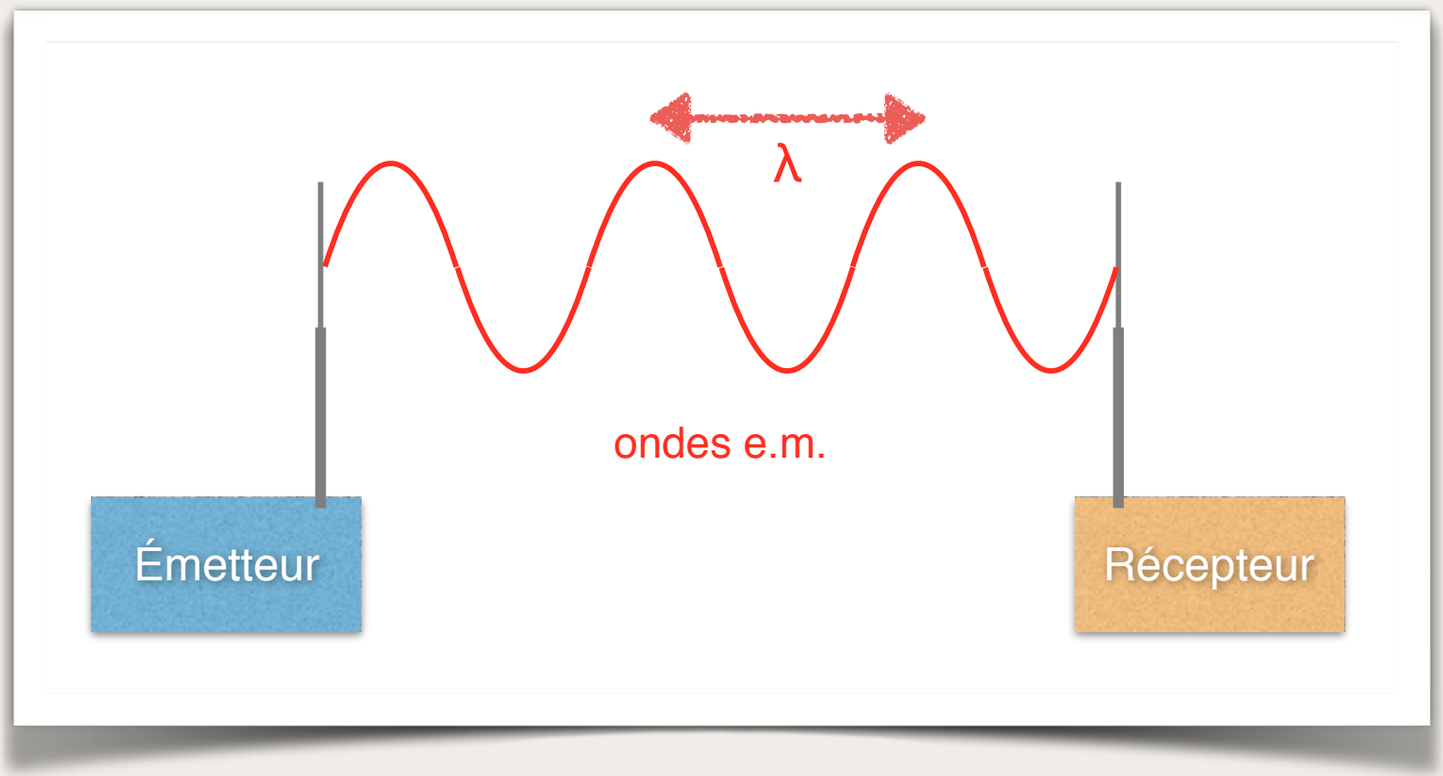


Fig 1.1. - Principe des ondes électromagnétiques

Réseaux sans fil ; présentation

Le spectre de fréquences

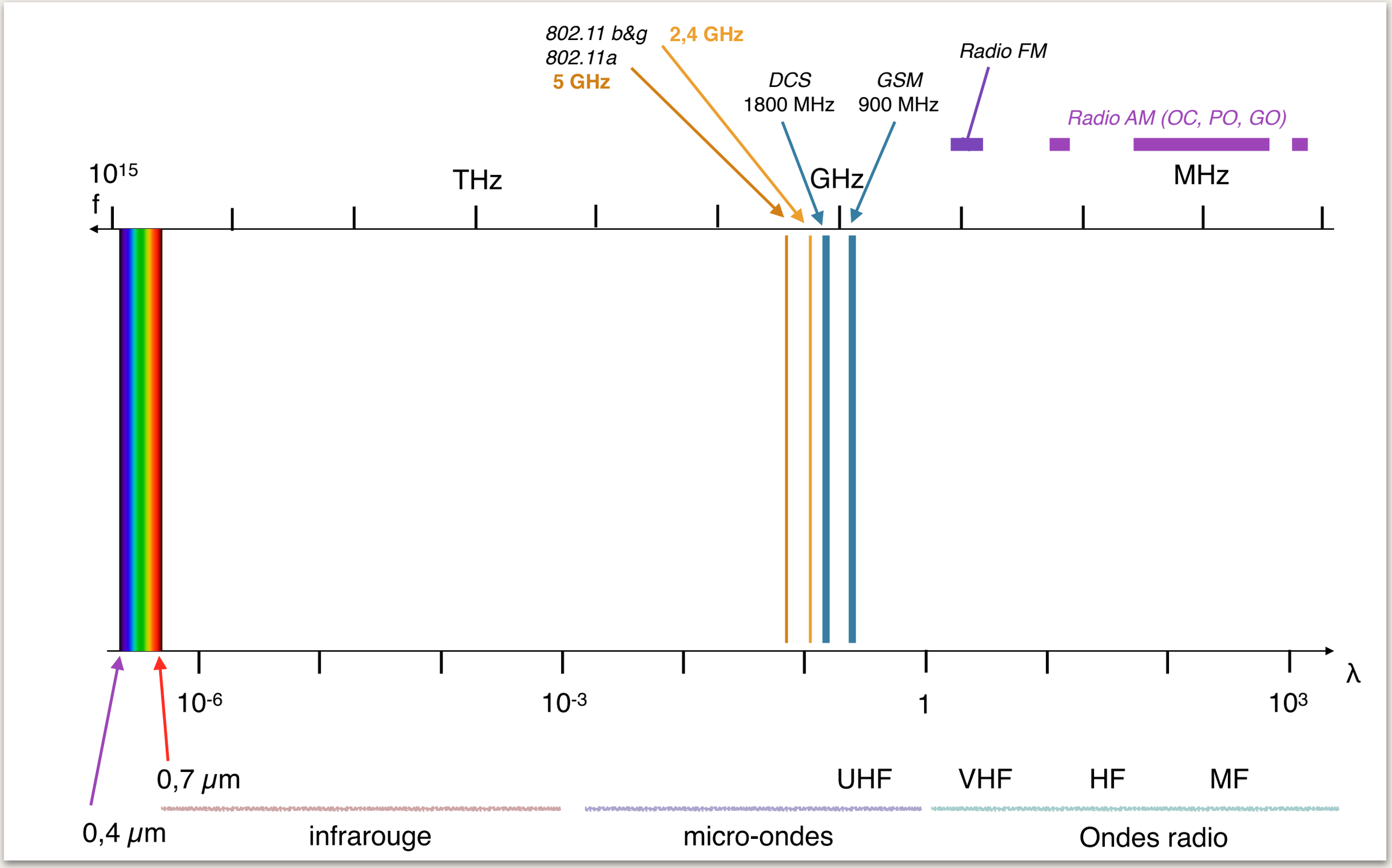


Fig 1.2. - Spectre de fréquences

Réseaux sans fil ; présentation

Types de réseaux sans fil

- WPAN - *Wireless PAN*
  - Normalisation par le groupe de travail **IEEE 802.15** et par le *Bluetooth Special Interest Group*
  - Bluetooth : **IEEE 802.15.1**
  - ZigBee : **IEEE 802.15.4**
- WLAN - *Wireless LAN* - RLAN - Radio LAN (Réseaux locaux radioélectriques)
  - Wi-Fi [ouaille fa]
  - Ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11

Réseaux sans fil ; présentation

Types de réseaux sans fil

- WiMAX - boucle locale radio
  - La boucle locale désigne les infrastructures de transmission d'un réseau de télécommunications ouvert au public reliant directement les clients aux équipements de commutation auxquels ils sont rattachés. Elle représente un segment important du réseau d'un opérateur, à travers lequel celui-ci peut accéder directement à ses clients et maîtriser les services offerts.
  - Les technologies radio dans la boucle locale constituent aujourd'hui une solution de substitution aux moyens filaires pour le raccordement direct de clients et la fourniture de services de télécommunications fixes.
- WWAN - Wireless Wide Area Network
  - Réseaux cellulaires GSM, UMTS, LTE
  - Liaison satellite
- IoT - IdO
  - *Internet of Things / Internet des objets*

Réseaux sans fil ; présentation

Normalisation & réglementation

- Le partage du spectre impose une forte règlementation. Les acteurs sont :

- ANFR : Agence Nationale des Fréquences

- ARCEP : Autorité de Régulation des Communication Électronique et des Postes

- CEPT : *European Conference of Postal and Telecommunications Administrations*

- ETSI : *European Telecommunications Standards Institute*

- UIT-T : Union internationale des télécommunications - Secteur de la normalisation des télécommunications

Wi-Fi

Généralités ; normalisation

- Wi-Fi ~ Wireless Fidelity
- Réseaux sans fil normalisés par IEEE, *Institute of Electrical and Electronics Engineers*
- Fréquences
  - ANFR, Agence Nationale des Fréquences. Voir la frise des bandes de fréquences
  - ARCEP, Autorité de régulation des communications électroniques et des postes
- IEEE 802.11 :
  - Spécifications de IEEE pour l'implémentation de réseaux numériques locaux à liaison sans fil
  - Les bandes de fréquences ont été choisies dans des bandes sans licence :
    - Une bande ISM (Industriel, Scientifique et Médical) définie par UIT-R (2,4 à 2,485 GHz aux USA)
    - Une bande U-NII, *Unlicensed National Information Infrastructure,* vers 5 GHz, en 2 larges sous-bandes (de 5,150 à 5,350 GHz et de 5,470 à 5,850 GHz)

Wi-Fi

Généralités ; normalisation

- IEEE 802.11 :
  - Spécifications de IEEE pour l'implémentation de réseaux numériques locaux **à liaison sans fil**
  - 1997 : norme initiale
  - 1999 : 802.11a - 54 Mbit/s max
  - 1999 : 802.11b - 11 Mbit/s max - portée 20 à 100 m
  - 2003 : 802.11g - 54 Mbit/s max - portée 20 à 75 m
  - 2009 : 802.11n ou **Wi-Fi 4** - 450 Mbit/s max - portée 50 à 125 m
  - 2014 : 802.11ac ou **Wi-Fi 5** - 1300 Mbit/s max - portée 80 à 125 m
  - fin 2019 : 802.11ax ou **Wi-Fi 6** - 10,5 Gbit/s max
    - Wi-Fi 6E en 2021 : Nouvelle bandes autour de 6 GHz
    - Wi-Fi 6 version 2 en janvier 2022
  - mi 2024 : 802.11be ou **Wi-Fi 7**
    - Wi-Fi 802.11be EHT pour Extremely High Throughput
    - Des équipements supportant un pré-standard prévus en 2023

Généralités ; normalisation

- IEEE 802.11 :

Principaux standards 802.11

Standard	Date	Frequence	Débit binaire	Largeur de bande	Portée (m) Intérieur/extérieur
802.11	1997	2.4 GHz	1,2 Mbit/s	79 ou 22 MHz	20/100
802.11a	1999	5 GHz	6 à 54 Mbit/s	20 MHz	35/120
802.11b	1999	2.4 GHz	1 à 11 Mbit/s	22 MHz	38/140
802.11g	2003	2.4 GHz	6 à 54 Mbit/s	20 MHz	38/140
802.11n	2009	2.4/5 GHz	7 à 150 Mbit/s	20 ou 40 MHz	12 à 70 / 250
802.11ac (Wi-Fi 5)	déc. 2013	5 GHz	6,5 Mbit/s à 3,4 Gbit/s	20 à 160 MHz	70/250
802.11ax (Wi-Fi 6)	fév. 2021	2.4/5 GHz	8 Mbit/s à 10,5 Gbit/s	20 à 160 MHz	12 à 35 / 300
802.11be (Wi-Fi 7)	mars 2024 ?	2.4/5/6 GHz	jq'à 46 Gbit/s	80 à 320 MHz	30 / 120

Fig 2.1. - Principaux standards 802.11

Généralités ; normalisation

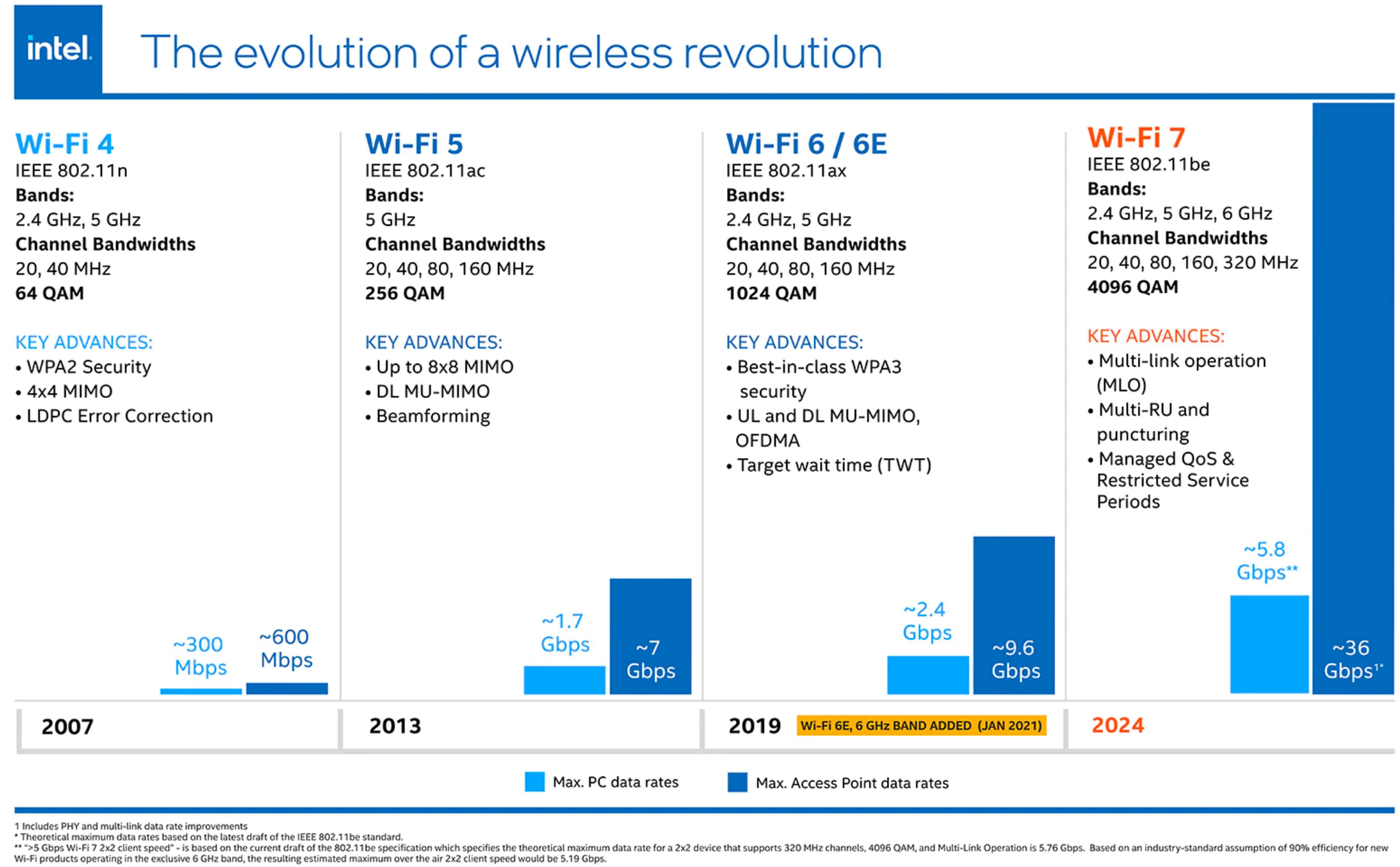


Fig 2.3. - De Wi-Fi 4 à Wi-Fi 7

Généralités ; normalisation

- IEEE 802.11 : autres normes
  - Certaines normes de IEEE complètent les précédentes :
  - 802.11e - QoS, au niveau MAC, pour améliorer le transport de la voix, audio et vidéo.
  - 802.11f - Recommandation aux fournisseurs de point d'accès pour faciliter l'itinérance (*roaming*).
  - 802.11i - Améliorer la sécurité des transmissions.
    - Gestion et distribution des clés, chiffrement et authentification.
    - Cette norme s'appuie sur l'AES, *Advanced Encryption Standard,* et propose l'authentification (WPA2) et un chiffrement des communications pour les transmissions utilisant les standards 802.11a, 802.11b et 802.11g.
  - 802.11r - H*andover.* Améliorer la mobilité entre cellules.
  - 802.11s - *Mesh networking*. Implémenter la mobilité sur les réseaux de type **ad hoc**. Tout point qui reçoit le signal est capable de le retransmettre. Routage avec OLSR, *Optimized Link State Routing Protocol.*
  - 802.11u - Améliorer l'identification d'un terminal et l'interopérabilité avec d'autres réseaux Wi-Fi (ayant des SSID, *Service Set Identifier,* différents) et avec les réseaux de téléphonie mobile.

Généralités ; normalisation

- Définitions

  - **Point d'accès** (PA) (AP, *Access Point*) : dispositif tel qu'un routeur permettant à des appareils Wi-Fi de se connecter au réseau local.
    - Le point d'accès crée un réseau Wi-Fi en émettant des signaux radio qui permettent aux dispositifs compatibles Wi-Fi de se connecter et de communiquer avec le réseau.
    - Un SSID est associé au point d'accès.
  - **SSID,** ***Service Set Identifier,*** est le nom attribué à un réseau Wi-Fi.
    - Le SSID est le nom que vous choisissez pour votre réseau Wi-Fi.
    - Un même SSID peut être affecter à plusieurs point d'accès de votre LAN.

Modes d'accès

- Le mode infrastructure ; un réseau 802.11 est alors constitué :
  - de postes clients (PC, smarphones etc)
  - d'équipements d'infrastructure : points d'accès (*Access Point* ou AP) [ou stations de base ou borne sans fil], configurés avec le même **SSID,** *Service Set Identifier,* (soit le même nom de réseau) et eux-même reliés à un réseau filaire.
    - **SSID,** *Service Set Identifier,* est un nom logique, sensible à la casse, de 32 octets maximum.
- Le mode ad hoc :
  - les postes se connectent directement, de machine à machine, sans point d'accès. Toutes les machines sont alors configurés avec un même canal de fréquence et le même SSID : elles forment un même **IBSS**, *Independant Basic Service Set*.
- Le mode Pont (*Bridge*) :
  - 2 points d'accès sont en mode pont pour, par ex., étendre un réseau filaire entre 2 bâtiments.
- Le mode répéteur (*Range-extender*)
  - Pour répéter un signal Wi-Fi plus loin.

Généralités ; Couches OSI

Couche Liaison de données *Data Link Layer*	802.11 Logical Link Control (LLC)							
	802.11 Medium Access Control (MAC)							
Couche Physique *Physical Layer*	802.11 PLCP (*Physical Layer Convergence Protocol*)							
	FHSS	DSSS	IR	Wi-Fi 802.11a	Wi-Fi 802.11b	Wi-Fi 802.11g	Wi-Fi 802.11n	Wi-Fi 802.11ac

Le modèle en couche pour IEEE 802.11

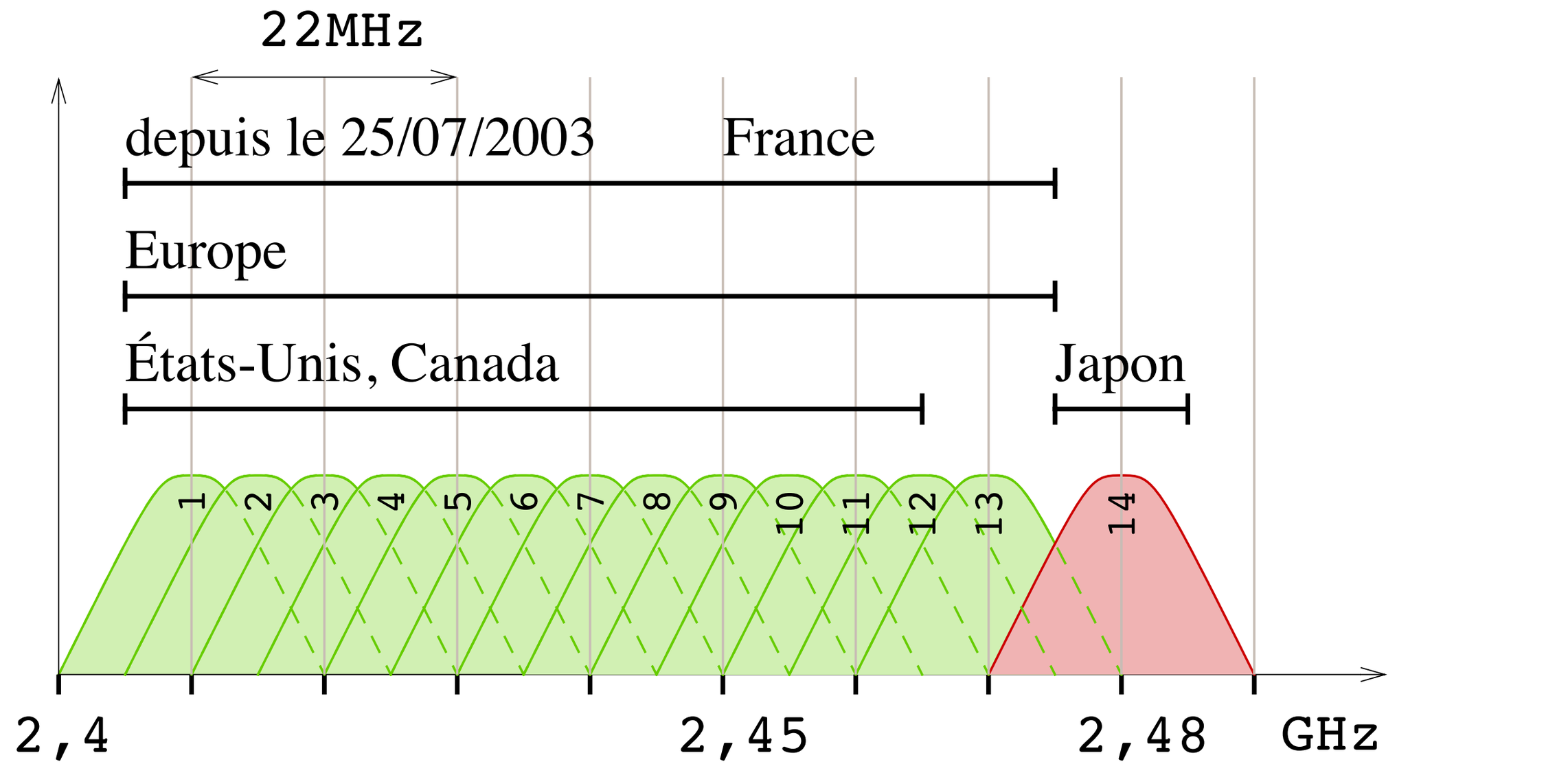
- FHSS : *frequency-hopping spread spectrum* ; étalement de spectre par saut de fréquence
- DSSS : *direct-sequence spread spectrum* ; étalement de spectre à séquence directe
- IR : Infrarouge

Le niveau physique

- Le niveau physique est découpé en 2 couches :
  - **PMD**, *Physical Medium Dependent*
    - chargée de la transmission des bits sur le support hertzien
    - Gère l'encodage des données et effectue la modulation
  - **PLCP**, *Physical Layer Convergence Protocol*
    - chargée de l'écoute du support
    - fournit un CCA, *Clear Channel Assessment*) à la couche MAC pour signaler que le canal est libre

- Les bandes de fréquence
  - Les couches radio des standards IEEE 802.11 utilisent des bandes sans licence (sans autorisation nécessaire si les puissances limites sont respectées)
    - la bande **ISM**, *Industrial, Scientific & Medical* : 2,400 à 2,4835 GHz en Europe (ETSI)
    - Une bande **U-NII**, *Unlicensed National Information Infrastructure*, vers 5 GHz, en 2 larges sous-bandes (de 5,150 à 5,350 GHz et de 5,470 à 5,850 GHz)
  - Voir aussi :
    - la frise des bandes de fréquences
    - Le tableau national de répartition des bandes de fréquences (TNRBF)

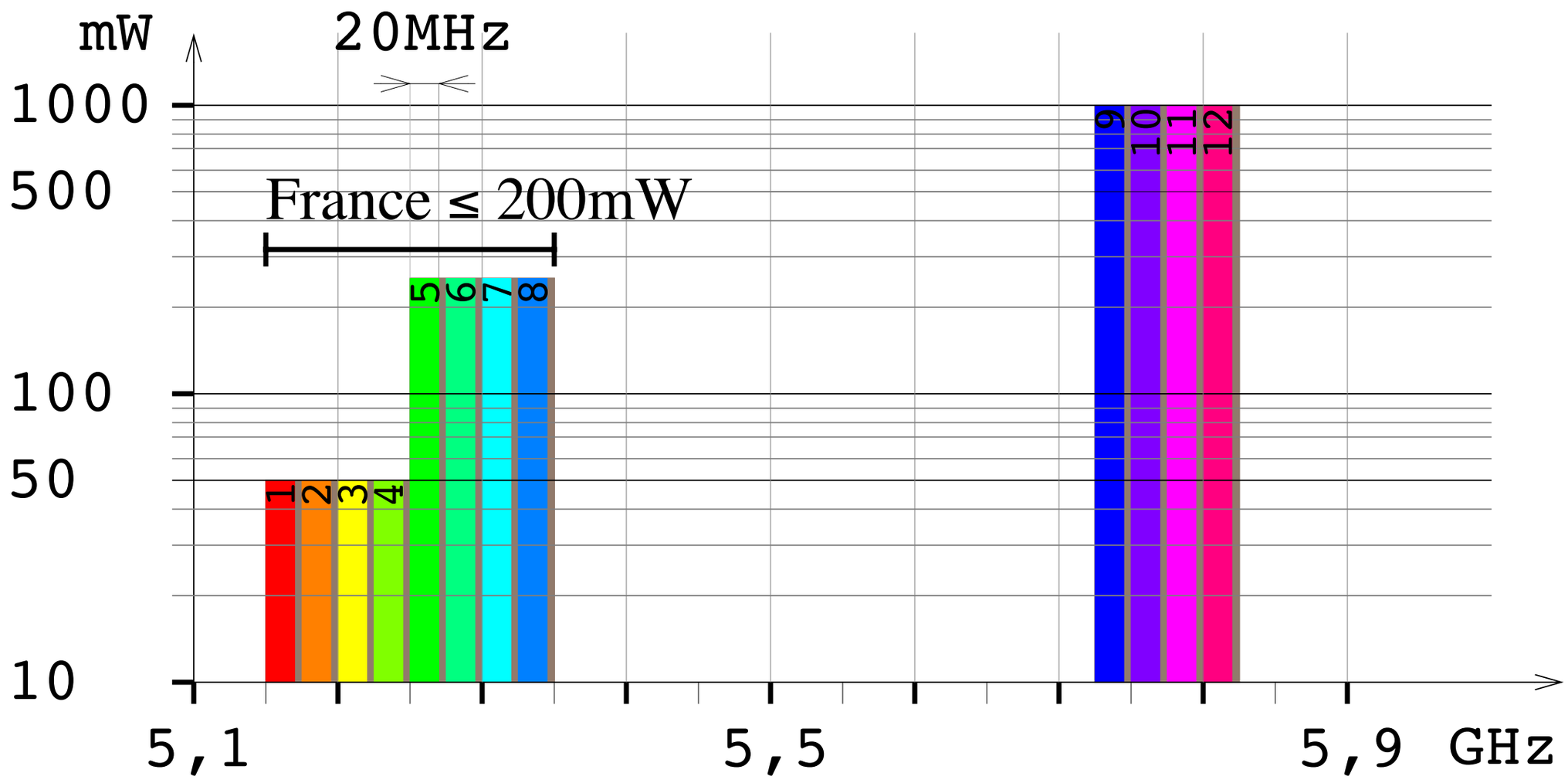
Le niveau physique



Bande ISM (Industrial, Scientific, and Medical).

https://portail.jacquenod.net/Web/SansFil/DHTML/CV-sansfil.htm

Le niveau physique

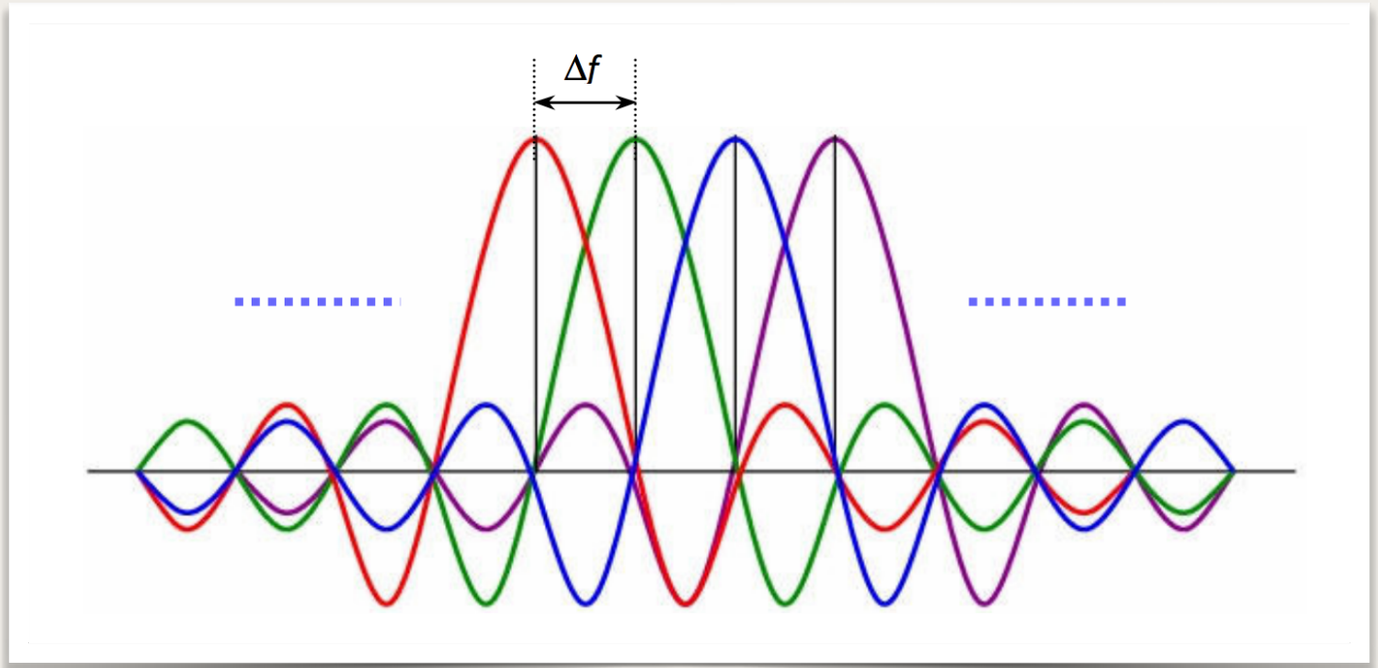


Bande UNII (Unlicensed National Information Infrastructure).

Wi-Fi

Modulation

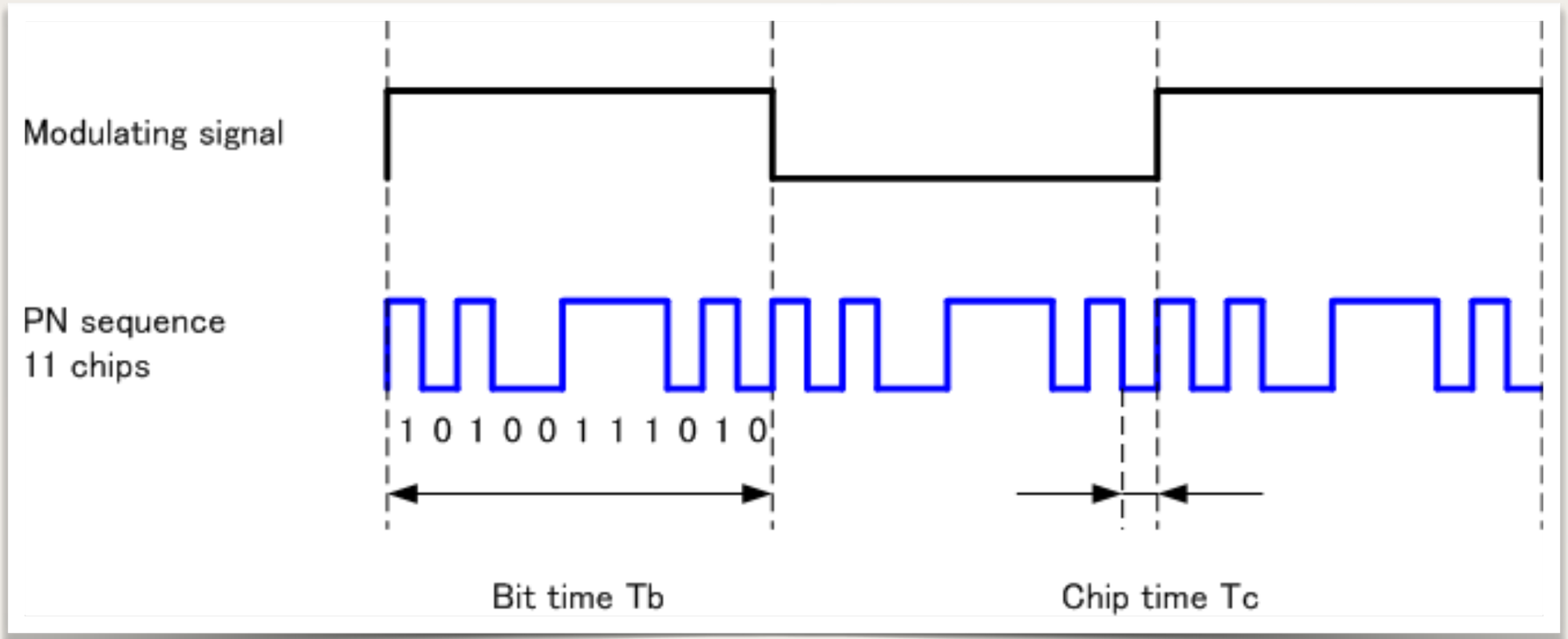
- Avec les normes IEEE 802.11, on distingue 2 types de modulation
- **OFDM**, *Orthogonal frequency-division multiplexing*
  - https://fr.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing
  - de type DMT (*Discrete Multitone modulation*)
  - **Principe** : Répartir sur un grand nombre de sous-porteuses le signal numérique que l'on veut transmettre.
    - Ce codage tient compte des trajets d'ondes indirects qui interfèrent avec un trajet direct.
    - OFDM est utilisé pour les standards 802.11a, 802.11n, 802.11ac, 802.11g
    - OFDMA, *Orthogonal Frequency-Division Multiple Access* est une variante utilisée pour Wi-Fi 6 alias IEEE 802.11ax.



Wi-Fi

Modulation

- **DSSS** : *Direct-sequence spread spectrum*
  - https://fr.wikipedia.org/wiki/Direct-sequence_spread_spectrum
  - Technique d'**étalement de spectre** à séquence directe.
  - DSSS permet à chaque canal d'utiliser toute la bande de fréquence allouée, en utilisant un code unique (technique CDMA : *Code Division Multiple Access*).
  - 1 bit est codé en une séquence de N chips, ce qui étale le spectre
  - Résistant aux brouillages et aux interférences
  - DSSS : utilisé pour les standards 802.11b et 802.11g



Portée des réseaux Wi-Fi

- Accroître la portée d'un point d'accès =>
  - Permettre de gérer plus de stations mobiles…
  - Qui se partagent alors un même domaine de collision
  - En émission, la puissance croît avec le carré de la portée, et consomme donc de l'énergie. Un mécanisme d'économie d'énergie est mis en œuvre dans la norme 802.11
- Pour couvrir une zone géographique :
  - Utiliser plusieurs cellules, avec un jeu de fréquences distinctes
  - Augmenter la portée des points d'accès
- La puissance d'émission est réglementée ; en France :
  - Dans un bâtiment (*Indoor*)
    - 100 mW (bande 2,400 - 2,4835 GHz)
    - 40 mW (5,15 - 5,25 GHz) ou 200 mW (5,25 - 5,35 GHz)
  - En extérieur (*Outdoor*)
    - 100 mW (bande 2,400 - 2,457 GHz) ou 10 mW (bande 2,454 - 2,4835 GHz)
    - 40 mW (bande 5,725 - 5,825 GHz)

La couche MAC

- La couche liaison de données des réseaux Wi-Fi
  - La sous-couche LLC, *Logical Link Control*
  - La sous-couche MAC, *Medium Access Control*
- La couche MAC décrit 2 modes d'accès au canal
  - DCF, *Distribution Coordination Function*, un accès à compétition du type CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance)*, à esquive de collision
  - PCF, *Point Coordination Function*, avec un contrôle centralisé par le point d'accès

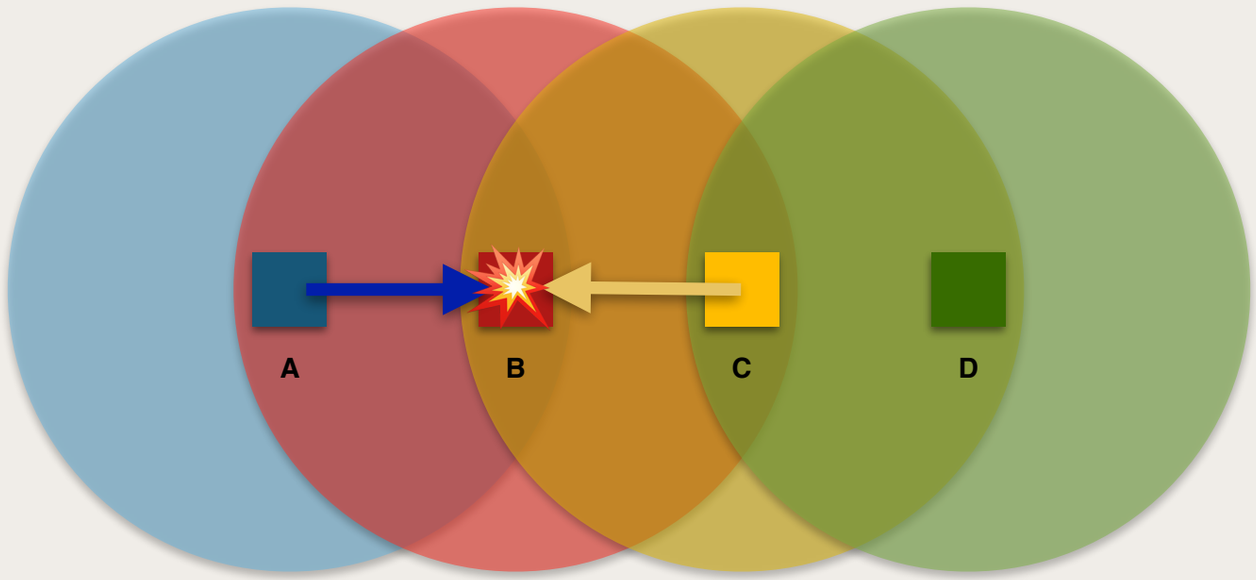
La couche MAC

- Silences inter-trames
  - Contrôle de l'accès au support à l'aide de silences inter-trames, IFS, *Interframe Spacing*
  - 4 types d'IFS :
    - SIFS, *Short Interframe Spacing*, avant un acquittement (ACK) ; 28µs
    - PIFS, *Point Coordination Function Interframe Spacing*, utilisé par un point d'accès pour des données prioritaires ; 78µs
    - DIFS, *Distribution Coordination Function Interframe Spacing*, pour des **trames normales** ; 128µs
    - EIFS, *Extended Interframe Spacing*, retransmission après une trame incorrecte

Wi-Fi

La couche MAC

- Un réseau Wi-Fi est un réseau à diffusion nécessitant des protocoles adaptés
- Problème de la **station cachée**
  - A et C souhaitent communiquer avec B
    - C est **hors de portée** de A
  - A émet
  - Si C émet aussi, des interférences se produisent pour B



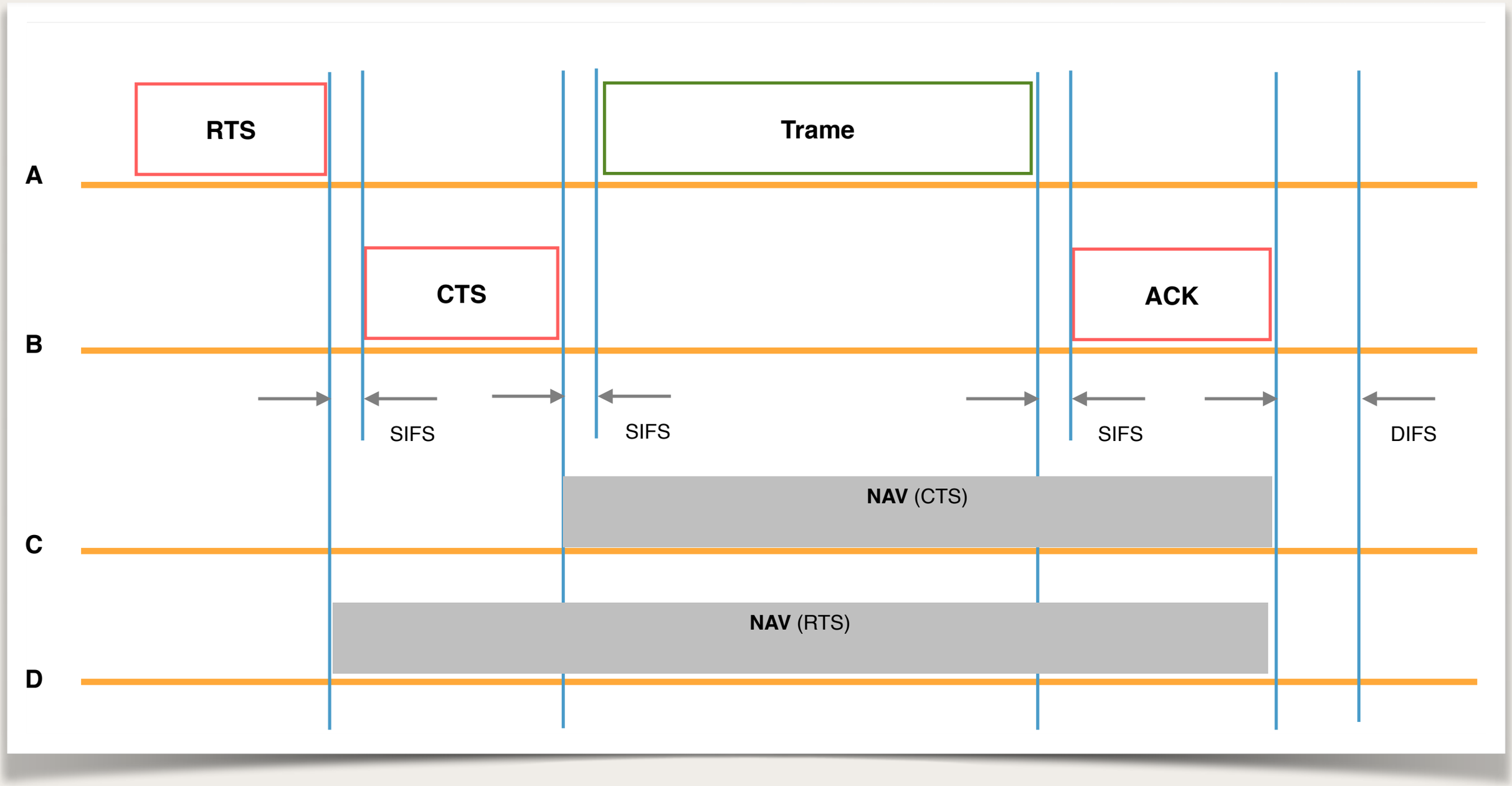
- Voir : Stations-cachee-exposee.pdf

La couche MAC

- La méthode RTS/CTS
  - A écoute le support ; celui-ci est libre pendant DIFS ;
    - A émet une courte trame, **RTS**, *Request to Send*, avec une information de réservation du support (NAV, *Network Allocation Vector*)
  - B reçoit le **RTS** de A.
    - B attend SIFS et il acquitte avec une courte trame, **CTS**, *Clear to Send*, avec l'information de réservation du support NAV adapté
  - A reçoit le CTS de B.
    - A attend SIFS et émet sa trame de **données**
  - B vérifie la trame,
    - B attend SIFS et émet **ACK**
  - Lorsque C, à portée de B, reçoit le **CTS** de B il s'interdit toute émission en fonction du NAV reçu.

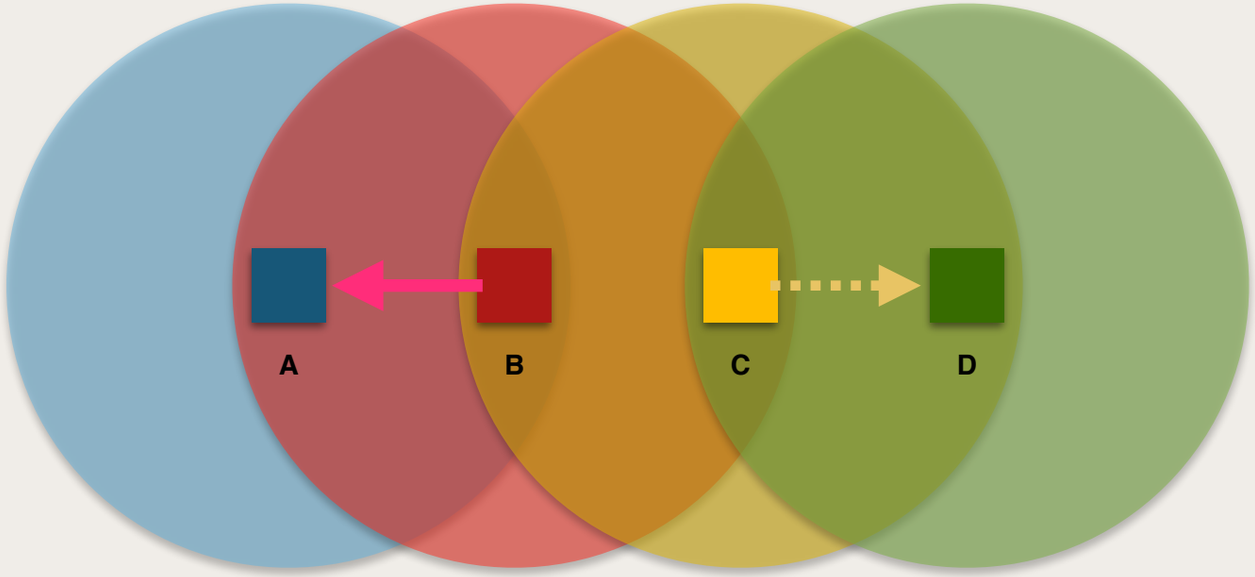
- Voir : https://www.ccs-labs.org/teaching/rn/animations/csma/

La couche MAC



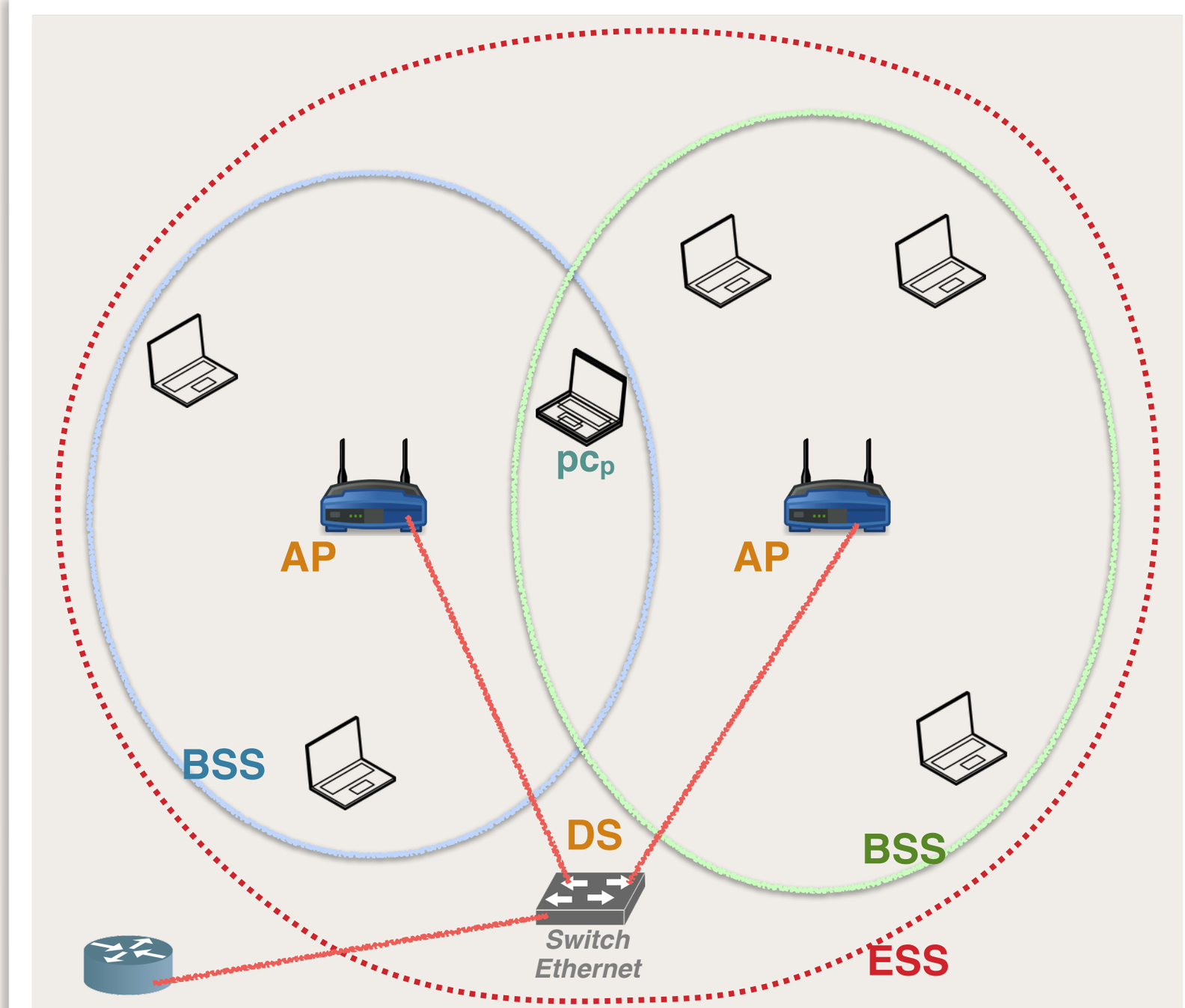
La couche MAC

- Problème de la **station exposée**
  - B transmet vers A alors que C souhaite transmettre vers D
  - Les interférences n'affecteraient ni A ni D. La double transmission est possible
  - C, qui trouve le canal occupé par B, estime à tord qu'il ne peut pas émettre vers D
  - CSMA/CA ne résout pas ce problème



Mode infrastructure

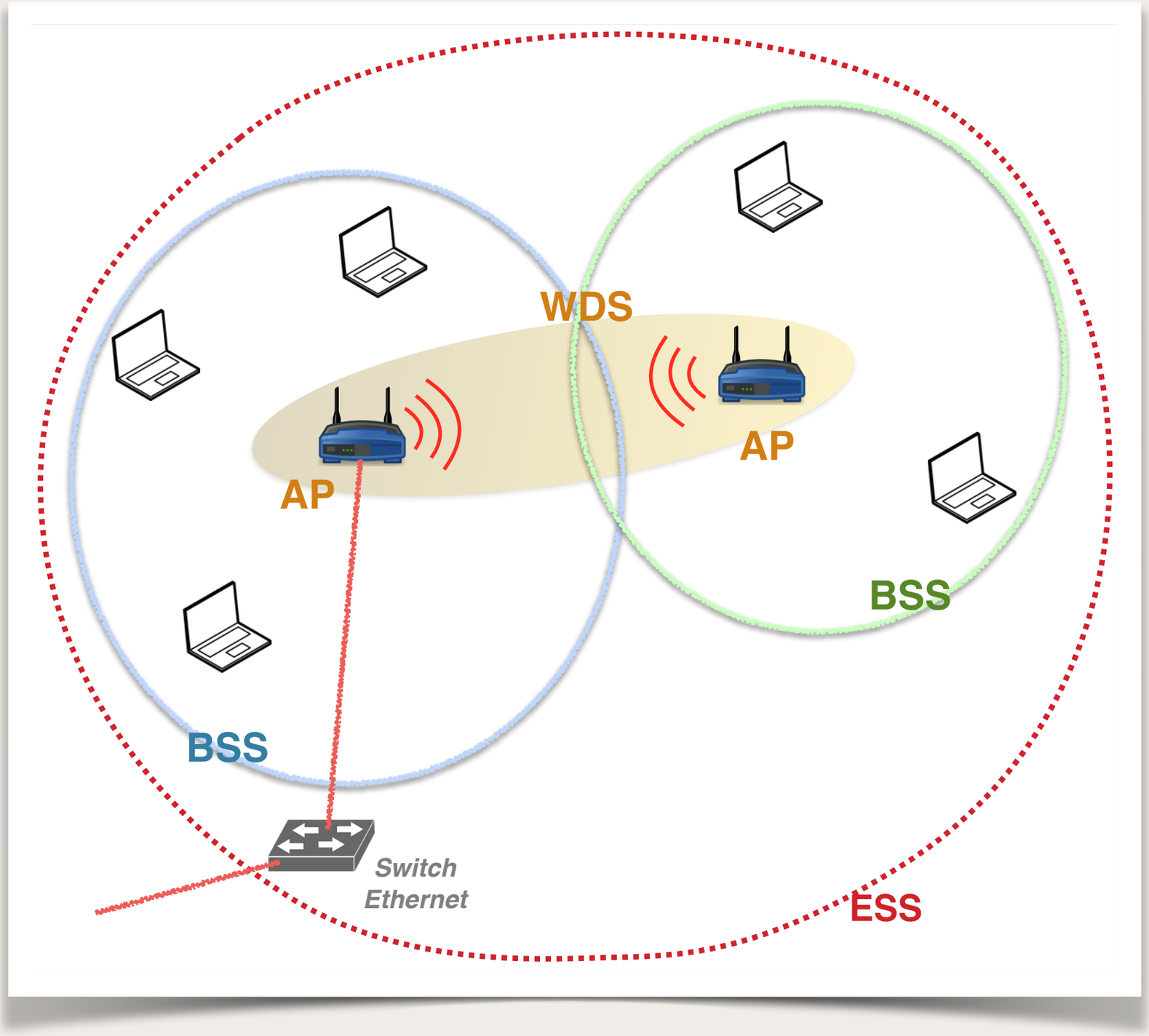
- AP : *Access Point*
- BSS : *Basic Service Set*
- ESS : *Extended Service Set*
- DS : *Distributed System*
  - Réseau Ethernet d'interconnexion des BSS
- pc_p risque de subir des interférences entre 2 BSS.
  - Avec Wi-Fi 6, *BSS color* résout certains problèmes d'OBSS, *Overlapping basic service set*



Mode infrastructure

- *WDS : Wireless Distributed System*
  - Réseau sans fil d'interconnexion des BSS

- AP : *Access Point*
- BSS : *Basic Service Set*
- ESS : *Extended Service Set*

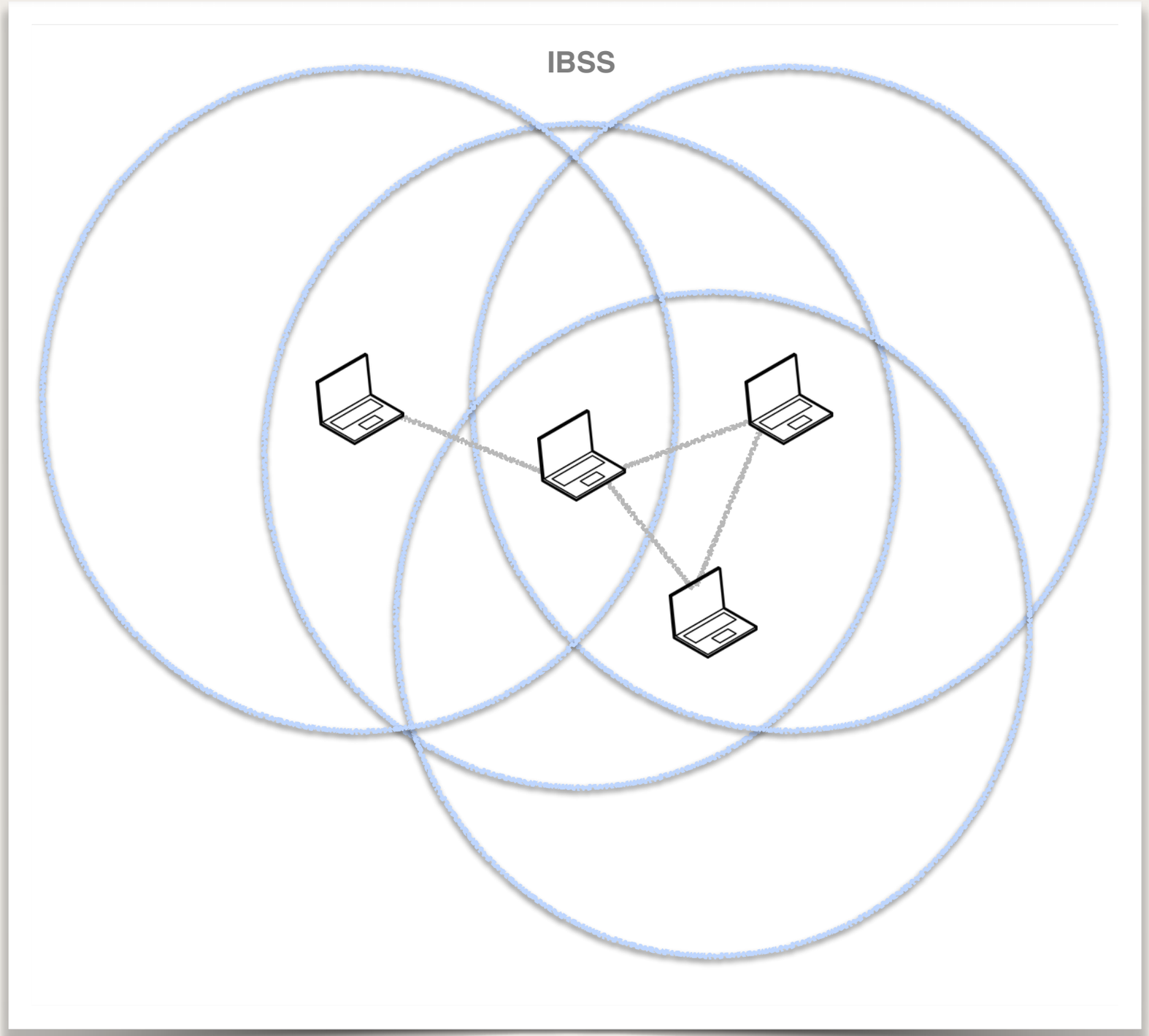


Mode infrastructure

- L'association d'une station et d'un point d'accès
  - Une station qui entre dans une cellule diffuse une **trame de sondage** (*probe request*) indiquant l'ESSID, *Extended Service Set Identifier,* qu'elle préfère et son débit préféré
    - un point d'accès (AP) examine la trame de sondage et si l'ESSID correspond, elle retourne une réponse en indiquant sa charge et des informations de synchronisation. Cette réponse permet à la station de constater la qualité du signal et ainsi de choisir le meilleur AP
    - si l'ESSID ne répond pas, la station écoute le réseau et recherche les SSID présents
  - Le point d'accès AP diffuse périodiquement une **trame balise** (*beacon*) indiquant :
    - le BSSID, *Basic Service Set Identifier*, qui est l'adresse MAC du AP
    - les caractéristiques du BSS
    - par défaut, le nom du réseau étendu (ESSID, *Extended Service Set Identifier*) est aussi diffusé mais cette option peut être désactivée pour renforcer (faiblement) la sécurité

Mode ad hoc

- Topologie **ad-hoc** : *mesh topology*
- IBSS : *Independent Basic Service Set*

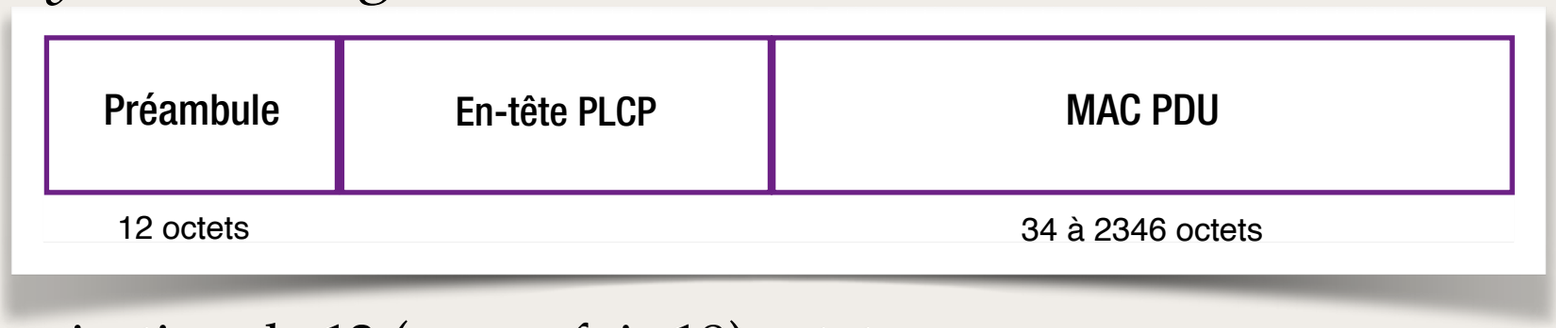


Mode ad hoc

- Les stations se connectent les unes aux autres
  - Elles constituent un réseau point à point (*peer to peer*) ;
  - Chaque machine est en même temps client et point d'accès ;
  - L'ensemble forme un IBSS, I*ndependent Basic Service Set*, identifié par un même SSID ;
  - Pas de système de distribution pour le mode ad hoc ;
  - La configuration de la sécurité au sein de l'IBSS est laissée aux utilisateurs ; ce mode d'opération est **contraire aux politiques de sécurité** d'un grand nombre d'entreprises.

La couche MAC

- La trame PLCP, *Physical Layer Convergence Protocol*



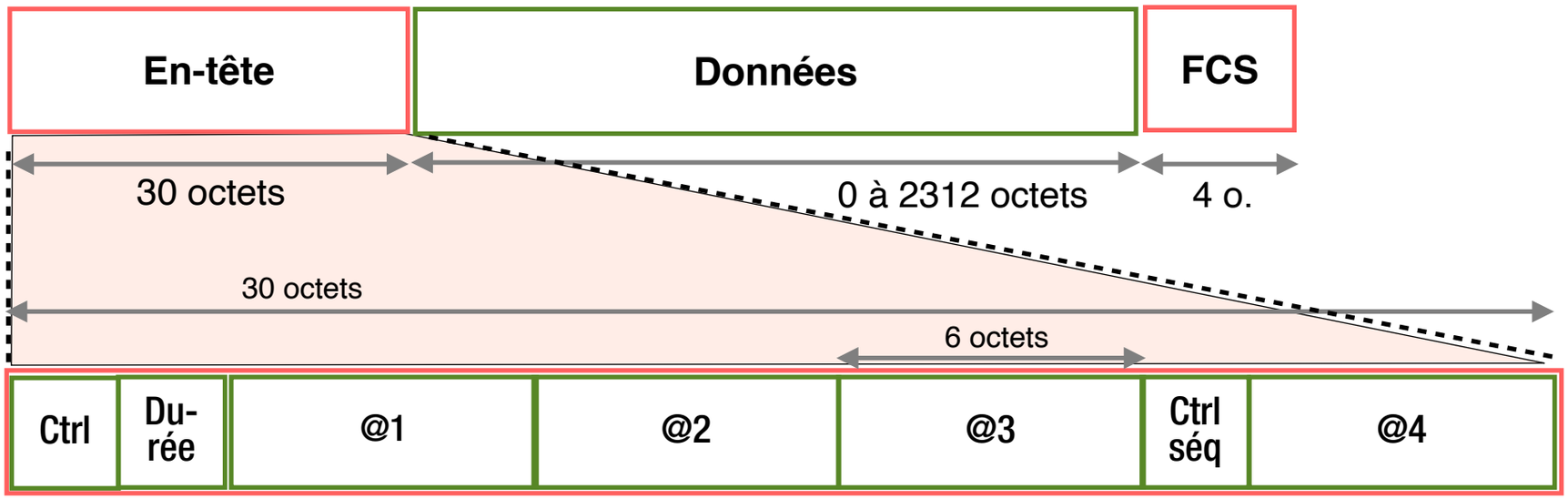
  - Elle contient :
    - Un préambule de synchronisation de 12 (ou parfois 18) octets :
      - Synch, une séquence de 80 bits alternant 0 et 1
      - SFD, *Start Frame Delimiter,* avec une suite de 16 bits : 0000 1100 1011 1101
    - Un en-tête PLCP de 6 octets (d'infos liées au décodage de la trame)
      - La longueur en octets du PLCP_PDU, pour permettre à la couche physique de détecter la fin de la trame PLCP
      - Un fanion de signalisation PLCP
      - Un CRC sur 16 bits
    - MAC PDU : La trame MAC est encapsulée dans la trame PLCP
      - En-tête MAC
      - Données
      - FCS

La couche MAC

- Types de trames MAC
  - Trame de données
  - Trame de contrôle
    - RTS, CTS, ACK
  - Trame de gestion
    - trame d'association

La couche MAC

- Les trames MAC de données



Mode ad-hoc	@ destination	@ source	BSSID	0
Infrastructure AP -> Sta.	@ destination	@ AP	@ source	0
Infrastructure Sta. -> AP	@ AP	@ source	@ destination	0
Infrastructure AP -> AP WDS	@ AP suiv.	@ AP	@ destination	@ source

- Dans le champ Ctrl, un flag ‘To Ds’ indique si la trame est destinée à un point d’accès et un flag ‘From Ds’ indique si la trame provient d’un point d’accès

La couche MAC

- Les trames MAC de données (suite)
  - **Ctrl** ; 2 octets ; contrôle de trame ; il contient différents sous-champs :
    - Version de protocole 802.11 ; 2 bits ; valeur 0 actuellement
    - Type de trame ; 2 bits ; trame de gestion (00), de contrôle (01) ou de données (10)
    - Sous-type ; 4 bits ; pour l'association ou la ré-association, l'authentification, RTS, CTS, ACK, etc.
    - ToDS, *To Distribution System* ; 1 bit, à 1 si la trame **est destinée** au point d'accès
    - FromDS, *From Distribution System* ; 1 bit, à 1 si la trame **provient** du point d'accès
    - More Fragments ; 1 bit, à 1 si d'autres fragments suivent le fragment en cours
    - Retry ; 1 bit, à 1 si le fragment est une retransmission d'un fragment précédemment transmis
    - Power Management ; 1 bit, à 1 si la station sera en mode de gestion d'énergie après la transmission de cette trame.
    - More Data ; 1 bit ; le point d'accès a d'autres données pour la station
    - WEP ; 1 bit ; les données sont chiffrées avec WEP
    - Order ; 1 bit ; classe de service strictement ordonné (*Strictly-Ordered service class*)

La couche MAC

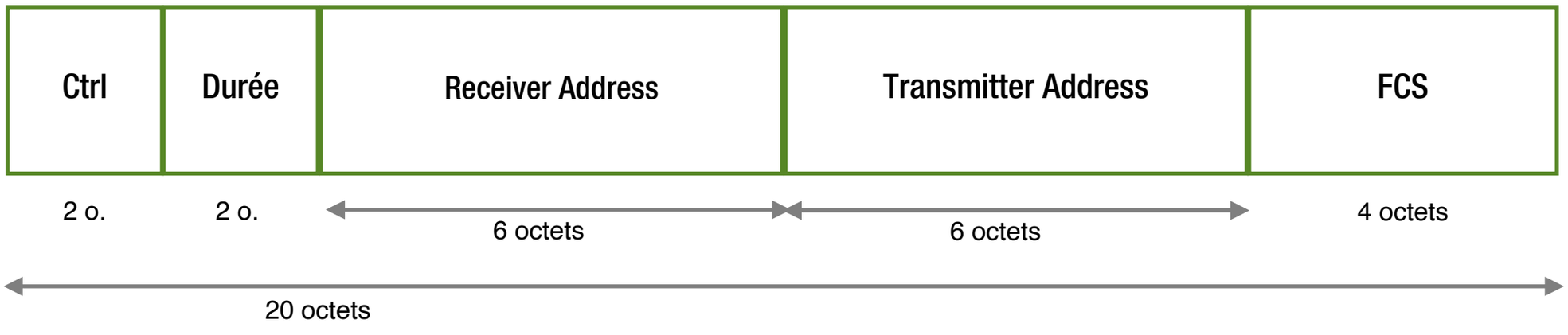
- Les trames MAC de données (suite)
  - **Durée** ; 2 octets ; ce champ à deux sens, dépendant du type de trame
    - Pour les trames de polling en mode d'économie d'énergie, c'est l'ID de la station
    - Dans les autres trames, c'est la valeur de durée utilisée pour le calcul du NAV
  - **Les champs adresses** (en-tête MAC) ; jusqu'à 4 champs de 6 octets
    - Une trame peut contenir jusqu'à 4 adresses, selon les bits ToDS et FromDS définis dans le champ de contrôle :
      - Adresse 1 : l'adresse du récepteur. Si ToDS est à 1, c'est l'adresse du Point d'Accès, sinon, c'est l'adresse de la station.
      - Adresse 2 : l'adresse de l'émetteur. Si FromDS est à 1, c'est l'adresse du Point d'Accès, sinon, c'est l'adresse de la station émettrice.
      - Adresse 3 est l'adresse de l'émetteur original quand le champ FromDS est à 1. Sinon, et si ToDS est à 1, Adresse 3 est l'adresse destination.
      - Adresse 4 est utilisé dans un cas spécial, quand une trame est transmise d'un Point d'Accès à un autre. Dans ce cas, ToDS et FromDS sont tous les deux à 1 et il faut donc renseigner à la fois l'émetteur original et le destinataire final.

La couche MAC

- Les trames MAC de données (suite)
  - **Contrôle de séquence** ; 2 octets
    - Numéro de trame et numéro de fragment
  - **Données** ; 0 à 2312 octets
  - **CRC** : *Cyclic Redundancy Check* ou FCS : *Frame Check Sequence* ; 4 octets
    - CRC sur 32 bits

La couche MAC

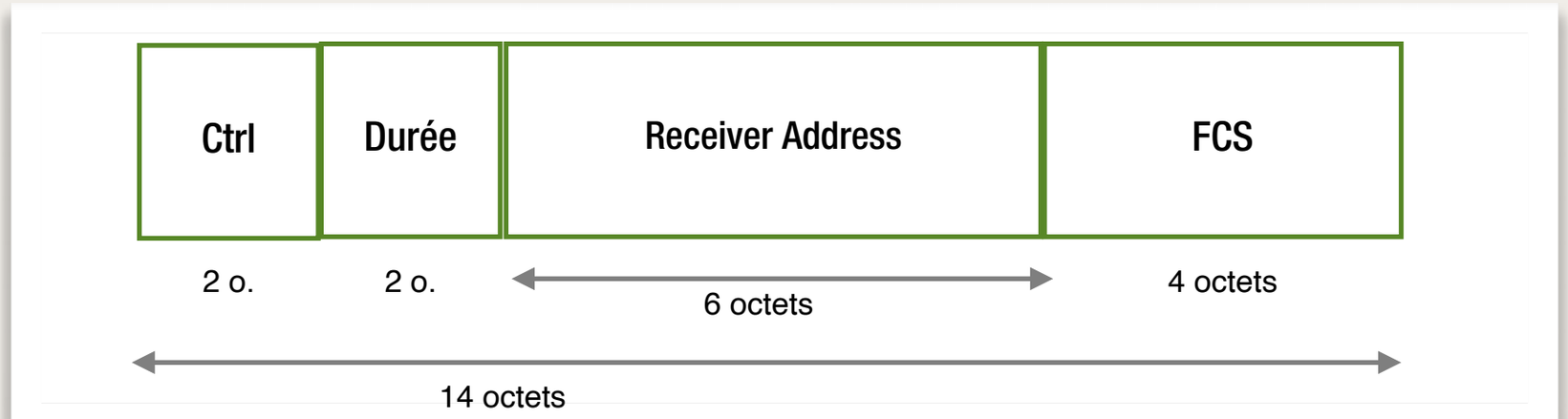
- Les autres trames MAC
  - **La trame RTS** contient cinq champs :



- Ctrl : Frame Control
- Durée : temps de transmission en μs de la prochaine trame + CTS + ACK + intervalles SIFS
- RA, *Receiver Address*, l'adresse MAC de la station qui recevra la trame de données
- TA, *Transmitter Address*, l'adresse MAC de la station qui doit émettre la trame de données
- FCS, *Frame Check Sequence*

La couche MAC

- Les autres trames MAC
  - **Les trames CTS et ACK** contiennent quatre champs :



- Ctrl : Frame Control
- Durée :
  - Trame CTS : temps de transmission en μs de la prochaine trame + ACK + intervalles SIFS et DIFS
  - Trame ACK : intervalle DIFS
- RA, *Receiver Address*, l'adresse MAC de la station destinataire de la trame de données
- FCS, *Frame Check Sequence*

Sécurité

- Généralités
  - Les communications sans fil peuvent être interceptées…
    - Il est nécessaire d'assurer l'authentification, la confidentialité et l'intégrité
  - Les principaux algorithmes de sécurité sont :
    - WEP, *Wired Equivalent Privacy*, depuis 1999
    - *WPA, Wireless Protected Access*
    - *WPA2, Wireless Protected Access v.2*, lié à 802.11i
    - *WPA3, Wireless Protected Access v.3*, publié par Wi-Fi Alliance en janvier 2018
  - **IEEE 802.1X** : standard de sécurité des réseaux informatiques, utilisant le protocole EAP, *Extensible Authentication Protocol*
  - Détecter et empêcher les ***rogues AP*** alias *rogues access points* (point d'accès Wi-Fi non-autorisé)
    - Le but d'un **rogue AP** est de :
      - Contourner les vérifications de sécurité pour accéder à un réseau interne,
      - D'intercepter le trafic (dont les identifiants & mots de passe) d'utilisateurs abusés.
    - Un système de prévention d'intrusion est basé par la **surveillance du spectre radioélectrique** (avec un analyseur de spectre RF. *Exemple*)

Wi-Fi

Sécurité

- WEP : Wired Equivalent Privacy
  - Le WEP fait partie de la norme IEEE 802.11 ratifiée en septembre 1999.
  - Le WEP utilise l'algorithme de chiffrement par flot RC4 pour assurer la confidentialité et la somme de contrôle CRC-32 pour assurer l'intégrité
  - Il est possible de pénétrer un réseau protégé par du WEP en 3 minutes en utilisant des outils disponibles publiquement (par exemple grâce au logiciel *Aircrack-ng* disponible sous Linux et Windows)
  - Il faut donc **proscrire le WEP** et le remplacer par WPA2 ou WPA3

- WPA et WPA2 : Wi-Fi Protected Access
  - WPA respecte une bonne partie de la norme IEEE 802.11i et est utilisé depuis 2003
    - Il utilise en général **TKIP**, *Temporal Key Integrity Protocol*, pour le chiffrement
  - WPA2 respecte toute la norme **IEEE 802.11i**
    - Il est utilisé depuis 2004, suite à la ratification de 802.11i
    - La compatibilité est obligatoire pour les équipement certifiés Wi-Fi depuis 2006
    - Le standard 802.11i définit un réseau de sécurité robuste (RSN, *Robust Security Network*), utilisant l'authentification et les chiffrements suivants :
      - Authentification avec IEEE 802.1x pour WPA entreprise
      - Chiffrement avec TKIP encore possible
      - Chiffrement avec CCMP, *Counter-mode/CBC-Mac Protocol* (soit *Counter-mode/Cipher Block Chaining Message Authentication Code)*, qui s'appuie sur **AES**, *Advanced Encryption Standard,* beaucoup plus sûr

- WPA et WPA2 : Wi-Fi Protected Access (suite…)
  - Modes de fonctionnement (pour WPA et WPA2)
    - **WPA Personal** (WPA personnel) utilise une clé partagée, PSK, *Pre-shared Key*, qui doit être renseignée sur le point d'accès et sur les postes clients
      - Cela évite de mettre en œuvre un serveur d'authentication
      - Sur les box, ou sur certain point d'accès, une étiquette indique en générale le SSID par défaut et la clé de sécurité par défaut. Il est conseillé de **modifier les paramètres de la box** pour modifier le SSID et la clé de sécurité
    - **WPA Enterprise**, alias WPA-802.1x ou WPA-EAP, impose la mise en œuvre un serveur d'authentication, souvent de type RADIUS.
      - L'installation est plus complexe mais plus sécurisée.
      - Le serveur d'authentification 802.1x est chargé de distribuer les clés
      - L'authentification repose sur **EAP**, *Extensible Authentication Protocol* et utilise une variante comme EAP-TLS, EAP-TTLS et EAP-SIM

- WPA et WPA2 : Wi-Fi Protected Access (suite…)
  - Fin 2017, une grave vulnérabilité, nommée *Krack* pour *Key Reinstallation AttaCK,* a été divulguée…
    - Cela a rendu le standard d'authentification Wi-Fi WPA2 obsolète et a contraint la Wi-Fi Alliance à développer le standard WPA3
    - https://www.numerama.com/tech/297968-wi-fi-une-faille-serieuse-remet-en-question-la-securite-des-communications.html
  - En 2019, de plusieurs vulnérabilités, appelées *Dragonblood,* sont trouvées dans le standard WPA3…
    - https://www.zdnet.fr/actualites/dragonblood-de-nouvelles-vulnerabilites-trouvees-dans-le-standard-wifi-wpa3-39888783.htm

Sécurité

- WPA3
  - La **Wi-Fi Alliance** a annoncé le 8 janvier 2018 des améliorations et de nouvelles fonctionnalités pour *Wi-Fi Protected Access*.
  - **WPA3** est construit sur les composants de base de WPA2 et apportera des fonctionnalités supplémentaires, dans le cadre de *WPA3 Wi-Fi CERTIFIED :*
    - Simplifier la configuration de sécurité Wi-Fi pour les utilisateurs et les fournisseurs de services, tout en améliorant les protections de sécurité du réseau Wi-Fi
    - Offrir des protections robustes même si les utilisateurs choisissent des mots de passe faibles
    - Simplifier la configuration de la sécurité pour les périphériques dont l'interface d'affichage est limitée ou inexistante.
    - Rendre les réseaux Wi-Fi publics plus sécurisés
      - Chiffrement individualisé de données entre le terminal et le point d'accès
    - Possibilité de choisir une suite de sécurité 192 bits, alignée sur la suite CNSA, *Commercial National Security Algorithm,* du Comité sur les systèmes de sécurité nationale, protégera davantage les réseaux Wi-Fi avec des exigences de sécurité plus élevées propres aux gouvernements, à la défense et aux industriels.

Wi-Fi

Sécurité

- WPA3…

  - WPA3 : vers un nouveau protocole Wi-Fi pour mieux sécuriser les réseaux sans fil - Numerama

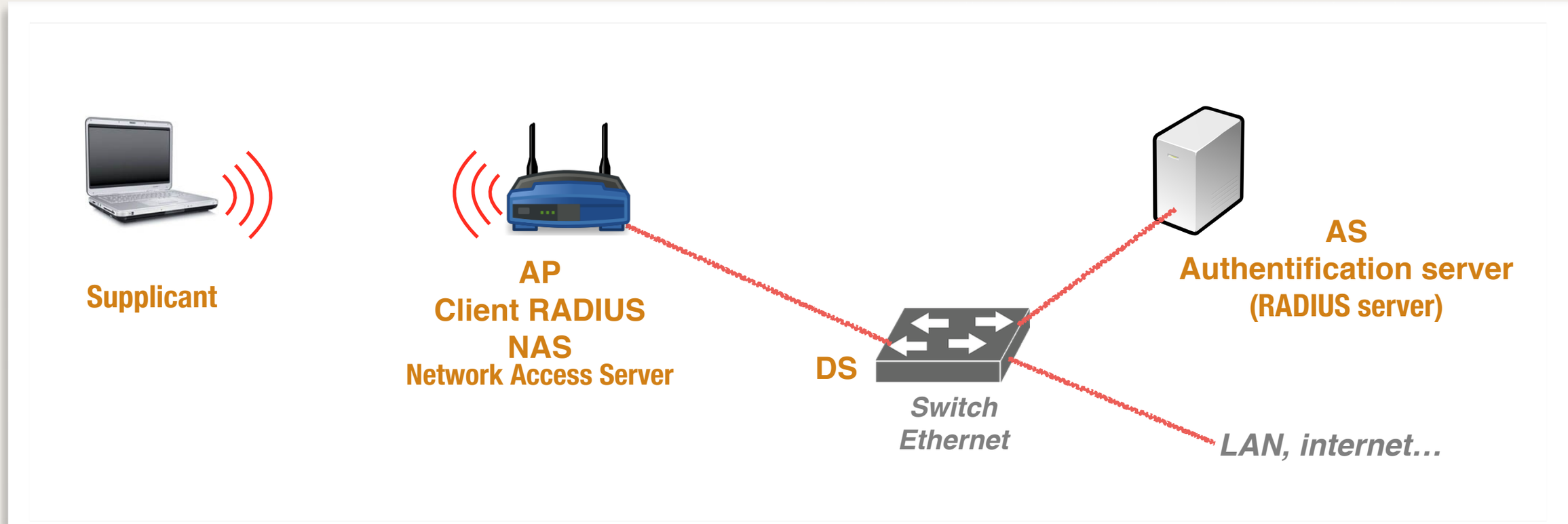
  - Wi-Fi : le protocole WPA3 en vue pour 2018 - ZDNet

  - Le WPA3 finalisé : une sécurité toute neuve pour son Wi-Fi - tomshardware.fr

  - Wi-Fi Alliance® introduces Wi-Fi CERTIFIED WPA3™ security

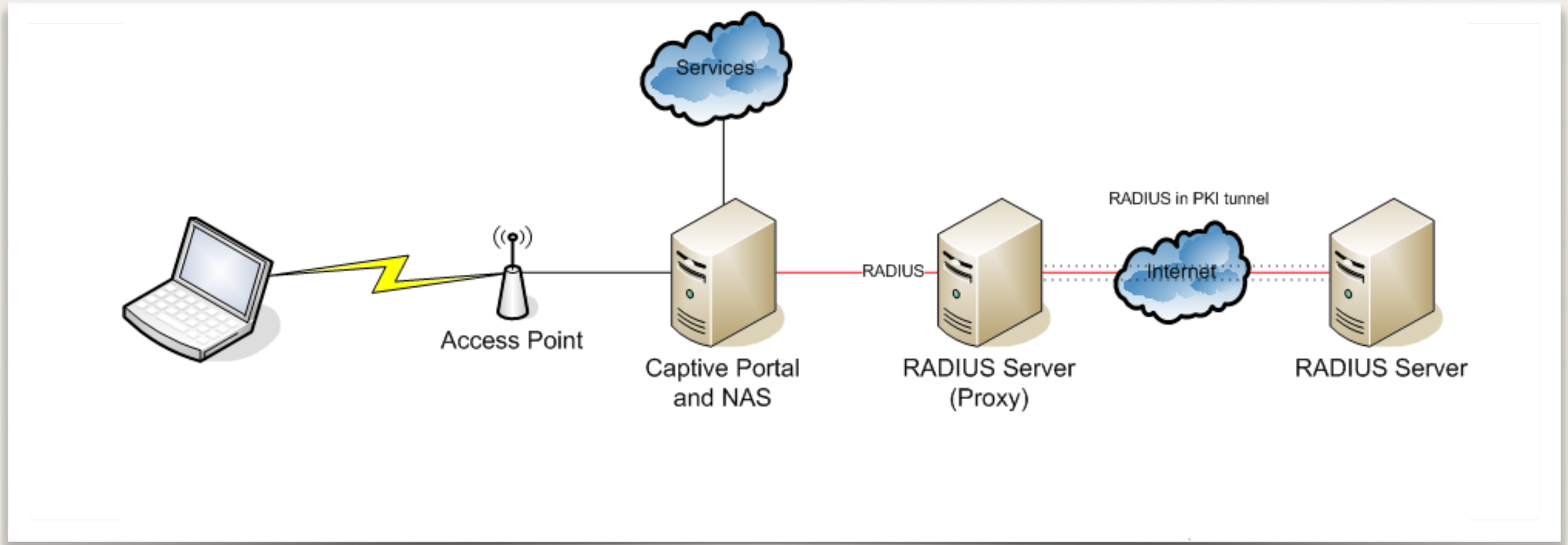
  - Sécuriser les accès Wi-Fi - ANSSI

- RADIUS, *Remote Authentication Dial-In User Service*
  - Architecture client-serveur et protocole d'authentification à distance



- Le poste utilisateur (*supplicant*) sera authentifié (ou non) suite à des échanges avec un **client RADIUS**, alias NAS, *Network Access Server*, qui communique avec un **serveur RADIUS**.
- RADIUS utilise le protocole de transport **UDP**, sur le port 1812
- Normalisation en 1997 et 2000 (RFC 2058, 2059, 2865 et 2866)
- Initialement RADIUS était utilisé par les FAI pour authentifier leurs utilisateurs

- RADIUS, *Remote Authentication Dial-In User Service*
  - Architecture client-serveur et protocole d'authentification à distance



- Le poste utilisateur (*supplicant*) sera authentifié (ou non) suite à des échanges avec un **client RADIUS**, alias NAS, *Network Access Server*, qui communique avec un **serveur RADIUS**.
- Dans cette figure, un proxy RADIUS est un intermédiaire

- RADIUS, *Remote Authentication Dial-In User Service* (suite…)
  - **Protocole AAA**, *Authentication Authorization Accounting*
    - **Authentification**
      - Le poste utilisateur (*supplicant*) transmet une requête d'accès à un client RADIUS (NAS, *Network Access Server*)
      - Le client RADIUS demande un identifiant de connexion et un mot de passe au poste utilisateur
      - PAP, *Password Authentication Protocol* , CHAP, *Challenge Handshake Authentication Protocol ou* EAP, *Extensible Authentication Protocol* peuvent être utilisés
      - Ces informations d'authentification sont transmissent au serveur RADIUS via une requête *Access-Request*
        - le serveur RADIUS interroge une base de données (LDAP, SQL ou autres)
        - le serveur répond par *Access-Accept* ou *Access-Reject*.
      - Il existe également une requête *Access-Challenge,* envoyée par le serveur pour demander des infos complémentaires ou la re-émission d'un *Access-Request*

- RADIUS, *Remote Authentication Dial-In User Service* (suite…)
  - **Protocole AAA**, *Authentication Authorization Accounting* (suite…)
    - **Autorisation** (*Authorization*)
      - L'identification RADIUS peut s'accompagner de paramètres d'autorisation
    - **Comptabilisation** (*accounting*)
      - Le serveur RADIUS assure la journalisation des accès (et comptabilise des éléments de facturation s'il y a lieu)

- TACACS et TACACS+, *Terminal Access Controller Access-Control System (Plus)* sont d'autres protocoles AAA, de Cisco

- RADIUS, *Remote Authentication Dial-In User Service* (suite…)
  - Les extensions de RADIUS
    - **EAP**, *Extensible Authentication Protocol*, est un protocole de transport de protocole d'authentification.
      - Permet des identifications plus complexes et plus robustes
      - Utilisé pour les réseaux sans fil
      - EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-MS-CHAP-V2, EAP-AKA, EAP-LEAP, EAP-FAST (Cisco), EAP-SIM, etc.
        - Par ex., EAP-SIM est dédiés aux opérateurs de téléphonie mobile, disposant de base de données clients et de cartes SIM
    - 802.1X
  - Évolution
    - **Diameter**, qui utilise TCP comme couche transport, est utilisé en téléphonie 3G et LTE/4G
- Voir aussi :
  - ANSSI, Agence nationale de la sécurité des systèmes d'information https://www.ssi.gouv.fr

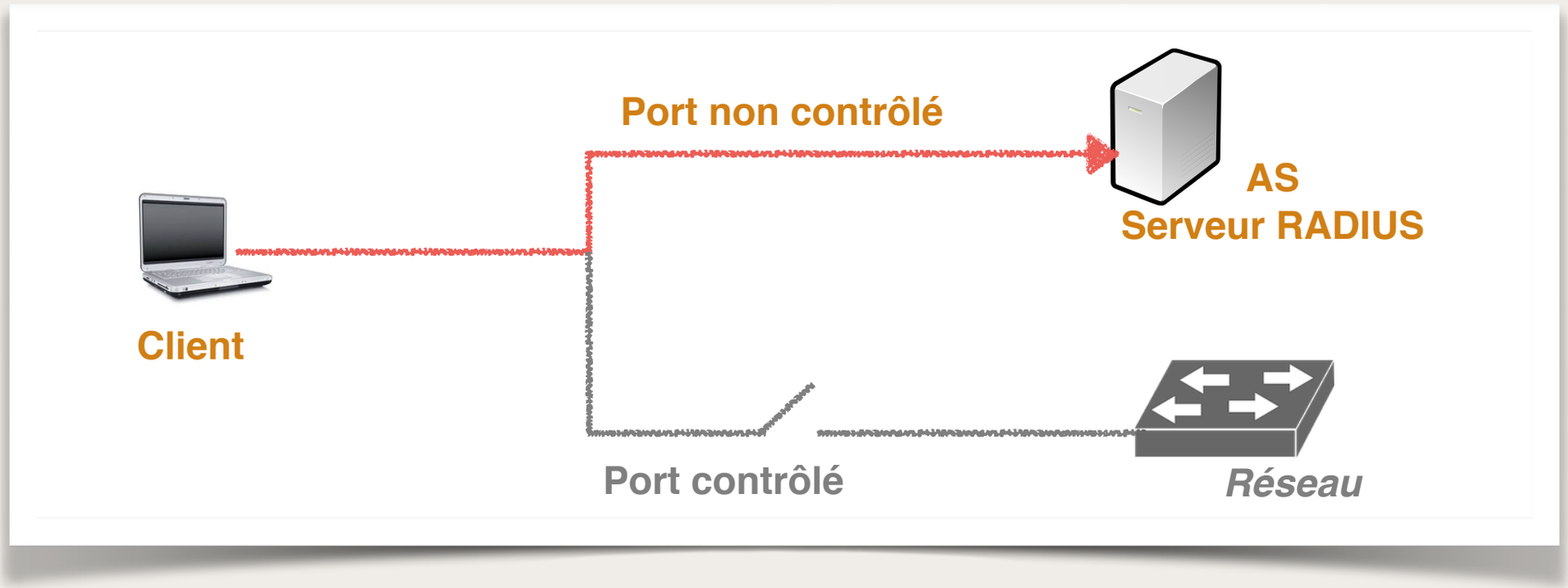
Sécurité

- RADIUS, *Remote Authentication Dial-In User Service* (suite…)
  - Il existe plusieurs solutions logicielles libres ; la plus utilisée et la plus aboutie est
    - **FreeRadius** (www.freeradius.org),
  - Voir aussi :
    - GNU-Radius (www.gnu.org/software/radius),
    - Yard-Radius (http://sourceforge.net/projects/yardradius),

Wi-Fi

Sécurité

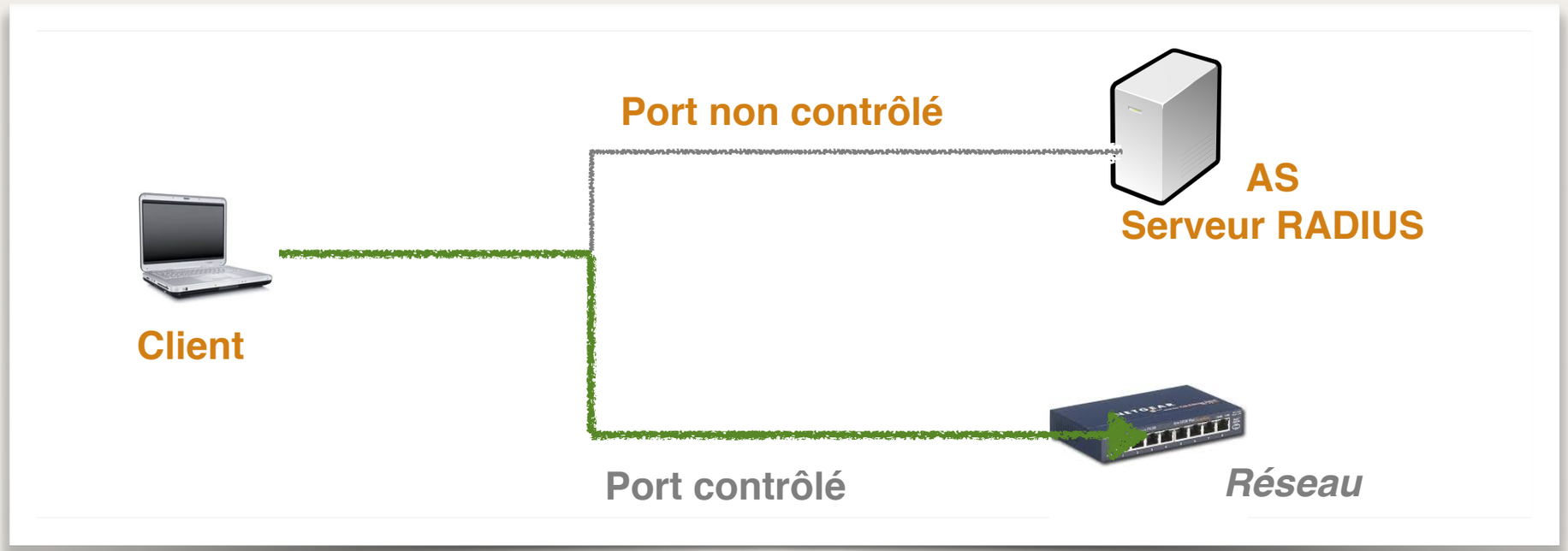
- Le protocole IEEE 802.1X
  - Voir : Déploiement du protocole 802.1x
  - Basé sur le **contrôle des ports**, 802.1X permet d'authentifier un client (de réseau filaire ou sans fil) avant d'autoriser (ou non) l'accès au réseau.
  - Le protocole EAP est utilisé ; le serveur d'authentification est généralement un serveur RADIUS
  - Chaque port de connexion sera contrôlé avec 802.1X
    - Au début de la connexion, le port est dans l'état **non contrôlé** et seuls les trames 802.1X sont autorisées.
  - Après une authentification réussie, le port passe à l'état **contrôlé** et le client peut accéder aux ressources partagées



Wi-Fi

Sécurité

- Le protocole IEEE 802.1X
  - Voir : Déploiement du protocole 802.1x
  - Basé sur le **contrôle des ports**, 802.1X permet d'authentifier un client (de réseau filaire ou sans fil) avant d'autoriser (ou non) l'accès au réseau.
  - Le protocole EAP est utilisé ; le serveur d'authentification est généralement un serveur RADIUS
  - Chaque port de connexion sera contrôlé avec 802.1X
    - Au début de la connexion, le port est dans l'état **non contrôlé** et seuls les trames 802.1X sont autorisées.
  - Après une authentification réussie, le port passe à l'état **contrôlé** et le client peut accéder aux ressources partagées



- Wi-Fi Protected Setup

  - Conçu par la Wi-Fi Alliance, WPS a été lancé début 2007
  - Le but du protocole WPS, *Wi-Fi Protected Setup*, est de simplifier la phase de configuration de la sécurité des réseaux sans fil. Il permet à des particuliers ayant peu de connaissances sur la sécurité de configurer un accès WPA, supporté par les appareils Wi-Fi.
  - L'utilisateur voulant ajouter un périphérique au réseau peut utiliser au choix :
    - La méthode PIN, *Personal Identification Number*, un numéro à lire sur une étiquette (ou un écran) du nouvel appareil, et à reporter sur le « représentant » du réseau (le point d'accès ou le registrar).
    - La méthode PBC, *Push Button Configuration*, où l'utilisateur presse un bouton (physique ou virtuel), à la fois sur le point d'accès et sur le nouvel appareil.
    - La méthode NFC, *Near Field Communication*, où l'utilisateur approche le nouvel appareil du point d'accès pour établir une communication en champ proche entre eux.

Wi-Fi

IEEE 802.11n et 802.11ac

- La norme IEEE 802.11n, alias Wi-Fi 4, ratifiée en septembre 2009
  - 2 bandes de fréquences différentes : 2,4 GHz et 5 GHz
  - Portée
    - en intérieur : env. 50 m (70 m pour 2,4 GHz et 35 m pour 5 GHz)
    - en extérieur : env. 250 m
  - Six fois plus rapide que IEEE 802.11g
  - Débit théorique de 300 Mbit/s
  - Débit pratique : 50 à 100 Mbit/s
  - MIMO, *Multiple Input, Multiple Outputs*
    - Émission et réception multiple de signaux radios depuis plusieurs antennes
  - Regroupement des canaux radio
  - Des paquets de données mieux organisés avant envoi
  - Largeur de bande 20 ou 40 MHz
  - Modulation : OFDM, *Orthogonal frequency-division multiplexing*

Wi-Fi

IEEE 802.11n et 802.11ac

- La norme IEEE 802.11ac, ratifiée en décembre 2013
  - Nouvelle appellation Wi-Fi 5
  - Bande de fréquences des 5 GHz (de 5 150 à 5 850 MHz)
  - Portée en intérieur : env. 35 m
  - Débit théorique de 1,3 Gbit/s, avec 3 antennes pour émetteur **et** récepteur
  - Débit pratique : jusqu'à 900 Mbit/s en utilisant 4 canaux simultanés
  - MIMO, *Multiple Input, Multiple Outputs*
    - Émission et réception multiple de signaux radios depuis plusieurs antennes
  - Évolution en 2015 avec **802.11ac wave 2** avec MU-MIMO, MIMO multi-utilisateurs. Le point d'accès peut traiter les signaux MIMO de plusieurs clients en simultané
  - Regroupement de canaux radio
  - Largeur de bande 20, **40, 80** ou 160 MHz
  - Modulation : OFDM, *Orthogonal frequency-division multiplexing*

Wi-Fi

IEEE 802.11ad

- La norme IEEE 802.11ad, alias WiGig
  - Bande de fréquences des 60 GHz
  - Portée très limitée : env. 10 m
  - Débit théorique < 7 Gbit/s (jusqu'à 4,6 Gbit/s sur une seule porteuse)
  - Largeur de bande 2160 MHz
  - Modulation : OFDM, *Orthogonal frequency-division multiplexing* ou simple porteuse
  - Pas de rétrocompatiblité directe
  - Peu d'équipements compatibles

Wi-Fi

À suivre…

- Wi-Fi Aware
  - La Wi-Fi Alliance a présenté en 2015 une nouvelle norme Wi-Fi : le Wi-Fi Aware.
    À l'instar d'iBeacon d'Apple, le Wi-Fi Aware est un système de positionnement en intérieur qui permet de repérer les terminaux compatibles afin de communiquer directement avec eux sans passer par un réseau mobile.
- IEEE 802.11be
  - Appelé Wi-Fi 7
  - Norme publiée vers mars 2024, le 802.11be supplantera le Wi-Fi ax ; Wi-Fi 7 promet des vitesses de transfert 2,4 à 5 fois plus rapides que Wi-Fi 6. Il devrait ainsi supporter des bandes passantes théoriques de 30 Gb/s par points d'accès
  - Il combine diverses améliorations désignées sous l'acronyme EHT, *Extremely High Throughput*.
  - Il introduit un fonctionnement multiliaison : **MLO**, *Multi-Link Operation*.
  - Modulation et multiplexage : OFDMA, *Orthogonal Frequency-Division Multiple Access*.
  - Rétrocompatibilité prévue avec les normes 802.11a/b/g/n/ac/ax.

Wi-Fi

À suivre…

- IEEE 802.11ah ou Wi-Fi HaLow
  - Le comité de standardisation IEEE 802 investit le champ d'applications relatif à **l'internet des objets** avec le 802.11ah
  - Wi-Fi HaLow, annoncé début 2016 et normalement finalisé fin 2016, sera en concurrence avec les protocoles Zigbee et Z-Wave, ainsi qu'avec Bluetooth LE.
  - Le Wi-Fi ah a pour avantage de fonctionner dans la bande des 900 MHz plus favorable à la propagation des ondes que la porteuse à 2,4 GHz (Wi-Fi n) ou à plus forte raison 5 GHz (Wi-Fi n et ac). Une plus grande portée que les Wi-Fi ac et n (de 50% plus élevée que le Wi-Fi n à 2,4 GHz par exemple) qui pourrait lui permettre de décharger les réseaux cellulaires.
- Wi-Fi Direct
  - Le Wi-Fi Direct, (ex Wi-Fi P2P), est une technologie qui permet de connecter deux appareils en Wi-Fi, sans passer par un point d'accès. Il est ensuite possible d'échanger des fichiers à une vitesse bien supérieure qu'avec le Bluetooth

Bluetooth

Généralités

- Technologie d'échange de données directionnelles sur des courtes distances, avec des ondes radio UHF (~ 2,4 GHz)
  - Un réseau Bluetooth fonctionne en relation maître / esclave :
    un terminal Bluetooth, maître, distribue le droit de parole (*polling* des esclaves)
- Adapté aux réseaux domestiques (WPAN, *Wireless Personal Area Network*)
  - Connectique sans fil
- Dent bleue ?
  - L'appellation **Bluetooth** est inspiré d'un roi danois, Harald Ier (910-986) surnommé Harald à la dent bleue, soit *Harald Blåtand* en danois et *Harald Bluetooth* en anglais.
  - Harald Ier a unifié le Danemark et la Norvège, comme Bluetooth unifie les appareil entre eux.
  - Le logo est une combinaison des initiales H et B en alphabet runique : 

Bluetooth

Généralités

- Historique
  - 1994 : création par Ericsson, en Suède
  - 1998 : Bluetooth Special Interest Group (Bluetooth SIG) regroupe neuf sociétés (Ericsson, IBM, Intel, Nokia, Toshiba, puis 3Com, Lucent Technologies, Microsoft et Motorola).
  - 1999 : spécification Bluetooth 1.0
  - 2004 : spécification Bluetooth 2.0
  - 2005 : normalisation IEEE 802.15.1: WPAN / Bluetooth v1.1
  - 2013 : spécification Bluetooth 4.1, adapté à l'IoT, *Internet of Things*
    - Transferts plus rapides, plus sécurisés, plus économes en énergie
  - 2014 : spécification Bluetooth 4.2
    - Transferts plus rapides, plus sécurisés, plus économes en énergie par rapport à Bluetooth 4.1
  - Fin 2016 : spécification Bluetooth 5
    - Transferts plus rapides (4 Mbit/s), meilleures portées (jusqu'à 200 m) par rapport à Bluetooth 4.2 et sans consommer plus d'énergie
    - Concerne aussi bien la domotique, l'audio que l'Internet des Objets (IoT). Premiers produits compatibles en 2017.

Bluetooth

Généralités

- Objectif de Bluetooth
  - Permettre de **transmettre des données ou de la voix** entre des équipements possédant un **circuit radio de faible coût**, sur un rayon de l'ordre d'une dizaine de mètres à un peu moins d'une centaine de mètres et avec une **faible consommation électrique**.

- Deux types de Bluetooth :
  - Bluetooth BR/EDR, *basic rate/enhanced data rate* ou *Classic Bluetooth*
    - Spécifications Bluetooth version 2.0 & 2.1
    - Portée réduite, connexion continue, appliqué par ex. au streaming audio
    - Vitesse de transfert des données : 2 Mbit/s
    - Consommation d'énergie élevée ; utilisation en voiture, etc.
    - Le protocole est limité à 7 esclaves maximum

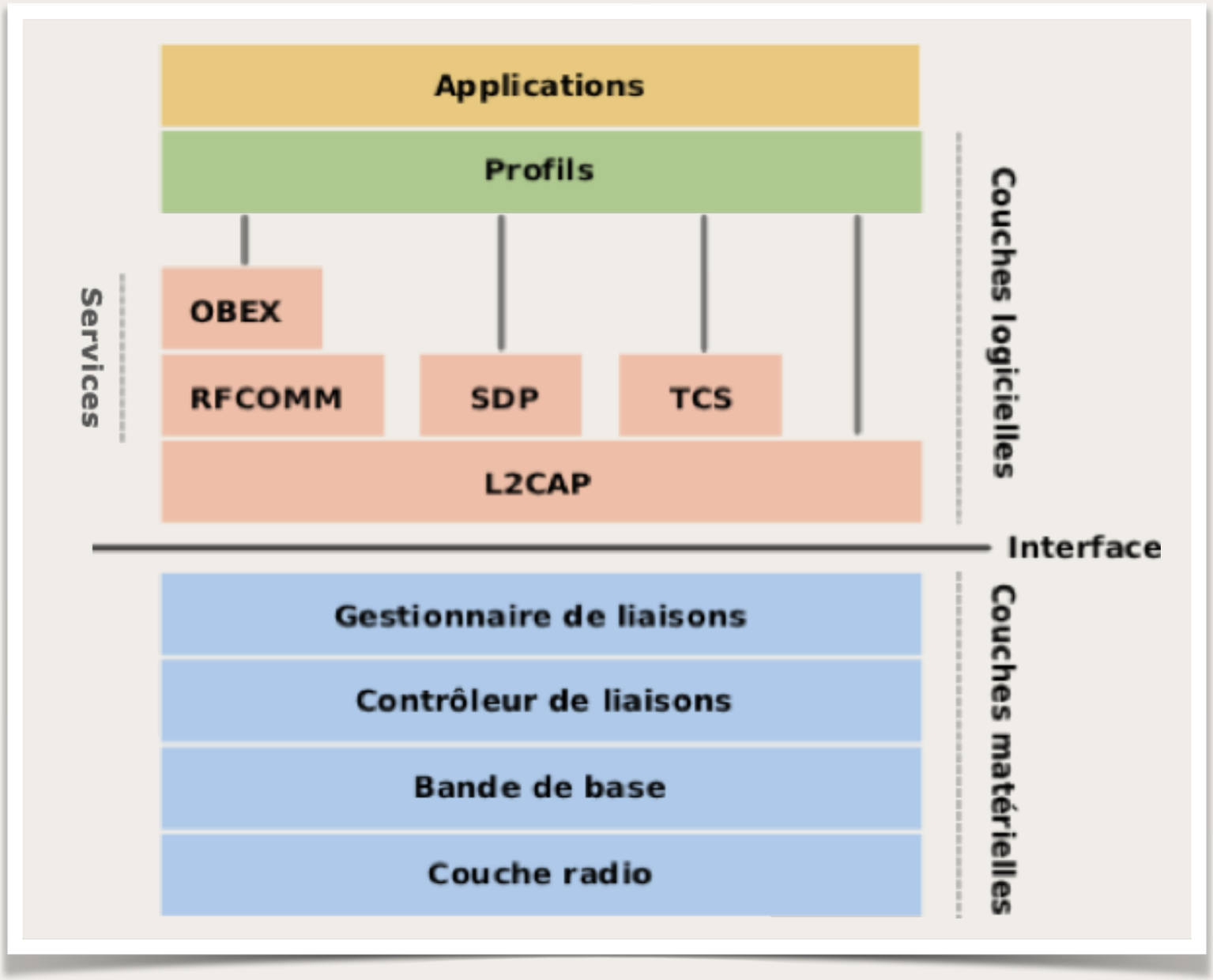
Bluetooth

Généralités

- Deux types de Bluetooth (suite…)
  - Bluetooth LE (*Bluetooth with Low Energy*)
    - Ex. **Wibree**, déposé sous le nom **BlueTooth Smart**
    - Spécifications Bluetooth version 4.0 à 4.2
    - Permet de courtes rafales de connexion radio, de longue portée, il est adapté par ex. aux applications d'internet des objets (**IoT**, *Internet of Things*)
    - Très faible consommation d'énergie
    - Vitesse de transfert des données : < 100 Kbit/s.
    - Prise en charge d'un grand nombre d'esclaves.
    - Délai de connexion réduit, aucun processus d'appairage. Bluetooth LE a seulement besoin de se connecter au périphérique pour lire ou écrire des informations.
    - Technologie basée sur le profil GATT, *Generic Attribute Profile*
  - Les **puces *Dual-Mode*** intégrées aux tablettes et smartphones, supportent les deux modes

Bluetooth

Généralités

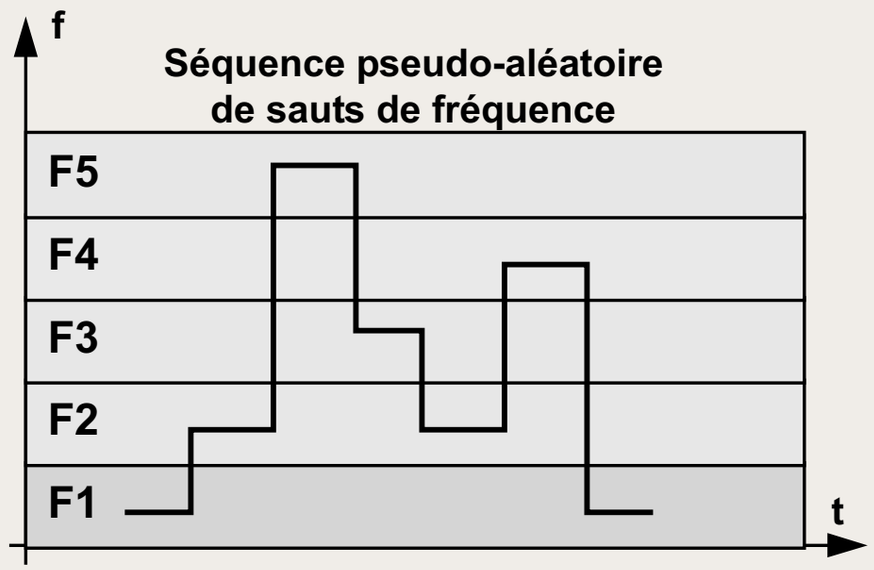


Couches Bluetooth CC BY-SA 3.0 - THA-Zp

Bluetooth

Couche physique

- Fréquences
  - La couche radio utilise la bande de fréquence sans licence ISM, *Industrial Scientific and Medical* à 2,4 GHz.
  - Cette bande de 2 400 à 2 483,5 MHz est découpée en 79 canaux séparés de 1 MHz, numérotés de 0 à 78.
  - Bluetooth utilise la technique **FHSS**, *Frequency Hopping Spread Spectrum*, (étalement de spectre par saut de fréquence).
  - La transmission utilise une commutation rapide entre plusieurs canaux de fréquence, utilisant un ordre pseudo aléatoire connu tant de l'émetteur que du récepteur.
  - Ainsi, les équipements radio participant à une transmission utilisant FHSS doivent utiliser la même séquence de saut de fréquence pour pouvoir communiquer.
  - Dans cette technique, tout le spectre de fréquence disponible est occupé par l'ensemble des canaux. Cependant, périodiquement, selon une séquence pseudo aléatoire connue des couples émetteur-récepteur, la fréquence (canal) utilisée change.



Bluetooth

Couche physique

- Fréquences
  - Le codage de l'information se fait par **sauts de fréquences** et la période est de 625 μs, ce qui permet 1 600 sauts par seconde.
  - Il n'y a jamais de longue transmission sur une même fréquence, mais une série de transmissions de courts paquets sur une suite pseudo-aléatoire de fréquences.
  - En changeant de canal jusqu'à 1600 fois par seconde, le standard Bluetooth permet d'éviter les interférences avec les signaux d'autres modules radio.

Bluetooth

Couche physique

- Modulations
  - Deux modulations sont définies :
    - Une modulation obligatoire utilise une modulation de fréquence binaire pour minimiser la complexité de l'émetteur ;
    - Une modulation optionnelle utilise une modulation de phase (PSK à 4 et 8 symboles).
    - La rapidité de modulation est de 1 Mbaud pour toutes les modulations. La transmission duplex utilise une division temporelle.

- Trois classes d'émetteur radio Bluetooth

Classe	Puissance	Portée
1	100 mW (20 dBm)	100 mètres
2	2,5 mW (4 dBm)	10 à 20 mètres
3	1 mW (0 dBm)	Quelques mètres

Bluetooth

Couche physique

- La bande de base (*baseband*)
  - On y définit les adresses matérielles des périphériques (équivalentes à l'adresse MAC d'une carte réseau). Ces adresses sont gérées par la IEEE Registration Authority.
    - Adresse nommées BD_ADDR, *Bluetooth Device Address*
    - Codage sur 48 bits.
  - La bande de base gère les différents types de communication entre les appareils
    - Les liaisons de base, utilisés pour la **gestion** des connexions au sein du réseau bluetooth
  - Les connexions établies entre 2 appareils Bluetooth peuvent être synchrones ou asynchrones,
  - Ces connexions sont appelées « Liens Logiques » (*Logical Link*), avec 2 types majeurs :
    - les liens SCO, *Synchronous Connection-Oriented*, adaptés par ex. au streaming ou à la transmission de voix
    - les liens ACL, *Asynchronous Connection-Less*, adaptés aux échanges de données
  - Les données transportées sur ces liens logiques sont sous forme de paquets.

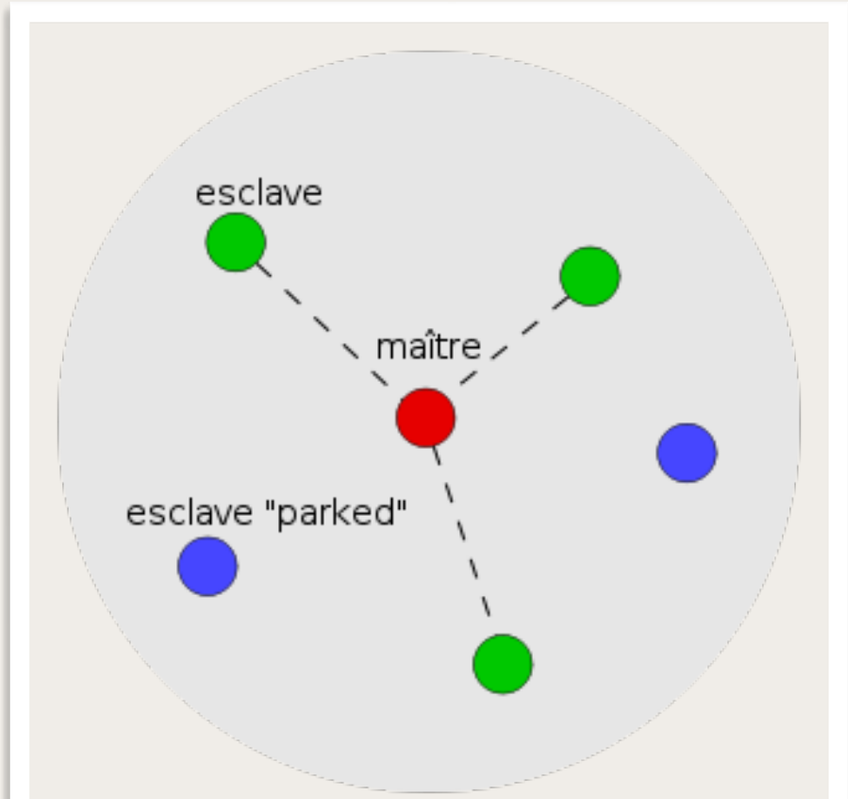
Couche physique

- La bande de base (*baseband*), suite…
  - Format des paquets :
    - Le code d'accès → 72 ou 68 bits ; synchronisation des composants Bluetooth
    - L'entête (*header*) → 54 bits ; N° de paquet, adresses source et destination, type de paquet, CRC…
    - La charge utile (*Payload*) → de 0 à 2 745 bits.

Bluetooth

Couche physique

- Organisation d'un réseau Bluetooth
  - Les réseaux Bluetooth fonctionnent dans une relation maître/esclave.
  - Le maître distribue le droit de parole (*polling* des esclaves) et synchronise le dialogue à l'aide d'un multiplexage temporel.
  - Le temps est découpé en slots de 625 μs
  - On distingue deux topologies : *piconet* et *scatternet*
- Piconet
  - Pico-réseau ou ***piconet*** est un réseau créé automatiquement lorsque plusieurs équipements Bluetooth sont dans le même rayon
  - Un *piconet* est un réseau en étoile autour d'un maître qui peut administrer jusqu'à 7 esclaves actifs et jusqu'à 255 esclaves en mode *parked*.

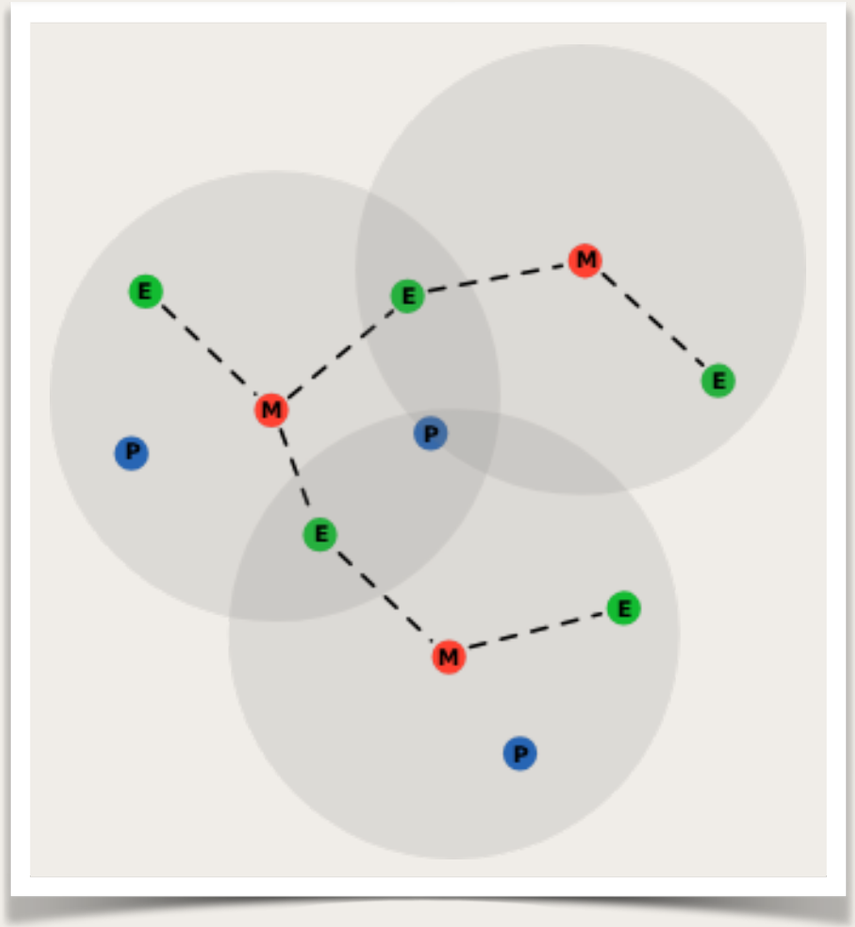


Piconet

Bluetooth

Couche physique

- Scatternet
  - Inter-réseau Bluetooth ou s*catternet* (réseau dispersé)
  - Un esclave peut avoir plusieurs maîtres et différents *piconets* peuvent donc être reliés entre eux
    - Le maître d'un piconet peut devenir l'esclave du maître d'un autre piconet
    - Un esclave peut être l'esclave de plusieurs maîtres
    - Un esclave peut se détacher provisoirement d'un maître pour se raccrocher à un autre piconet, puis revenir vers le 1er maître, une fois sa communication terminée avec le second
  - Ces différents *piconets* forment alors un *scatternet*



Scatternet
CC BY-SA 3.0 - THA-Zp

Bluetooth

Couche Liaison

- La couche gestionnaire de liaison, *Link Manager Layer*
  - Cette couche supervise des différentes connexions, gère l'authentification des appareils et le chiffrement. Elle gère également les mises en veille des différents appareils.
  - Ce gestionnaire de liaisons implémente les mécanismes de sécurité comme :
    - l'authentification
    - le pairage
    - la création et la modification des clés
    - le chiffrement.
- La couche L2CAP, *Logical Link Control & Adaptation Protocol*
  - Couche d'**adaptation des protocoles** supérieurs au réseau Bluetooth.
    - Elle comporte un mécanisme permettant d'identifier le protocole de chaque paquet envoyé pour permettre à l'appareil distant de passer le paquet au bon protocole, une fois celui-ci récupéré.
    - Cette couche supporte la segmentation et le réassemblage, ainsi que le multiplexage de protocole

Bluetooth

Services et profils

- Les services
  - RFCOMM, *Radio frequency communication*, émule les liaisons séries RS-232
  - SDP, *Service Discovery Protocol*, pour rechercher d'autres appareils et identifier les services disponibles
  - TCS, *Telephony Control protocol Specification*, interface téléphonique
  - OBEX, *OBject EXchange*, permet de transférer des objets grâce au protocole d'échange développé pour l'IrDA.

- Les profils
  - Ils correspondent à différents modèles fonctionnels d'usage particulier ou lié à un type de périphérique
  - Ils utilisent des services ci-dessus ou ceux de L2CAP directement
  - Ils définissent :
    - la manière d'implémenter un usage défini
    - les protocoles spécifiques à utiliser
    - les contraintes et les intervalles de valeurs de ces protocoles

Services et profils

- Les profils (suite…)
  - Tous les profils héritent d'un profil d'accès générique, GAP, *Generic Access Profile*, qui définit les procédures génériques de recherche d'appareils, de connexion et de sécurité
  - Bluetooth 4.x utilise également GATT, *Generic Attribute Profile*,
    - GATT organise le transfert de données utilisant des concepts nommés S*ervices* et *Characteristics*
    - Il utilise un protocole de données générique appelé le ATT, *Attribute Protocol*

Services et profils

- Les profils (suite…)
  - Exemples de profils :
    - Advanced Audio Distribution Profile (A2DP) : profil de distribution audio avancée
    - Basic Printing Profile (BPP) : profil d'impression basique
    - Dial-up Networking Profile (DUNP) : profil d'accès réseau à distance
    - File Transfer Profile (FTP) : profil de transfert de fichiers
    - Generic Object Exchange Profile (GOEP) : profil d'échange d'objets
    - Hands-Free Profile (HFP) : profil mains libres
    - Human Interface Device Profile (HID) : profil d'interface homme-machine
    - Headset Profile (HSP) : profil d'oreillette
    - LAN Access Profile (LAP) : profil d'accès au réseau
    - Personal Area Networking Profile (PAN) : profil de réseau personnel
    - SIM Access Profile (SAP) : profil d'accès à une carte SIM

Bluetooth

Le présent et le futur

- Le Bluetooth SIG annonce Bluetooth 5.0 en décembre 2016
  - Des vitesses plus élevées,
  - Une portée améliorée (x 4)
  - Ainsi que un meilleur maillage du réseau (*Bluetooth mesh*) pour les réseaux domotiques
  - Des applications pour la maison connectée, l'industrie et l'infrastructure des villes
- Décembre 2019 : Bluetooth 5.2 est publié
  - LE audio : avec un nouveau profil audio qui inclut un codec LC3, *Low Complexity Communication Codec*
  - Voir : CES 2020 : Bluetooth LE Audio, ou la future révolution sonore
- Juillet 2021 : Bluetooth 5.3 (des petits changements, sans nouvelles fonctionnalités majeures)
- Février 2023 : Bluetooth 5.4 (ajouts pour ESL, *Electronic Shelf Labels*, PAwR, *Periodic Advertising with Responses*)
- Concurrence de IEEE 802.11ah - Wi-Fi HaLow
  - *Low Energy*, grandes portées, faibles débits => IoT
  - Standard de Wi-Fi Alliance
  - Ratification en mai 2017

Bluetooth

À suivre…

- Quelques liens :
  - Bluetooth SIG
  - Bluetooth Technology Overview - Bluetooth SIG
  - Bluetooth® Core Specification Version 5.4 – Technical Overview - Bluetooth SIG
  - Auracast™ broadcast audio - Bluetooth SIG
  - The Bluetooth® Low Energy Primer - Bluetooth SIG

- Bluetooth : définition et fonctionnement - JDN journaldunet.fr
- BlueBorne : 8 failles dans le protocole Bluetooth, des milliards d'appareils touchés - CNET

Internet des objets

— Hors programme RSX116 —

Généralités

Internet des objets

— Hors programme RSX116 —

Généralités

- IoT, *Internet of Things*
  - Infrastructure mondiale qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication.

  - Échange d'informations et de données provenants de **dispositifs** identifiés vers le réseau internet ou un réseau local ou domestique.
    - Objets équipés de capteurs (*sensors*)
    - Réseau dédié ou non
    - Services, actionneurs (*actuators*)

- En général les objets connectés produisent de **grandes quantités de données** dont le stockage et le traitement entrent dans le cadre de ce que l'on appelle les **big data**
  - L'informatique en périphérie de réseau, *edge computing* : méthode d'optimisation employée dans le cloud computing. Cela consiste à traiter les données à la périphérie du réseau, près de la source des données.

Internet des objets

— Hors programme RSX116 —

Généralités

- Domaines concernés par l'IoT
  - *Weareable devices*
    - Montres
    - Santé, sport et bien-être (*Quantified self* ; mesure de soi)
  - *Smart home*
    - Domotique ; maison connectée
    - Objets et centrales domotiques (thermostats, éclairage, surveillance, alarme, serrure, robot, etc.)
  - *Smart city* et transport
    - Ville intelligente (panneaux interactifs, feux de signalisation, etc.)
    - Transport public intelligent (ITS, *intelligent transportation systems*)
  - Divers
    - Automobile ; voiture connectée
    - Loisirs et jouets
    - Environnement
    - Logistique

Généralités

- Lectures

  - L'Internet des objets (IoT) - 21e siècle
    [www.21siecle.quebec/table-des-matieres-2/linternet-des-objets/]

  - Rapport CES 2020 d'Olivier Ezratty. Voir pages 183 à 261 pour les objets connectés. Voir [https://www.oezratty.net/wordpress/2020/rapport-ces-2020/].

    - CES, *Consumer Electronics Show,* est un important salon organisé tous les ans à Las Vegas, par Consumer Technology Association.

- Systèmes technologiques nécessaires au fonctionnement de l'IoT

Systèmes technologiques liés à l'Internet des objets

Type de systèmes	Identification	Capteurs	Connexion	Intégration	Traitement de données	Réseaux
Enjeux	Reconnaître chaque objet de façon unique et recueillir les données stockées au niveau de l'objet.	Recueillir des informations présentes dans l'environnement pour enrichir les fonctionnalités du dispositif.	Connecter les systèmes entre eux.	Intégrer les systèmes pour que les données soient transmises d'une couche à l'autre.	Stocker et analyser les données pour lancer des actions ou pour aider à la prise de décisions.	Transférer les données dans les mondes physiques et virtuels.
Technologies anciennes	• radio-identification simple • code-barres • URI • GPS	• Luxmètre • capteur de proximité • thermomètre • hydromètre	• câbles • radio	• middleware simples	• Base de données • tableur • Progiciel de gestion intégré • Gestion de la relation client	• Internet
Technologies récentes	• radio-identification complexe • onde acoustique de surface • ADN	• Accéléromètre • gyroscope • capteurs miniaturisés • nanotechnologies	• Bluetooth • Wi-Fi • ZigBee • Z-Wave • communication en champ proche	• middleware complexes • analyse décisionnelle des systèmes complexes	• Entrepôt de données 3D (compatible avec les puces RFID) • Web sémantique	• EPC Global

Internet des objets

Types de réseaux

- Infrastructures réseau
  - **WAN** : Internet, 3G, 4G, **5G**
  - **LAN / PAN** : Wi-Fi, Bluetooth, **Zigbee, Z-Wave, Thread**
- Réseaux M2M, M*achine to Machine*
  - Réseaux dédiés à la communication entre objets connectés et les infrastructures Internet (smartphones, serveurs, data-centers, cloud, etc.) qui exploitent les données qu'ils génèrent voire les pilotent quand ils sont actifs
- EPCglobal Network
  - Réseau utilisé pour l'échange et le traitement de données basées sur EPC, *Electronic Product Code*, (identifiant unique d'objet dans une chaine de production) avec les standards ou services suivants :
    - ONS, *Object Naming Service*
    - EPCDS, *EPC Discovery Services*
    - EPCIS, *EPC Information Services*
    - *EPC Security Services*

Types de réseaux

- Exemples de réseaux M2M
  - Sigfox (à Labège près de Toulouse), opérateur télécom de l'Internet des objets
    - Norme : Sigfox ; Fréquence : 900 MHz ; Portée : 30-50 km (environnements ruraux), 3-10 km (environnements urbains) ; Vitesses de transmission : 10-1000 bit/s.
  - LoRA, une alliance supportant une technologie propriétaire issue de l'américain Semtech.
    - Les opérateurs Bouygues Télécom et Orange ont annoncé en 2015 le lancement de leur propre réseau M2M à base de technologie LoRA.
      - Norme : LoRaWAN ; Fréquence : variable ; Portée : 2-5 km (environnement urbain), 15 km (environnement suburbain) ; Vitesses de transmission : 0,3-50 Kbit/s.
- Standard ouvert **Weightless-N**
  - Weightless Alliance

Internet des objets

— Hors programme RSX116 —

Définitions

- RFID, R*adio Frequency IDentification*
  - Méthode pour récupérer les données à distance d'une radio-étiquette, *RFID tag*
  - Un lecteur est un équipement actif, émetteur de radiofréquences, qui va activer un RFID tag (passif) en lui fournissant l'énergie nécessaire

- Qu'est-ce-qu'un beacon ?
  - Un beacon est une petite balise de géolocalisation dont la précision est colossale
  - Un boîtier de quelques centimètres, que l'on peut installer là où l'on veut, émet dans un rayon de quelques dizaines de mètres via Bluetooth Low Energy
  - Une balise coûte quelques euros
  - 5 utilisations étonnantes du Beacon en entreprise

Internet des objets

— Hors programme RSX116 —

Protocoles de communication

- Z-Wave
  - Protocole radio conçu pour la domotique (éclairage, chauffage…)
  - Bande de fréquence de 868,42 MHz
  - L'alliance Z-wave a certifié env. 1500 produits, de 375 compagnies (en 2016)
- ZigBee
  - ZigBee, est un standard de communication sans-fils (comme le Wi-Fi ou le Bluetooth), basé sur IEEE 802.15.4 (LR WPAN, Low Rate Wireless PAN)
  - Les principaux avantages du standard sont :
    - Autonomie de l'émetteur, (plusieurs années à l'aide d'une batterie)
    - La possibilité de mettre en place une topologie de réseaux maillés
    - 65535 nœuds sont adressables sur le réseau
    - Le standard définie les méthodes de communication sur le réseau, mais aussi les fonctionnements des applications
    - Les produits sont certifiés par l'Alliance ZigBee

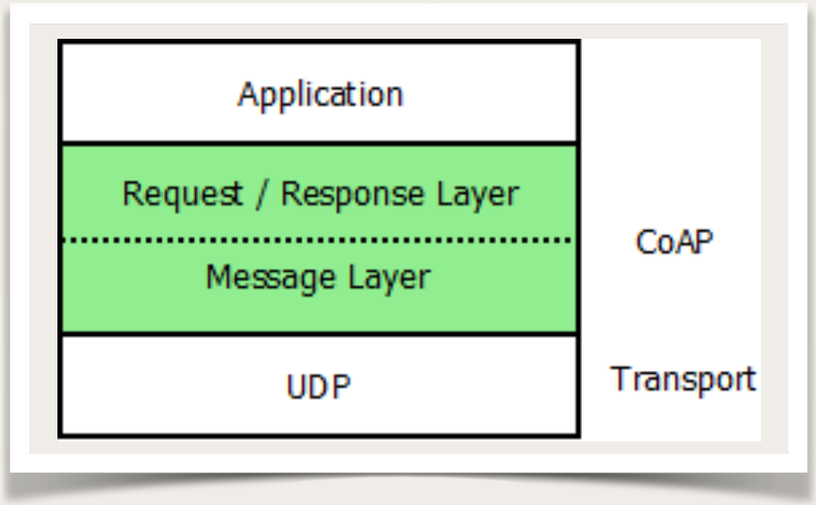
Protocoles de communication

- Thread
  - Nouveau protocole de réseau IPv6 basé sur IP, destiné à l'environnement domotique.
  - **Thread** est une technologie de réseau maillé basse consommation basée sur IPv6 et 6LoWPAN pour l'IoT, conçue pour être sécurisée et évolutive
  - Basée sur IEEE 802.15.4 et 6LowPAN, et similaire à cette dernière technologie, Thread n'est pas un protocole d'application IoT, comme le Bluetooth ou ZigBee.
  - En 2019, le projet *The Connected Home over IP* (CHIP), dirigé par Zigbee, Google, Amazon et Apple, a annoncé une large collaboration pour créer une base de code standard et open source sans redevance afin de promouvoir l'interopérabilité dans la connectivité domestique, en exploitant Thread ainsi que Wi-Fi et Bluetooth Low Energy
  - Voir :
    - Thread Group
    - openthread/openthread - github.com
      - OpenThread released by Google is an open-source implementation of the Thread networking protocol

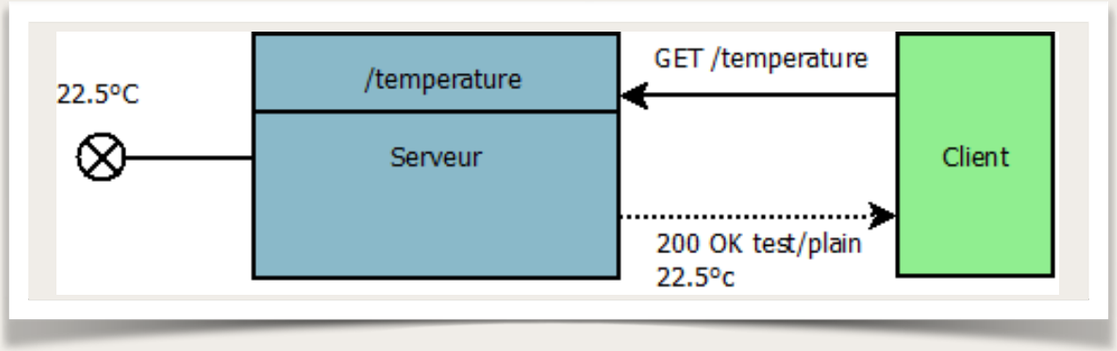
Internet des objets

Protocoles de communication

- **CoAP**, *Constrained Application Protocol*
  - Protocole (de niveau Application) de transfert Web optimisé pour les périphériques et réseaux contraints utilisés dans les réseaux de capteurs sans fil pour former l'Internet des objets.
  - RFC 7252
  - Basé sur le style architectural REST, il permet de manipuler au travers d'un modèle d'interaction client-serveur les ressources des objets communicants et capteurs identifiées par des URI via des requêtes-réponses et méthodes similaires au protocole HTTP.
  - Voir :
    - Constrained Application Protocol



Architecture CoAP CC BY-SA 4.0 - Gguinaude



Client interrogeant un capteur pour obtenir la température ambiante CC BY-SA 4.0 - Gguinaude

Internet des objets

— Hors programme RSX116 —

Équipements et données

- Équipements
  - Senseur et Capteur
  - Caméra
  - Chronomètre
  - Microphone
  - Thermostat
  - Drone et robot
- Origine des données
  - Vision : Lumière, ambiance, couleurs
  - Mouvements : Géolocalisation, position, déplacement, vitesse, accélération, rythme, pré-collision
  - Température et mesure : chaleur, gel, humidité, fumée, gaz, énergie
  - Son : messages, vibrations, commandes vocales, bruits
  - Pression : forces, tensions, fuites
- Stockage
  - Local | Cloud

Internet des objets

— Hors programme RSX116 —

Acteurs

- Écosystèmes
  - Allseen Alliance (Fondation Linux, Cisco, D-Link, Panasonic, Qualcomm, Microsoft, etc.)
    - Plateforme logicielle open-source
    - Technologie de connexion, *AllJoyn*, conçue par Qualcomm
  - Apple : interface HomeKit
  - Google :
    - API pour Nest
    - Avec Samsung et ARM, promotion de *Thread*, protocole de communication en concurrence avec Bluetooth
  - OIC, *Open Interconnect Consortium* (Cisco, Dell, IBM, Intel, Samsung, etc.)
    - Projet de normes d'interopérabilité
    - Plateforme logicielle open-source
  - IIC, *Industrial Internet Consortium* (AT&T, Cisco, General Electric, IBM, Intel, etc.)
    - Normes pour des scénarios d'usage, les architectures de connexion et les alimentations électriques des objets connectés

Divers

- Systèmes
  - **ITS**, *Intelligent transportation systems* : Systèmes de Transport Intelligents
    - V2V : *Vehicle to Vehicle* (communication entre véhicules)
    - V2I : *Vehicle to Infrastrure*
    - GPS / Galiléo
  - RFID, *Radio Frequency Identification*
  - NFC, *Near Field Communication*
    - Technologie favorisant des interactions bidirectionnelles simples et sûres entre deux dispositifs électroniques (les smartphones en particulier), pour :
      - effectuer des transactions par paiement sans contact,
      - accéder à des contenus numériques et de se connecter à des dispositifs électroniques.
      - Norme : ISO/CEI18000-3 ; Fréquence : 13,56 MHz (ISM) ; Portée : 10 cm ; Vitesses de transmission : 100–420 Kbit/s
  - Zigbee

Internet des objets

— Hors programme RSX116 —

Voir aussi…

- *Documents de* Etudes et FORmations en Télécommunication
  - Machine To Machine (M2M) Définition, Services et Adressage
  - COAP (Constrained Application Protocol) : Protocole d'Application pour l'Internet des Objets
  - Les WPANs pour M2M/IoT : L'exemple ZIGBEE
- Internet of Things Comic Book (Business Edition)
- project-chip/connectedhomeip - GitHub
  - Project Connected Home over IP is a new Working Group within the Zigbee Alliance. This Working Group plans to develop and promote the adoption of a new connectivity standard to increase compatibility among smart home products, with security as a fundamental design tenet.
- 11 protocoles à connaître pour l'Internet des objets (IoT)
- Mozilla IoT
- Arcep - Grand dossier - L'internet des objets