

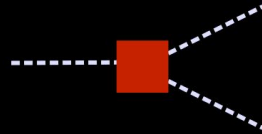
# Internet of Things

## architectures et technologies

décembre 2019 - Master “Big Data” - Telecom Paristech

# Chapitre #2

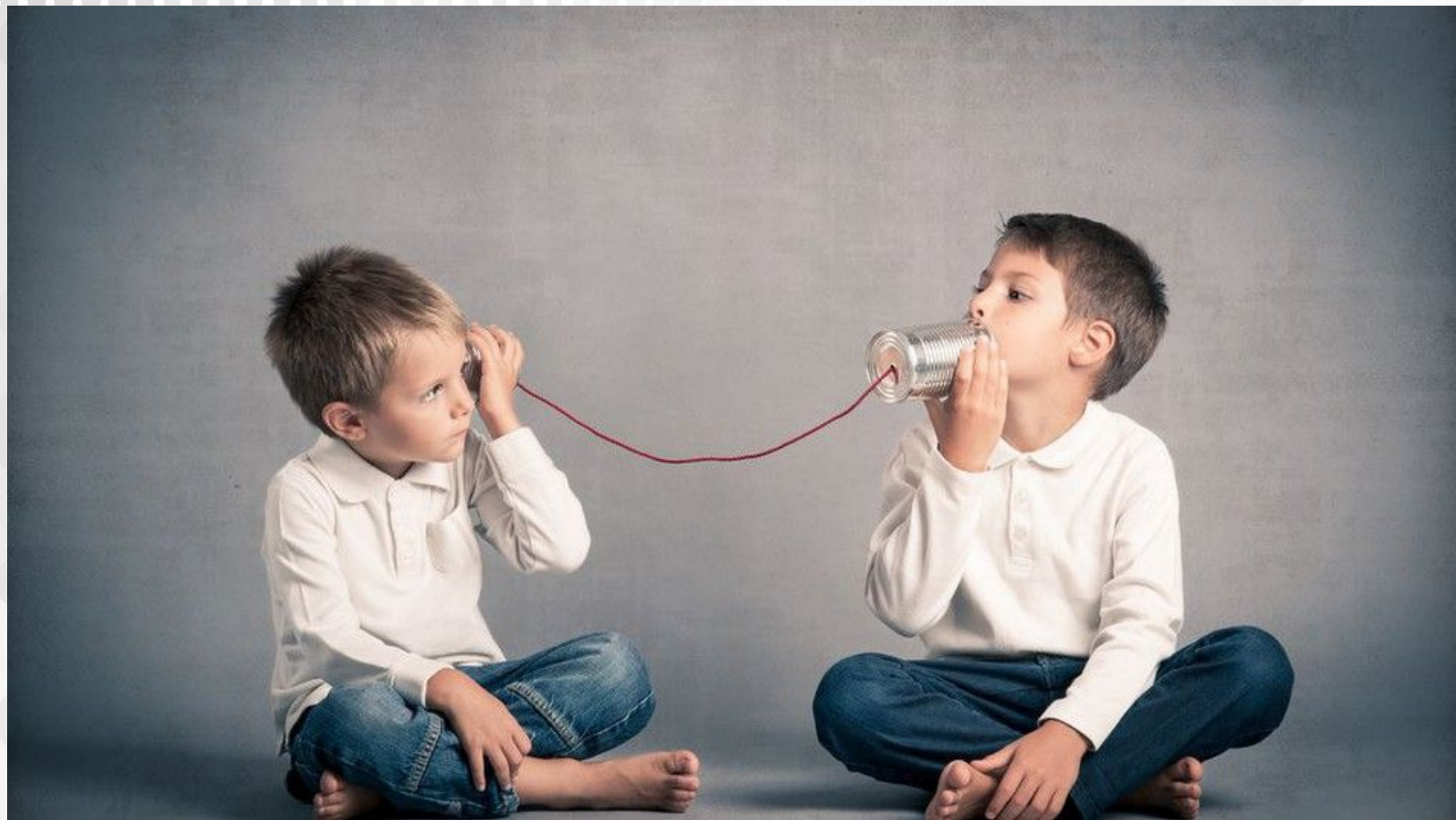
## Protocoles





?

“Communiquer”?



## Communiquer

= rendre commun, partager, transmettre

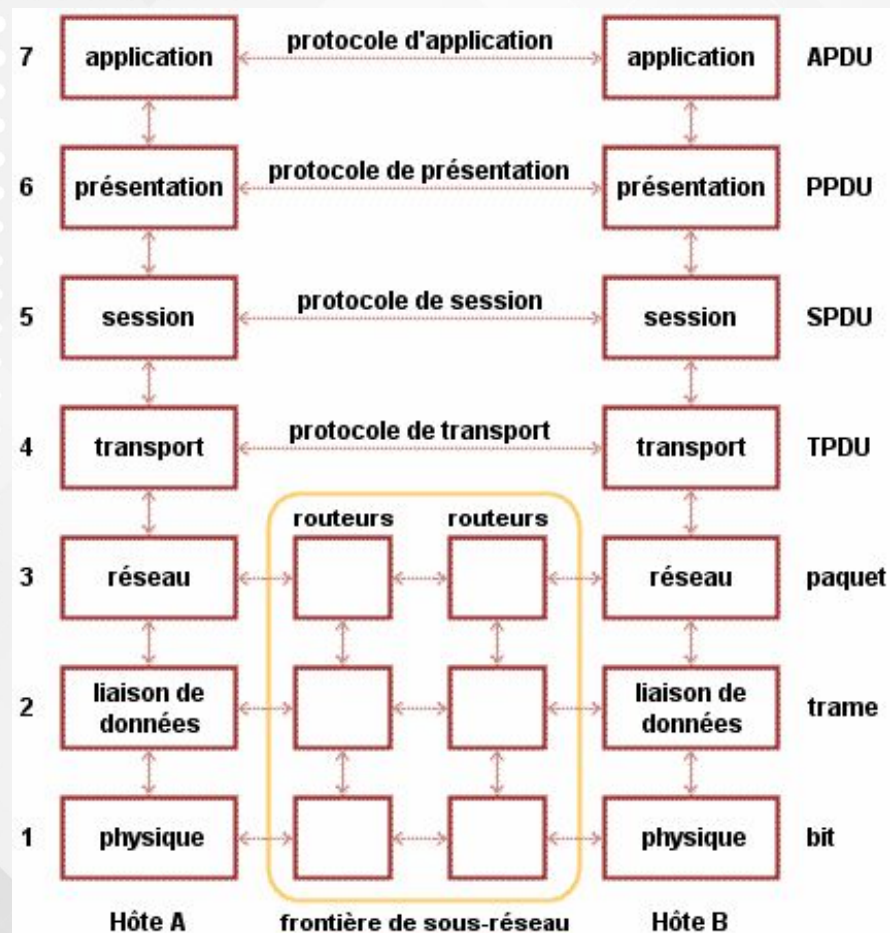
Techniquement, il s'agit d'un échange d'information, uni ou bi-directionnel, au travers d'un « **medium** » accessible aux 2+ interlocuteurs.

# Principes

modèle de référence: OSI

# Modèle OSI ('70)

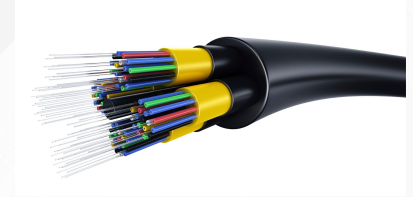
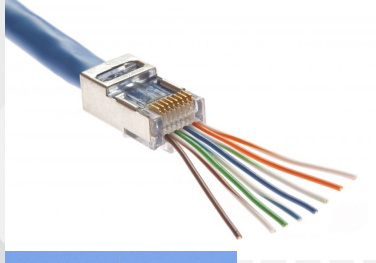
s'applique imparfaitement à la réalité, mais donne une liste exhaustive des concepts existants.



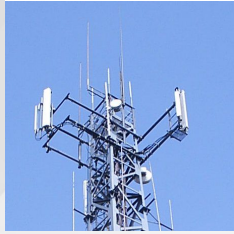


# OSI #1 - lien physique

- lien filaire



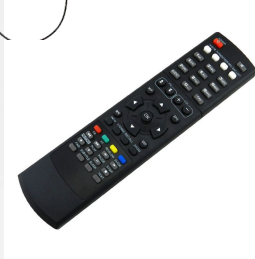
- onde radio



- lumière



- onde mécanique





# OSI #2 - liaison de données

## Fonctions:

- découpage du flux en “trames”
- correction/détection d’erreurs
- acquittement de transmission
- dédoublonnage

Exemple: Ethernet, RS-232, protocoles radio...



# OSI #3 - couche “réseau”

=> comment “router” l’information dans un réseau multi-sauts

## Fonctions:

gestion de sous-réseaux,

routages des trames/paquets

Exemple: IP



# OSI #4 - transport

## Fonctions:

garantir la délivrance,  
optimisation des ressources réseau,  
contrôle de flux

Exemple: TCP



# OSI #5 - session

## Fonctions:

- interface applicative,
- traduction adresse logique / adresse physique,
- coopération entre interlocuteurs de bout en bout

Exemples: DNS, session web (cookies), VoIP, jeu en ligne...



# OSI #6 - présentation

## Fonctions:

- syntax et sémantique de l'information échangée,
- encryption,
- compression,
- etc.

Exemples: Content-Types HTTP, HTML/CSS



# OSI #7 - application

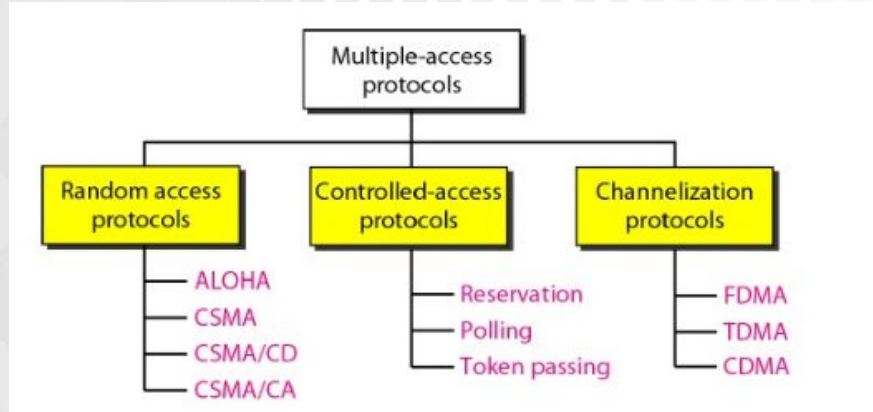
## Fonctions:

- interaction avec l'utilisateur final,
- expose le service offert

Exemples: application web (webmail, réseau social...)



# Algorithmes d'accès au medium



ALOHA: back-off exponentiel

CSMA: Carrier Sense Multiple Access

CD = collision detection

CA = collision avoidance

CR = collision resolution

FDMA = Frequency Division Multiple Access

TDMA = Time ...

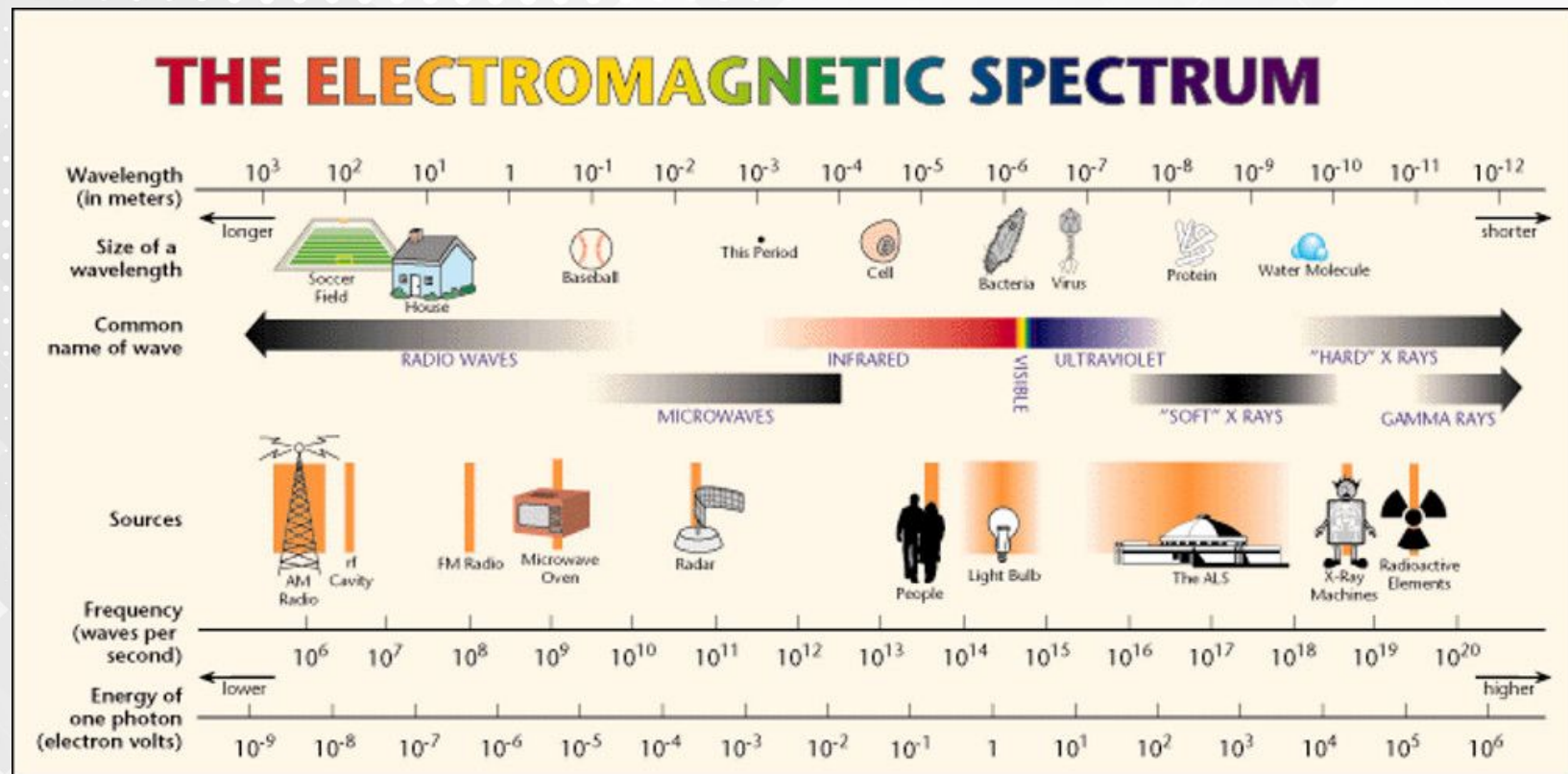
CDMA = Code ...



# Protocoles Radio



# Les bandes de fréquence

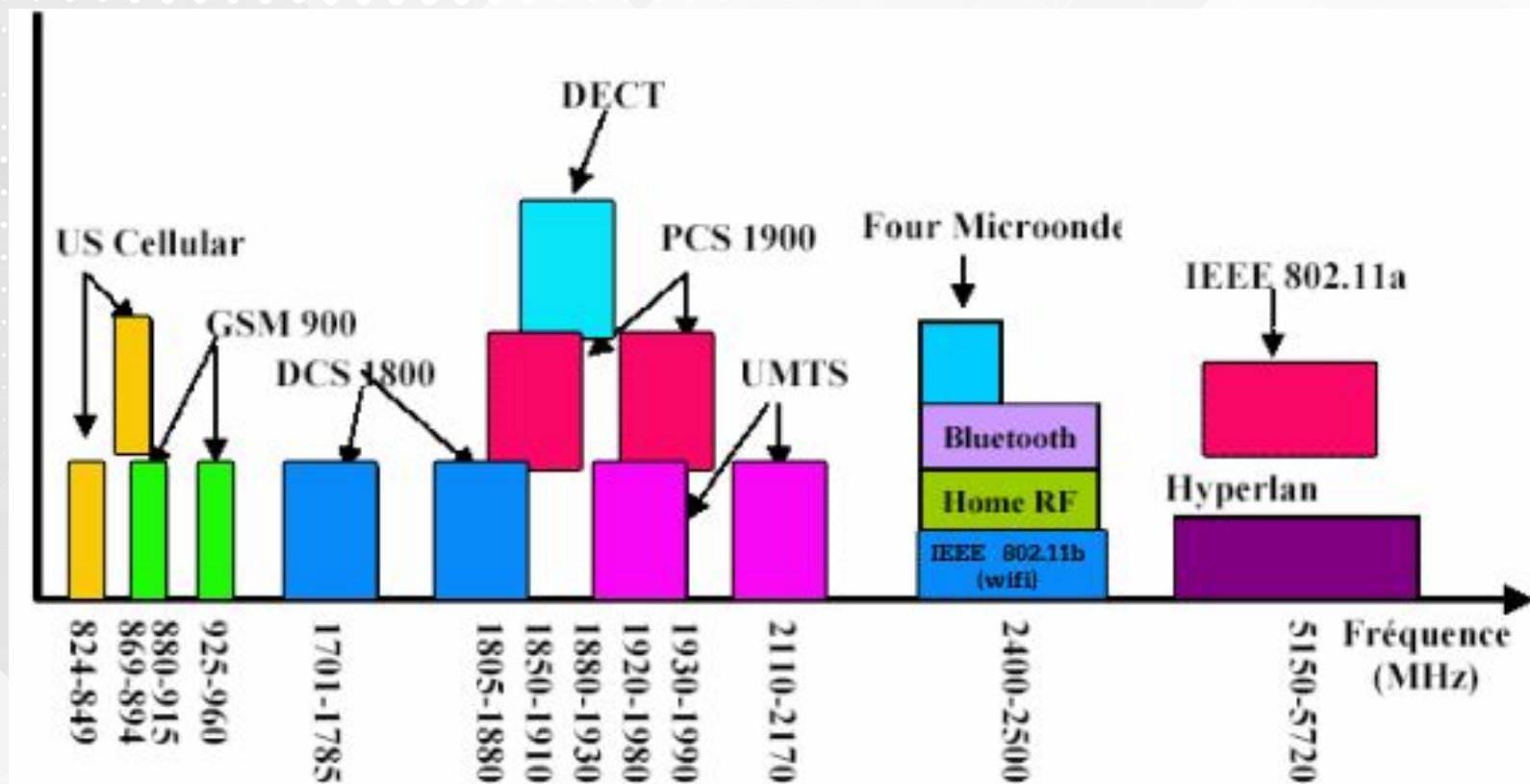




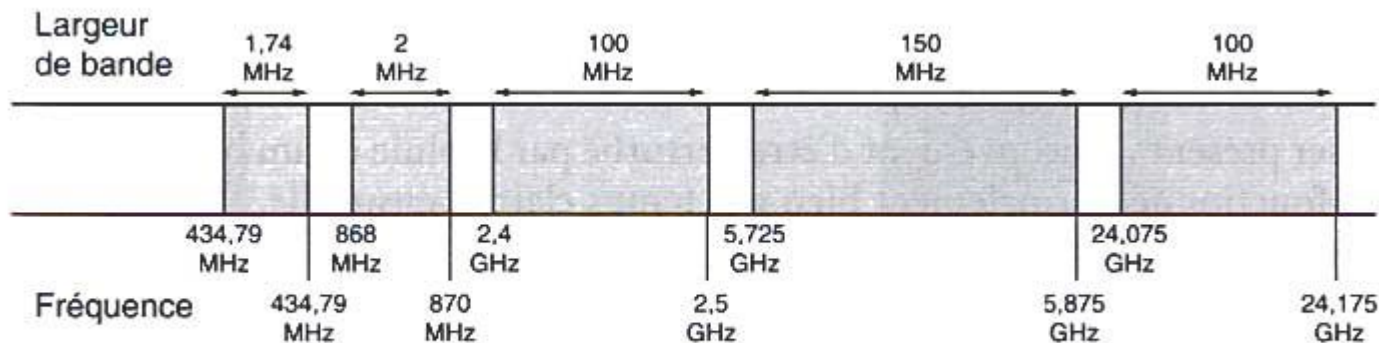
# Les bandes de fréquence



# Les bandes de fréquence



# Bandes “industrielles, scientifiques et médicales” (ISM)



**Figure 2.13** • Répartition des bandes ISM en France et en Europe.

(radio-communications => directive RED, émission <500mW)

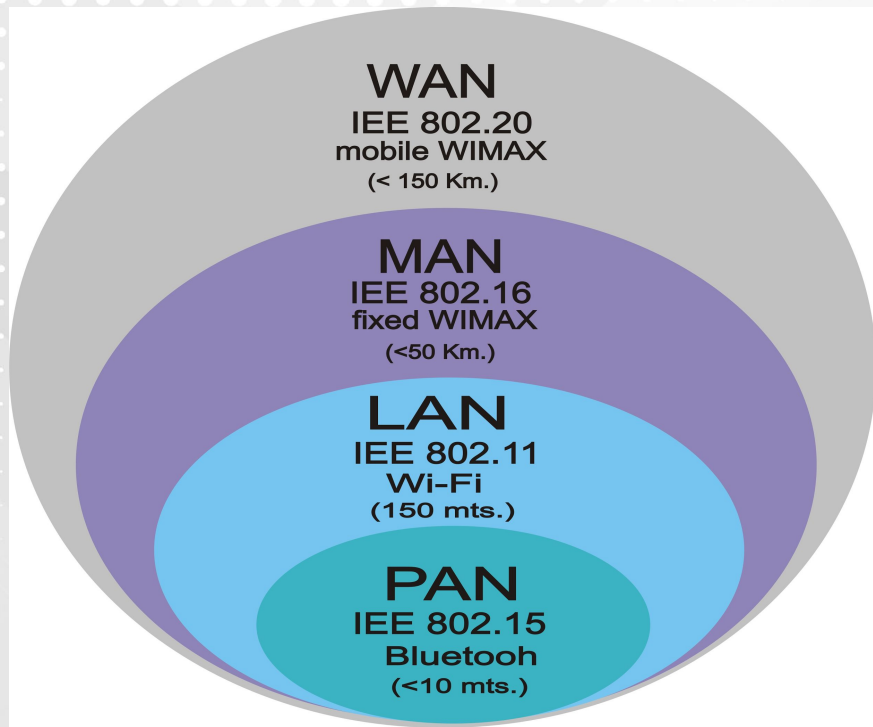
- 26 Mhz: téléphonie sans fil CTO
- 433 Mhz: domotique, télécommandes (voitures, portails), portiers vidéo, alarmes, jouets...
- 868 MHz: EnOcean, Z-Wave, Sigfox, LoRa
- 2,4 GHz: Bluetooth, Wifi, vidéo-surveillance, transmetteurs audio/video (max 10mW)
- 5,4 GHz: video “FPV” (25 mW)



**PAN / LAN / WAN**



# PAN / LAN / WAN ...



Échelle: Région / pays...

Echelle  
quartier/ville

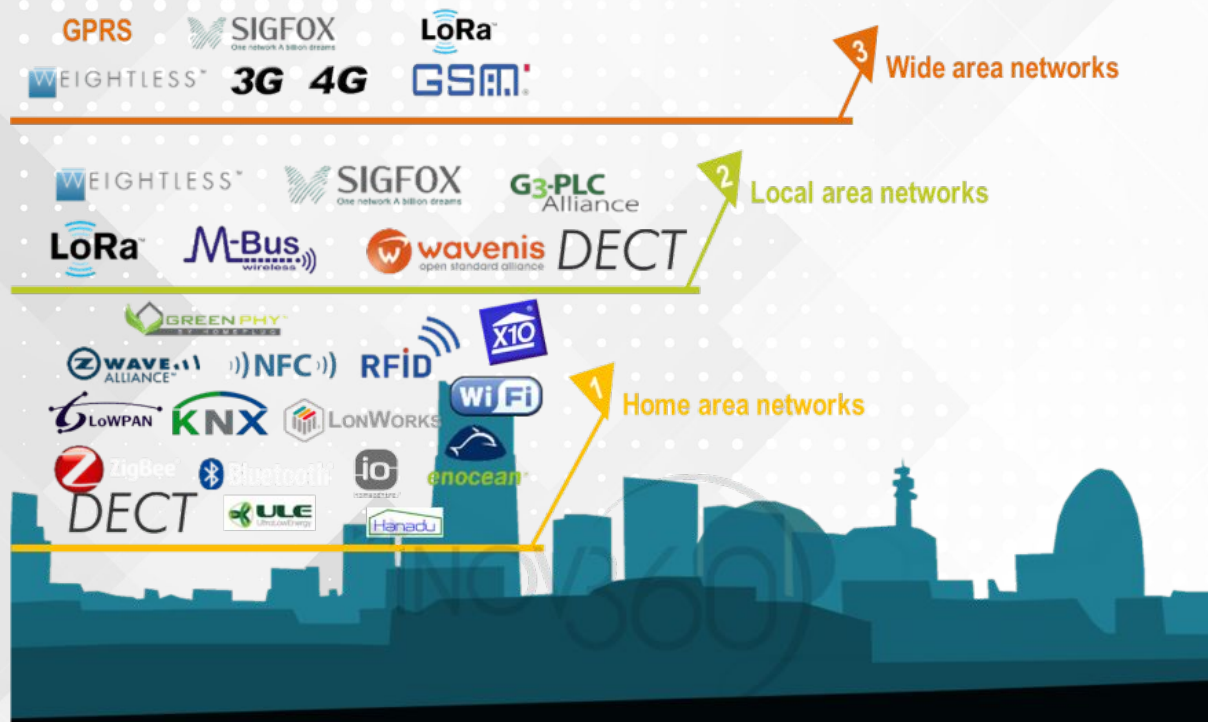
Echelle: pièce / bâtiment

Réseau "personnel"

ref: <http://sahinerbay.com/2016/06/04/lan-man-wan/>



# Protocoles Radio



# Technologies PAN

# PAN - lien série / bus

UART / I<sup>2</sup>C / SPI (Serial Peripheral Interface) : échanges internes à l'équipement

RS-232 / RS-422... : liaisons série asynchrones

USB = Universal Serial Bus

bus CAN (Controller Area Network): automobile / industrie



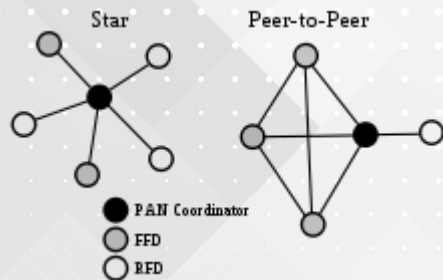
# PAN - NFC (Near Field Communications)

ou CCP = communication en champ  
proche



fréquence	13,56 MHz
portée	10 cm (1,5 m?)
débit	106 / 212 / 424 kbit/s
création	norme ISO/CEI 14443 (2004, Sony & Philips > NFC forum)
usages	carte puce sans contact, tags / badge RFID, synchronisation courte portée (vCard...)
propriétés	mode carte, lecteur (tags) ou pair à pair courte portée > sécurité fonctionnelle tag passif ou actif

# PAN - IEEE 802.15.4



fréquence	ISM : 868 Mhz (EU), 915 MHz (US) ou 2,4 GHz
débit	20 - 250 kbits/sec
création	IEEE, 2003
usages	base de nombreux protocoles domotique (ANT, EnOcean, ...)
propriétés	optimisé pour basse conso et bas coût CSMA/CA link quality energy detection couche MAC topologie étoile / mesh

# PAN - Zigbee

basé sur 802.15.4  
propriété Zigbee Alliance  
spécifications libres



fréquence	ISM: 868 Mhz (europe) ou 2.4Ghz
portée	10m
débit	20 - 250 kbits/sec
création	2004, ZigBee Alliance
usages	domotique
propriétés	simple, jusqu'à 65k noeuds, fiable, routage réactif, au-dessus de IEEE 802.15.4, peu sécurisé? profils spécialisés: home automation, remote control, smart energy...
coût chip	~1\$



# 6LOWPAN

**6LowPan = UDP/IPv6 over 802.15.4**

principal problème: MTU

(IPv6: 1280 bytes,  
802.15.4: 127 bytes)

various optimizations

>> payload = 33 bytes per frame

header & payload compression

neighbor discovery

fragmentation / reassembly

fréquence	ISM : 868 Mhz (EU), 915 MHz (US) ou 2,4 GHz
création	IETF, 2007
usages	capteur contraint connecté à Internet!
propriétés	idem 802.15.4 + accès à Internet / adressage IP



# PAN - Z-Wave / ZWave+



fréquence	ISM 868 Mhz (Europe)
portée	~50m
débit	<40 kbits/sec
création	Zen-Sys (start up danoise, maintenant Sigma Designs), 2005
usages	domotique (leader?)
propriétés	protocole propriétaire (un seul fondateur) certification via alliance ZWave réseau mesh (jusqu'à 232), sécurité relative



# PAN - EnOcean



fréquence	ISM 868 Mhz (Europe)
portée	~30m en intérieur, jusqu'à 300m en extérieur
débit	125 kbits/sec (trame: 14 bytes)
création	EnOcean devient standard international ISO/IEC en 2012
usages	interrupteur sans fil sans pile
propriétés	ultra-simple, ultra-basse consommation

# PAN - 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

fréquence	2.4Ghz
portée	5m à 100m
débit	100 kbits/sec - 1Mbits/sec
versions	1.0 - 5 , “Low Energy”
création	Ericsson, 1994
usages	téléphonie/audio, communication très locale (accessoire personnel)
coût chip	~3\$

# PAN - ANT / ANT+



fréquence	2.4Ghz
portée	30m
débit	20 kbits/sec
versions	1.0 - 4.1, "Low Energy"
création	Ericsson, 1994
usages	fitness, sport heart-monitor
propriétés	protocole propriétaire, basse consommation (22mA en réception, 13mA en émission), broadcast, ack, point à point, étoile, mesh (jusqu'à 65k noeuds) chiffrement AES 128

# PAN - DECT

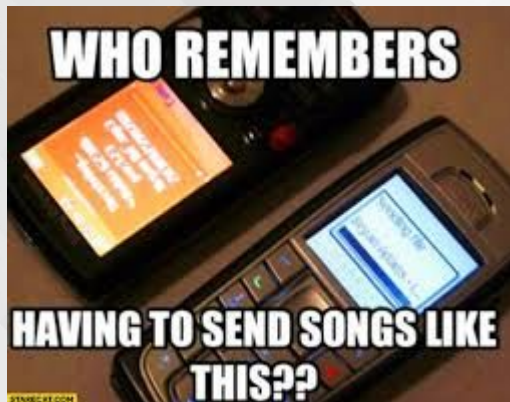
(Digital Enhanced Cordless Telecom.)



fréquence	1880 - 1920 Mhz (réservé en EU puis US)
portée	10m
débit	32 kbits/sec par channel*slot
création	1988-1992, ETSI
usages	téléphonie sans fil, baby monitoring
propriétés	FDMA, TDMA jusqu'à 120 comm. simultanées chiffrement optionnel différents profils (allant jusqu'au roaming et lien GSM) émission 10mW



# PAN - infra-rouge



Consumer IR : héritage HiFi / TV

S-Link (Sony)

RC-5 / RC-6 (Philips)

NEC

Infrared Data Association - groupement industriel ('90)

standard utilisé par PDAs, désormais désuet

IrLAP: Infrared Link Access Protocol

IrCOMM (=serial)

OBEX (object Exchange: vCard etc.)

etc.

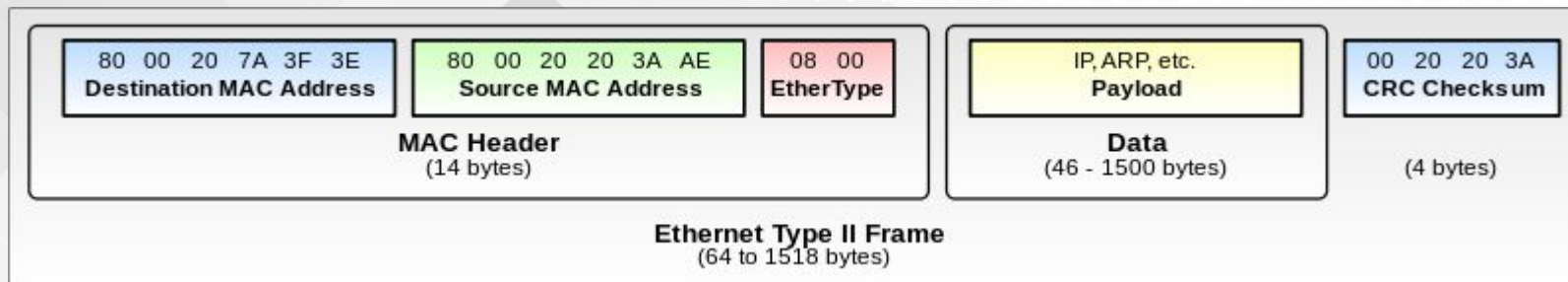


# Technologies LAN

# LAN - Ethernet

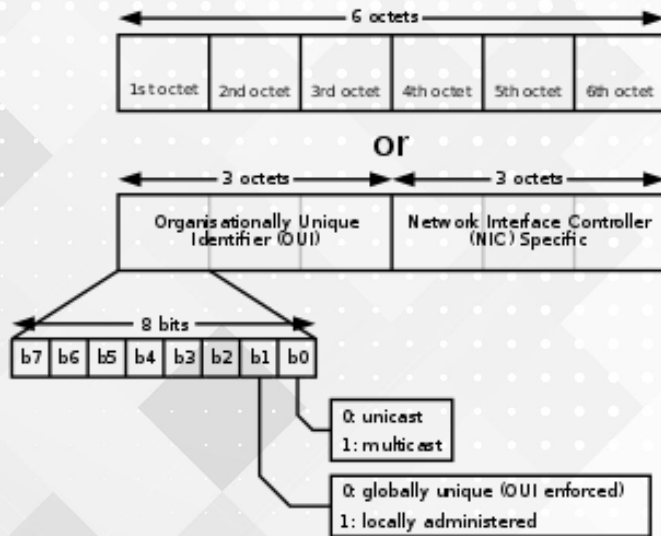


débit	fonction du câble (10BASE-T... 10GBASE-T) jusqu'à 10Gb/sec
création	1973, Xerox PARC Robert METCALFE, David BOGGS
IEEE	IEEE 802.3



# LAN - Ethernet

Un équipement réseau Ethernet est identifiable par son adresse “MAC” (Media Access Control): un identifiant physique sur 6 octets défini par le fabricant de la carte.



## Structure d'une adresse MAC

(source: [https://fr.wikipedia.org/wiki/Adresse\\_MAC](https://fr.wikipedia.org/wiki/Adresse_MAC) )

```
pi@RedRpi: ~  
pi@RedRpi ~$ ifconfig -a  
eth0      Link encap:Ethernet  HWaddr b8:27:eb:26:aa:b4  
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:3351 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:755 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:214476 (209.4 KiB)  TX bytes:74116 (72.3 KiB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)  
  
wlan0     Link encap:Ethernet  HWaddr 00:e0:4c:10:44:3c  
          UP BROADCAST MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)  
  
pi@RedRpi ~$
```

MAC ethernet = **b8:27:eb:26:aa:b4**  
avec **b8:27:eb** => Raspberry Pi Foundation

MAC Wifi = **00:e0:4c:10:44:3C**  
avec **00:e0:4c** => REALTEK SEMICONDUCTOR CORP.

## Develop

AUDIO CAMERA **CONNECTIVITY** GRAPHICS INTERACTION MEDIA STORAGE

## Overview

- Bluetooth and NFC
- Calling and Messaging
- Carrier
- Wi-Fi
  - Overview
  - Wi-Fi HAL
  - Wi-Fi Infrastructure Features
  - STA/AP Concurrency
  - MAC Randomization**
  - Passpoint R1
  - Carrier Wi-Fi
  - Wi-Fi Aware
  - Wi-Fi Round Trip Time (RTT)
  - Testing, Debugging, and Tuning Wi-Fi

## Privacy: MAC Randomization



Starting in Android 8.0, Android devices use random MAC addresses when probing for new networks while not currently associated to a network.


In Android 9, a developer option can be enabled (it is **disabled** by default) to cause the device to use a randomized MAC address when connecting to a Wi-Fi network. A different randomized MAC address is used per SSID.

MAC randomization prevents listeners from using MAC addresses to build a history of device activity, thus increasing user privacy.

Additionally, MAC addresses are randomized as part of [Wi-Fi Aware](#) and [Wi-Fi RTT](#) operations.

### Implementation

To implement MAC randomization on your device:

1. Work with a Wi-Fi chip vendor to implement the `IWifiStaIface.setMacAddress()` HAL method.
  - The AOSP reference implementation brings the interface down, changes the MAC address, and brings the interface back up. This reference implementation behavior may not work with certain chip vendors.
2. Set `config_wifi_support_connected_mac_randomization`  to **true** in the Settings `config.xml` (this can be done in a device custom overlay).
  - This flag is used to control whether the *Connected MAC Randomization* toggle is shown in the developer option of the reference Settings implementation. If **true**, the toggle is shown; if **false**, the toggle is not shown.
3. Test your implementation using the methods described in [Validation](#).

- Contents
- Implementation**
- Validation

# LAN - WiFi



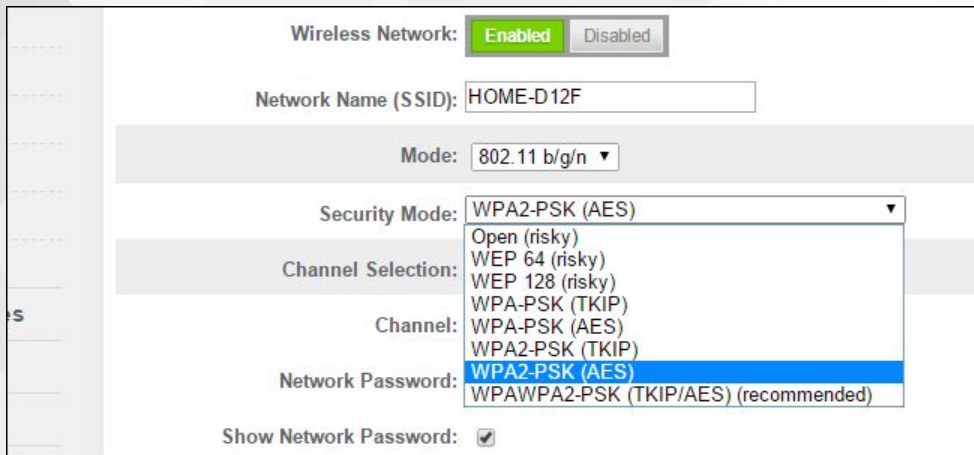
<b>fréquence</b>	2,4 Ghz
<b>portée</b>	plusieurs mètres
<b>débit</b>	(b) 6 Mbits/sec, (a, g) 25 Mbits/sec, (n) 600 Mbits/sec (ac) 1,3 Gbits/sec
<b>création</b>	IEEE, 1997
<b>IEEE</b>	IEEE 802.11
<b>propriétés</b>	modes: infrastructure, ad hoc, bridge, range-extender  encryption: WEP, WPA/WPA2



# LAN - WiFi

Une “passerelle” Wifi est identifiée par un “SSID” qui peut être “broadcasté” de manière répétée, permettant sa découverte.

WEP et WPA sont des mécaniques d'autorisation et de chiffrement des échanges WiFi.



The image shows a screenshot of a wireless network configuration interface. The interface is divided into several sections. At the top, there is a 'Wireless Network' section with two buttons: 'Enabled' (highlighted in green) and 'Disabled'. Below this is the 'Network Name (SSID)' field, which contains the text 'HOME-D12F'. The 'Mode' is set to '802.11 b/g/n'. The 'Security Mode' is set to 'WPA2-PSK (AES)'. A dropdown menu is open, showing a list of security options: 'Open (risky)', 'WEP 64 (risky)', 'WEP 128 (risky)', 'WPA-PSK (TKIP)', 'WPA-PSK (AES)', 'WPA2-PSK (TKIP)', 'WPA2-PSK (AES)' (highlighted in blue), and 'WPAWPA2-PSK (TKIP/AES) (recommended)'. The 'Channel Selection' and 'Channel' fields are empty. The 'Network Password' field is empty. At the bottom, there is a 'Show Network Password' checkbox, which is checked.

Wireless Network: **Enabled** Disabled

Network Name (SSID): HOME-D12F

Mode: 802.11 b/g/n ▼

Security Mode: WPA2-PSK (AES) ▼

Channel Selection: Open (risky)  
WEP 64 (risky)  
WEP 128 (risky)  
WPA-PSK (TKIP)  
WPA-PSK (AES)  
WPA2-PSK (TKIP)  
**WPA2-PSK (AES)**  
WPAWPA2-PSK (TKIP/AES) (recommended)

Channel:

Network Password:

Show Network Password: ☒





# LAN/WAN - Wavenis



## Wavenis et les autres "prétendants" aux faibles consommations

	Wavenis	802.15.4 ZigBee	KNX	Bluetooth
Bandes de fréquence	868 MHz (Europe) 915 MHz (USA) 433 MHz (Asie)	868 MHz (Europe) 915 MHz (USA) 2,4 GHz (monde)	433 MHz 868 MHz (Europe)	2,4 GHz
Couche physique PHY	FHSS Mono-canal	DSSS	Monocanal	FHSS
Débit effectif	4K < 20 K < 100 Kbps	25 Kps	16 Kbps	1 Mbps
Autonomie de la pile (typique)	10 ans	3 ans	2 ans	-
Portée	200 m à l'extérieur 1 km à l'extérieur	20 m	50 m	10 m

fréquence	ISM: 868 MHz
portée	jusqu'à 1km en champ libre
débit	19 kbit/s (max 100)
création	Coronis Systems (FR)
usages	télé-relève, smart lighting
propriétés	technologie propriétaire (mais alliance ouverte) longue portée trame courte (max ques centaines de bytes) basse consommation gestion batterie pas de crypto (couche app.)

source: <http://www.mesures.com/pdf/old/Wavenis.pdf>



# LAN - M-Bus



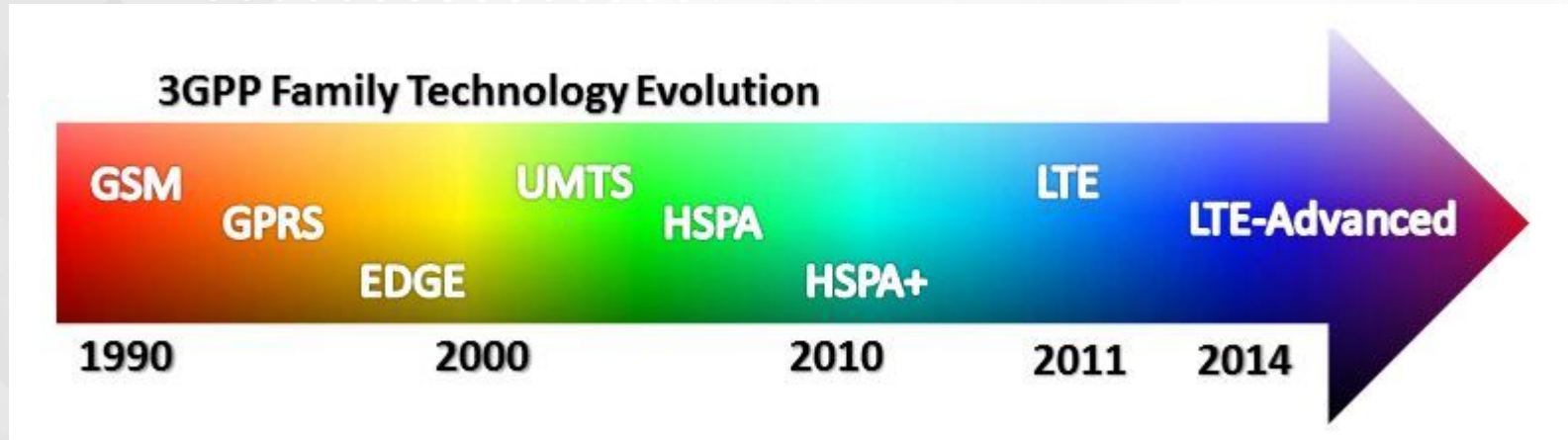
fréquence	ISM: 868MHz, 433MHz, 169MHz
création	europe, 2013
usages	télé-relève gaz ou électricité
propriétés	standard européen (EN 13757-4) différents mode (et freq.) France: mode N, très simple, standard industriel (Grdf)

Mode	Frequency(MHz)	Notes
S (Stationary)	868	Meters send data few times a day
T (Frequent Transmit)	868	Meters send data several times a day
C (Compact)	868	Higher data rate version of mode T
N (Narrowband)	169	Long range, narrow band system
R (Frequent Receive)	868	Collector reads multiple meters on different frequency channels
F (Frequent Tx and Rx)	433	Frequent bi-directional communication

source: <http://www.adeunis-rf.com/>  
/ <http://pages.silabs.com/rs/634-SLU-379/images/introduction-to-wireless-mbus.pdf>

# Technologies WAN

# GSM / GPRS / 3G / 4G...



source:

<http://blog.thiga.fr/innovation-digitale/mobile-mieux-comprendre-les-frequences-et-les-technologies/>

# GSM / GPRS / 3G / 4G...

'70 – '80	<b>Radiocom 2000</b> (analogique) / <b>Nordic Mobile Telephone (NMT)</b> (numérique)	1G
1990	<b>GSM:</b> tout numérique, standard européen (ETSI) puis mondial (3GPP) interopérabilité et roaming	2G
2000	<b>General Packet Radio Service (GPRS) :</b> connexion de données (data)	
2003	<b>EDGE</b> (Enhanced Data Rates for GSM Evolution) optimisation data (compression)	
2004	<b>UMTS</b> voix et data en simultané + meilleur bande passante	3G
2005 / 2006 (2008 / 2010)	<b>HSDPA (H) / HSPA (H+)</b>	3.5 G
2008 / 2009	<b>LTE</b> (Long Term Evolution) / <b>LTE Advanced</b> ("4G") standard mondial (3GPP), 100% paquets	4G

# Evolution réseaux cellulaire pour l'IoT

Enjeux: optimiser bande passante / consommation énergétique  
+ focalisation sur échanges data

**LTE cat M1 (3gpp)**

évolution LTE pour IoT

**NB-IoT (Huawei)**

protocole IoT compatible avec gateways LTE Huawei

**CG-GSM:**

évolution 2G pour IoT

**5G IoT ???**



# WAN - Sigfox

Techno / Réseau privé (licensing)  
couverture internationale  
“LPWAN” (long range, low power)



<b>fréquence</b>	ISM: 868MHz (EU)
<b>création</b>	Sigfox (FR), 2010
<b>débit</b>	< 100 bit/s
<b>usages</b>	télé-relève, transport
<b>propriétés</b>	propriétaire low power long range ( 30 - 50km) bi-directionnel ultra narrow band  jusqu'à récemment unidirectionnel (=> émission multiples et pas de garantie)





# WAN - LoRa (LoRaWAN)

concurrent Sigfox,  
standardisation via LoRa Alliance,  
spec ouverte mais un seul fondateur,  
réseaux privés ou publiques



<b>fréquence</b>	ISM: 868MHz (EU)
<b>création</b>	Cycléo (FR) puis Semtech, 2012
<b>débit</b>	0,3 - 50 kbit/s
<b>usages</b>	télé-relève, smart city...
<b>propriétés</b>	low power long range (1 - 15km) communication large bande réseaux privés ou publique (basestation très peu chère) sécurisé (double crypto) bi-directionnel / ack



# Protocoles

# Internet Protocol (IP)

Protocole standard (RFCs) - a permis la naissance d'Internet!

Adresse uniquement le routage d'un paquet (= "datagram")

Information de source / destination

Fragmentation / réassemblage

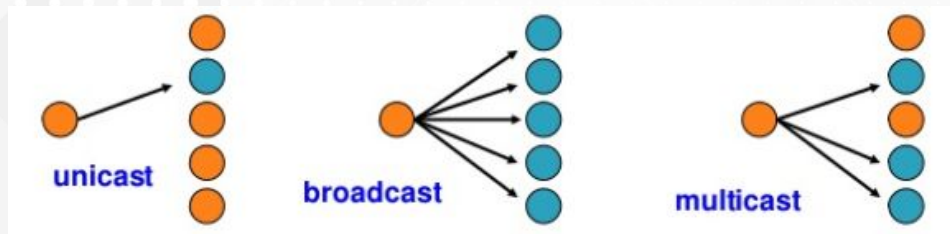
Unicast / Multicast / Broadcast

**1980 - IPv4:**

adresses 32 bits

**1998 - IPv6 (IETF):**

adresses 128 bits, intègre IPSec, optimisations pour réseaux privés

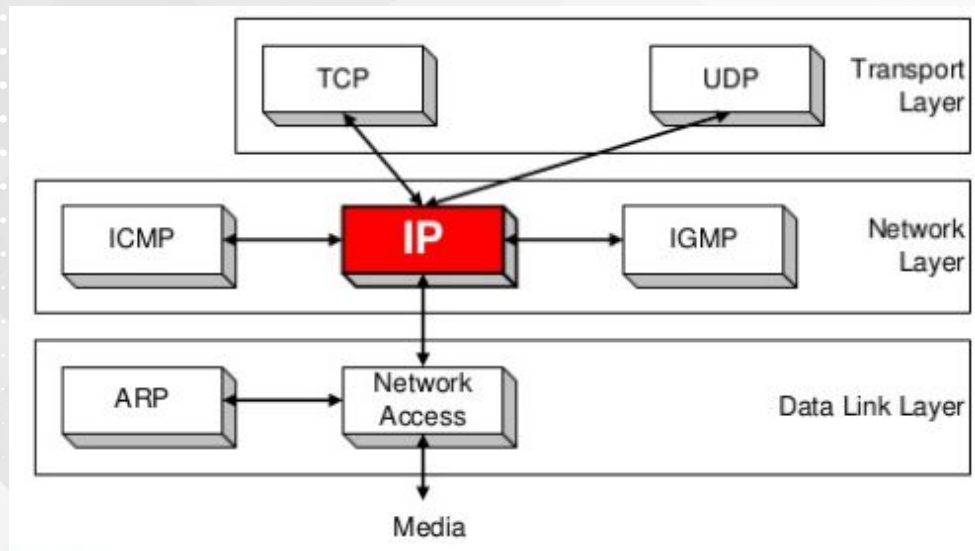


# Internet Protocol (IP)

header IPv4:

Version	IHL	ToS	Total Length	
Identification			Flgs	Fragment Offset
Time To Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options				Padding

# Internet Protocol (IP)



- **ICMP (Internet Control Message Protocol):**  
signalisation liée à IP (ex: ping, notification de problème de transmission...)
- **IGMP (Internet Group Message Protocol):**  
gestion souscriptions multicast
- **ARP (Address Resolution Protocol):**  
pour résolution MAC / IP IPv4  
(en IPv6 : NDP = Neighbor Discovery Protocol)



# Internet Protocol (IP)

Reserved address blocks

Range	Description	Reference
0.0.0.0/8	Current network (only valid as source address)	<a href="#">RFC 6890</a>
10.0.0.0/8	Private network	<a href="#">RFC 1918</a>
100.64.0.0/10	Shared Address Space	<a href="#">RFC 6598</a>
127.0.0.0/8	Loopback	<a href="#">RFC 6890</a>
169.254.0.0/16	Link-local	<a href="#">RFC 3927</a>
172.16.0.0/12	Private network	<a href="#">RFC 1918</a>
192.0.0.0/24	IETF Protocol Assignments	<a href="#">RFC 6890</a>
192.0.2.0/24	TEST-NET-1, documentation and examples	<a href="#">RFC 5737</a>
192.88.99.0/24	IPv6 to IPv4 relay (includes 2002::/16)	<a href="#">RFC 3068</a>
192.168.0.0/16	Private network	<a href="#">RFC 1918</a>
198.18.0.0/15	Network benchmark tests	<a href="#">RFC 2544</a>
198.51.100.0/24	TEST-NET-2, documentation and examples	<a href="#">RFC 5737</a>
203.0.113.0/24	TEST-NET-3, documentation and examples	<a href="#">RFC 5737</a>
224.0.0.0/4	IP multicast (former Class D network)	<a href="#">RFC 5771</a>
240.0.0.0/4	Reserved (former Class E network)	<a href="#">RFC 1700</a>
255.255.255.255	Broadcast	<a href="#">RFC 919</a>



# Internet Protocol (IP)

```
% ifconfig
```

```
wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  
    inet 192.168.43.43  netmask 255.255.255.0  broadcast 192.168.43.255  
    inet6 fe80::f425:7aeb:24cd:6539  prefixlen 64  scopeid 0x20<link>  
    ether e0:94:67:75:5b:9d  txqueuelen 1000  (Ethernet)  
    RX packets 430830  bytes 537633029 (537.6 MB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 112598  bytes 14531015 (14.5 MB)  
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

# Internet Protocol (IP)

```
% traceroute google.fr
```

```
traceroute to google.fr (216.58.206.227), 64 hops max
```

```
1  192.168.43.1  1,397ms  1,146ms  1,267ms
2  10.125.116.5  33,115ms  41,063ms  40,006ms
3  10.125.120.28  33,564ms  36,529ms  40,065ms
4  10.125.120.50  41,584ms  89.89.100.226  30,213ms  38,649ms
5  89.89.100.226  39,677ms  212.194.171.148  48,507ms  89.89.100.226  29,912ms
6  212.194.171.148  48,818ms  41,455ms  38,826ms
7  * * 212.194.171.153  54,967ms
8  * 209.85.148.0  36,251ms  28,879ms
9  209.85.148.0  28,171ms  108.170.252.227  26,019ms  23,790ms
10 108.170.252.226  27,502ms  64.233.175.243  32,163ms  36,535ms
11 216.239.35.201  35,001ms  72.14.238.52  33,994ms  35,852ms
12 108.170.235.98  34,871ms  108.170.244.225  33,287ms  34,869ms
13 108.170.244.161  38,731ms  216.239.48.147  37,382ms  33,764ms
14 216.239.48.151  36,393ms  216.58.206.227  34,924ms  216.239.48.151  32,685ms
```

# UDP (User Datagram Protocol)

Fine couche au dessus d'IP:

- port source/cible,
- somme de contrôle additionnelle

Port Source (16 bits)	Port Destination (16 bits)
Longueur (16 bits)	Somme de contrôle (16 bits)
Données (longueur variable)	

Usages: NTP, DNS, temps-réel / faible latence (VoIP, jeux), CoAP

=> de nouvelles tendances pour optimiser latence (QUIC / draft HTTP 3)



# TCP (Transmission Control Protocol)

le plus répandu au dessus de IP.

- protocole connecté (couche "session")
- ré-ordonnancement de paquets ("segments")
- détection de perte / reprise
- contrôle de flux (windowing)

Usages: protocoles haut niveau session (Telnet, SSH, HTTP, FTP, SMTP...)

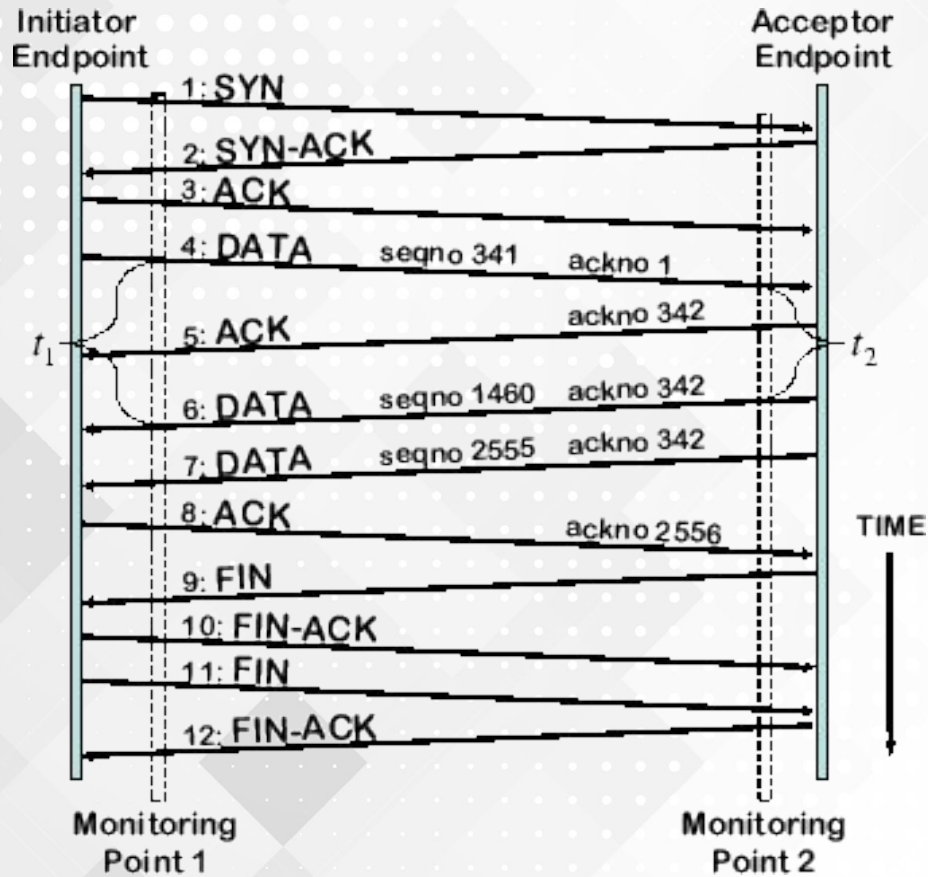


# TCP

## Format d'une trame:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Port Source 2 octets																Port destination 2 octets															
Numéro de séquence																															
Numéro d'acquittement																															
Taille de l'en-tête		Réservé	ECN / NS		CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Fenêtre																		
Somme de contrôle																Pointeur de données urgentes															
Options																						Remplissage									
Données																															

# TCP



Source: <http://www.cs.unc.edu/~fhernand/diss-html/img88.png>



# DNS protocol

“Domain Name System”, 1983.

bâti sur UDP (ou TCP)

permet d'interroger un inventaire pour obtenir  
des informations sur un nom de domaine:

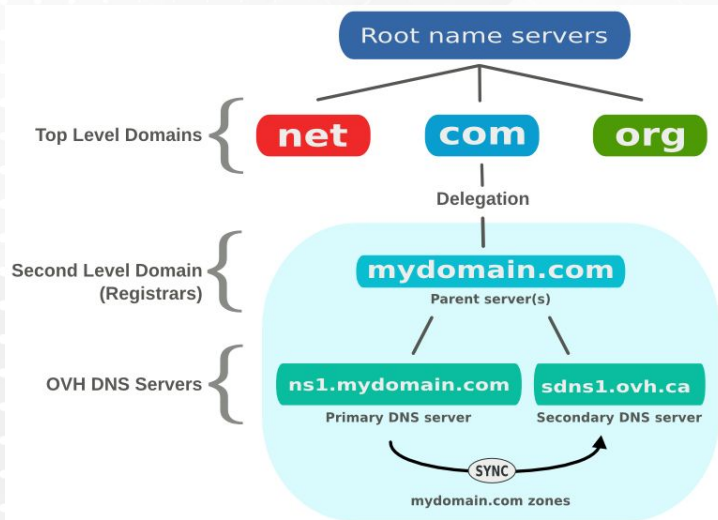
adresse(s) IP (par type de service: mail, etc.)

DNS secondaires

info sécurité

info contact

serveurs racine: ICANN



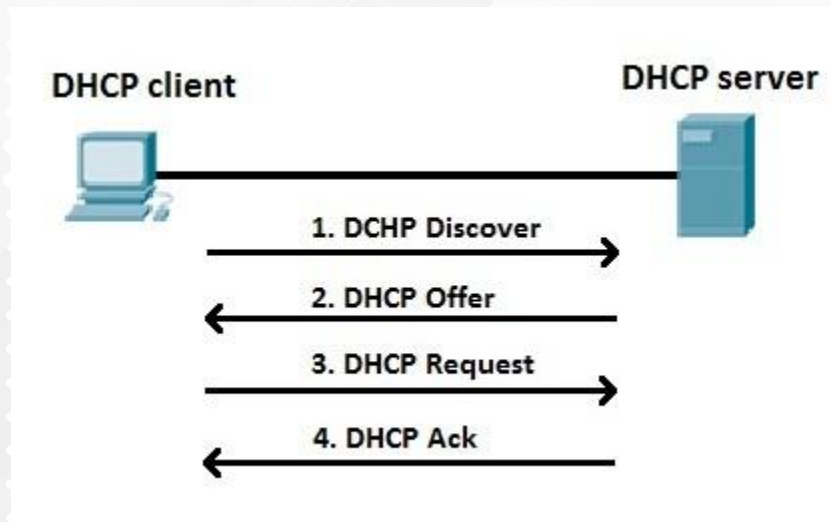
# DHCP

"Dynamic Host Configuration Protocol"

Configuration IP dynamique:

- attribution d'une IP
- IP passerelle
- ...

Emission / réception en Broadcast IP.



# HTTP

“HyperText Transfer Protocol”

le protocole du “web”

(1991 - Tim Berners-Lee)

Requête / réponse au dessus de  
TCP/IP.

Verbe (GET/POST...) + URL.

Headers

Version 2 (2015):

échanges asynchrones

<pre>\$ telnet www.perdu.com 80 Trying 208.97.177.124... Connected to www.perdu.com. Escape character is '^J'.</pre>	Connexion au serveur par telnet
<pre>GET / http/1.1 Host: www.perdu.com</pre>	Requête HTTP
<pre>HTTP/1.1 200 OK Date: Sat, 17 Aug 2013 11:59:04 GMT Server: Apache Accept-Ranges: bytes X-Mod-Pagespeed: 1.1.23.1-2169 Vary: Accept-Encoding Cache-Control: max-age=0, no-cache Content-Length: 204 Content-Type: text/html</pre>	Réponse du serveur : headers
<pre>&lt;html&gt;&lt;head&gt;&lt;title&gt;Vous Etes Perdu ?&lt;/title&gt;&lt;/head&gt;&lt;body&gt;&lt;h1&gt;Perdu sur l'Interne t ?&lt;/h1&gt;&lt;h2&gt;Pas de panique, on va vous aider&lt;/h2&gt;&lt;strong&gt;&lt;pre&gt;    * &lt;----- vous &amp;ccirc;tes ici&lt;/pre&gt;&lt;/strong&gt;&lt;/body&gt;&lt;/html&gt;</pre>	Réponse du serveur : body



# CoAP

“Constrained Application Protocol”  
équivalent HTTP compact sur UDP (ou SMS ou TCP)

Authentication via DTLS.

Mécanisme de Pub/Sub.

## CoAP: The Web of Things Protocol

- Open IETF Standard
- Compact 4-byte Header
- UDP, SMS, (TCP) Support
- Strong DTLS Security
- Asynchronous Subscription
- Built-in Discovery

CoAP	
DTLS	SMS
UDP	
IP	

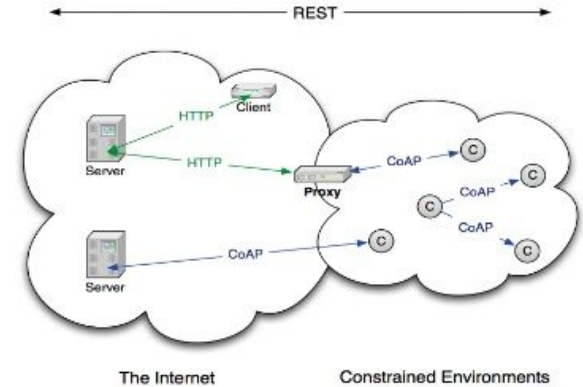


Table 3 Message Format

0				1				2				3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Ver	T	OC	Code							MessageID											
Token (if any, TKL bytes)...																					
Options (if any)...																					
Payload (if any)...																					

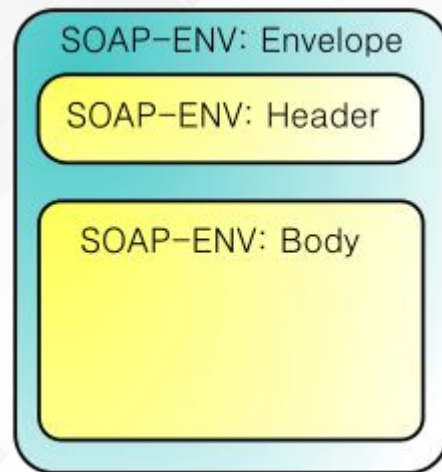
source: <http://www.cse.wustl.edu/~jain/cse574-14/ftp/coap/>

# SOAP

“Simple Object Access Protocole”

Protocol RPC (remote procedure call) via échanges XML sur HTTP.

WSDL (WebService Description Language): contrat d'interface pour Webservice SOAP.

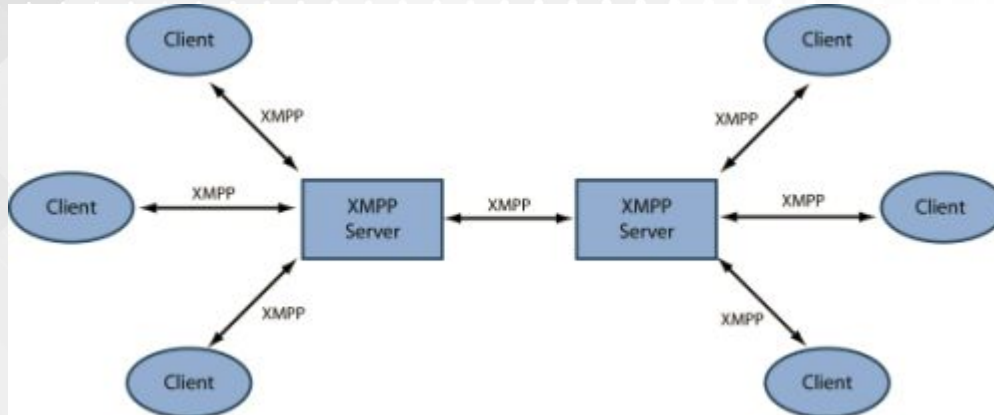


# XMPP

“eXtensible Messaging and Presence Protocole”

Protocole de messaging, XML sur TCP.

(Jabber, repris par IETF)



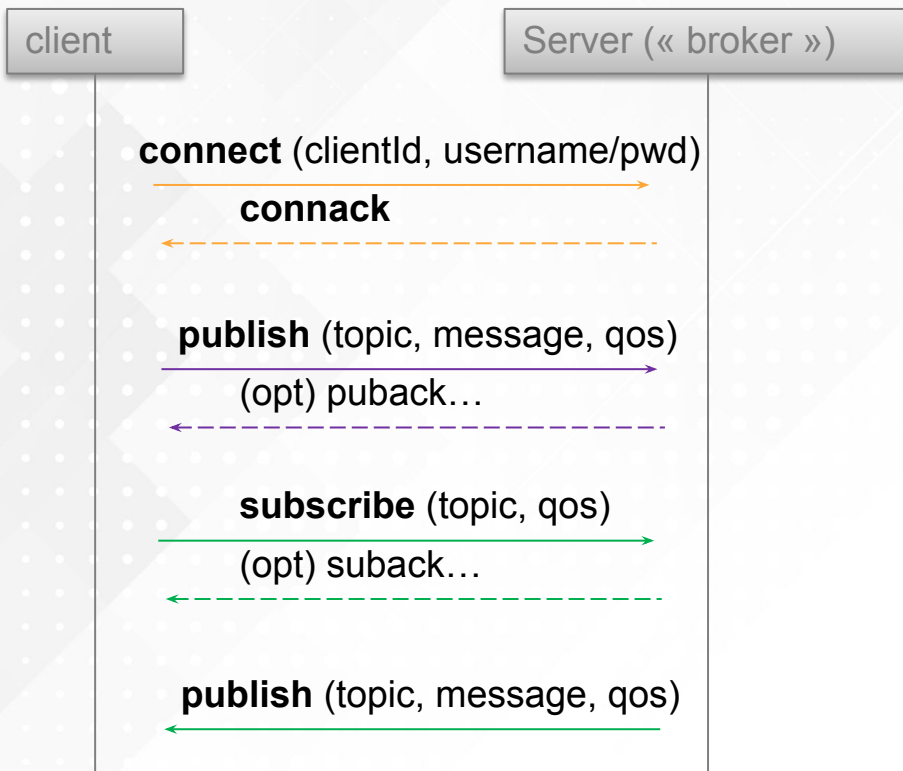
# MQTT

“MQ Telemetry Protocol”

Protocole publish/subscribe au dessus de TCP/IP.

authentification clients

contrôle fin de qos de publication  
(niveau d’acquittement)





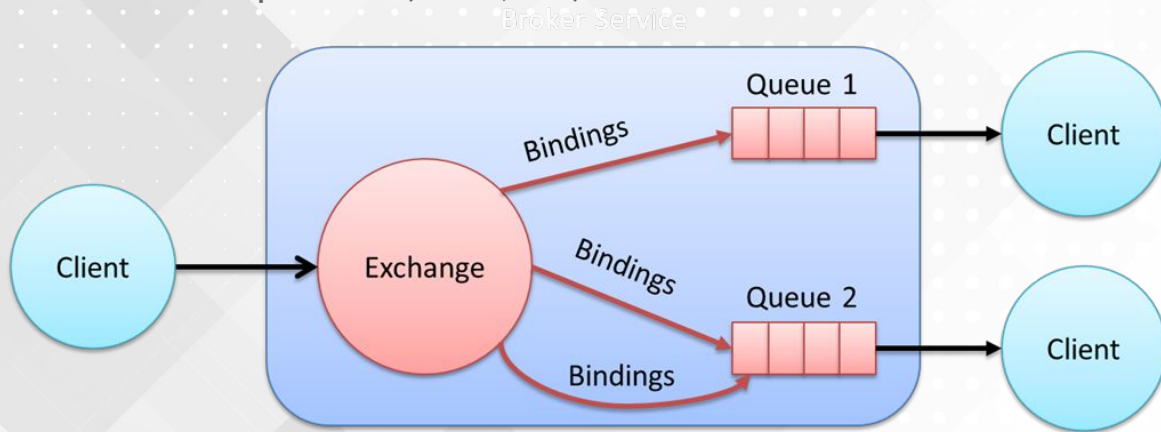
# AMQP

“Advanced Message Queue Protocol”

Publish/Subscribe (et admin de router/topics) via TCP/IP.

Porté par consortium bancaire / IT(JP Morgan) depuis 2003.

Plusieurs version incompatibles (0.9.1, 1.0)

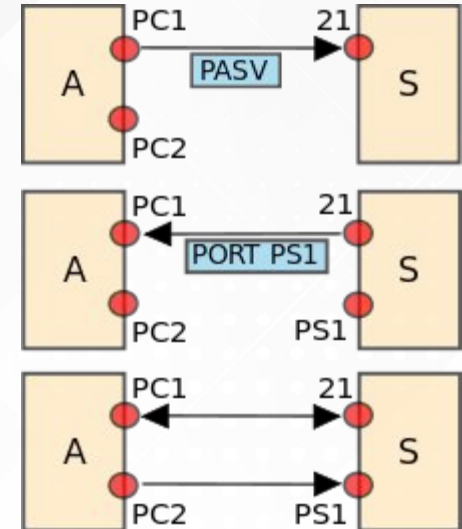
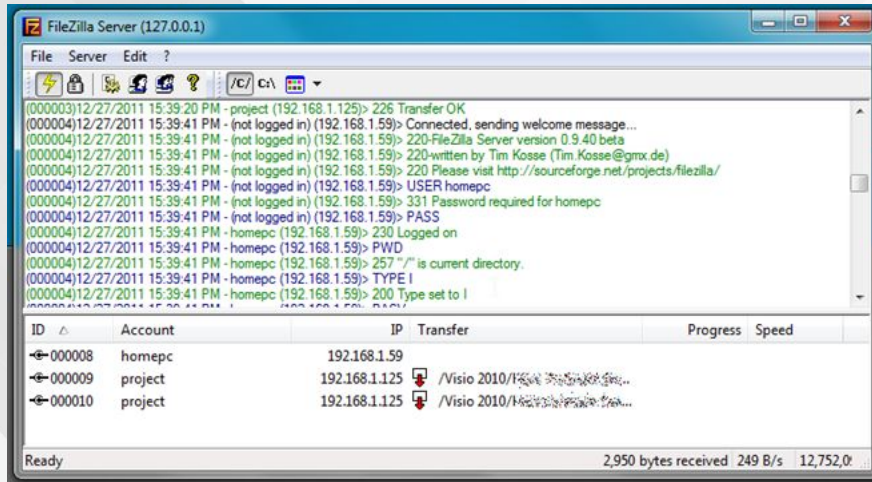


# FTP

“File Transfer Protocol”

Partage (list, lecture, suppression) et transfert de fichiers.

Double connections TCP: contrôle et transfert.



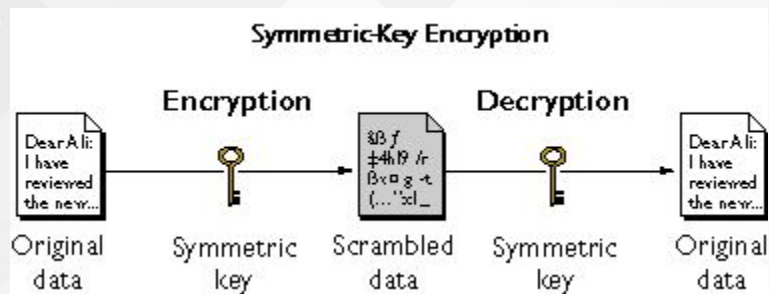
# Autres protocoles notables

- BitTorrent: partage de fichiers
- SSH ("secure shell"): terminal à distance
- SCP ("secure copy") : transfert de fichier (basé sur SSH)
- NTP (network time protocol) : synchronisation d'horloges
- SMTP / POP / IMAP : messagerie électronique (email)
- ...

# Cryptographie

= outils et techniques pour sécuriser des échanges

# Chiffrement symétrique



## Principe:

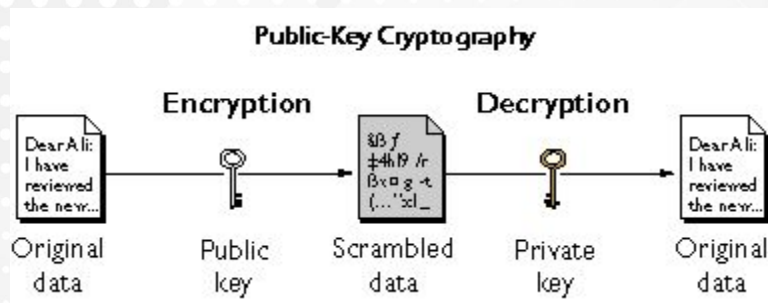
un secret (ou « clé ») est connu de l'émetteur et du destinataire,  
un algorithme permet de passer du contenu en clair au contenu chiffré et inversement au moyen du secret (S).

## Implémentations:

- Chiffrement par bloc: DES, 3DES, IDEA, Blowfish, **AES\***
- Chiffrement par flux: RC4, SEAL



# Chiffrement Asymétrique



## Principe:

une paire clé privée / clé publique est utilisée,  
un contenu peut être chiffré via la clé publique puis déchiffré par la clé privée,  
ou encore signé via la clé privée et vérifié par la clé publique.

La clé publique est diffusable librement.

## Implémentations / Algorithmes:

RSA (1978) / Diffie et Hellman / Courbes elliptiques



# Certificat cryptographique

## Principe:

un certificat cryptographique associe une clé publique à une identité, pour une plage de temps donnée.

Un certificat peut lui-même être signé par une « autorité de certification », on peut ainsi créer des « chaine de certification ».

Standard: **X.509**

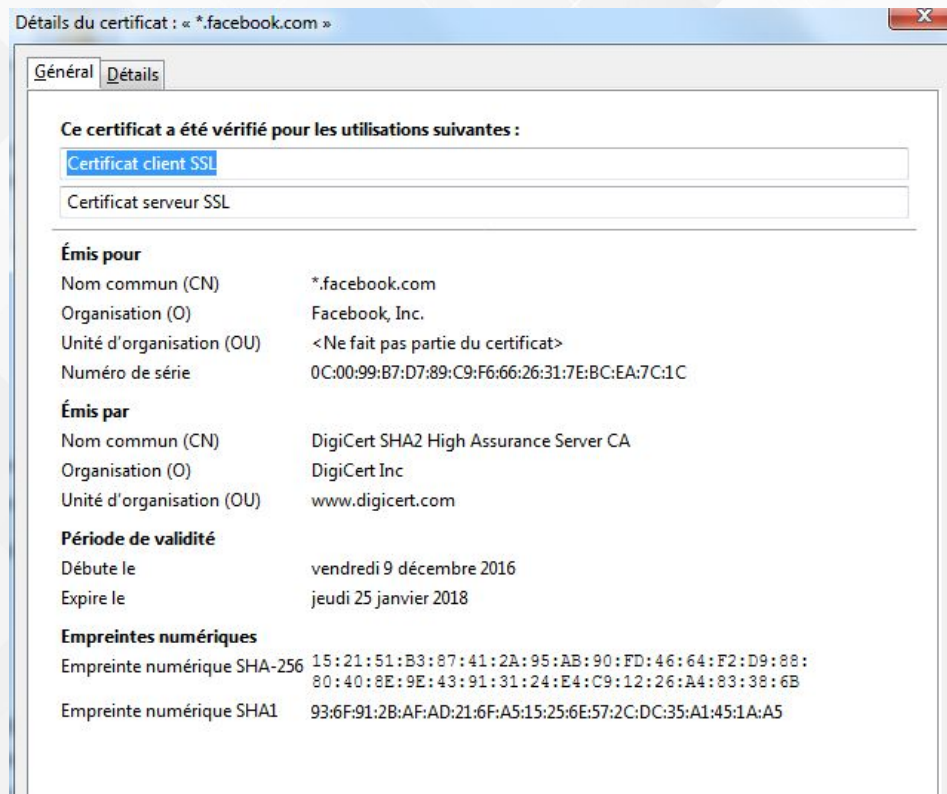






#### Identité du site web

Site web : **www.facebook.com**  
Propriétaire : **Ce site web ne fournit pas d'informations sur son propriétaire.**  
Vérifiée par : **DigiCert Inc**  
Expire le : **jeudi 25 janvier 2018**



# Certificats cryptographiques - compléments

## CSR

« Certificate Signature Request »

il s'agit d'une demande de signature d'un certificat auprès d'une autorité: la demande est chiffrée avec la clé publique de l'autorité.

## CRL

« Certificat Revocation List »

Permet de diffuser une liste de certificats « blacklistés » (parce que volés par exemple).

# Hash cryptographique

## Principe:

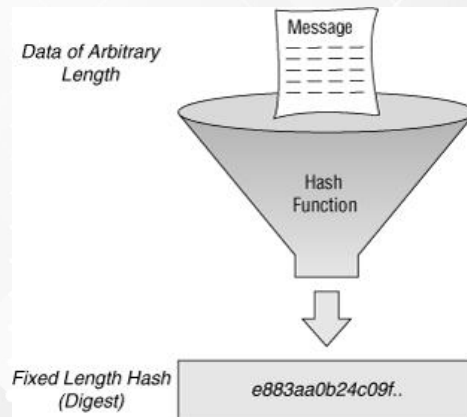
une fonction de « hashing » permet de produire une « empreinte » (le « hash ») compact d'un contenu.

On ne peut pas remonter du de l'empreinte au contenu d'origine.

On ne peut pas forger de contenu ayant une empreinte donné.

En disposant d'un hash, il est donc possible de s'assurer qu'un contenu n'a pas été altéré.

Implémentations / Algorithmes: MD5, SHA1, SHA256



# Résumé - outils cryptographiques

Chiffrement symétrique vs asymétrique

Symétrique:

AES

Asymétrique

RSa

ECC

Hash: md5, Sha

Certificat = identité + clé publique (format: x509)

CSR : certificate signature request

CRK: Certificate Revocation List

# Protocoles cryptographiques: SSL / TLS

SSL = « Secure Socket Layer » (Netscape, 1994)

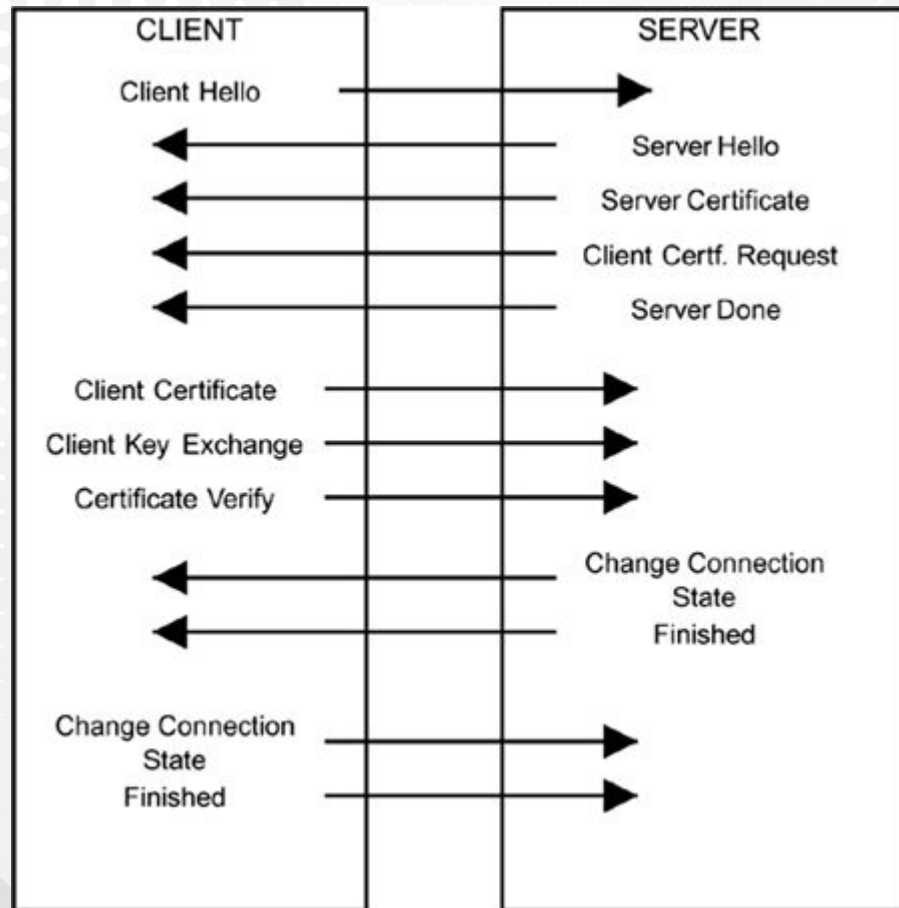
TLS = « Transport Layer Security » (= SSL v3.0) (1999 IETF)

## Fonctions:

- Authentification (serveur et/ou client)  
=> éviter l'usurpation d'identité d'un des interlocuteurs
- Confidentialité des échanges  
=> empêcher le vol de données sensibles par interception
- Intégrité des informations transmises  
=> empêcher l'injection de données fabriquées



# SSL / TLS



# DTLS (Datagram TLS)

= TLS appliqué à un transport "datagram" (UDP, SMS...)

- Échange de « records »
- numéro de séquence explicite
- Accepte doublons, pertes...
- Encryption « stateless » (pas de chiffrement par flot)



The background features a complex geometric pattern of overlapping squares and diamonds in various shades of gray. A dense grid of small white dots is visible in the upper-left and lower-right areas. A large, solid black rectangle is centered on the page, containing the word "Bilan" in white text.

**Bilan**

# Principes

- Modèle OSI:

modèle théorique en 7 couches distribuant les mécanismes utiles à une communication applicative:

couches physique / liaison / réseau / transport / session / présentation / application

- Communication radio:

l'utilisation des différentes bandes de fréquence est encadré,  
certaines bandes sont réservées (usage militaire, bandes sous licence opérateur),  
d'autres sont ouvertes (bandes "ISM")

- Protocoles:

un "protocole" est un ensemble de règle / convention qui permettent à deux interlocuteurs d'échanger et de se comprendre.

(ex: fréquences à utiliser et rythme d'échange, manière de détecter la présence / pallier aux collisions / erreurs, découpage et représentation des données...)



# Protocoles radio

il en existe de très nombreux, qui se démarquent par des différences de portée/débit/verbosité/sécurité, certains sont même spécifiques à un domaine d'application.

Exemples:

- Les standards (généralistes) : Wifi, Bluetooth / BLE, 802.15.4, NFC
- Domotique: zigbee, z-wave, EnOcean
- "LPWAN" - bas débit, basse consommation et longue portée: LoRa, Sigfox
- Spécifiques: Ant/Ant+ (sport), Dect (téléphonie fixe), Wavenis / MBus (relève de compteurs)
- Réseaux cellulaires (sur fréquences privées) : GSM, 2G/3G/4G... (derrière lesquels un forêt de technologies: GPRS, HSPA, LTE...=)

L'IoT a pour particularité de pousser à l'émergence de protocoles basse consommation, ce qui se diffuse dans les standards cellulaires par ex. (NB-IOT, LTE-M).



# Protocoles IP

- Internet repose sur la famille des protocoles “IP” qui permettent à des ordinateurs de communiquer d’un bout à l’autre du globe.
- TCP et UDP sont les deux protocoles de transport majeurs au dessus d’IP, sur lesquels se fondent l’ultra majorité des protocoles applicatifs modernes (HTTP pour le web, SMTP/POP/... pour les mails, FTP/bittorrent pour l’échange de fichiers...)
- HTTP est utilisé par ailleurs exposer des “services web / API”: des interfaces web applicatives permettant d’interconnecter des programmes (“services web”), associé aux formats JSON ou XML pour représenter la donnée.



# Cryptographie

= un ensemble d'outils fondés sur les mathématiques, permettant de sécuriser échanges ou secret:

- authentifier: s'assurer de l'identité d'un interlocuteur
- chiffrer: rendre un contenu / un échange incompréhensible pour un attaquant

TLS (et son pendant pour UDP: DTLS) est un protocole permettant de sécuriser une communication TCP.

Un "certificat" identifie un interlocuteur de confiance.



# Annexes

# Les bandes de fréquence

## Bandes de Fréquence attribuées en France

Rayon cellule



Fréquence

