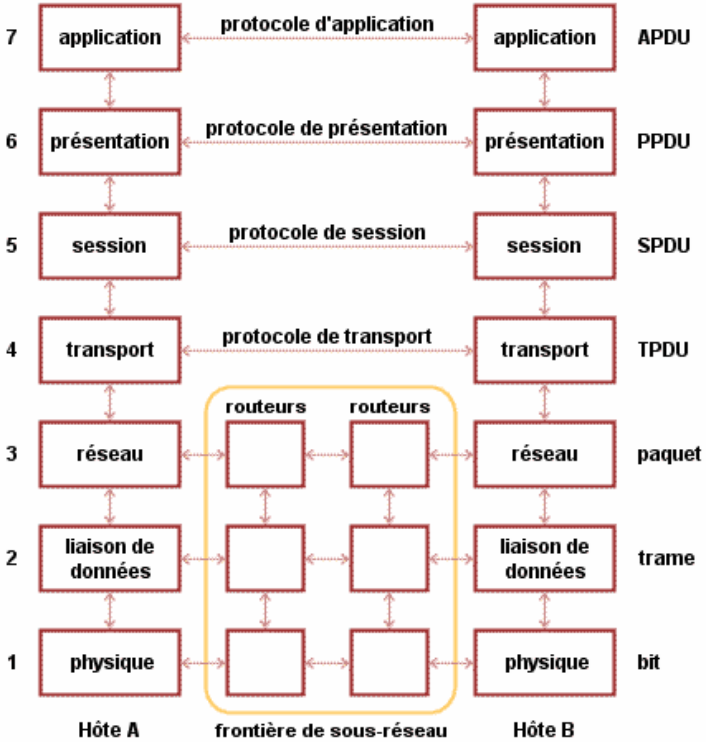
Internet of Things (IoT)

architectures et technologies

décembre 2016 - Master “Big Data” - Telecom Paristech

Chapitre #2 - Communications

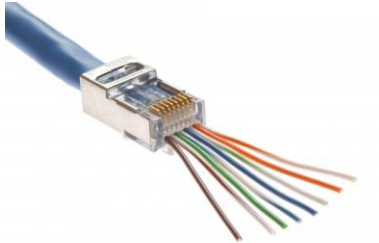
Modèle OSI



Ref. http://www.frameip.com/osi/

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

OSI #3 - couche “réseau”

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

Fonctions:

- gestion de sous-réseaux,
- routages des trames/paquets

OSI #4 - transport

Fonctions:

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

OSI #5 - session

Fonctions:

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

OSI #6 - présentation

Fonctions:

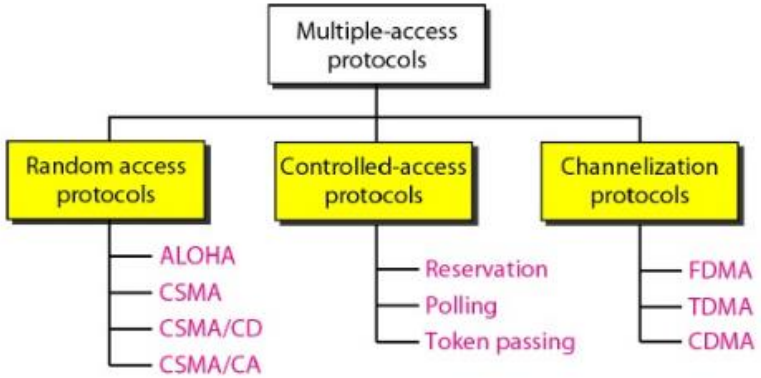
- syntax et sémantique de l’information échangée,
- encryption,
- compression,
- etc.

OSI #7 - application

Fonctions:

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

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 …

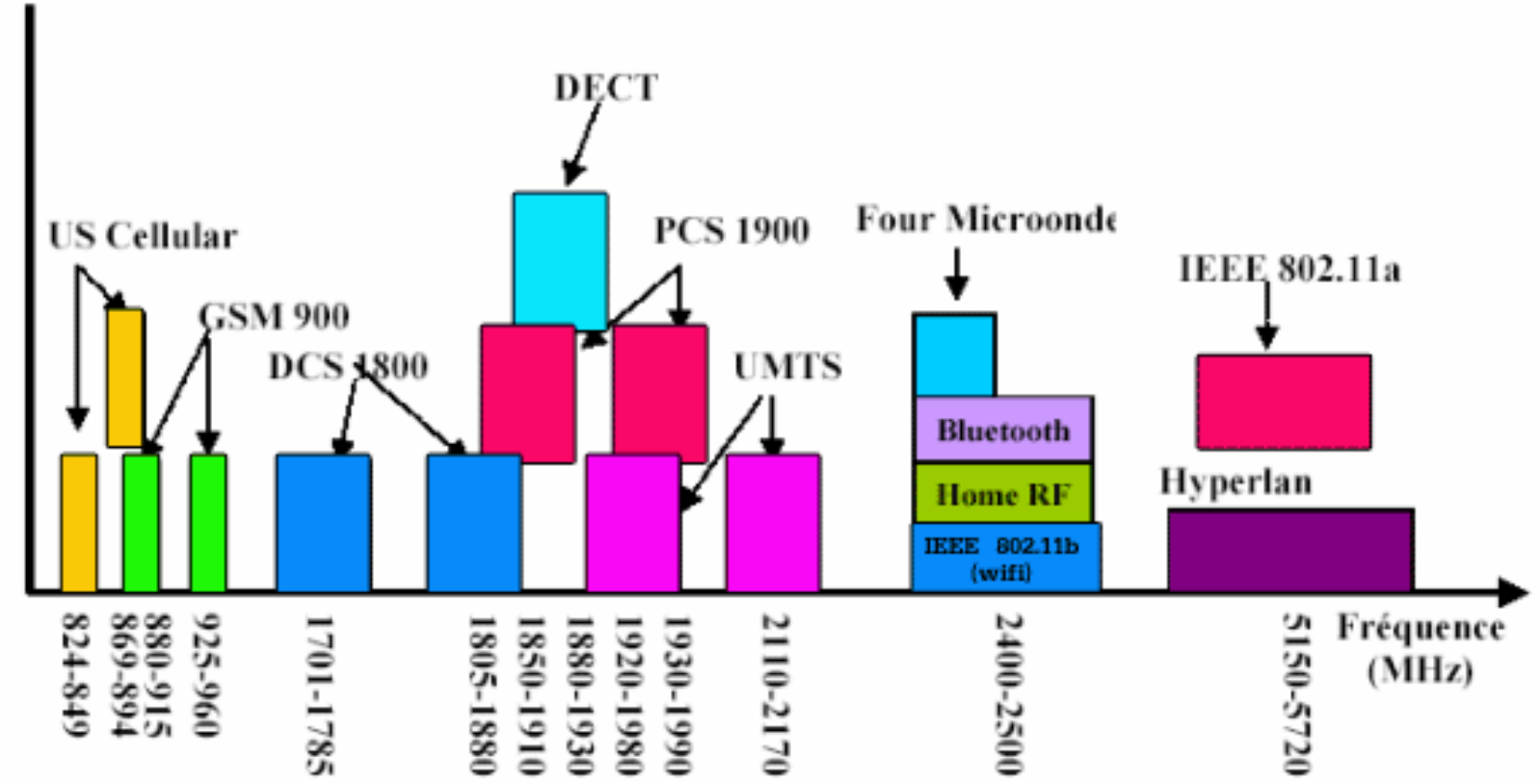
CDMA = Code ...

source http://fr.slideshare.net/mangal007/aloha-6646824

Radio

Les bandes de fréquence

Les bandes de fréquence



Bandes “industrielles, scientifiques et médicales” (ISM)

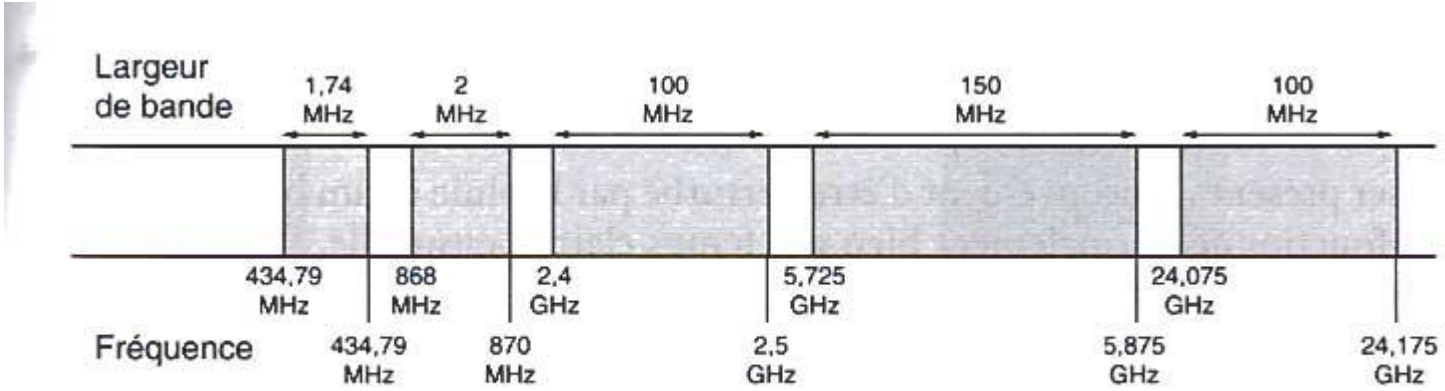


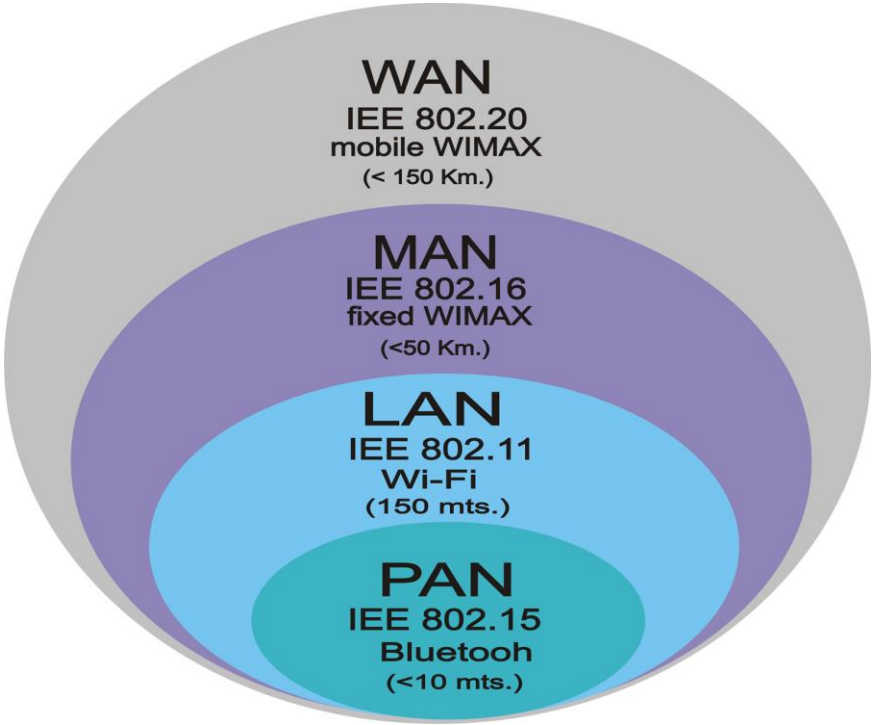
Figure 2.13 • Répartition des bandes ISM en France et en Europe.

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

- 26 Mhz: téléphonie sans fil CT0
- 433 Mhz: domotique, télécommandes (voitures, portails), porteiers vidéo, alarmes, jouets...
- 868 MHz: EnOcean, Z-Wave, Sigfox, LoRa
- 2,4 GHz: Bluetooth, Wifi, vidéo-surveillance, transmetters audio/video (max 10mW)
- 5,4 GHz: video “FPV” (25 mW)

PAN / LAN / WAN

PAN / LAN / WAN ...



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

Communications Radio

ref: http://www.inov360.com/blog/reseaux-sim-less-le-nouvel-eldorado-du-m2m-et-de-linternet-des-objets-2/

PAN

PAN - lien série / bus

UART / I²C / SPI (Serial Peripheral Interface) : échanges internes à l'équipement

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

USB = Universal Serial Bus

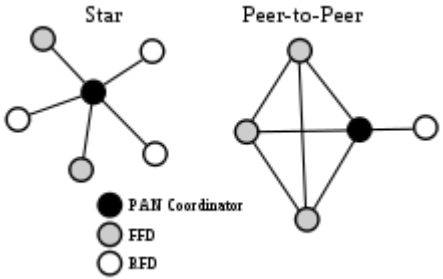
bus CAN (Controller Area Network): automobile / industrie

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, synchronoisation 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? profiles spécialisés: home automation, remote control, smart energy...
coût chip	~1$

6LOWPAN

6LowPan = UCP/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 fondeur) certification via alliance ZWave réseau mesh (jusqu'à 232), sécurité relative

PAN - EnOcean

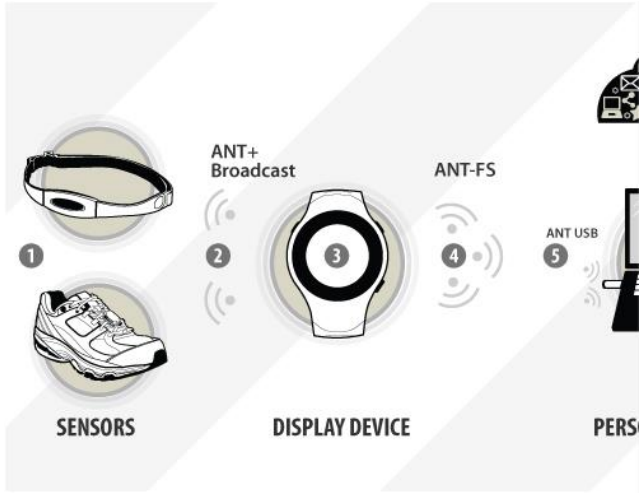
fréquence	ISM 868 Mhz (Europe)
portée	~30m en intérieur, jusqu'à 300m en extérieur
débit	125 kbits/sec (trame: 14 bytes)
création	EnOcean devient standard international ISO/IEC en 2012
usages	interrupteur sans file sans pile
propriétés	ultra-simple, ultra-basse consommation

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 - 4.1, “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 profiles (allant jusqu'au roaming et lien GSM) émission 10mW

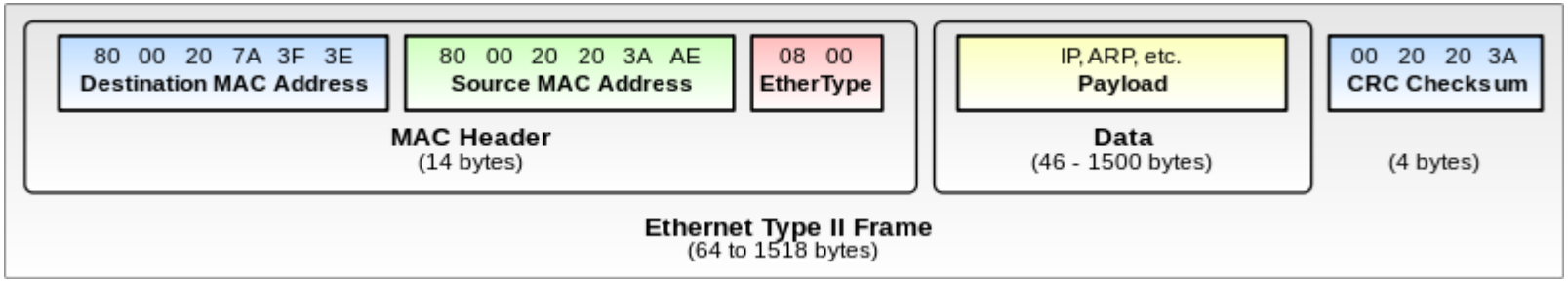
PAN - infra-rouge

- 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.

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 - WiFi

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

LAN/WAN - Wavenis

on air with 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

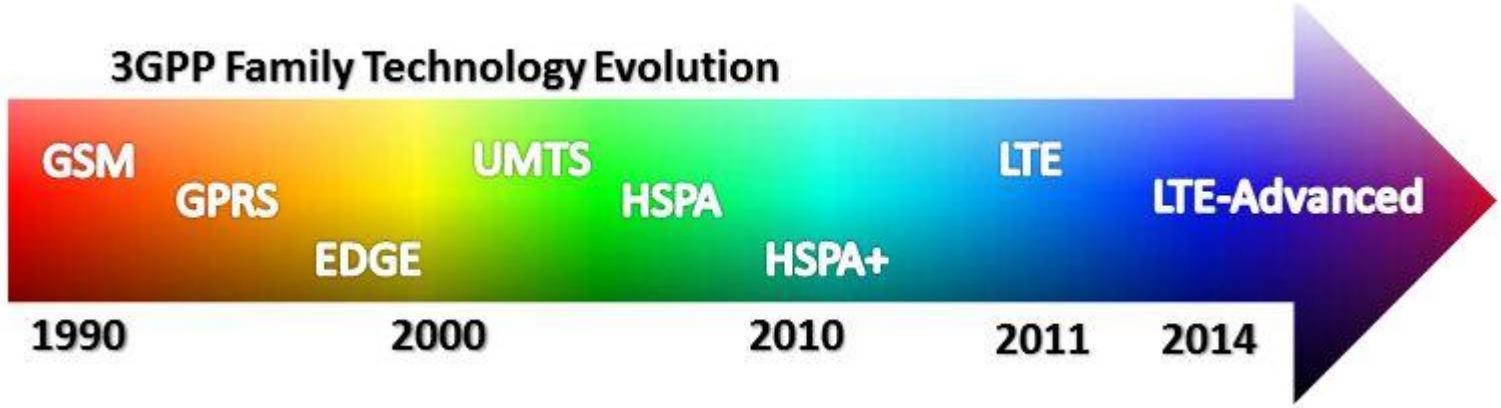
Mode	Frequency(MHz)	Notes
S (Stationary)	868	Meters send data few times a day
T (Frequent Transmit)	868	Meters send data several times a day
C (Compact)	868	Higher data rate version of mode T
N (Narrowband)	169	Long range, narrow band system
R (Frequent Receive)	868	Collector reads multiple meters on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

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

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

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

fréquence	ISM: 868MHz (EU)
création	Sigfox (FR), 2010
débit	< 100 bit/s
usages	télé-relève, transport
propriétés	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 fondeur,
réseaux privés ou publiques

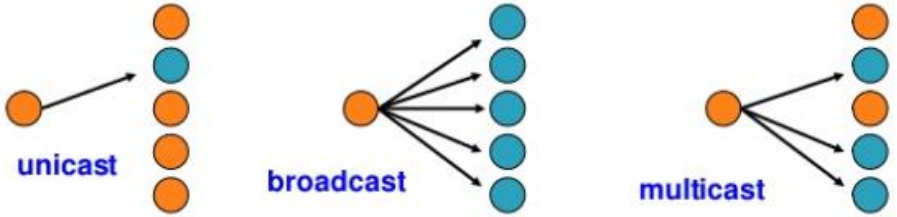
fréquence	ISM: 868MHz (EU)
création	Cycléo (FR) puis Semtech, 2012
débit	0,3 - 50 kbit/s
usages	télé-relève, smart city...
propriétés	low power long range (1 - 15km) communication large bande réseaux privés ou publique (basestation très peu chère) sécurisé (double crypto) bi-directionnel / ack

Transport

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

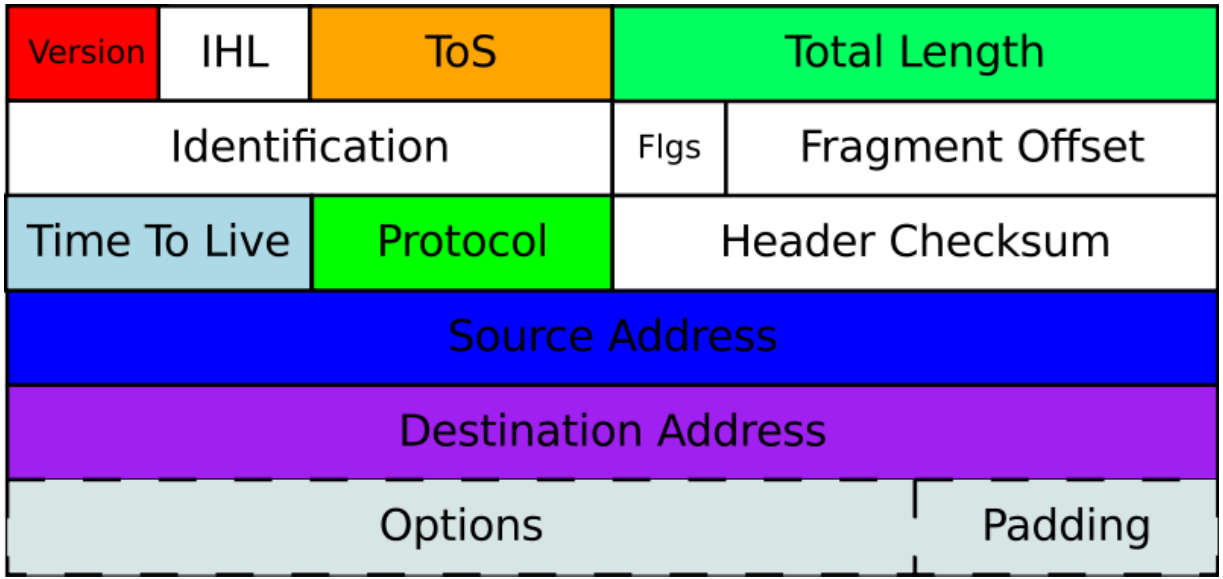


1980 - IPv4:
adresses 32 bits

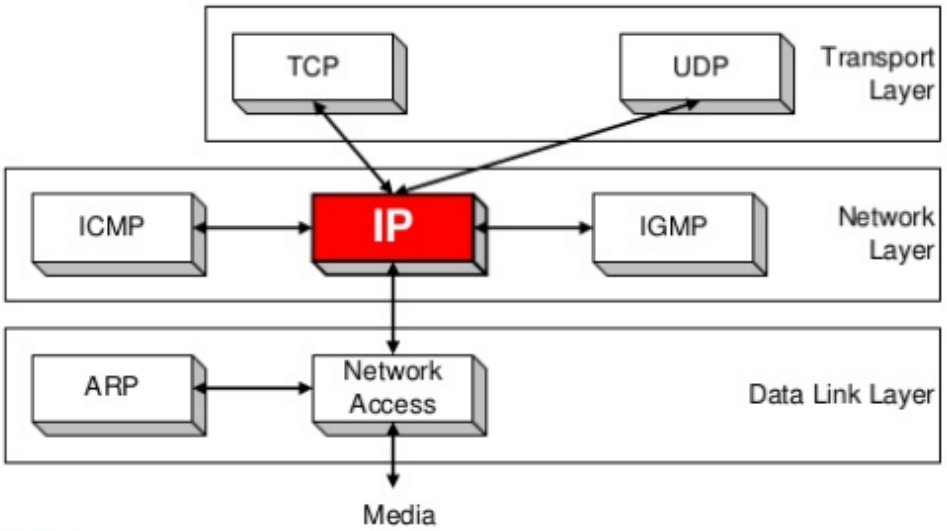
1998 - IPv6 (IETF):
adresses 128 bits, intègre IPSec, optimisations pour réseaux privés

Internet Protocol (IP)

header IPv4:



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 multicase
- **ARP (Address Resolution Protocol)**:
  pour résolution MAC / IP IPv4
  (en IPv6 : NDP = Neighbor Discovery Protocol)

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)	

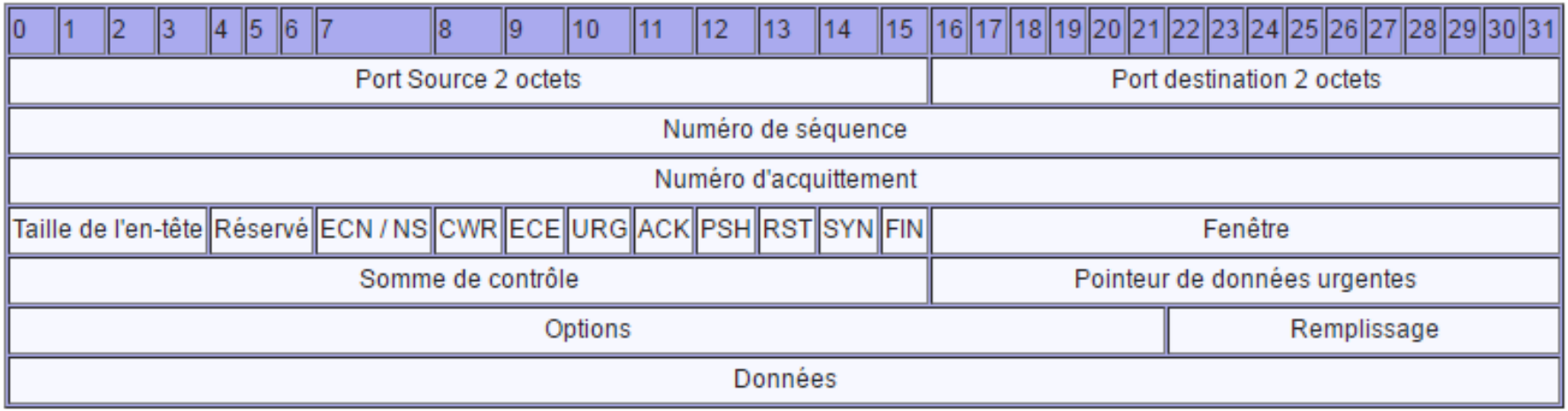
TCP

“Transmission Control Protocol”,
le plus répandu au dessus de IP.

- protocole connecté
- ré-ordonnancement de paquets (“segments”)
- détection de perte / reprise
- contrôle de flux (windowing)

TCP(/IP)

Format d’une trame:



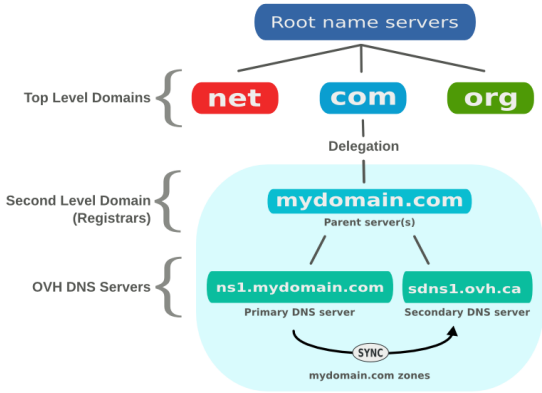
DNS protocol

“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



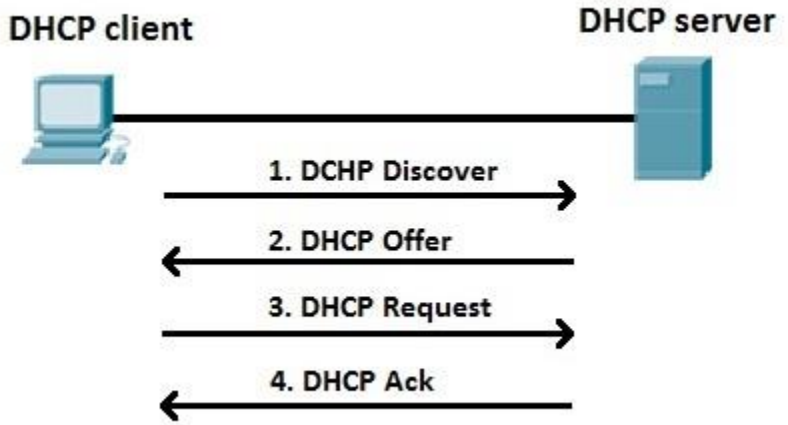
DHCP

"Dynamic Host Configuration Protocol”

Configuration IP dynamique:

- attribution d’une IP
- IP passerelle
- …

Emission / réception en Broadcast IP.

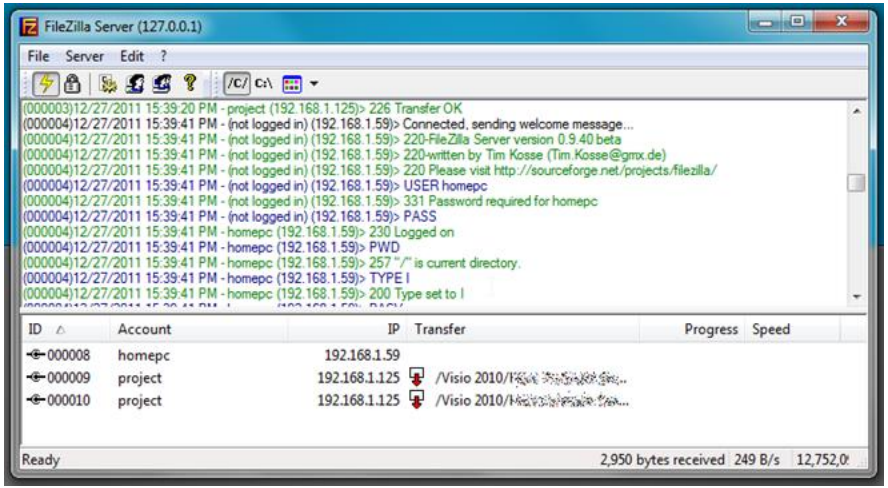


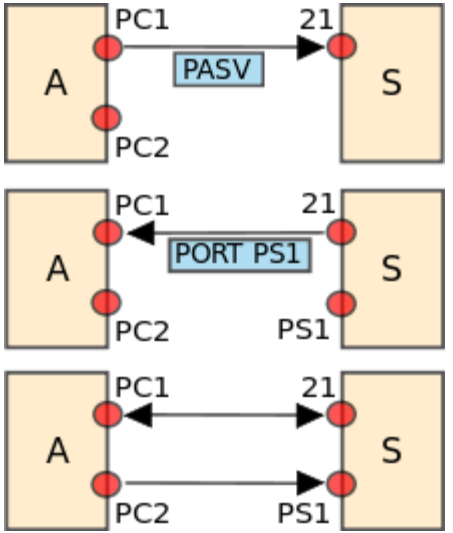
FTP

“File Transfer Protocol”

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

Double connections TCP: contrôle et transfert.





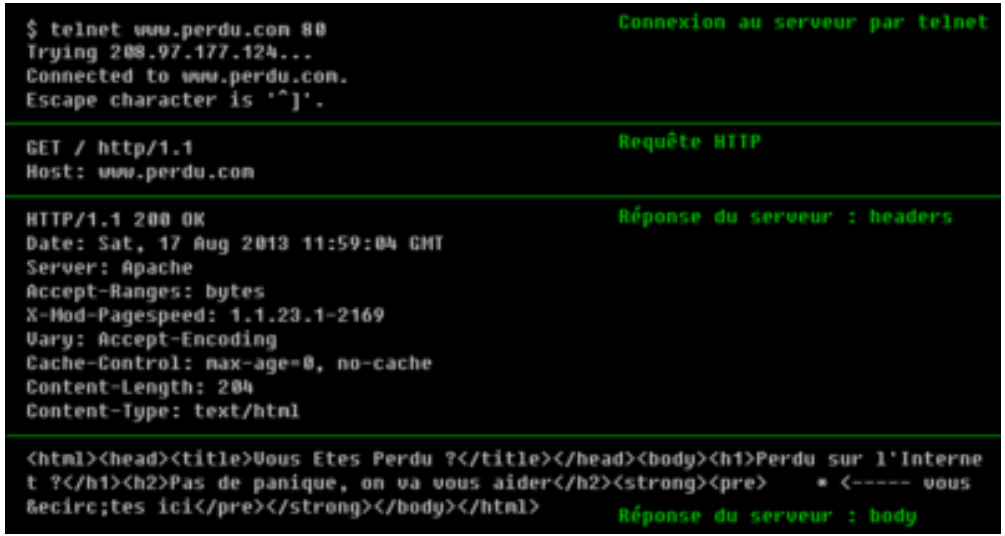
HTTP

“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



RTP / RTSP / RTCP

“Real-Time Transfer Protocol”

Transmission de flux multimédia temps réel.

- RTP: flux unidirectionnel (ex: diffusion satellite)
- RTSP: négociation de flux
- RTCP: contrôle

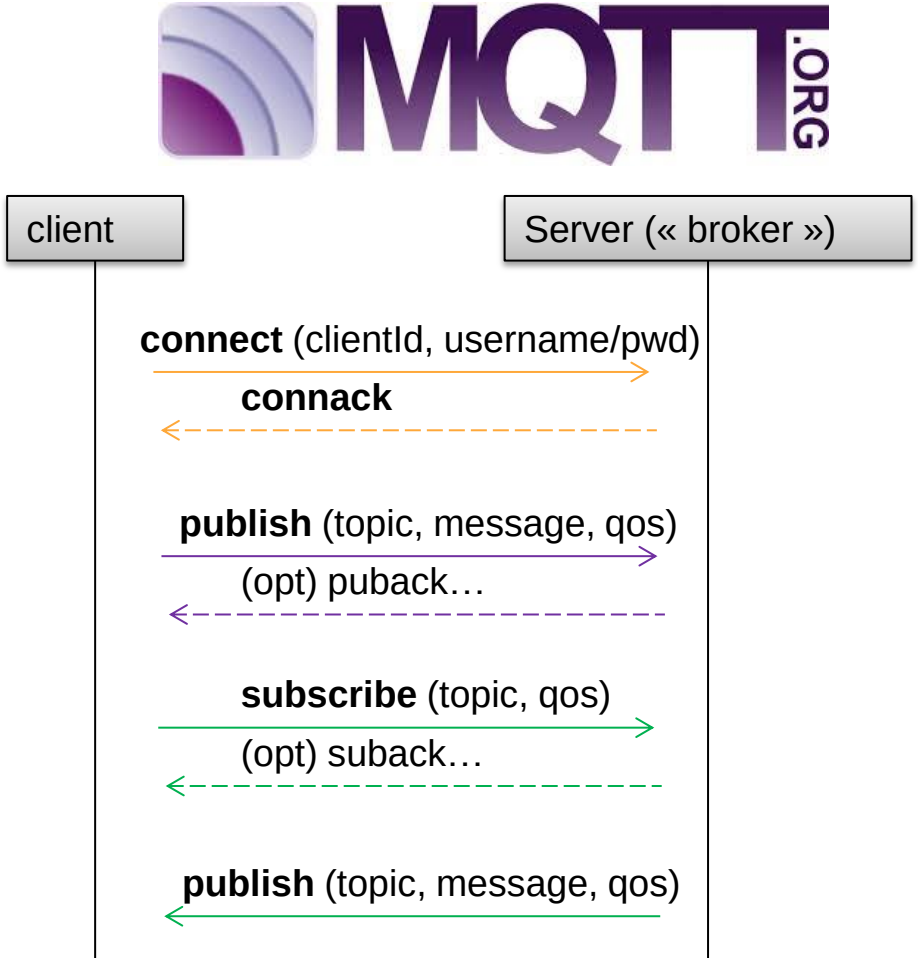
MQTT

“MQ Telemetry Protocol”

Protocole publish/subscribe au dessus de TCP/IP.

authentification clients

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



CoAP

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

Authentification via DTLS.

Mécanisme de Pub/Sub.

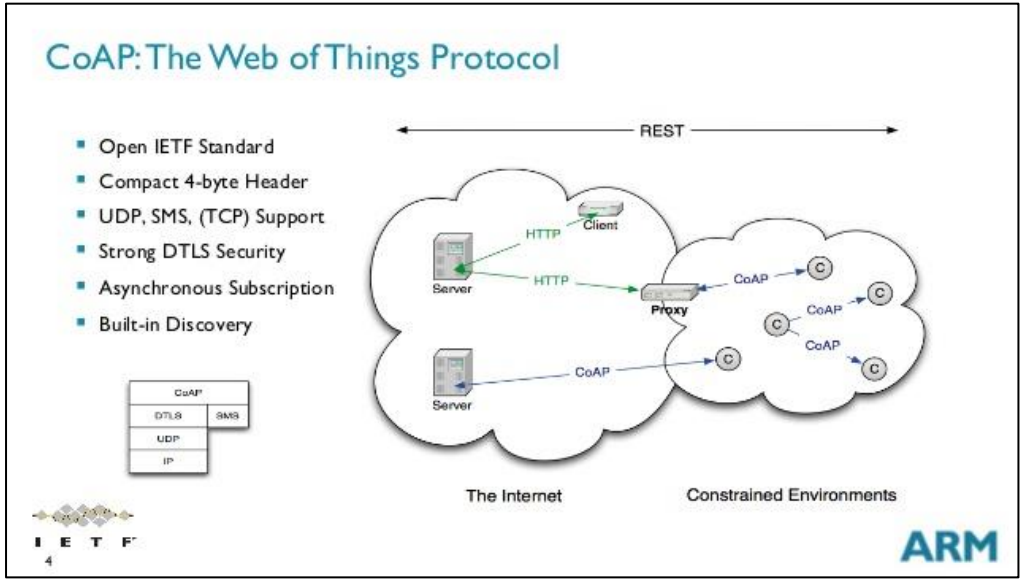


Table 3 Message Format

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	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)…																																

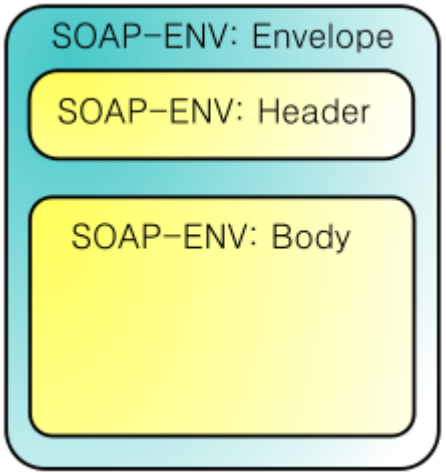
source: http://www.cse.wustl.edu/~jain/cse574-14/ftp/coap/

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.

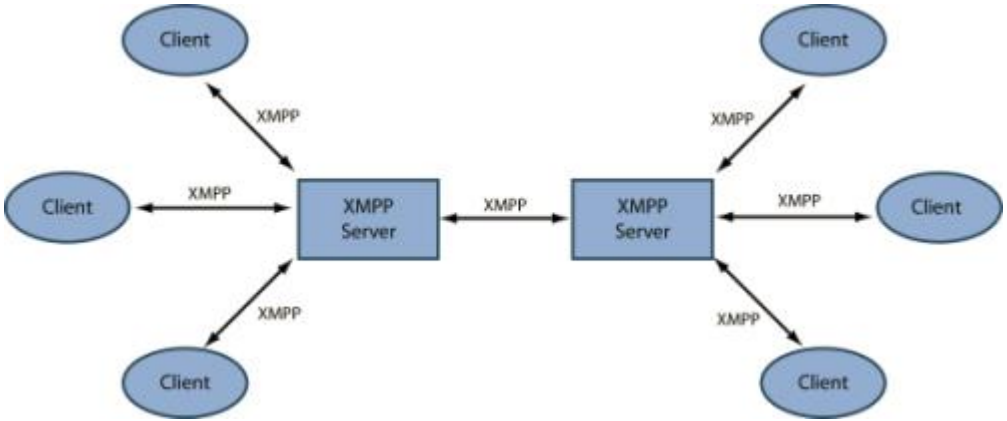


XMPP

“eXtensible Messaging and Presence Protocole”

Protocole de messaging, XML sur TCP.

(Jabber, repris par IETF)



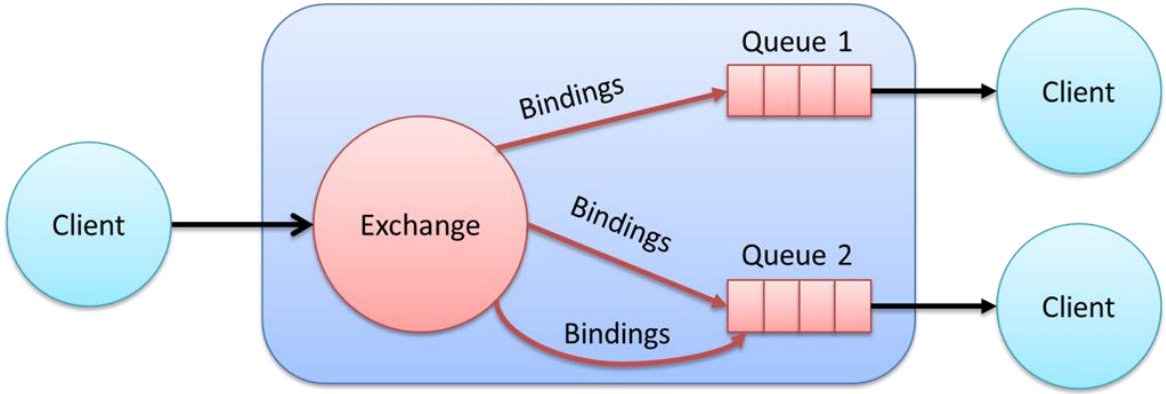
AMQP

“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)



Cryptographie

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 **A**symétrique

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 clée 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**

Certificats cryptographiques - compléments

CSR

« Certificate Signature Request »

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

CRL

« Certificat Revocation List »

Permet de diffuser une liste de certificats « blak listés » (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

Principes

- 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

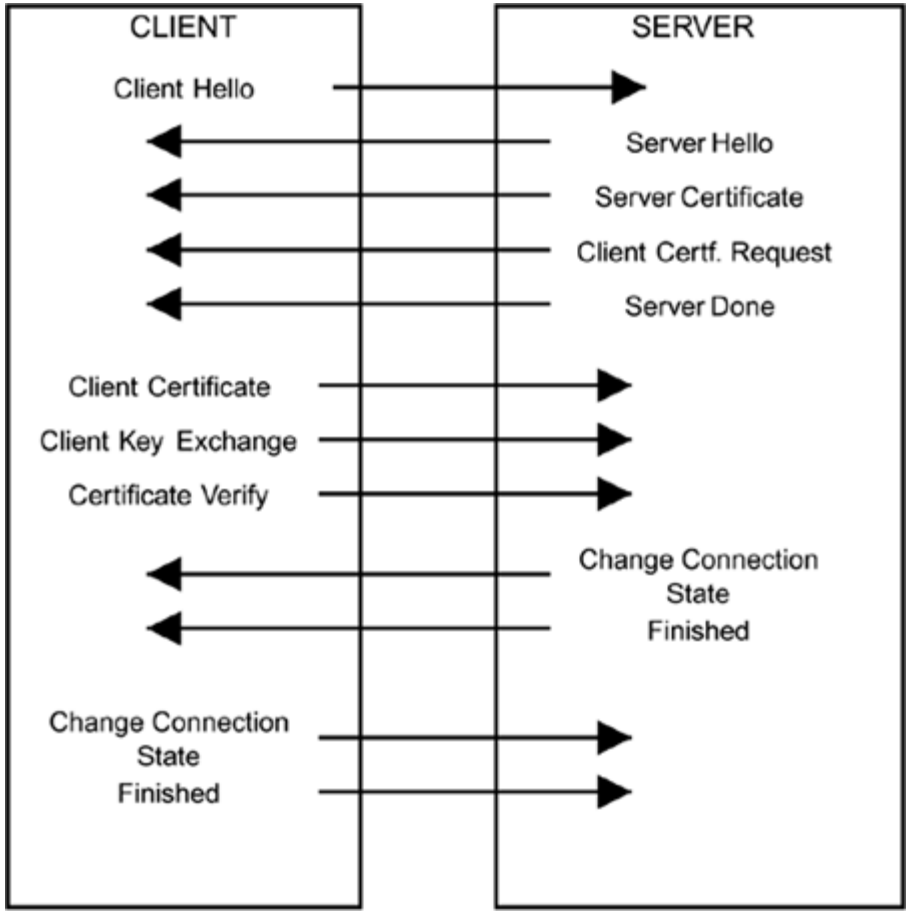
SSL / TLS

« Secure Socket Layer »
(Netscape, 1994)

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

- Authentification (serveur et/ou client)
- Confidentialité
- Intégrité

SSL / TLS


CLIENT
SERVER
Client Hello
Server Hello
Server Certificate
Client Certf. Request
Server Done
Client Certificate
Client Key Exchange
Certificate Verify
Change Connection State
Finished
Change Connection State
Finished

DTLS

« Datagram TLS »: TLS pour UDM/SMS

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

Annexes

Les bandes de fréquence