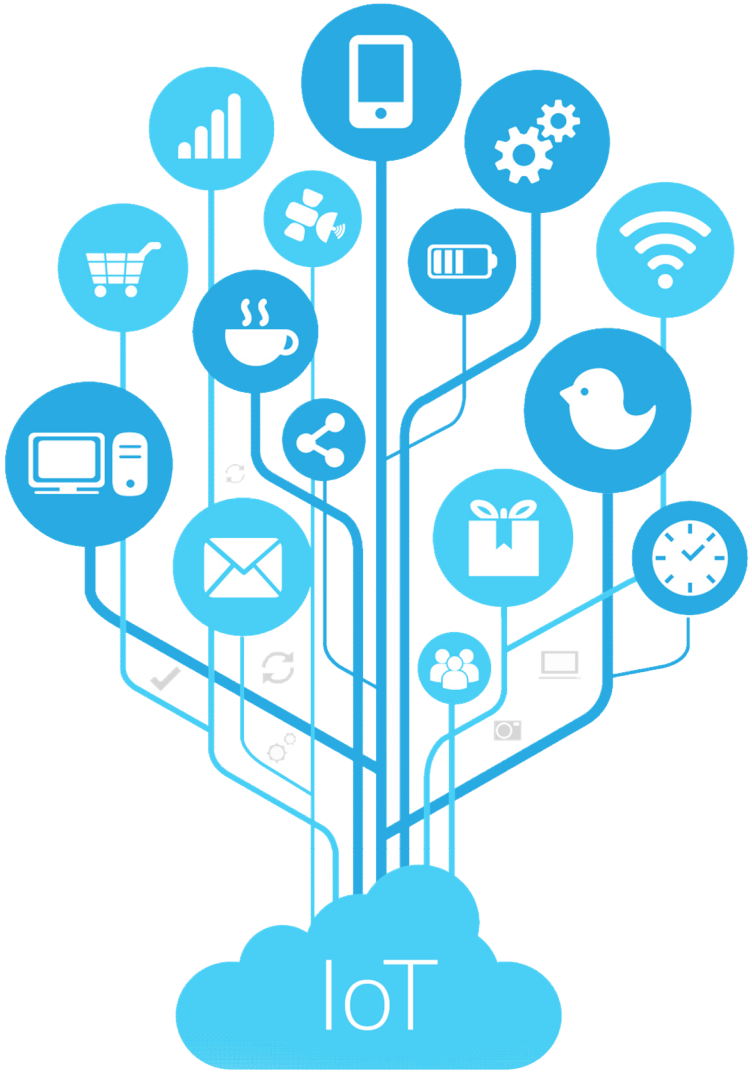


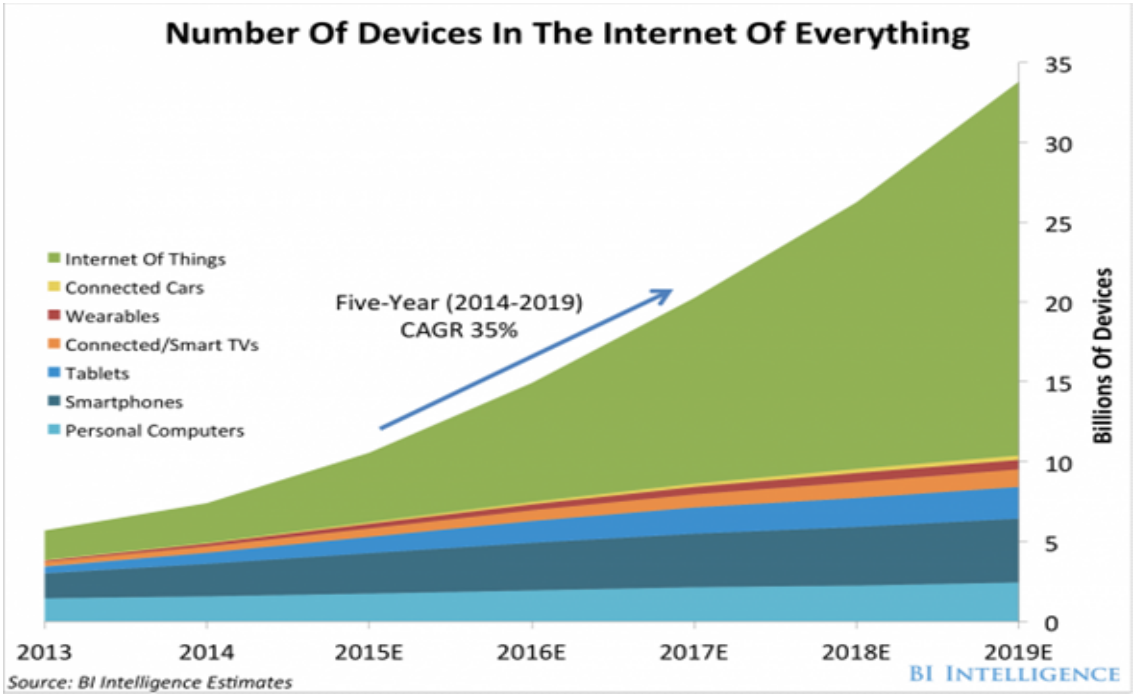
Internet of Things /M2M communication

I. Introduction

1. Motivation

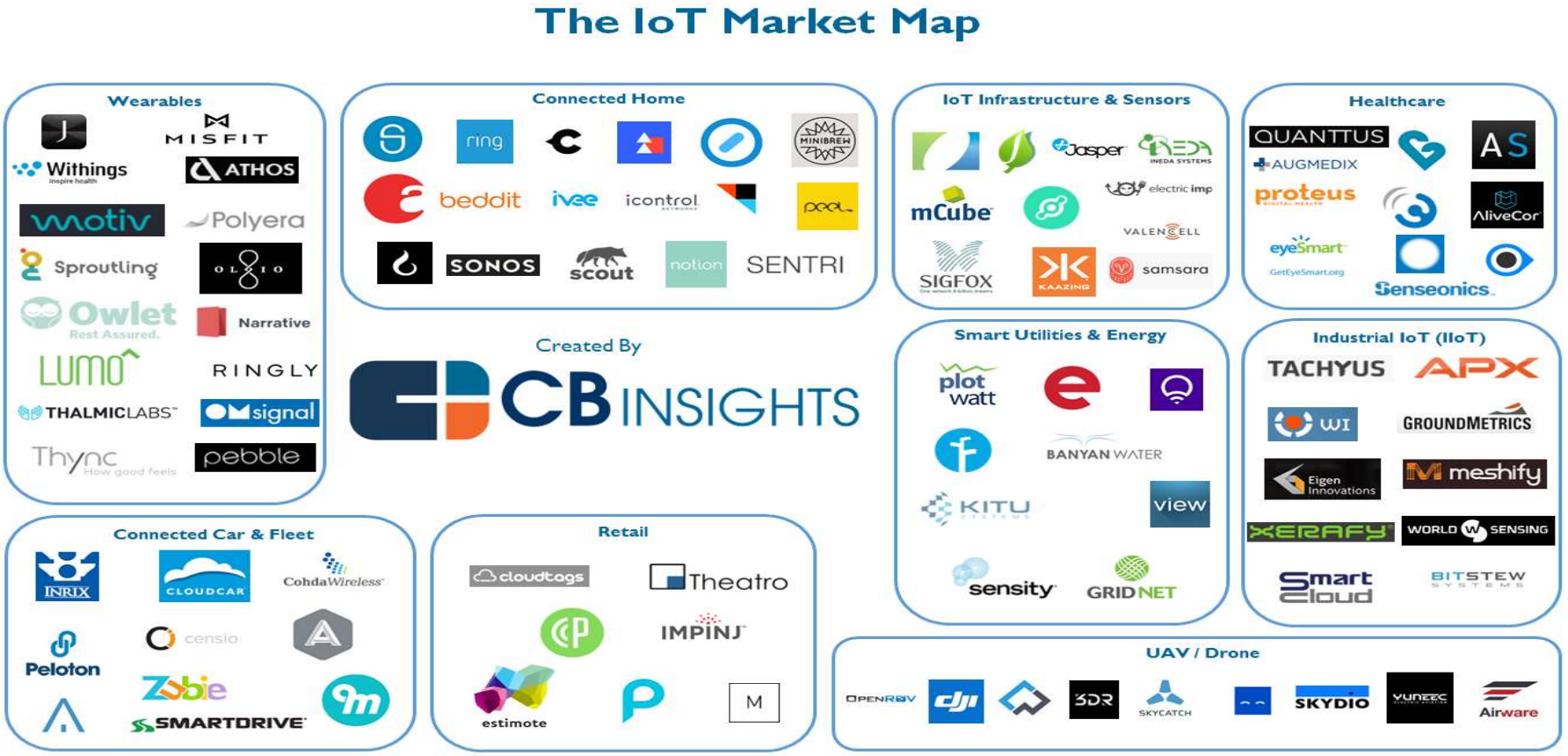
✓ Un marché de dizaine de millier de milliards de dollars dans les années avenir (3000 milliard de dollar en 2020)

✓ Des milliards d'objets connectées dans les années avenir (entre 30 et 50 milliards vers 2020)



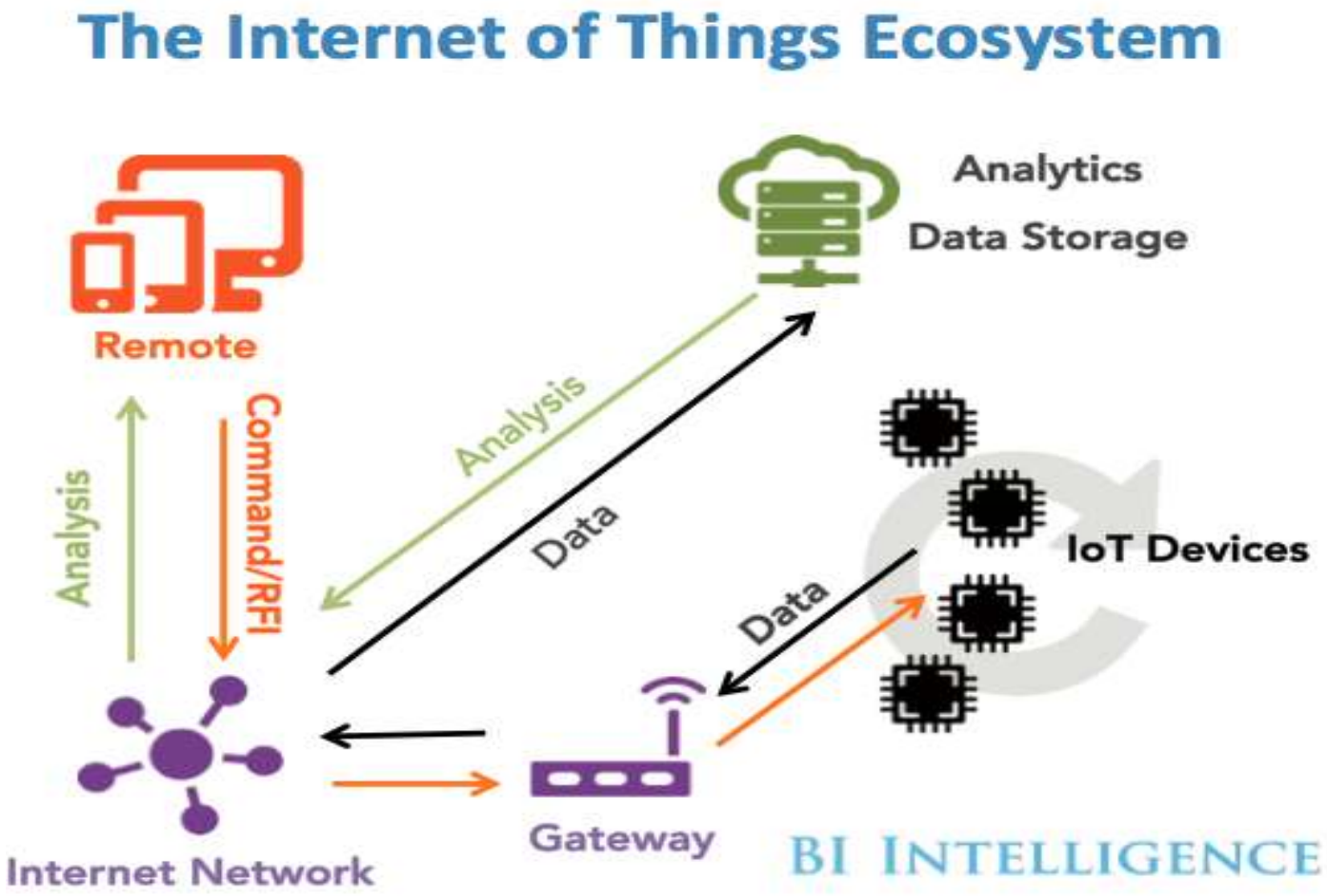
Internet Of Things

2. Marché de l'internet des objets



Quelques start-up couvrant les 9 catégories qui conduisent le future de l'internet des objets

3. Confusion de définition



3. Ecosystème de l'internet des objets

L'internet des objets n'est pas:

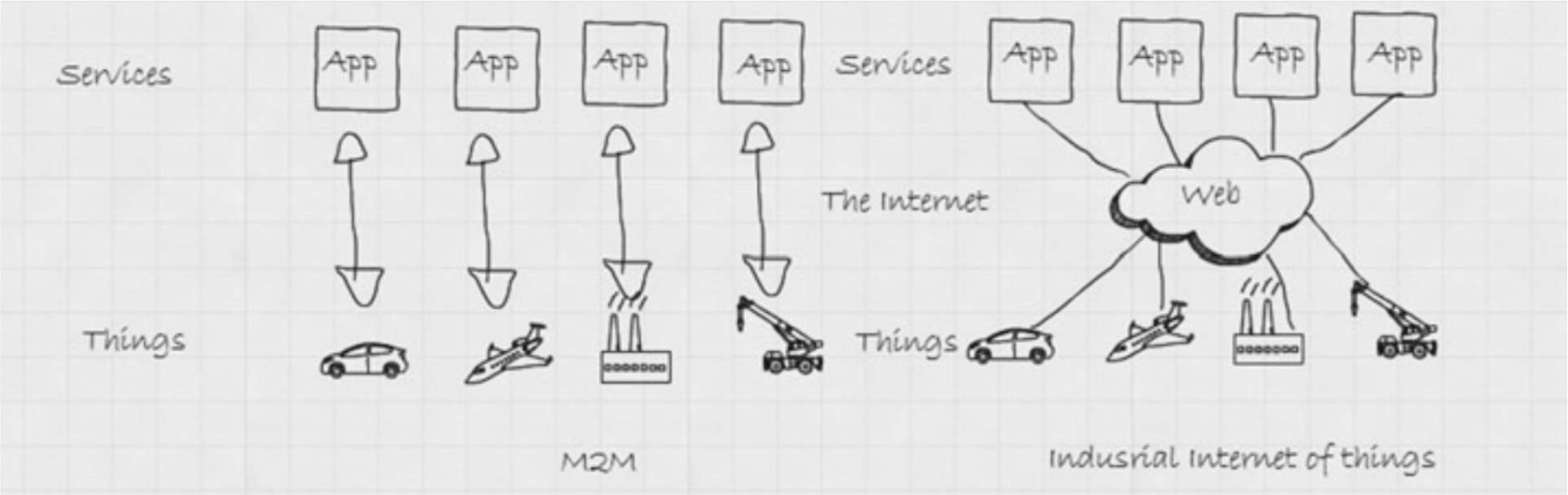
- ✓ WSN (WIRLESS SENSORS NETWORK)
- ✓ BIG DATA
- ✓ Cloud Computing
- ✓ M2M (machine to machine)
- ✓ CPS (Cyber Physical System)

Confusion de définition:

- ❑ Internet des gens et des objet
- ❑ Web of Things (WoT)

❖ Industriel Internet of Things vs M2M

L'industriel internet des objets peut être considérer comme une extension du M2M communication , on a juste ajouté une connexion internet au M2M pour avoir un industriel internet des objets .



❖ L'internet of Things peut être diviser en couches:

- *La première couche* : l'informations sur les objets est codée par *the unique identifiant (UID)* et/ou *electronique product code (EPC),* l'information est stocké dans des Tag RFID et lit a distance par des lecteur RFID.

- *la deuxième couche*: composé des objets ayant une intelligence embarquée (microprocesseur / microcontrôleur) et aussi une capacité de communication sans fil embarquée (wifi, Bluetooth…….) afin de réaliser des fonction de communication des informations et aussi des fonction de contrôles si c possible.

- une autre couche dans laquelle des capteurs plus sophistiqué peuvent être utiliser d'une manière distribuée: *Wirless Sensors Network (WSN)* :

  - collectée des informations sur l'environnement ambiant (température, pression……) , aussi des vidéos et des images de qualité plus ou moins bonne d'une localisation géographique.

  - peuvent réaliser optionnellement un pré-traitement d'une partie ou de l'intégralité de l'information collectée.

  - envoyer ces information vers une site centraliser pour un traitement plus avancé.

II. Les 10 communication sans fils les plus utilisées

1- Wi-Fi

- **Standard**: Basé sur la ***802.11 n*** (utiliser dans les maison)
- **Fréquence**: les bands ***2.4GHz*** et ***5GHz***
- **Porté**: environ 50m
- **Débit de données**: 600Mbps maximum, mais 150-200Mbps est très typique en fonction de nombre d'antenne et la fréquence utilisée, la dernière norme ***802.11–ac*** peut offrir un débit entre 500Mbps et 1Gbps

2- Bluetooth

- **Standard**: Bluetouth v5 core specification
- **Fréquence**: ***2.4GHz*** (ISM)
- **Porté**: dépend du classe pour le classique Bluetooth et peut atteind jusqu'a 150m pour le Smart/BLE bluetooth

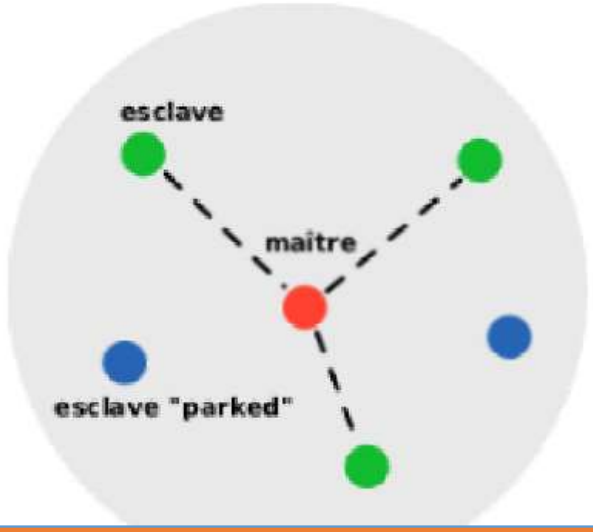
Débit de données: 1Mbps pour le Smart/BLE Bluetooth

❖ Bluetooth: topologie

Reseau piconet:

Un piconet est un réseau qui se crée de manière instantanée et automatique quand plusieurs périphériques Bluetooth sont dans un même rayon (10 m). Ce réseau suit une topologie en étoile : 1 maître / plusieurs esclaves. Un périphérique maître peut administrer jusqu'à 7 esclaves actifs ou 255 esclaves en mode parked (=inactif).

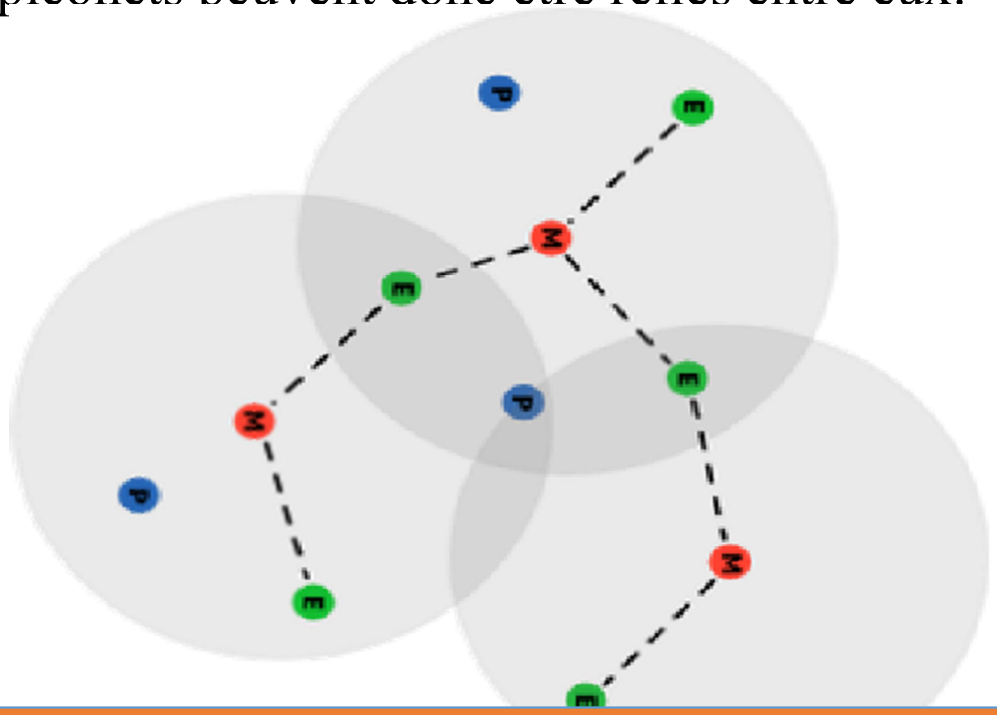
La communication est directe entre le maître et un esclave. Les esclaves ne peuvent pas communiquer entre eux. Tous les esclaves du piconet sont synchronisés sur l'horloge du maître.



❖ Bluetooth: topologie

Reseau scatternet:

Les Scatternets sont en fait des interconnexion de Piconets (Scatter = dispersion). Ces interconnexions sont possibles car les périphériques esclaves peuvent avoir plusieurs maîtres, les différents piconets peuvent donc être reliés entre eux.

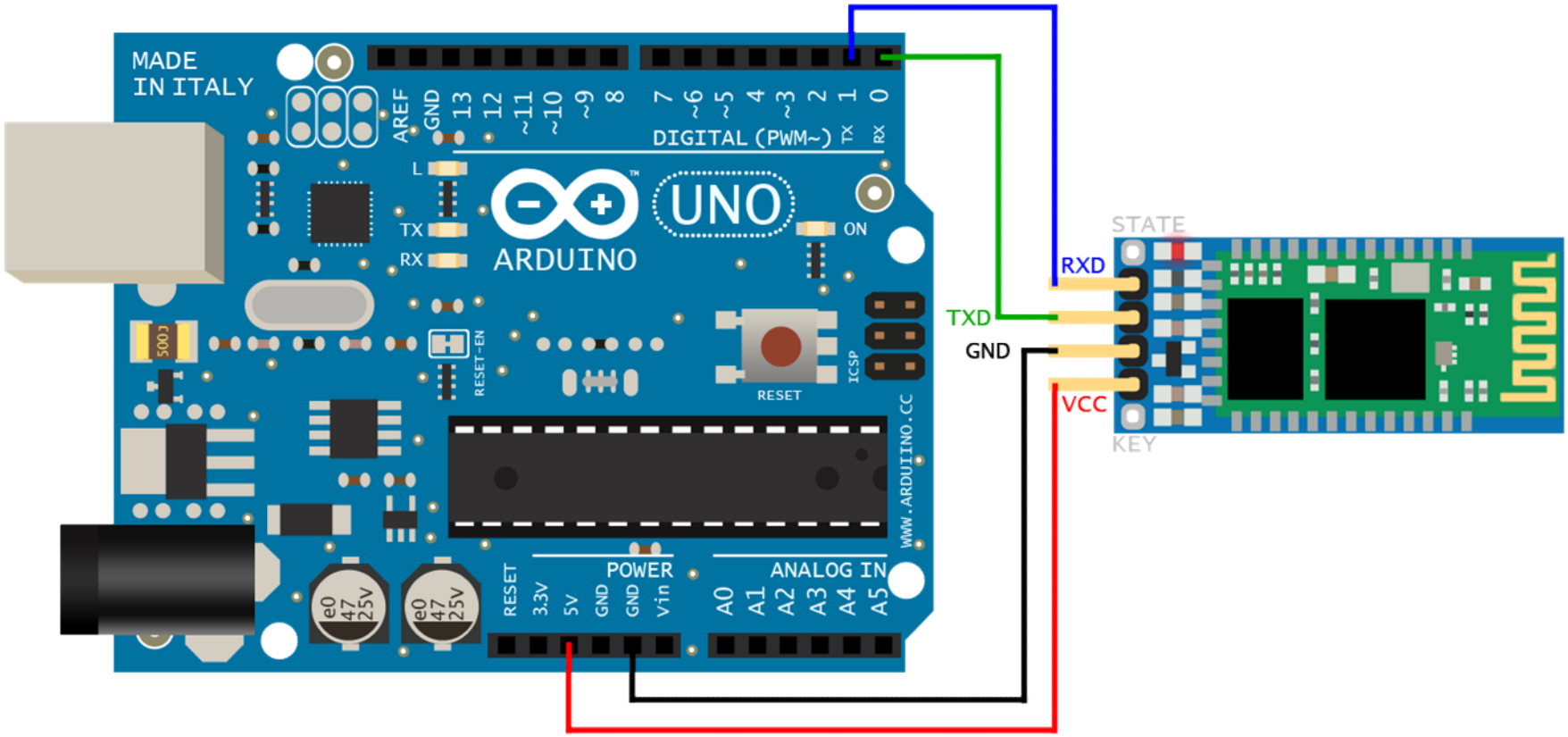


❖ Bluetooth: les classes

Les interfaces Bluetooth peuvent, selon leur puissance d'émission, être associées à trois classes différentes

Classe	Puissance (atténuation en dB)	Portée
Classe 3	1mW (0 dB)	< 10 mètres
Classe 2	2,5mW (4 dB)	10 à 20 m
Classe 1	100 mW (20 dB)	100 m

❖ Bluetooth


MADE
IN ITALY
DIGITAL (PWM~)
UNO
ARDUINO
POWER
ANALOG IN
WWW.ARDUINO.CC
STATE
RXD
TXD
GND
VCC
KEY

3- Zig Bee

- **Standard**: ZigBee 3.0 based on IEEE802.15.4
- **Fréquence**: 2.4GHz et 915MHz pou l'Amérique du nord et 868MHz pour l'europe
- **Porté**: 10m-100m
- **Débit de données**: 250Kbps pour 2.4GHz et 40Kbps pour 915MHz et 20Kbps pour 868MHz

❖ Zig Bee

Ils existent deux gammes de modules, la gamme Xbee « normale » et la gamme Xbee « pro ». Les modules peuvent fonctionner dans deux modes principaux distincts :

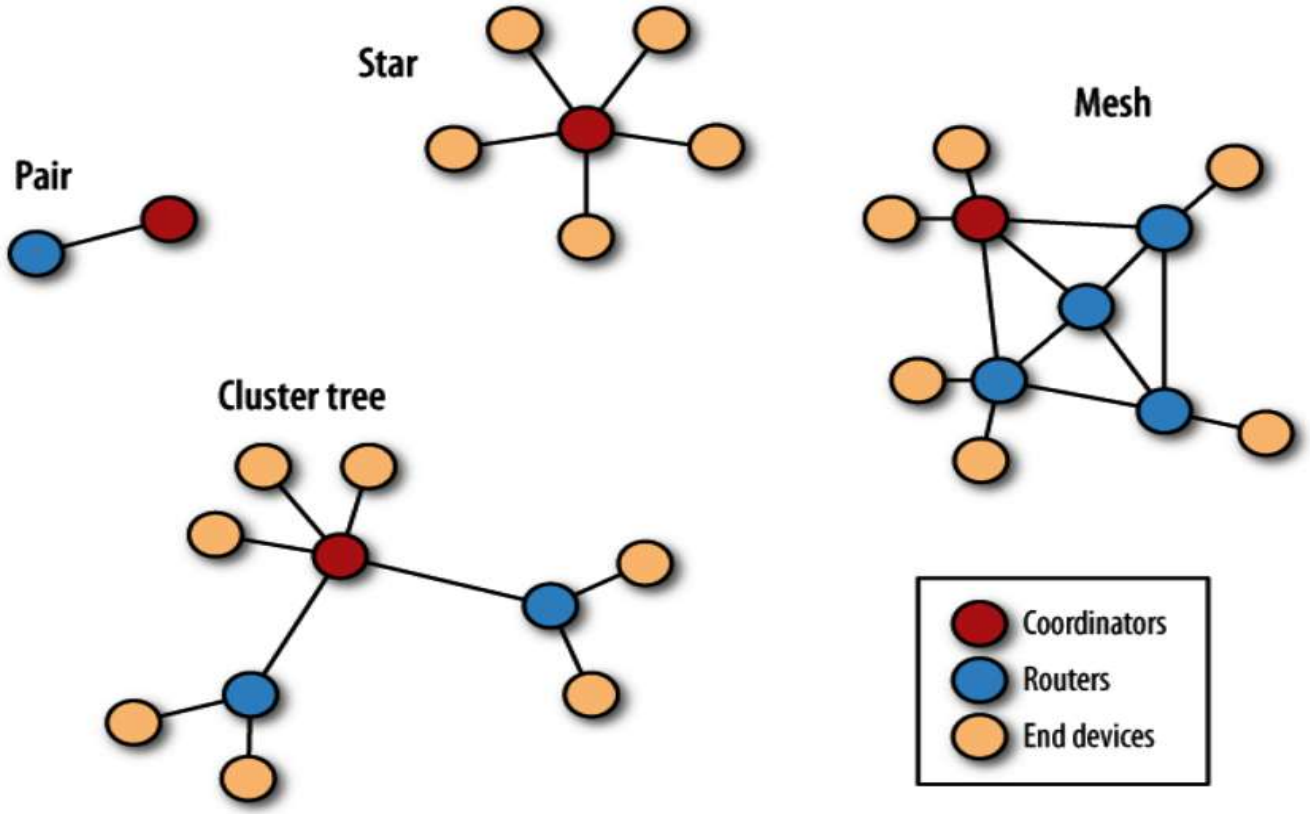
- **le mode transparent** qui permet le remplacement immédiat de n'importe quelle liaison série asynchrone filaire par une liaison radio sans aucune manipulation particulière au niveau des modules Xbee, ce mode peut supporter ou non, au gré de l'utilisateur, la programmation d'un certain nombre de fonctions du modem au moyen de commande dites commandes AT.

- **le mode API** qui permet d'accéder aux possibilités plus fines de mise en réseau des modules mais ne se justifie vraiment que lorsque l'on veut gérer tout un groupe de modules avec des possibilités de diffusion multiple, d'adressage, etc

❖ Zig Bee

- ❑ vitesse maximum de 250 kbits/s et la transmission peut être sécurisée si on le souhaite au moyen d'un algorithme de cryptage de type AES (Advanced Encryption Standard) avec une clé sur 128 bits.
- ❑ Les modules Xbee (série 1) ont une puissance haute fréquence de 1 mW, ce qui leur confère une portée moyenne de 30 m en intérieur et de 100 m en extérieur.
- ❑ les modules Xbee pro voient cette puissance portée à 60 mW (100 m pour l'intérieur et jusqu'à 1 50 m pour l'extérieur)
- ❑ Ces modules s'alimentent sous une tension pouvant varier de 2,8 à 3,4 V.

❖ Zig Bee: réseau



Topologie réseau ZigBee

❖ Zig Bee: réseau

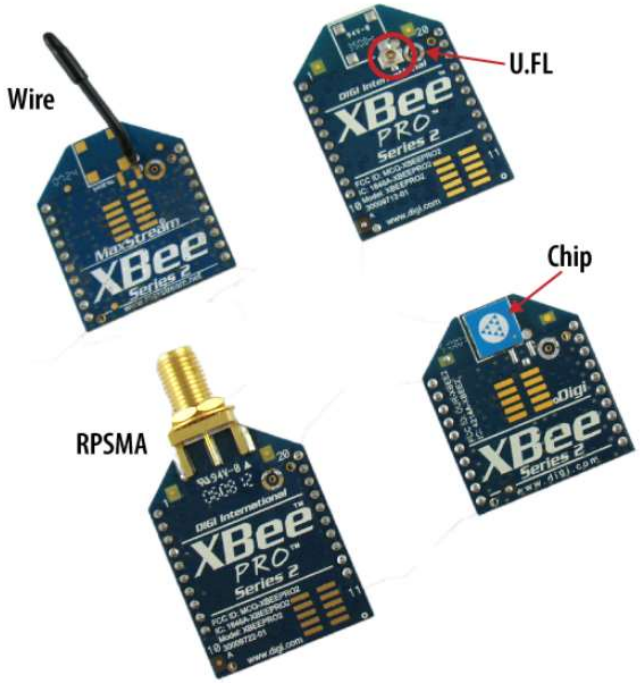
- ❑ Le coordinateur ZigBee (ZC) :
  - ➢ Un et un seul
  - ➢ Tiers de confiance
  - ➢ Racine du réseau et passerelle vers les autres réseaux
  - ➢ Alimentation permanente

- ❑ Le routeur ZigBee (ZR) :
  - ➢ Equipement intermédiaire
  - ➢ Qui route les paquets au sein du réseau
  - ➢ Alimentation permanente

- ❑ L'équipement terminal Zigbee (ZED)
  - ➢ Ne communique qu'avec un routeur ou le coordinateur
  - ➢ Endormi la plupart du temps

❖ Zig Bee :Antenne

- **wire** : simple, radiations omnidirectionnelles ;
- **chip** : puce plate en céramique, petite, transportable (pas de risques de casser l'antenne), le signal est atténué dans certaines directions
- **U.FL** : une antenne externe n'est pas toujours nécessaire;
- **RPSMA** : plus gros que le connecteur U.FL, permet de placer son antenne à l'extérieur d'un boîtier



4- Z-wave

- **Standard**: Z-Wave Alliance ZAD12837 / ITU-T G.9959
- **Fréquence**: 900MHz(ISM)
- **Porté**: 30m
- **Débit de données**: 9.6/40/100kbps

5- NFC (Near Field Communication/ Communication en Champs Pro

- **Standard**: ISO/IEC 18092 / ECMA-340—*Near Field Communication Interface and Protocol-1* (NFCIP-1)

  - ISO/IEC 21481 / ECMA-352—*Near Field Communication Interface and Protocol-2* (NFCIP-2)

  Compatible RFID ISO18000-3

- **Fréquence**: 13,56MHz(ISM)
- **Porté**: 10cm
- **Débit de données**: 100-240kbit/s

6 - 6LowPAN

Une technologie IP clé (Internet Protocol) :
6LowPAN (IPv6 réseau personnel sans fil à faible puissance). Plutôt que d'être une technologie de protocole d'application IoT comme Bluetooth ou ZigBee, 6LowPAN est un protocole réseau qui définit l'encapsulation et les mécanismes de compression d'en-tête. La norme a la liberté de bande de fréquence et de couche physique et peut également être utilisé sur plusieurs plates-formes de communication, y compris Ethernet, Wi-Fi, 802.15.4 et ISM sub-1GHz..

- **Standard**:RFC8262
- **Fréquence**: Adapté et utilisé par d'autre reseau (Zigbee, Smart Bluetooth, ……)
- **Porté**: N/A
- **Débit de données**: N/A

7- Cellular

- **Standard**: GSM/GPRS/EDGE (2G), UMTS/HPSA (3G), LTE(4G)
- **Fréquence**: ***900/1800/1900/2100 MHz***
- **Porté**: 35Km max pour le GSM , 200Km max pour HSPA
- **Débit de données**: 35-170Kps (GPRS), 120-384Kbps(EDGE), 384Kps-2Mps (UMTS), 600Kps-10Mbps(HSPA) , 3-10Mbps (LTE)

8- LoRa WAN

- **Standard**: LoRaWAN
- **Fréquence**: Variables
- **Porté**: 2-5km dans un environnement urbain et jusqu'à 15Km dans un environnement sub-urbain
- **Débit de données**: 0,3-50Kbps

9- SIGFOX

- **Standard**: SigFox
- **Fréquence**: 868 MHz en Europe (ISM)/ 902MHz en Amérique du nord/ 920MHz en Amérique du sud , australie.
- **Porté**: 30-50km environnement rural, 3-10Km environnement urbain
- **Débit de données**: 10-1Kbps

10- Neul

- **Standard**: Neul (weightless standard)
- **Fréquence**: 900MHz (ISM), 458MHz (UK), 470-790MHz (White Space)
- **Porté**: 10Km
- **Débit de données**: Quelques bite par seconde jusqu'à 100kbps

Complément:

- **ZigBee Ip:** zigBee supportant l'IPv6, il incorpore des technologie tel que 6LoWPAN et RPL (NB: ZigBee standard et ZigBee Ip ne peuvent pas coexister dans le même reseau , il faut utiliser une passerelle entre les deux).

- **Wi-Fi Backscatter:** permet d'alimenté les composants passive de l'internet de objets garce au ondes wi-fi issue d'un routeur par exemple

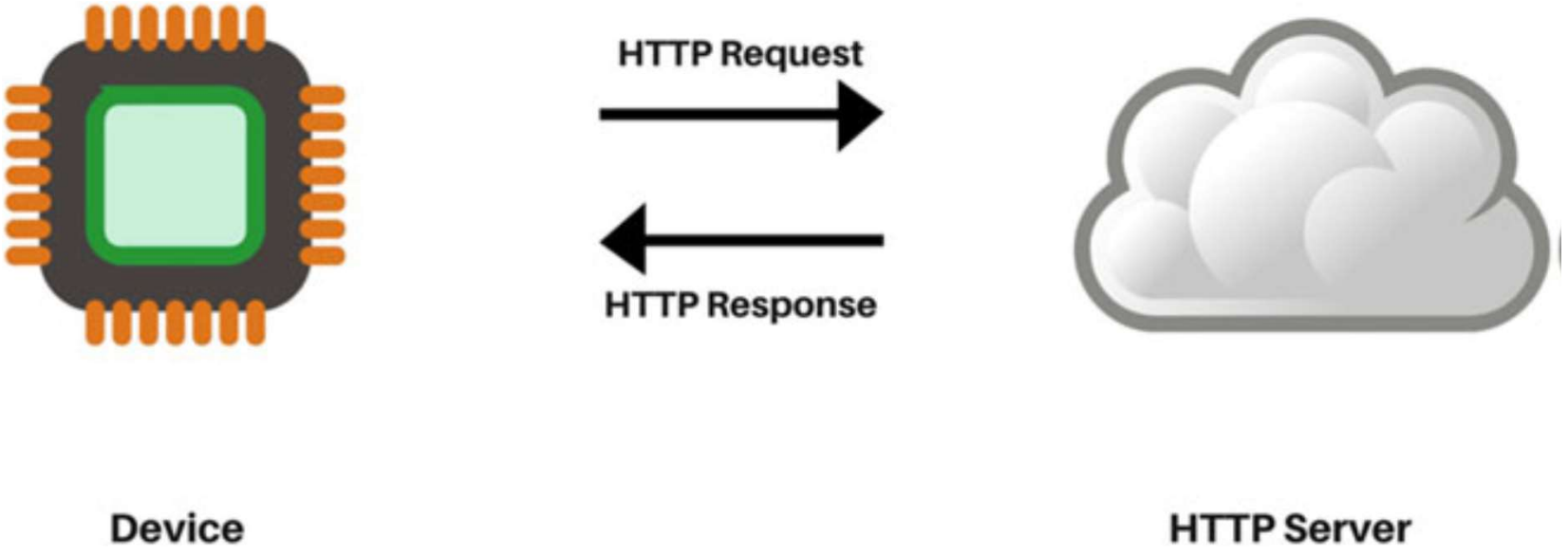
- **Thread:** il se base sur IPv6 et 6LopWan pour une compatibilité avec les derniers standards de l'Internet des objets. but :Harmoniser la connexion des objets entre eux dans les Smart Home

- **RPL**

III. Protocole de communication

1. HTTP:

Ceci est de loin le protocole le plus répandu. Il est largement accepté par les serveurs et soutenu par les normes Internet a moins de problèmes de compatibilité. Il mappe aussi naturellement avec les API RESTful. Cependant, il souffre d'une surcharge importante sous forme d'en-têtes HTTP et le format basé sur du texte. Il est apatride en dépit d'être exécuté sur le dessus de TCP. Cela le rend impropre à l'utilisation en temps réel. Le client doit envoyer une demande en vue d'obtenir une réponse (commande) à partir du serveur. Client doit garder interrogation pour les mises à jour à partir du serveur.



1. HTTP:

❑ Pourquoi le HTTP n'est pas suffisant:

- ✓ Un seul modèle simple: envoyer une demande, lire la réponse
- ✓ Disponible via toute tablette, ordinateur portable, téléphone, ordinateur, etc.

❑ L'Internet des objets a fondamentalement différents défis

- ✓ HTTP reste idéal pour demander des données à partir d'un source connue
- ✓ Nous avons également besoin d'un paradigme axé sur les événements:

  - ➢ Émettre des informations de un à plusieurs
  - ➢ Ecoute des événements quand ils se produisent
  - ➢ La distribution de paquets de données minimales en grand volumes
  - ➢ Pousser l'information sur les réseaux peu fiables

2. CoAP (Application Protocol contrainte) :

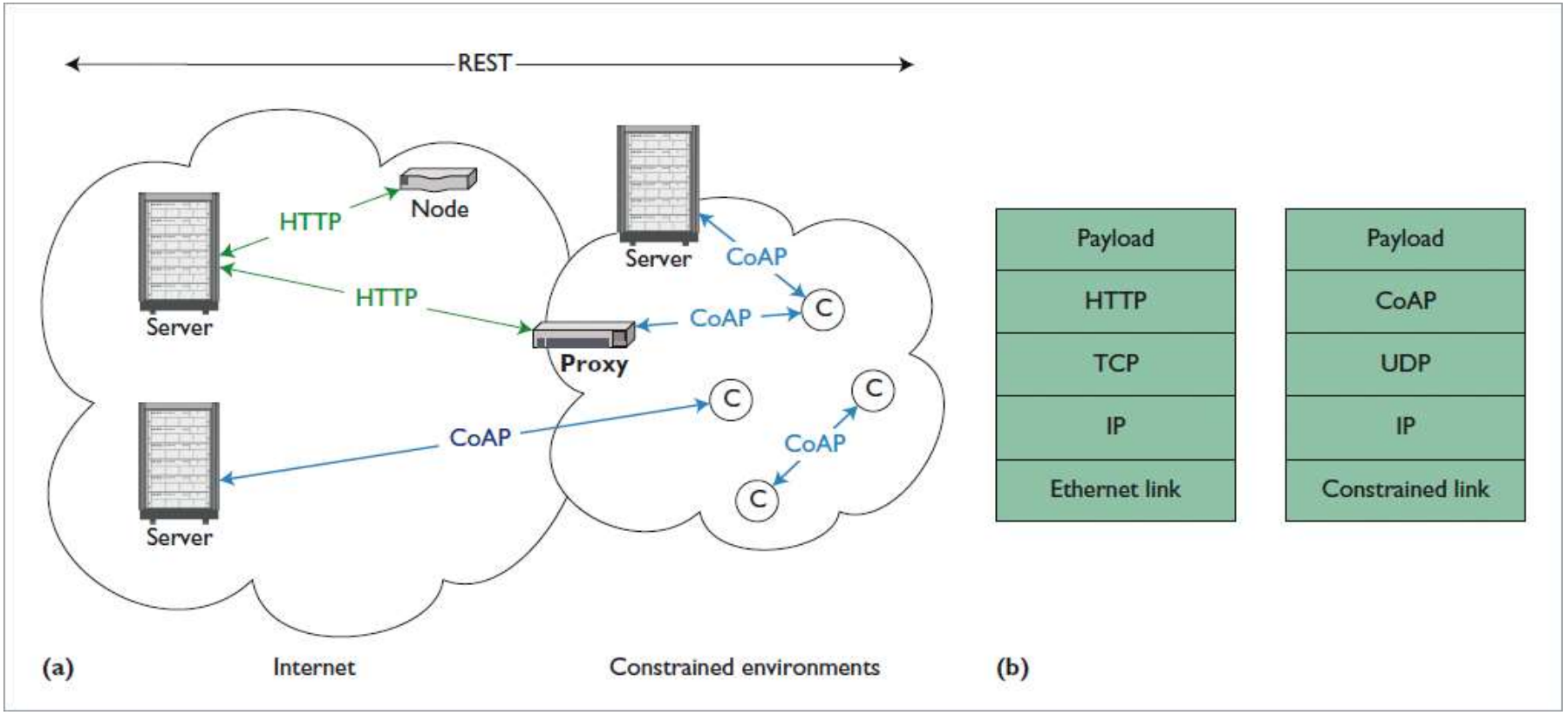
est un simple protocole du couche application, destiné à être utilisé dans des dispositifs électroniques très simples, leur permettant de communiquer de façon interactive sur Internet. Il est particulièrement ciblé pour les capteurs petits, de faible puissance(WSN), des commutateurs, des vannes et des composants similaires qui doivent être contrôlés ou surveillés à distance, par le biais des réseaux Internet standard.

il peut être considérée comme version binaire du protocole HTTP. Il améliore certaines limitations sur HTTP. CoAP n'est pas seulement confiné au réseau de proximité et il est plus souvent utilisé en tant que solution complète de bout en bout connectant des serveurs avec des périphériques de nœud final

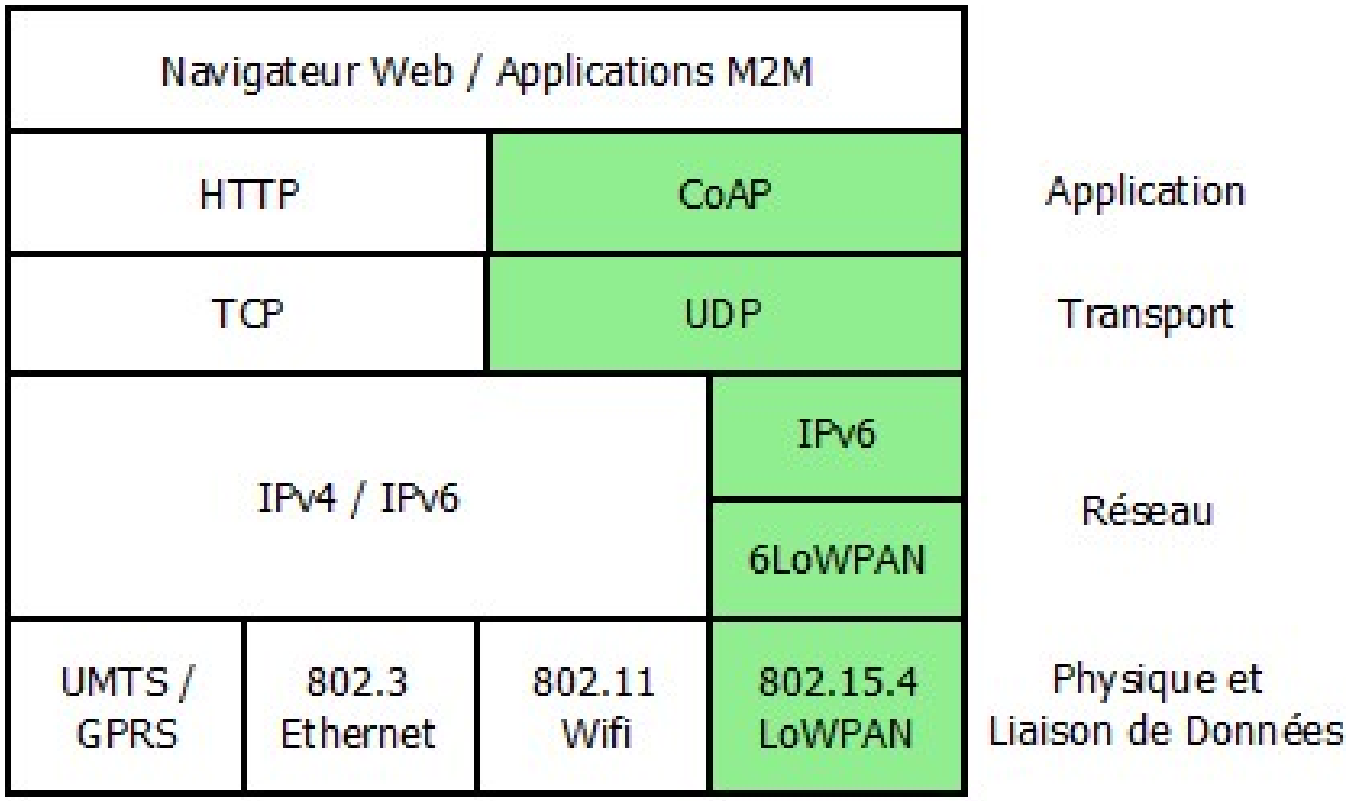
2. CoAP(Application Protocol contrainte):

- ✓ RFC 7252
- ✓ CoAP est un protocole spécialisé de transfert web pour une utilisation avec des nœuds contraints, et des réseaux contraintes (faible puissance, l) dans le IoT.
- ✓ Pour être utiliser sur des réseaux de faible puissance et faible bande passante, CoAP n'utilise pas TCP ou autre protocole de transport complexe, il utilise UDP
- ✓ il est designer pour des application Machine-to-Machine (M2M) comme la smart energy, building automation
- ✓ Les constrained nodes (nœud contraint) : souvent des microcontrôleur 8bits avec des petits capacité de mémoire RAM et ROM
- ✓ Les paquets CoAP peuvent être facilement convertis en paquets HTTP
- ✓ Il est facile d'integrer CoAP et HTTP via un proxy pour passer d'un constrained network vers un réseau a grande bande passante (WAN, LAN)

1. CoAP(Application Protocol contrainte):

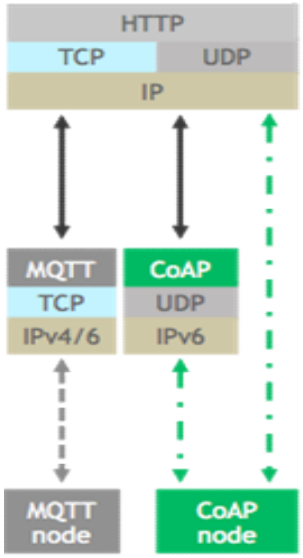


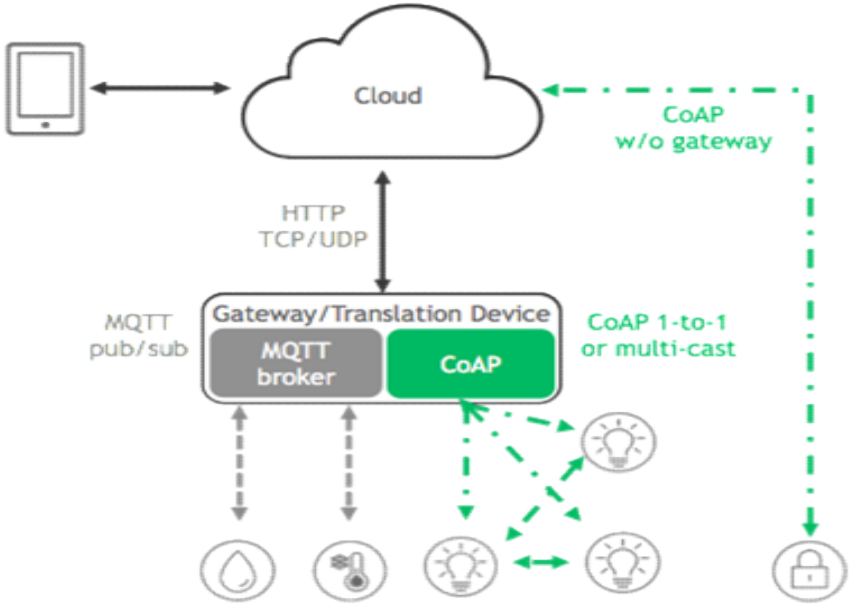
1. CoAP(Application Protocol contrainte):



1. CoAP(Application Protocol contrainte):

Une combinaison légère très commune est de combiner CoAP avec 6LoWPAN, qui est une version légère de l'IPv6, et le protocole MQTT, pour fournir un rendement très efficace de communications de bout en bout sur un réseau IPv6. Cela le rend idéal pour Cas d'utilisation IIoT





Le Modèle Publish /subscribe

- ✓ Une application peut s'inscrire au service publisher dont elle intéressée, ce qui réduit le Traffic non nécessaire
- ✓ Publish/subscribe protocole peut superviser un ou un ensemble de capteur et publié tous changement dans leur status aux souscripteur enregistrés
- ✓ un publisher ne nécessite pas une connexion 24h/4j au broker
- ✓ Un subscriber ne doit pas être en ligne toujours pour recevoir des notification, le broker va enregistrer les données des publisher jusqu'au moment de connexion du subscriber

Le Modèle Publish /subscribe

Les protocole basées sur le modèle Publish/subcribe les utilisé actuellement:

- ✓ MQTT
- ✓ XMPP
- ✓ AMQP
- ✓ DDS

3. **MQTT** (Message Query telemetry Transport)

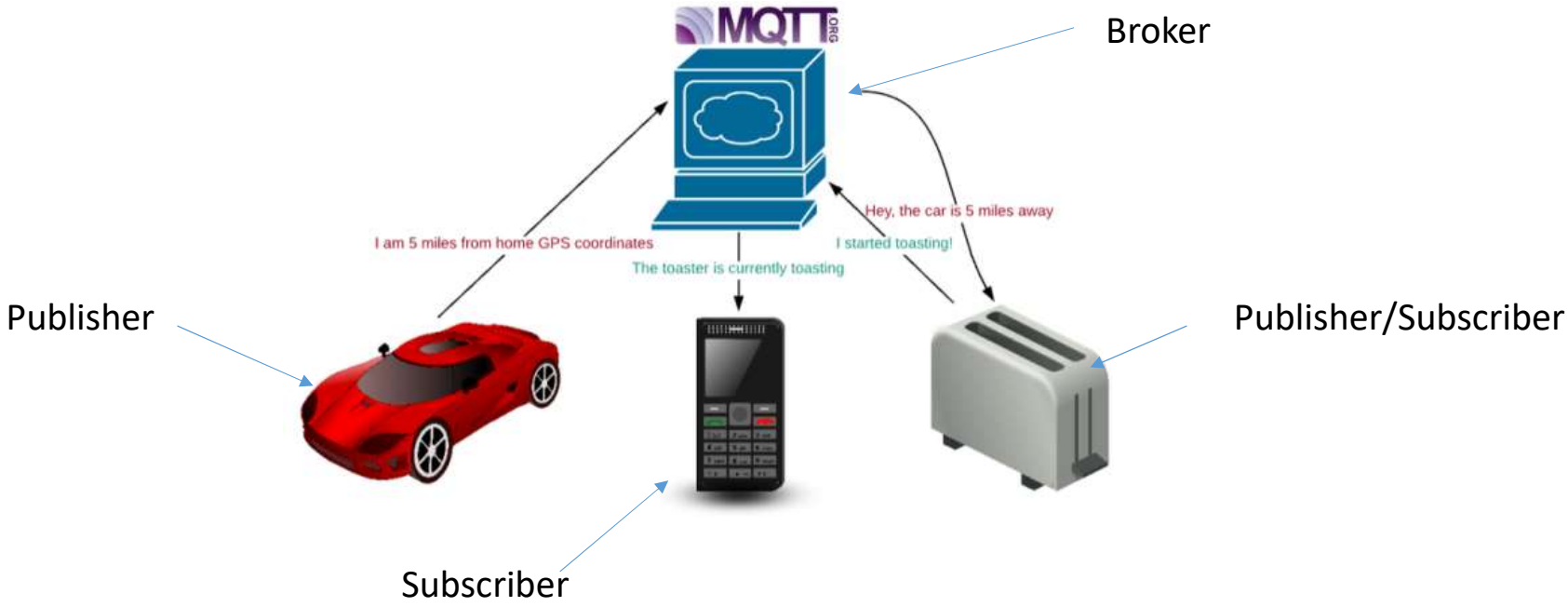
MQTT est un protocole machine to machine (M2M) utilisé pour l'IoT (Internet des objets). Il a été conçu pour être très léger et pour utiliser une bande passante réseau minime.

- MQTT est un service de messagerie TCP/IP simple
- Les messages sont envoyés par des publieurs (publishers) sur un canal (une chaîne d'information) appelé Topic. Ces messages peuvent être lus par les souscripteurs (subscribers) qui surveillent certains Topics.
- Un serveur (Broker) se charge de faire la liaison entre les publieurs et les souscripteurs.
- On peut évidemment installer un Broker sur une Rasspberry Pi, par exemple Mosquitto.

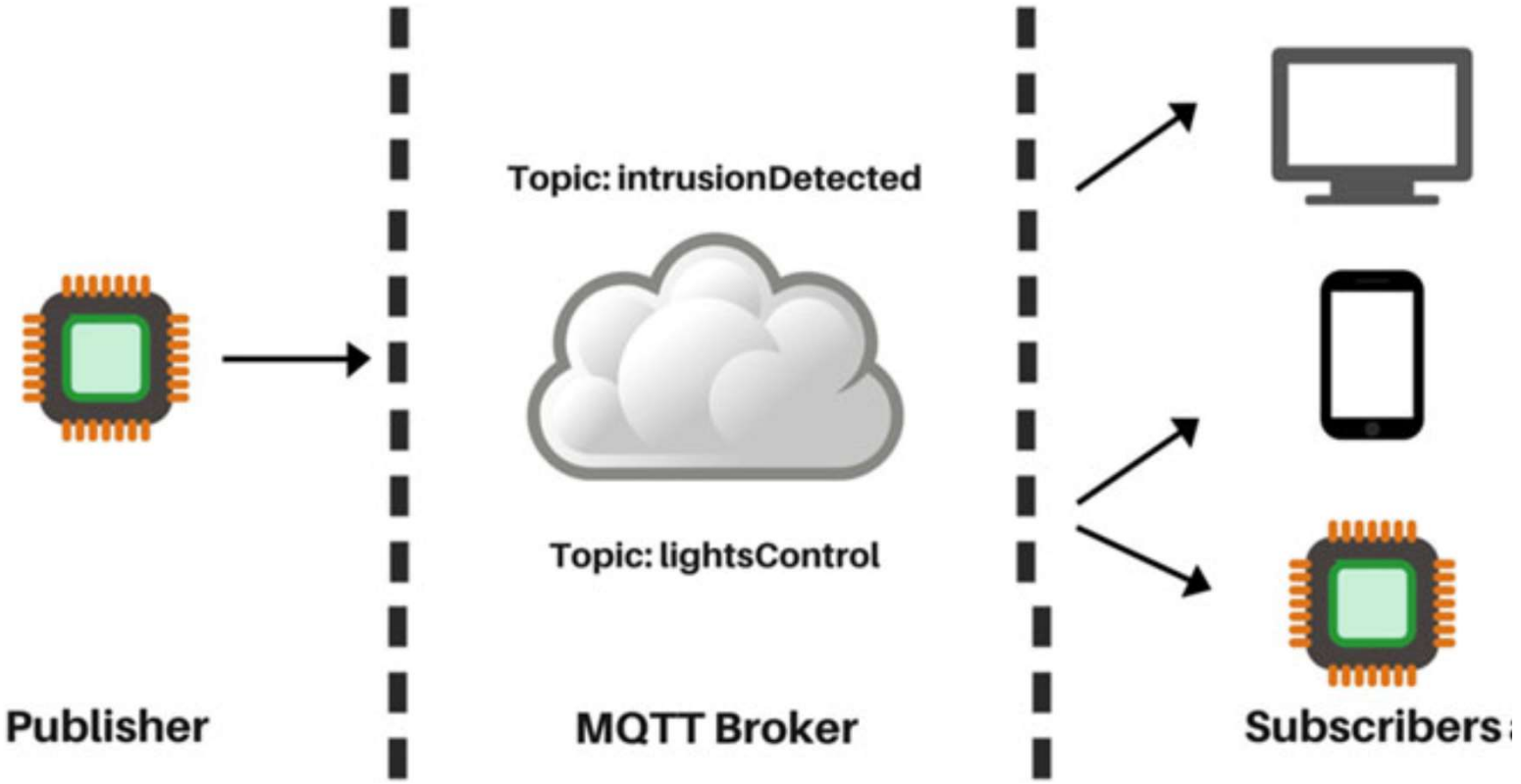
Exemple: Par exemple, le topic /sensor/temperature/salon ne me donnera que les températures du salon si je m'y abonne (et ma sonde de température dans le salon publiera sur le topic sa valeur régulièrement).
Je pourrais aussi m'abonner au topic /sensor/temperature/# pour avoir toutes les températures, ou au topic /sensor/# pour avoir toutes les remontées des sondes

3. MQTT (Message Query telemetry Transport)

Courtier MQTT(broker):
Pour utiliser le service MQTT, nous devons nous inscrire à l'un des courtiers MQTT (Broker). MQTT Broker est un système qui agit comme un concentrateur (hub) centralisé pour tous les périphériques qui publient des données et les périphériques qui souhaitent s'abonner aux données.

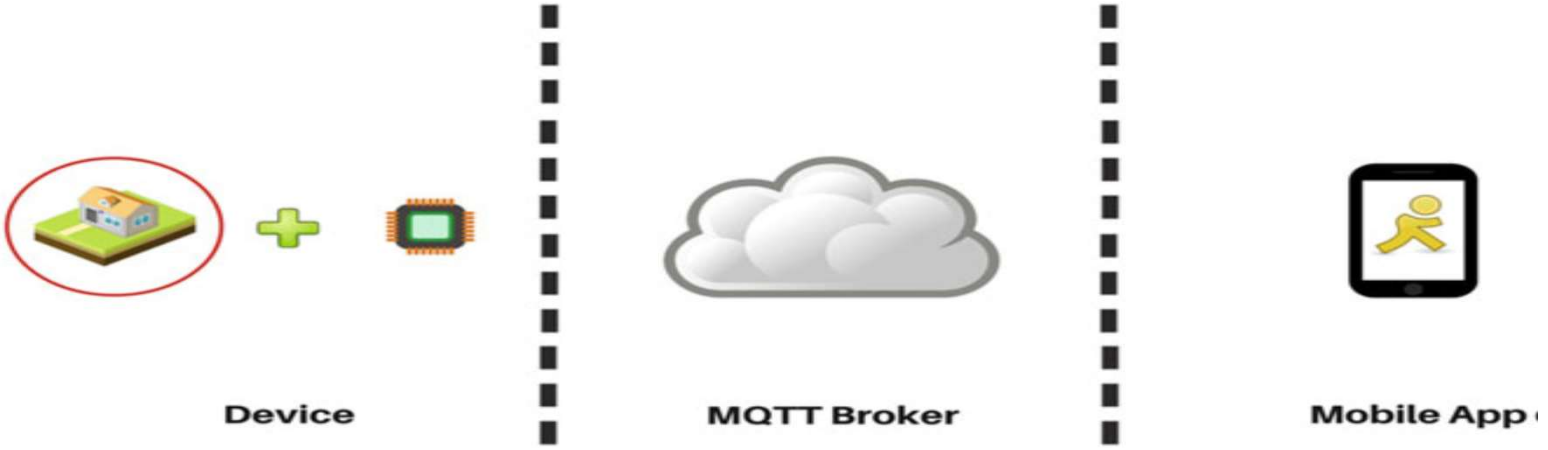


3. **MQTT** (Message Query telemetry Transport)



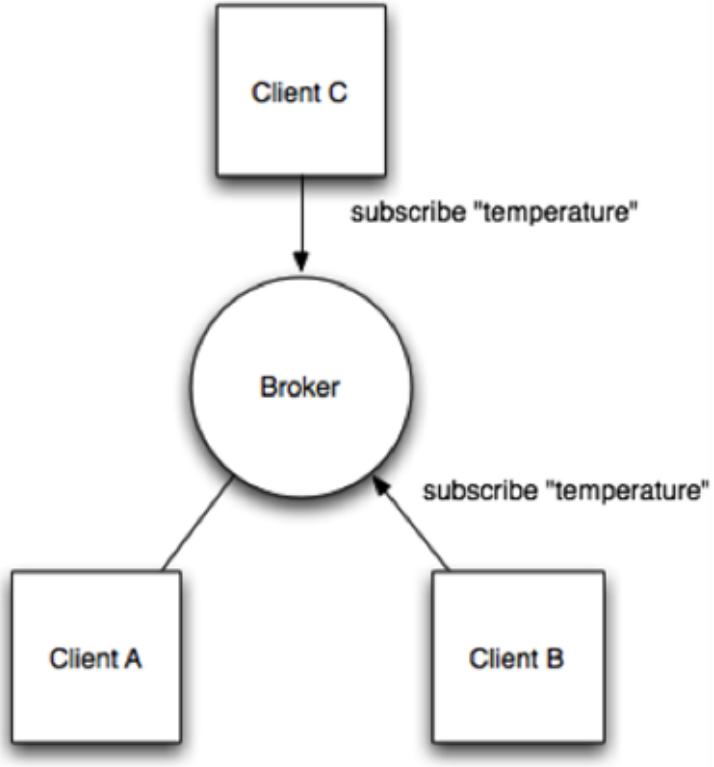
Exemple MQTT

❖ **MQTT** : système de détection d'intrusion

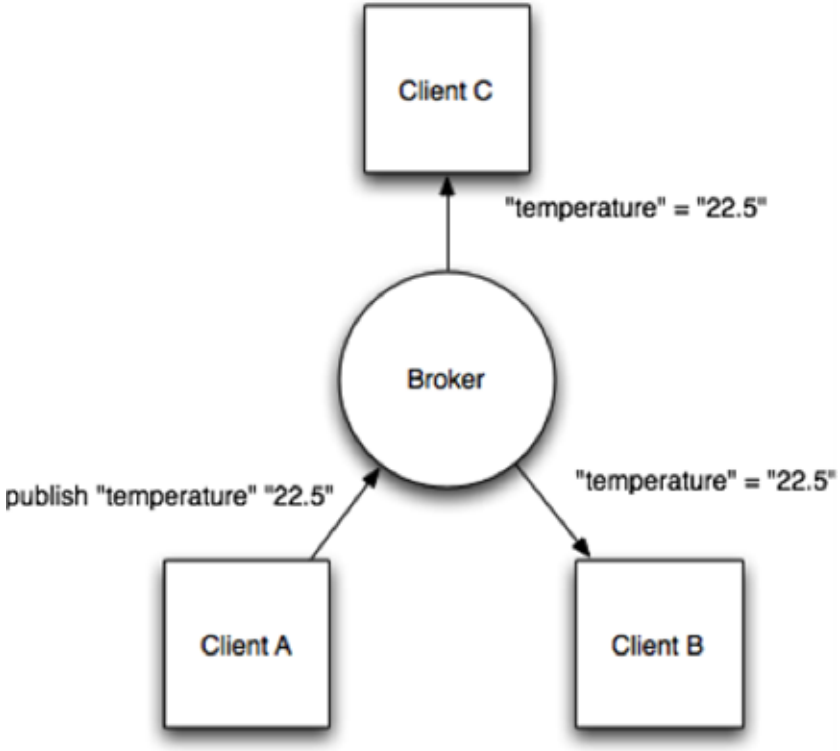


Le capteur agira comme un publisher et publie un nouveau message au Topic *intrusionDetected* sur le courtier MQTT (broker) dès qu'une intrusion est détectée.
L'application mobile sera un abonné (Subscriber) au topic *intrusionDetected*. Chaque fois qu'un nouveau message est publié ,elle obtiendra une notification. Cela se traduira par la création d'une notification sur l'application mobile utilisateur.

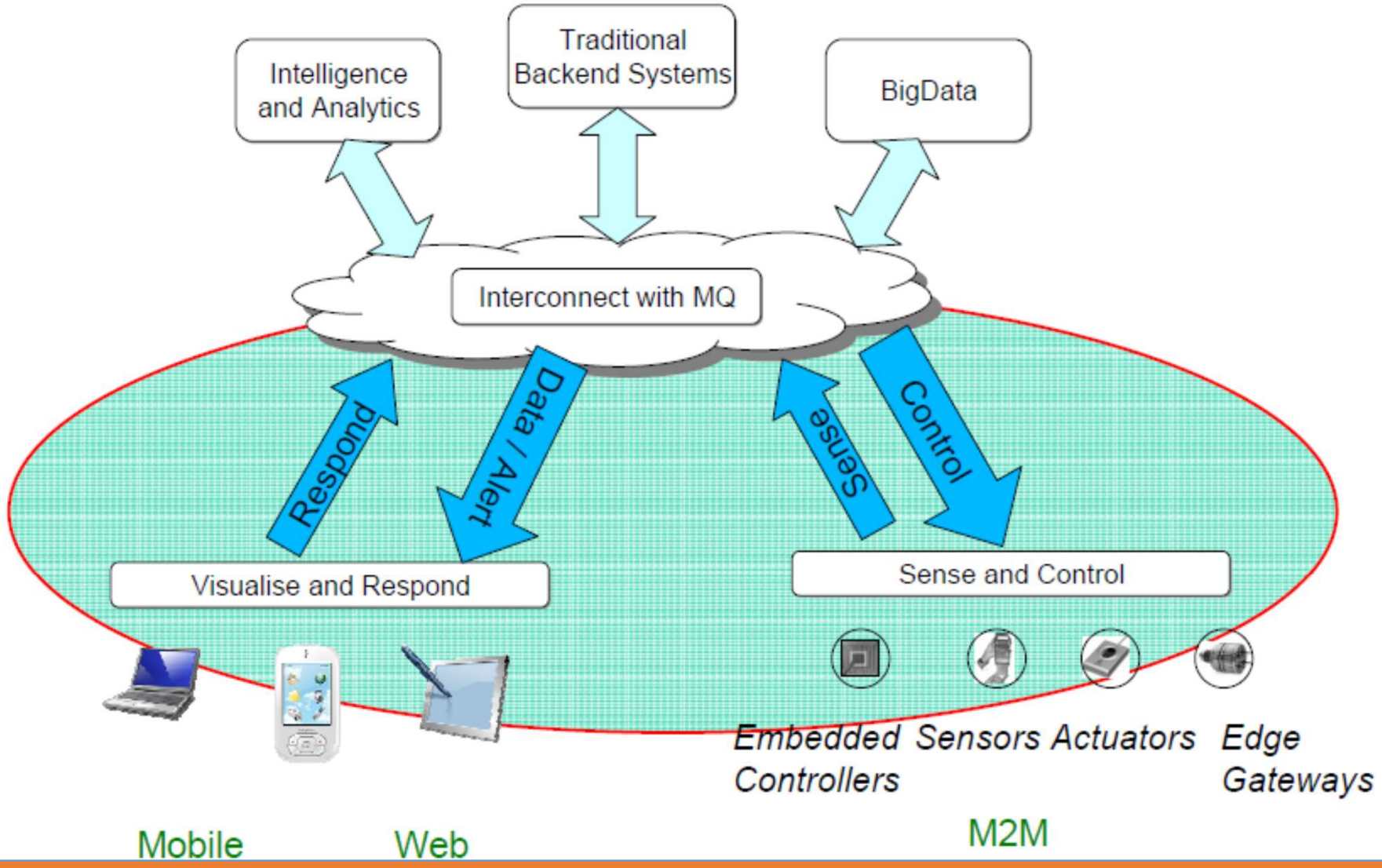
MQTT (Message Query telemetry Transport)



Les trois clients établissent une connexion TCP avec le broker. Les clients B et C souscrivent au topic température



Le Client A publie sur le topic température une valeur de 22,5°. Le broker propage le message à tous les clients ayant préalablement souscrit au topic Température.



Internet Of Things

Avantage du MQTT vs HTTP:

- ❑ livraison messages / données / événements
  - ✓MQTT - faible latence lors de livraison des messages du client au serveur et serveur vers le client
  - ✓ HTTP - pousser du client vers le serveur, mais interroger du serveur au client

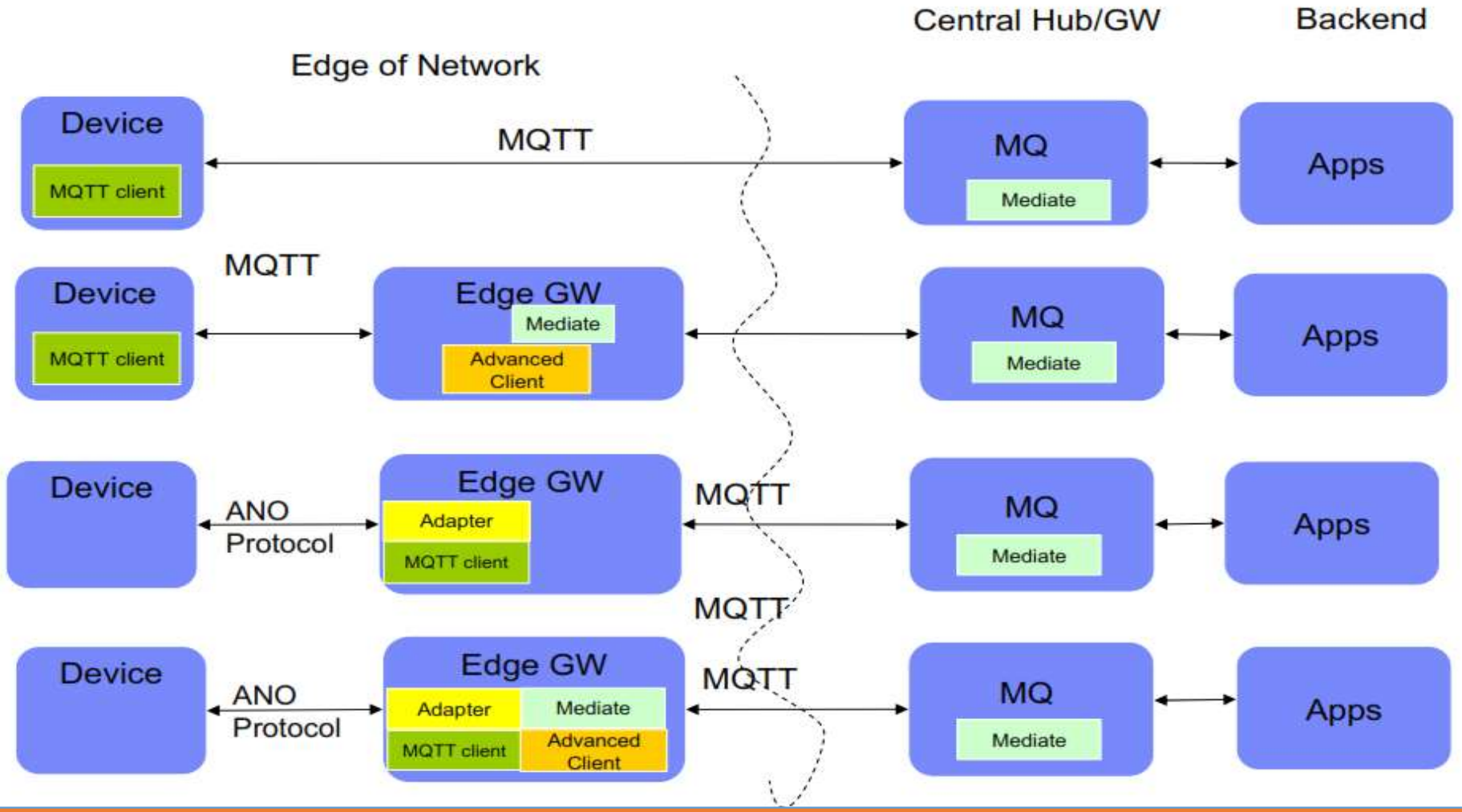
- ❑ L'utilisation efficace du réseau
  - ✓Pour un projet M2M le nombre d'octets avec MQTT est 137130 octets par dispositif par moi avec HTTP le nombre d'octets est 801000 octets par moi

- ❑ Livraison fiable sur le réseau fragile

  - ✓MQTT livrera un message à QOS même à travers les pauses de connexion

- ❑ Découplage entre publisher subscriber
- ❑ MQTT est un protocole très léger donc une faible consommation d'énérgie
- ❑ La communication entre les périphériques est toujours ouverte ce qui n'est pas dans le cas de HTTP où la connexion se ferme une fois la réponse donnée.

Schéma de connexion des périphériques avec MQTT



4. XMPP

XMPP: Extensible Messaging and Presence Protocole

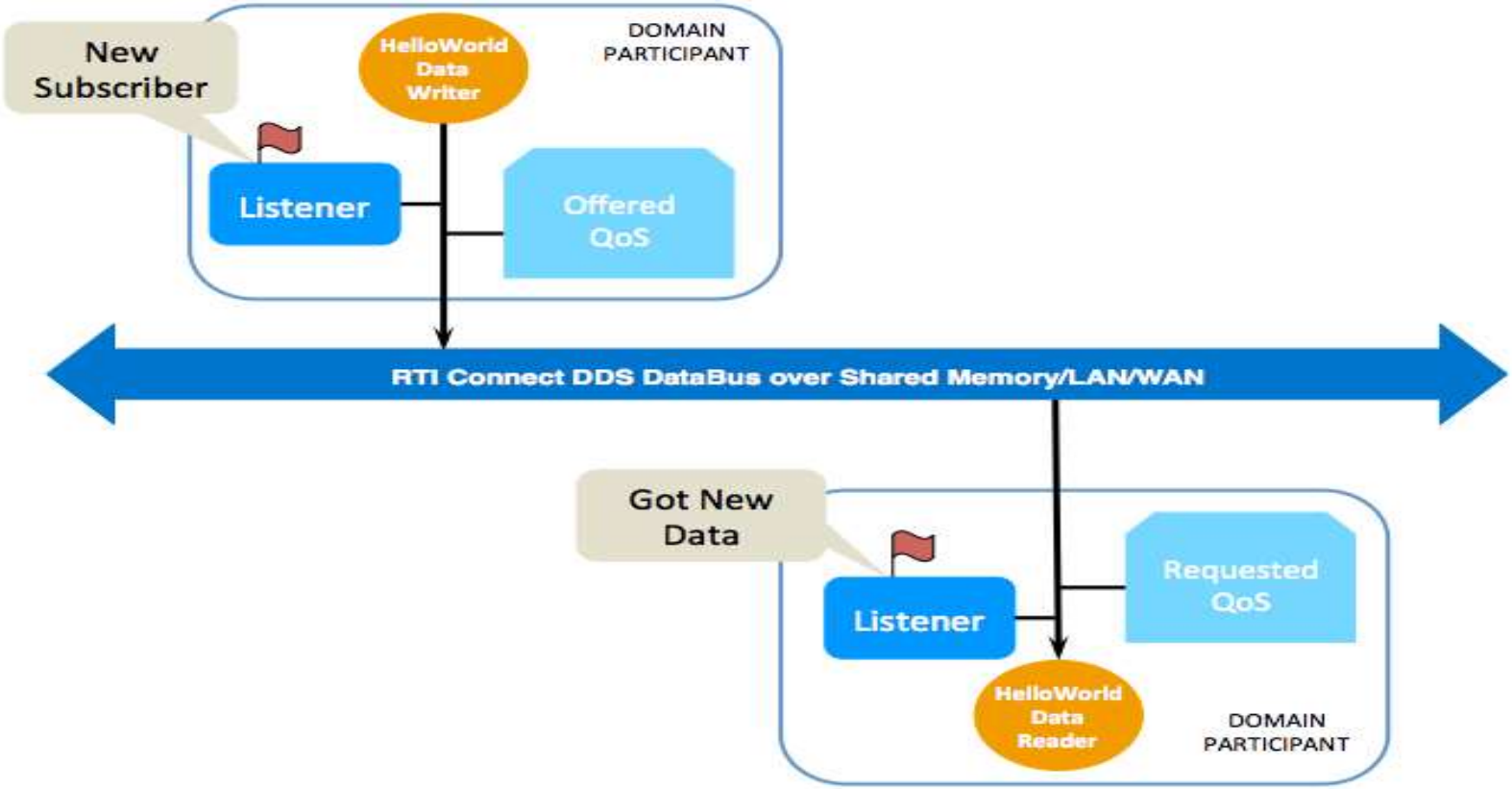
- ✓ Destiné a un usage humain, il n'est pas très rapide
- ✓ Les performance du XMPP sont basé sur la perception humain du temps réel qui est en seconde plutôt qu'en microseconde
- ✓ XMPP communique via HTTP en utilisant TCP/IP combiné avec le XML rendant ce protocole souhaitable pour les smartphone et les composant intelligent (intelligent devices)
- ✓ XMPP est le mieux adapté aux processus industriels qui ont des interfaces gérées par l'homme et qui favorisent la sécurité, l'adressabilité et l'évolutivité par rapport aux performances en temps réel,

6. DDS

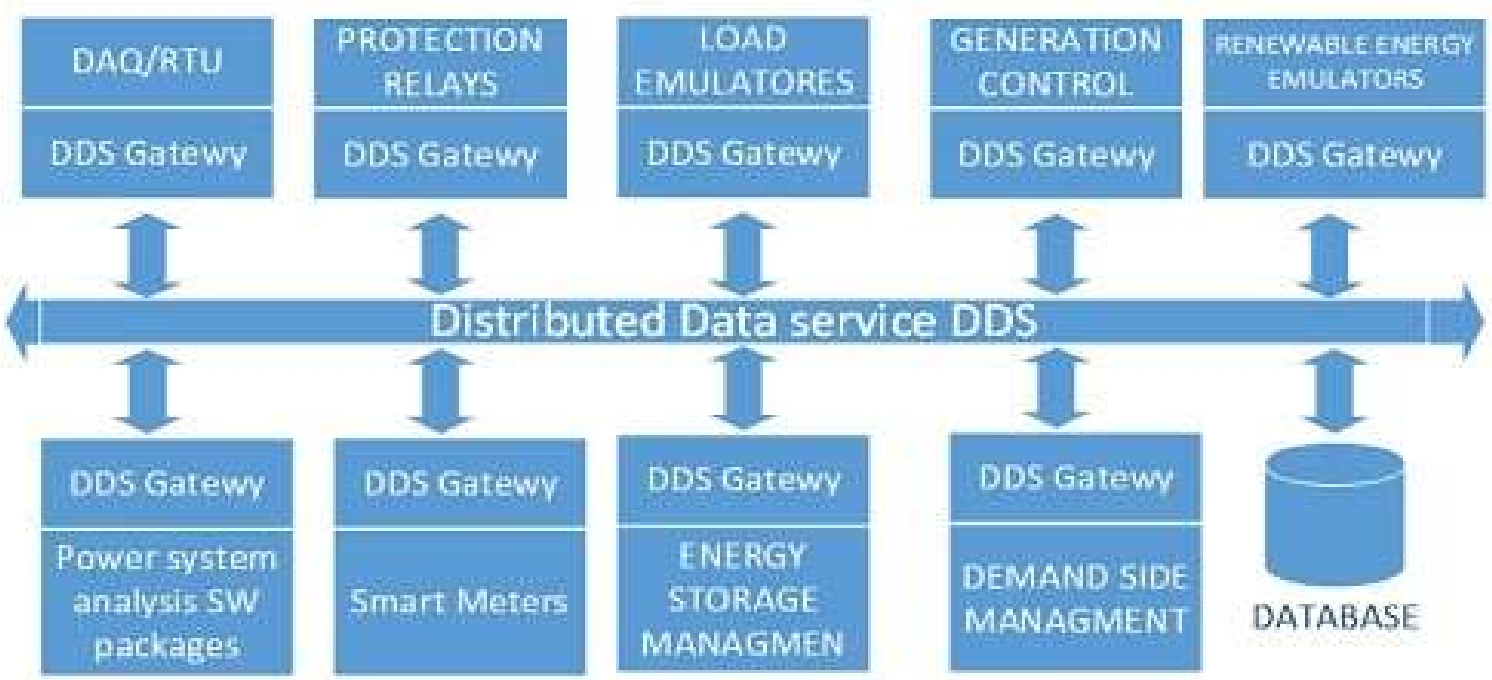
DDS: Data Distribution Service

- ✓ DDS distribue les données à d'autres périphériques sur un bus c'est un protocole Device to Device
- ✓ Device to Device signifie une communication rapide et une collaboration entre les périphériques sur le même segment, le protocole prend également en charge l'interaction entre les périphériques et les serveur : Device to Server
- ✓ DDS peut être accessible à distance et publier efficacement des millions de messages par seconde à de nombreux abonnés simultanés. En outre, DDS peut stocker et transférer les messages, si un abonné se trouve hors ligne.
- ✓ DDS peut également supporter une version lightweight du DDS qui s'exécutent dans des environnements contraints tels que les systèmes à faible puissance.
- ✓ DDS est conçu pour les systèmes haute performance, ce qui correspond parfaitement à l'IIoT , telles que les systèmes de manufacture, les parcs éoliens, l'intégration hospitalière, L'imagerie médicale, les systèmes de suivi des actifs et les tests et la sécurité automobile.

6. DDS


New Subscriber
HelloWorld Data Writer
DOMAIN PARTICIPANT
Listener
Offered QoS
RTI Connect DDS DataBus over Shared Memory/LAN/WAN
Got New Data
Requested QoS
Listener
HelloWorld Data Reader
DOMAIN PARTICIPANT

6. DDS



Smart Grid testbed infrastructure.

	Transport	Paradigm	Scope	Discovery	Content Awareness	Data Centricity	Security	Data Prioritisation	Fault Tolerance
AMQP	TCP/IP	Point-to-Point Message Exchange	D2D D2C C2C	No	None	Encoding	TLS	None	Impl. Specific
CoAP	UDP/IP	Request/ Reply (REST)	D2D	Yes	None	Encoding	DTLS	None	Decentralized
DDS	UDP/IP (unicast + mcast) TCP/IP	Publish/ Subscribe Request/ Reply	D2D D2C C2C	Yes	Content-Based Routing, Queries	Encoding Declaration	TLS, DTLS, DDS Security	Transport Priorities	Decentralized
MQTT	TCP/IP	Publish/ Subscribe	D2C	No	None	Undefined	TLS	None	Broker is the SPoF

TCP: Transmission Control Protocol **IP:** Internet Protocol **D2D:** Device-to-Device **D2C:** Device-to-Cloud **C2C:** Cloud-to-Cloud
TLS: Transport Layer Security **DTLS:** Datagram Transport Layer Security

Qualitative Comparison of IoT Standards

IV.IPv6 vs IPv4

IPv4:
Ce type d'**adresses IP** est codé en décimale sur 4 octets (chaque octet peut avoir un numéro de 0 jusqu'à 255) tel que chaque octet est séparé par un point «.».
Exemple : 192.168.1.1
Ce type d'adresses IP est le *protocole* le plus utilisé dans nos jours. Tel que le nombre maximal des ordinateurs qui peuvent se connecter en même temps sur un réseau est à peu près 4 milliards machines (2^32).

IPv6:
Ce type de **protocole** est beaucoup plus récent et amélioré par rapport à le protocole l'**IPv4**, car les **adresses IPv6** sont codées en hexadécimal sur 16 octets (8 parties tel que chaque partie est sur 2 octets). Les 8 parties du protocole IPv6 sont séparés par deux-points « : ».
Exemple : 3ac4:0567:0000:34b6:0000:0000:c6d4:4300
Le nombre d'ordinateurs qui peuvent se connectés sur un réseau qui utilise le protocole IPv6 est égale à (2128).

IV.IPv6 vs IPv4

Les avantages de la IPv6:

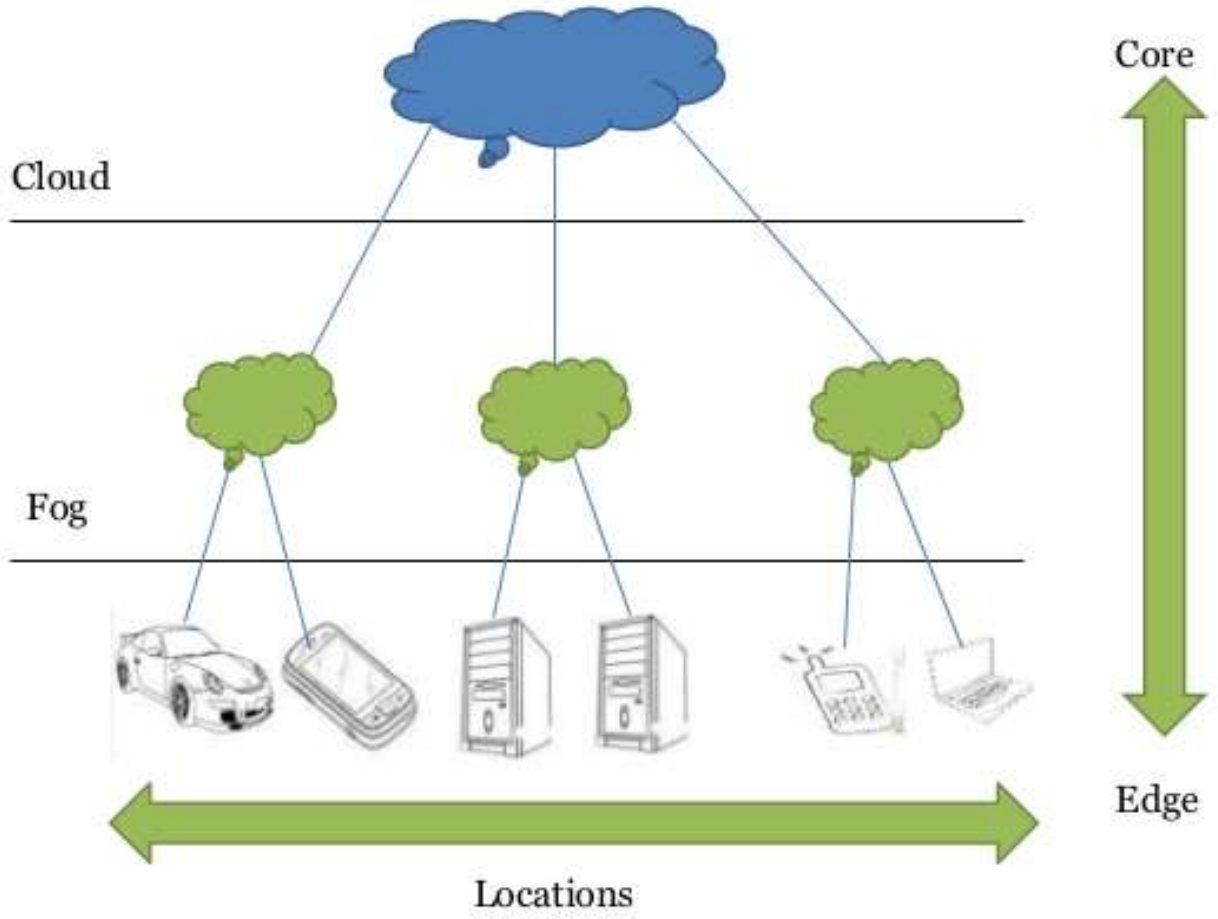
- Scalability : avec IPv6 on 182 bits d'adresse contre 32bits d'adresse pour l'IPv4, théoriquement on peut avoir 2^32=10^10 adresse IP possible pour l'IPv4, alors qu'on peut avoir 2^128=10^39 adresse IP possible pour l'IPv6.
- « plug-and-play » : l'IPv6 inclues des mécanisme plug-and-play qui facilite la connexion des équipement au réseau , la configuration se fait automatiquement.
- Security
- Mobility : lPv6 possède une efficace et robuste mécanisme de mobilité, spécialement l'ensemble des protocoles de l'IPv6 mobile (MIPv6) tels que le RFC3775.

V. Cloud Computing and Fog Computing

Cloud Computing, est défini comme un groupe d'ordinateurs et de serveurs connectés sur Internet pour former un réseau. Aujourd'hui, comme de nombreuses entreprises et de grandes organisations commencent à adopter l'Internet des objets, la nécessité de disposer d'une grande quantité de données plus rapidement et à l'échelle locale est toujours en croissance. C'est là que le concept de "Fog Computing" vient à jouer.

Fog Computing, ou "fogging", est une infrastructure distribuée dans laquelle certains processus ou services sont gérés au bord du réseau par un périphérique intelligent, mais d'autres sont encore gérés dans le cloud. Il s'agit, en substance, d'une couche intermédiaire entre le cloud et les composants (capteur …..) pour permettre un traitement, une analyse et un stockage plus efficaces des données, ce qui permet de réduire la quantité de données qui doit être transportée vers le cloud.

- ✓Ajouter des ressources de traitement et de mémoire à des périphériques du bord de réseau
- ✓Prétraitement des données collectées sur le bord du réseau
- ✓Envoi de résultats agrégés au cloud


Core
Cloud
Fog
Edge
Locations

FPGA and IOT

FPGA and IOT

In a recent development from Avnet, we have the MicroZed development module based on the Xilinx Zynq-7000 SoC. The SoC combines dual ARM Cortex-A9 processor cores with numerous programmable logic cells to provide hardware and software programmability for better developer experience. The abundant resources available on the module make it suitable even for high-end applications.

Developers working on the Internet of Things (IoT) have been seeing an increasing number of development platforms lately, catering to hardware and connected services in a common system. Most of such kits seem to target hobbyist or consumer applications, and even lesser provide a simpler path to production.

Avnet is seeking to change the situation with its latest introduction as the MicroZed Industrial IoT starter kit.
The kit consists of a carrier board for the MicroZed to plug into, which provides developers with an R3 Arduino-compatible expansion slot, two 2×6 peripheral module expansion slots, and a header for connection to the built-in UART, SPI, I2C, and GPIO interfaces,

At a price point of $300, the kit is intended as a serious product-development platform, and not just a demonstration or experimenter's board.