

Cours Internet des Objets (IoT) et Cloud Computing

CH3: Protocoles et Réseaux IoT

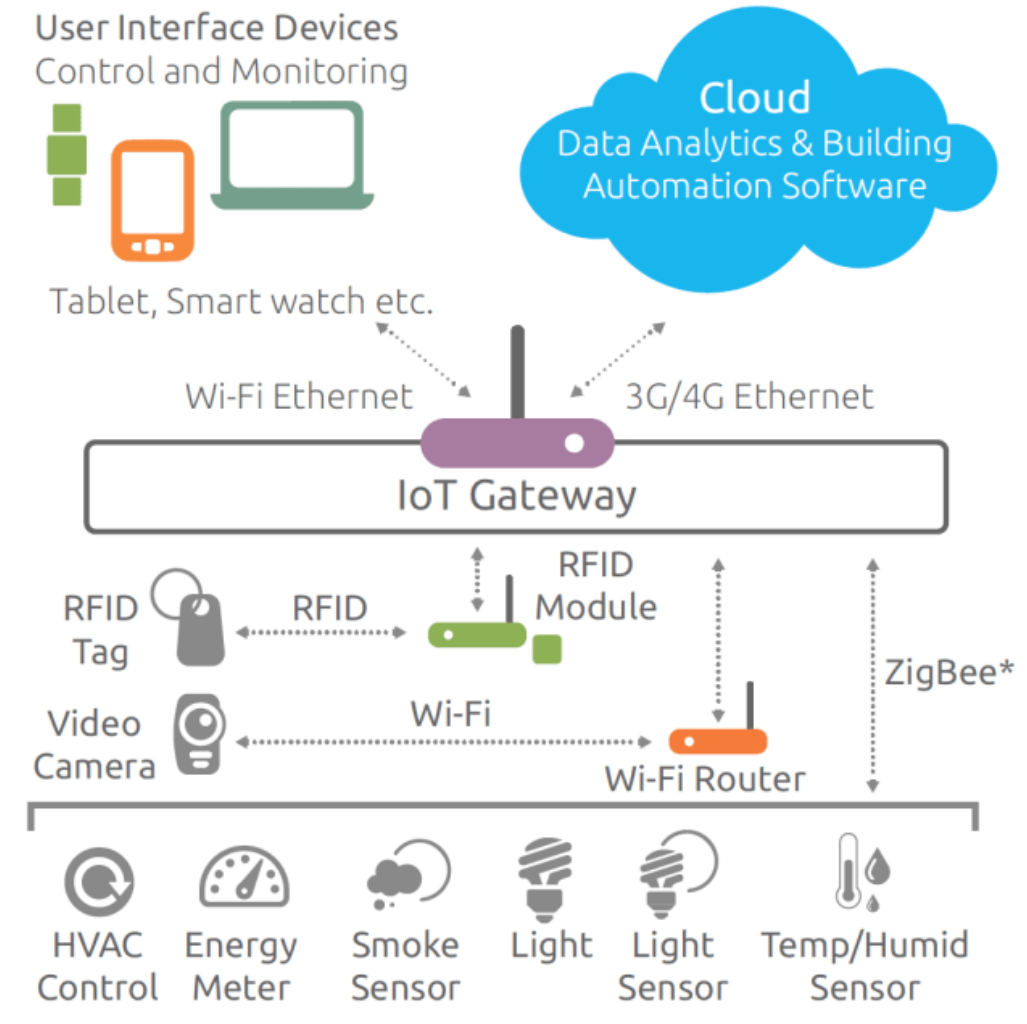
Par:

Hassan EL FADIL

elfadil.h@gmail.com

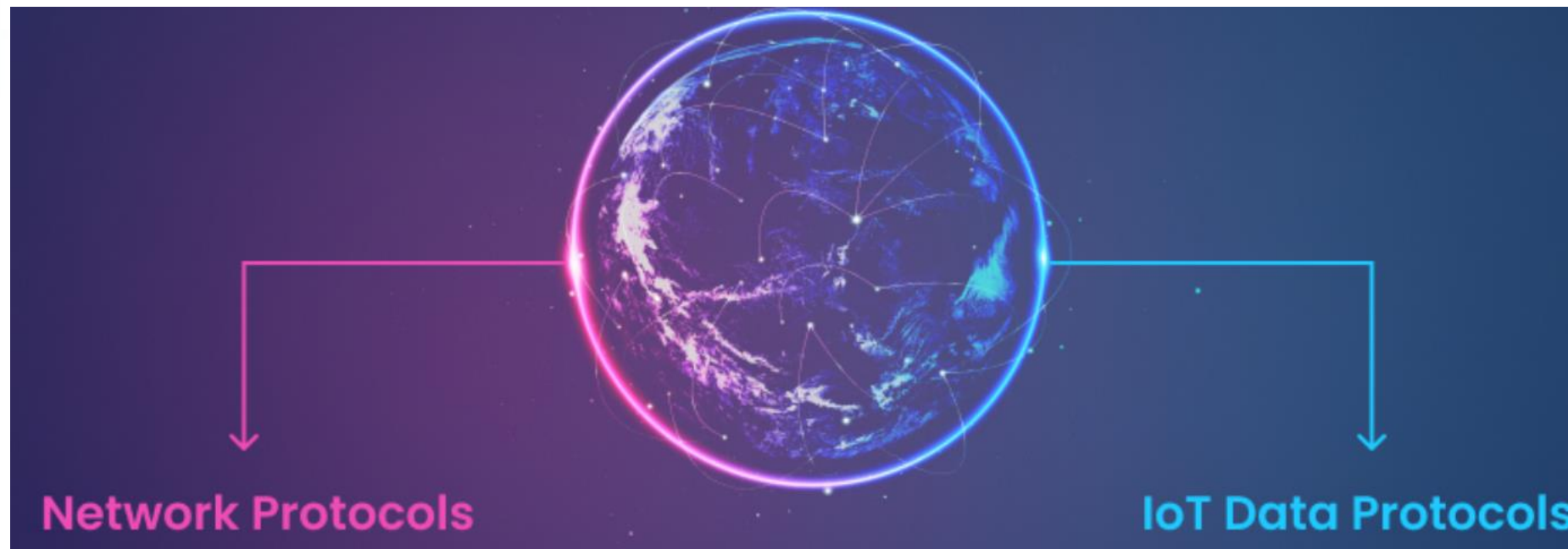
1. Introduction

- Les protocoles sont un ensemble de règles permettant de transmettre des données entre des appareils électroniques selon un accord prédéfini concernant la structure de l'information et la manière dont chaque partie enverra et recevra des données.
- En conséquence, les protocoles IoT sont des normes qui permettent l'échange et la transmission de données entre Internet et les objets.

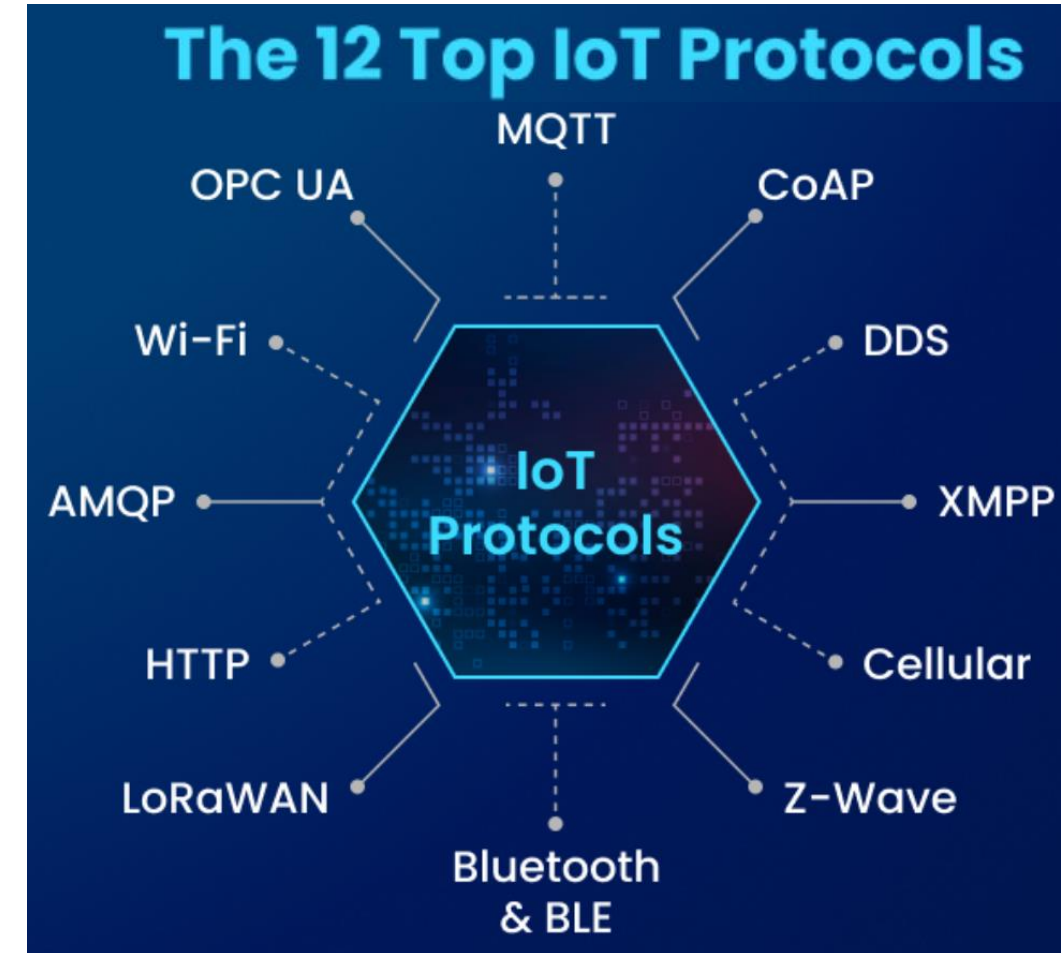


Les protocoles utilisés dans l'IoT peuvent être classés en deux grandes familles:

- Les protocoles de réseau IoT (IoT Network Protocols)
- Les protocoles de données IoT (IoT Data Protocols)



- Les protocoles de données se concentrent principalement sur l'échange d'informations,
- Les protocoles réseau fournissent des méthodes de connexion des objets IoT à d'autres objets ou à Internet.



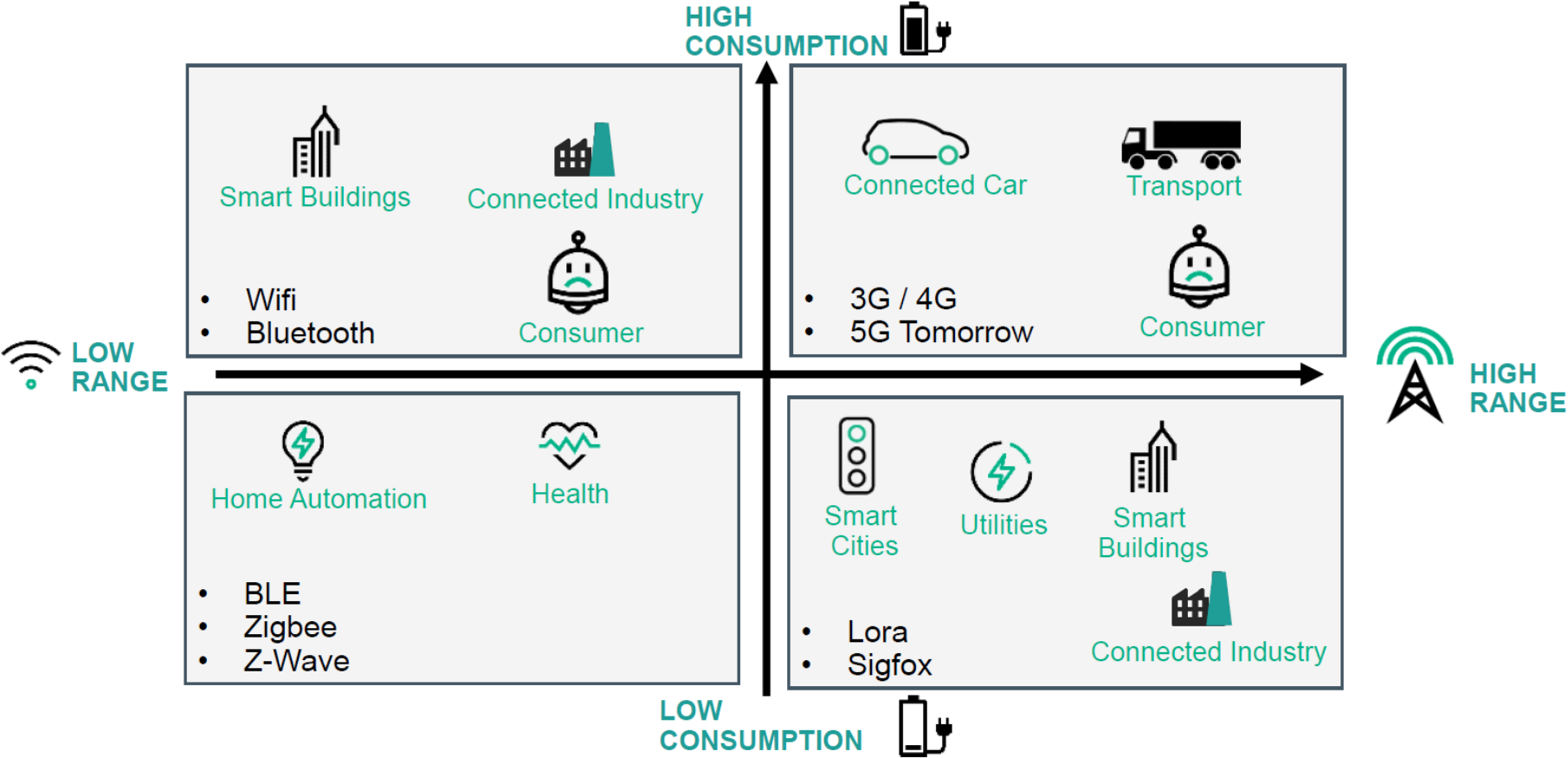
IoT Network Protocols

- **Wi-Fi & Wi-Fi HaLow**
- **Bluetooth & BLE**
- **Cellular: 4G & 5G**
- **LPWANs** (Low Power wide Area Network):
 - **NB-IoT**,
 - **LoRaWAN**
- **ZigBee**
- **Z-Wave**
- **6LoWPAN**

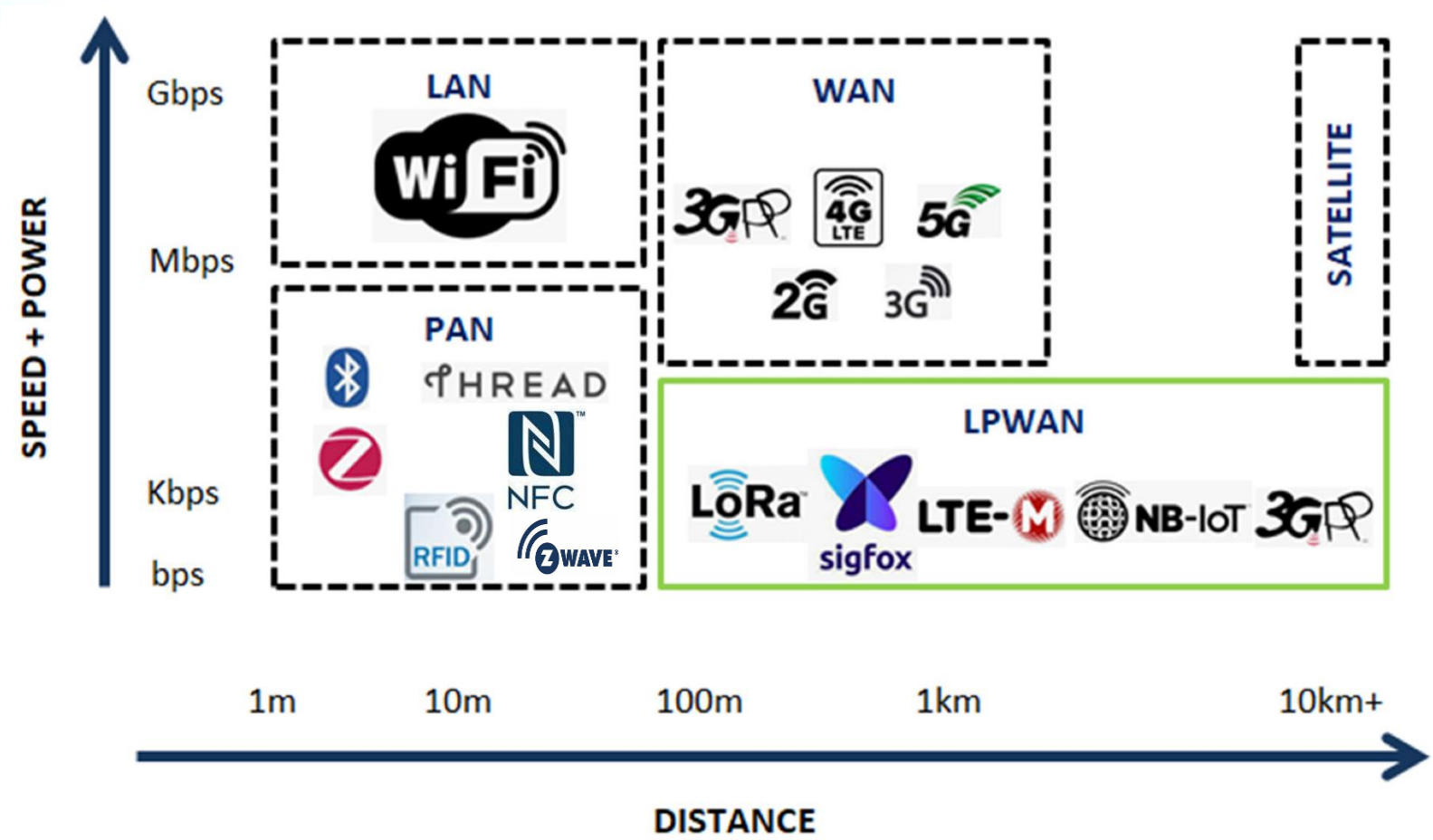
IoT Data Protocols

- **AMQP** (Advanced Message Queuing Protocol)
- **DDS** (Data Distribution Service)
- **MQTT** (Message Queuing Telemetry Transport)
- **HTTP** (Hypertext Transfer Protocol)
- **CoAP** (Constrained Application Protocol)
- **LwM2M** (Lightweight Machine-to-Machine)
- **OPC UA** (Open Platform Communication Unified Architecture)
- **WebSocket**

Classification de quelques protocoles réseaux selon la portée (distance) et la consommation d'énergie



Classification de quelques protocoles réseaux IoT selon la portée (distance) et le débit



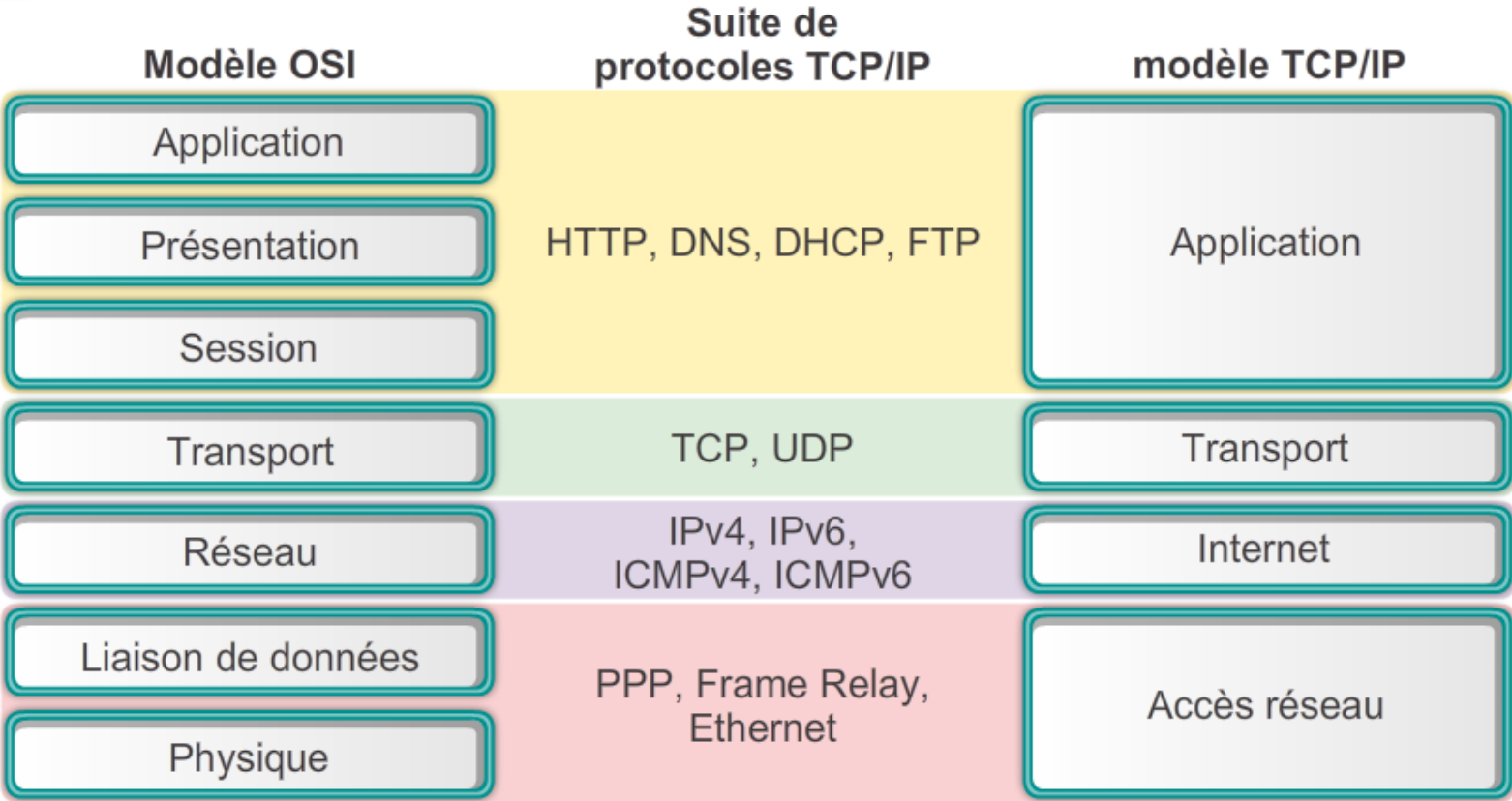
Caractéristiques de quelques protocoles réseaux IoT

Réseau/Protocole	Portée (mètres)	Fréquence (GHz)	Puissance	Coût
Wi-Fi	Jusqu'à 100 mètres (environ)	2,4 GHz, 5 GHz	Élevée	Moyen
Wi-Fi HaLow	Jusqu'à 1 km (environ)	0,9 GHz	Élevée	Moyen
Bluetooth	Jusqu'à 10 mètres (environ)	2,4 GHz	Faible	Faible
BLE (Bluetooth Low Energy)	Jusqu'à 100 mètres (environ)	2,4 GHz	Faible	Faible
4G Cellular	Kilomètres (couverture large)	0,7 GHz - 2,5 GHz	Élevée	Élevé
5G Cellular	Kilomètres (couverture large)	3,5 GHz - 30 GHz	Élevée	Élevé
NB-IoT	Jusqu'à plusieurs kilomètres	0,8 GHz - 2,2 GHz	Faible	Moyen
LoRaWAN	Jusqu'à plusieurs kilomètres	868 MHz (Europe), 915 MHz (Amérique du Nord)	Faible	Modéré
ZigBee	Jusqu'à quelques dizaines de mètres	2,4 GHz	Faible	Moyen
Z-Wave	Jusqu'à quelques centaines de mètres	868 MHz (Europe), 915 MHz (Amérique du Nord)	Faible	Modéré
6LoWPAN	Jusqu'à quelques centaines de mètres	2,4 GHz	Faible	Moyen

2. Protocoles de transport TCP/UDP

2.1. Comparaison du modèle OSI et TCP/IP

7 couches:
Modèle théorique pour comprendre les principes fondamentaux de la communication réseau



5 couches:
Celui qui est le plus couramment utilisé pour la mise en œuvre réelle des communications réseau, en particulier sur Internet

OSI (Open Systems Interconnection)

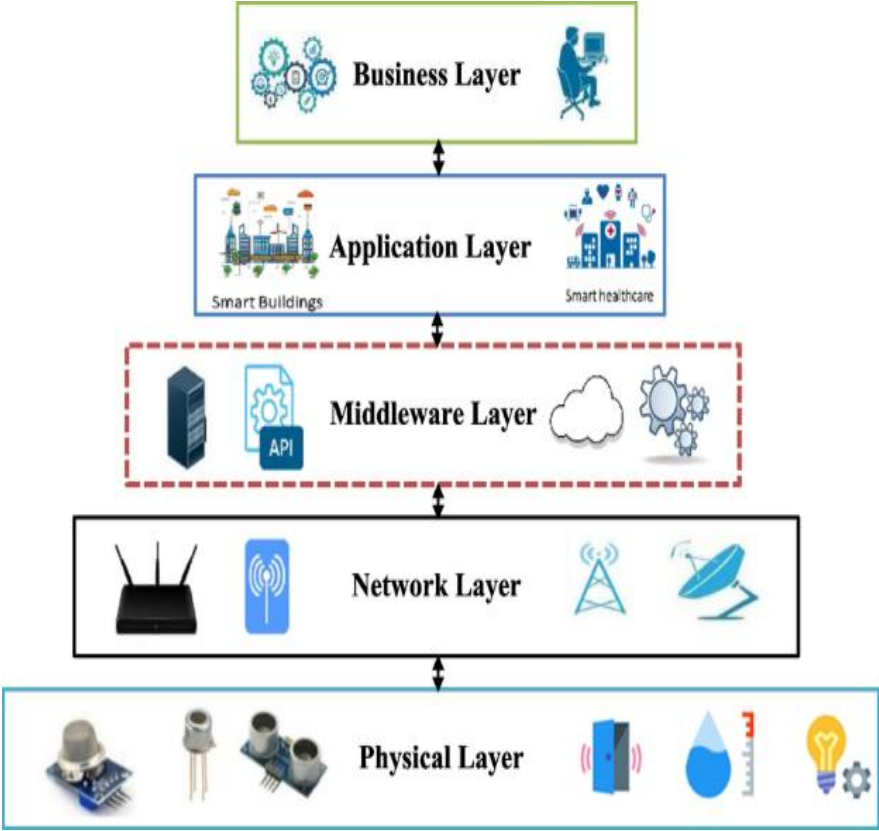
TCP/IP (Transmission Control Protocol/Internet Protocol)

2.2. TCP/IP et architecture IoT

Modèle TCP/IP

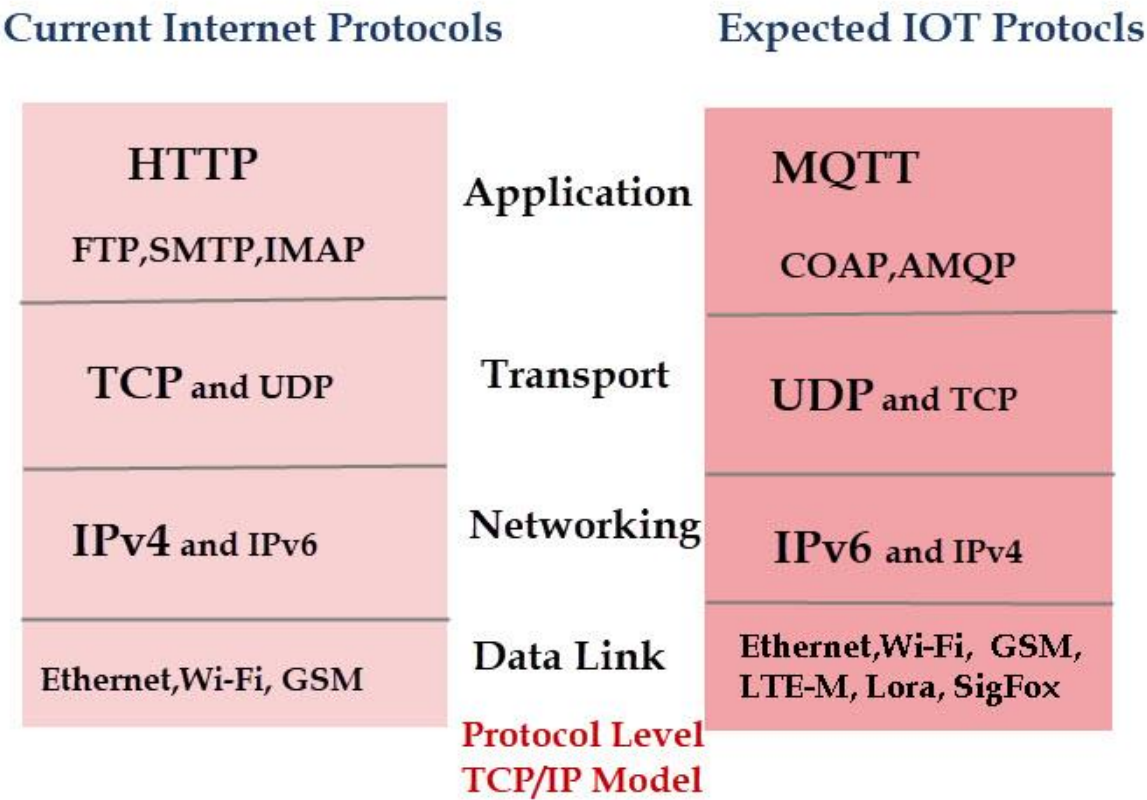
Layer	Protocols
Application	HTTP,FTP,POP3,SMTP,SNMP
Transport	TCP,UDP
Networking	IP,ICMP
Datalink	Ethernet, ARP

Architecture en 5 couches (IoT)



2.3. TCP et UDP:

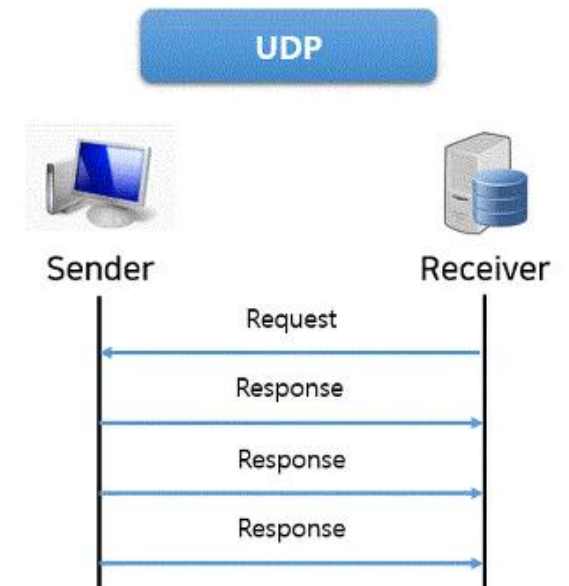
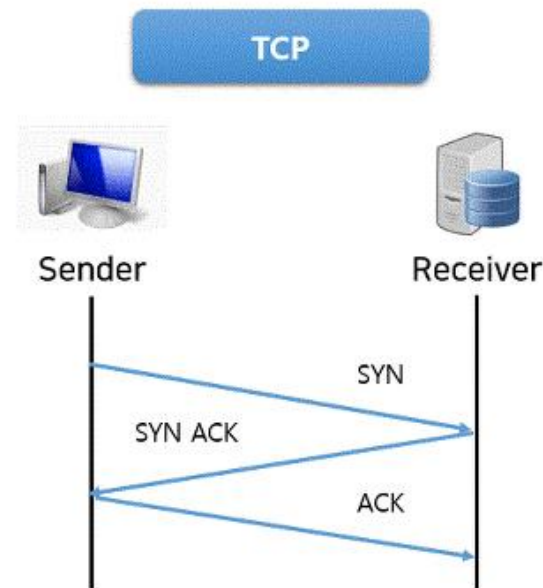
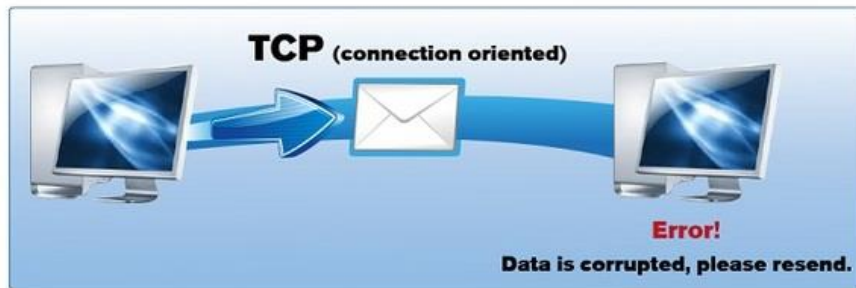
- TCP : Transmission Control Protocol
- UDP :User Datagram Protocol
- Les protocoles TCP et UDP sont largement utilisés dans les protocoles IoT pour la communication et le transfert de données entre les appareils connectés



IOT and Internet Protocols

Le TCP est de type « Connection oriented » l'UDP est de type « Connectionless »

Un protocole "connection oriented" est un protocole qui établit une connexion préalable avant de transférer des données entre les parties communicantes. Cela signifie que les dispositifs ou les systèmes communiquant via ce protocole doivent d'abord établir une liaison logique avant de pouvoir échanger des informations.



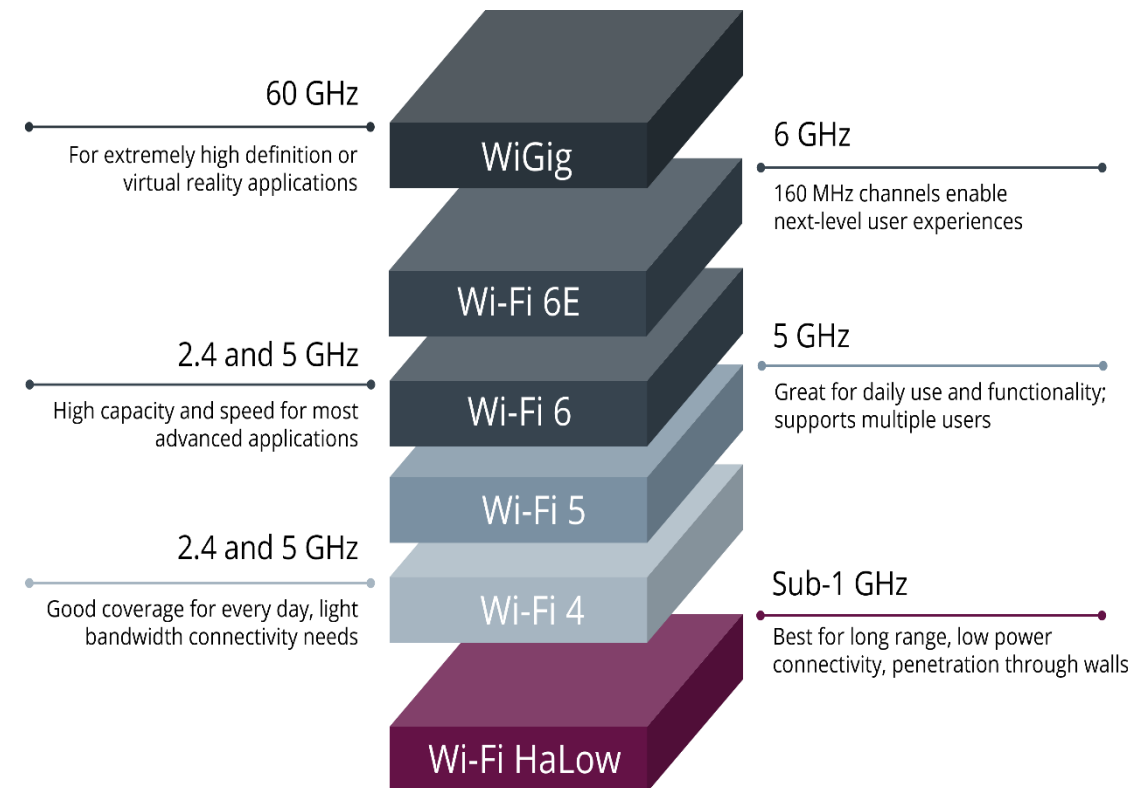
	TCP	UDP
Type de protocole	Orienté connexion	Sans connexion
Fiabilité	Elevée	Faible
Vitesse	Faible	Elevée
Détection des erreurs	Oui	Non
Correction des erreurs	Oui	Non
Contrôle de la congestion	Oui	Non
Accusé de réception (ACK)	Oui	Uniquement la somme de contrôle
Taille de l'entête de paquet	20 Octets	8 Octets
Exemple d'application	Email	VoIP (Voix sur IP)

3. Protocoles de réseau IoT (IoT Network Protocols)

3.1. Le protocole Wi-Fi



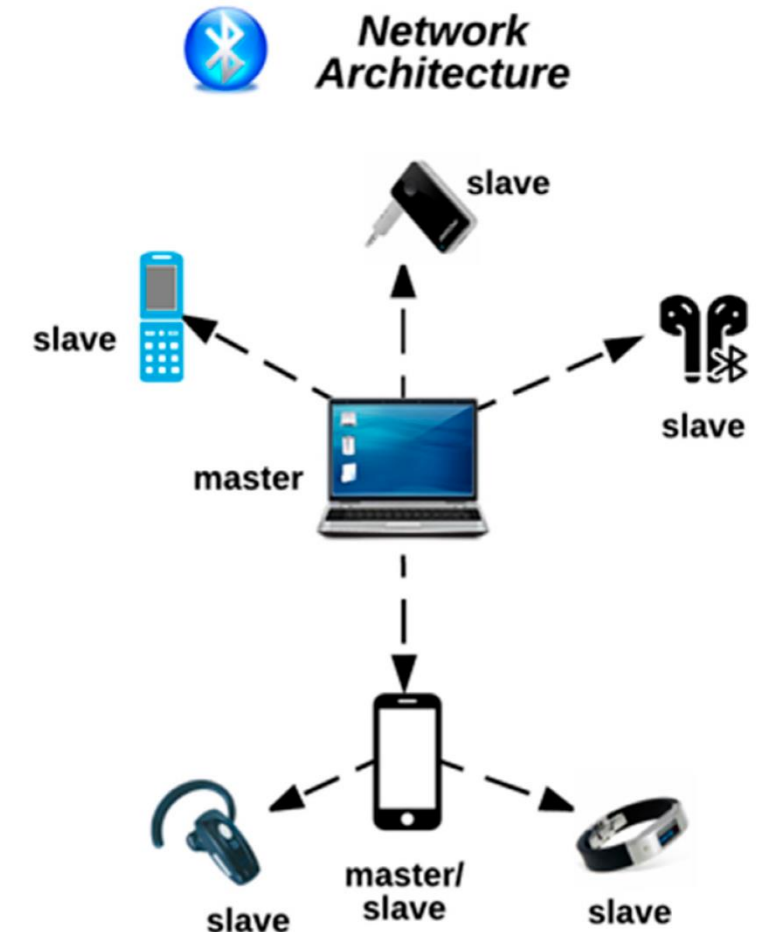
- **Wi-Fi (Wireless Fidelity) :**
 - Débit maximum : jusqu'à plusieurs Gbps (selon la norme Wi-Fi utilisée, comme 802.11ac ou 802.11ax).
 - Distance maximum : jusqu'à 100 mètres en intérieur.
 - Consommation d'énergie : plus élevée que Wi-Fi HaLow.
- **Wi-Fi HaLow (802.11ah):**
 - Débit maximum : varie entre 150 kb/s et 86.7 Mb/s.
 - Distance maximum : jusqu'à 3 km en champ libre.
 - Consommation d'énergie : plus faible que Wi-Fi standard.



3.2. Le protocole Bluetooth



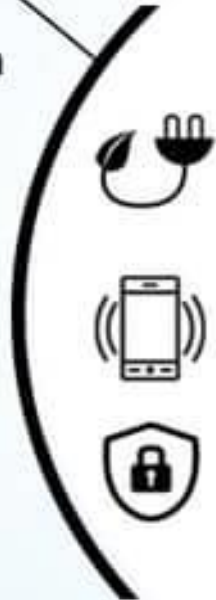
- **Bluetooth :**
 - Débit maximum : jusqu'à 3 Mbps.
 - Distance maximum : environ 100 mètres en champ libre.
 - Consommation d'énergie : plus élevée que BLE.
 - Communication directe P2P (Point-to-Point) ou réseau PAN (Personal Area Network)
- **BLE (Bluetooth Low Energy):**
 - Débit maximum : jusqu'à 1 Mbps.
 - Distance maximum : environ 100 mètres en champ libre.
 - Consommation d'énergie : plus faible que Bluetooth.
 - Communication directe: P2P (Point-to-Point)



Bluetooth Low Energy for Smart Applications

Key Features

- Ultra low power consumption
- Low cost
- Small size
- Faster connection
- Secure



Variety of BLE Applications

- IoT
- Health care
- Smart Home Automation
- Smart Energy
- Advertisement

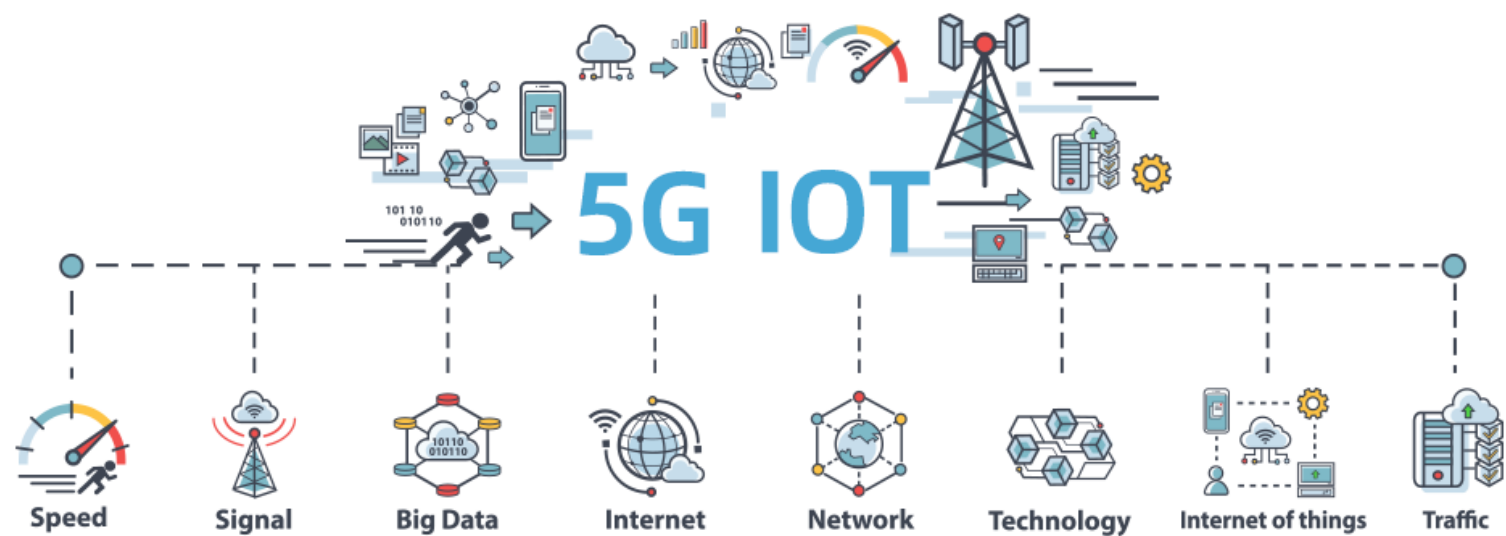


Applications BLE



3.3. Les réseaux cellulaires (4G et 5G):

Génération	Acronyme	Intitulé	Débit max	Distance max
4G	LTE WiMAX	Long Term Evolution Worldwide Interoperability for Microwave Access	50 à 150 Mbit/s théoriques LTE-A (4G+): 450 Mbit/s	15km
5G	NR NGAP	New Radio Next Generation Application Protocol	10 Gbit/s (théoriques montant) 5 Gbit/s descendant	1km



3.4. Les réseaux LPWANs (Low Power wide Area Network):

Technologie	Débit max	Distance max	Consommation
NB-IoT: Narrowband IoT 	jusqu'à 250 Kbps	10 km à 15 km en champ libre	faible, adaptée aux appareils IoT
LoRaWAN : Long Range Wide Area Network 	jusqu'à 50 Kbps	10 km à 20 km en champ libre	très faible, adaptée aux appareils avec une autonomie de plusieurs années sur une seule batterie

LoRA	NB-IoT
Older (2015)	Newer (2017)
Unlicensed spectrum	Licensed frequency bands
Lower cost per device (but gateway needed)	Higher cost per device (but no gateway needed)
Longer battery life	Shorter battery life
High latency / less frequent data transfer	Low latency / more frequent data transfer
7 to 10 mile range	11 to 13 mile range
Better rural/remote performance	Better urban/dense performance
Lower data rates	Higher data rates (10x LoRa's rates)

3.5. Le protocole Z-Wave:



- Le Z-Wave est un protocole de communication radio de faible puissance très utilisé pour les applications de domotique.
- Il émet une fréquence de 868,4 MHz et favorise l'échange d'information entre des modules compatibles de manière sécurisée.
- Il permet de gérer jusqu'à 232 appareils connectés différents grâce à une seule box domotique (un contrôleur).
- Débits typiques allant jusqu'à 100 kbps
- Portée: de 30 à 100m

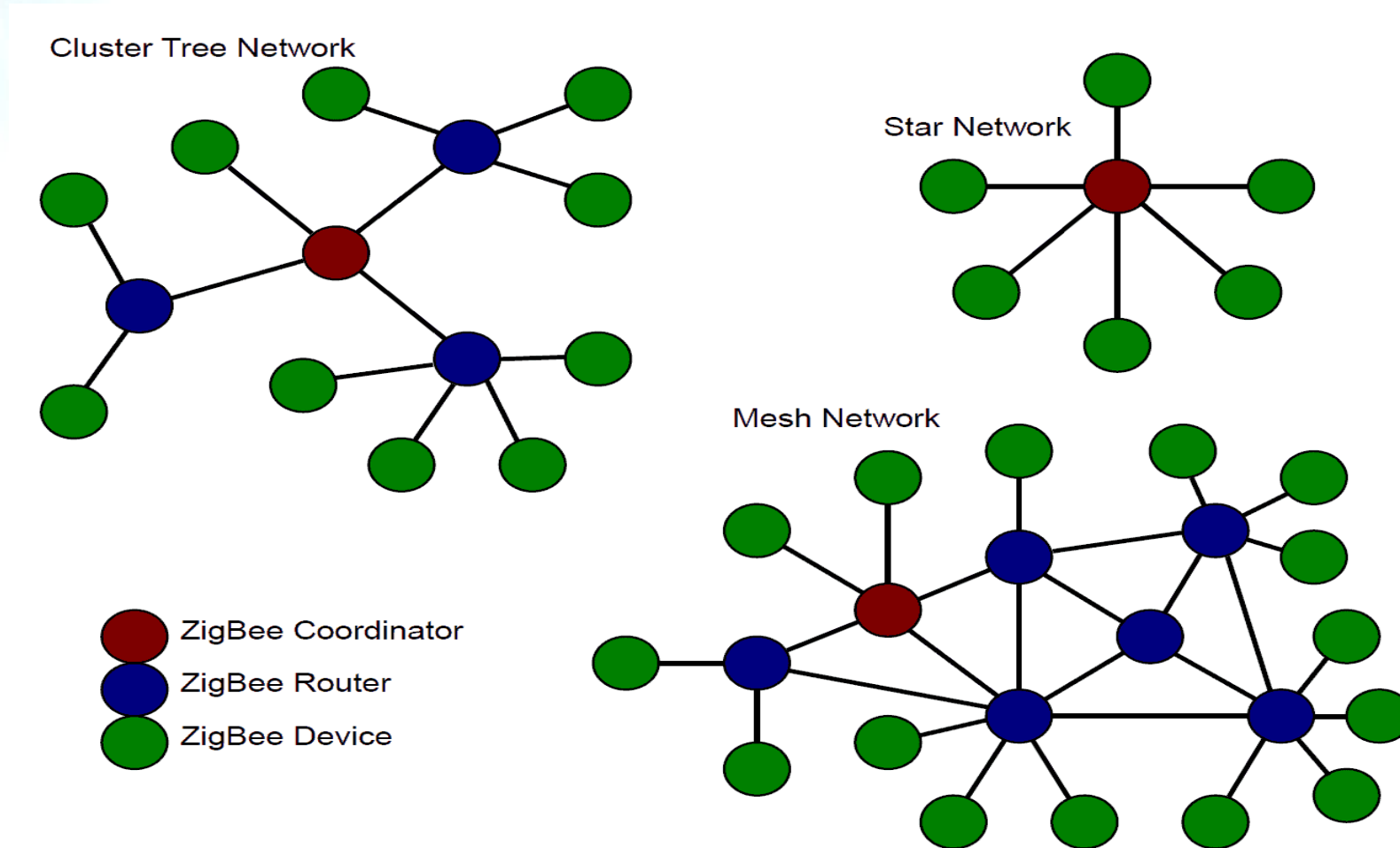


3.6. Le protocole Zigbee:

- Zigbee est un protocole radio de faible puissance tout comme le Z-Wave.
- Il émet non seulement sur la fréquence des **868,4 MHz**, mais également sur celle des **2,4 GHz** et autorise la transition d'un volume important de données grâce à son débit de **250 kbit/s**.
- Le Zigbee est un protocole domotique de courte portée.
- Portée: 10 à 100 mètres.
- Possibilité d'associer jusqu'à **65 000** périphériques différents.
- On notera également sa faible consommation énergétique. Cela peut permettre à certains appareils de fonctionner plusieurs années sous pile.
- En tant que protocole Open Source, Zigbee protocole est libre d'utilisation.

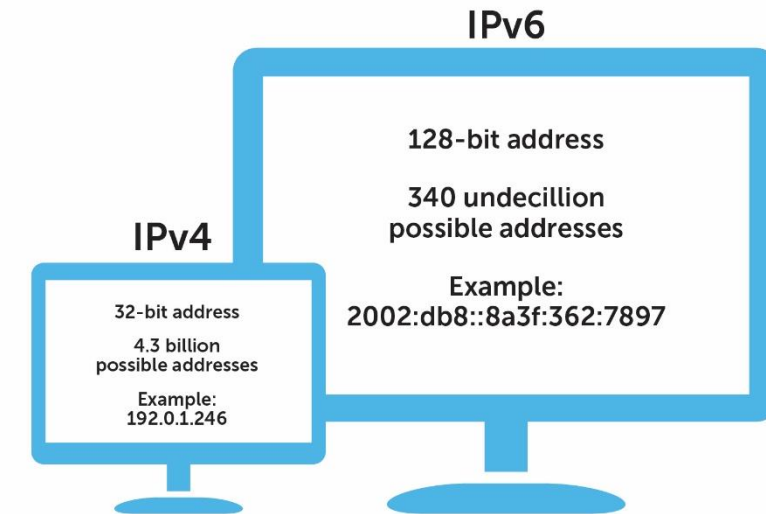


- ZigBee a défini 3 types de dispositifs vis-à-vis des capacités de routage:

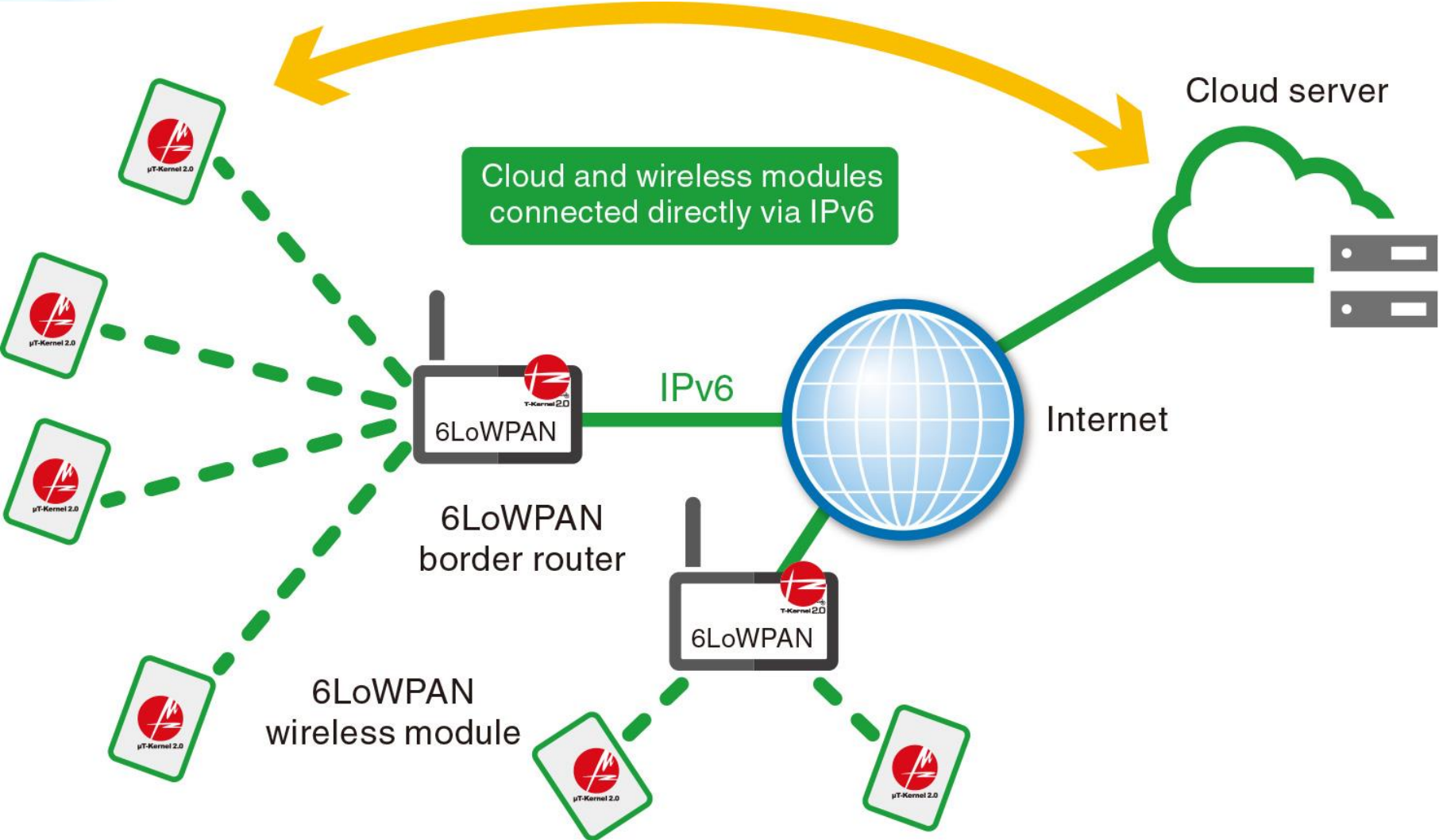


3.7. Le protocole 6LoWPAN :

- 6LoWPAN:IPv6 over Low-Power Wireless Personal Area Networks)
- Protocole de communication qui permet l'utilisation d'IPv6 (Internet Protocol version 6) sur des réseaux sans fil à faible puissance et à faible débit de données, tels que les réseaux de capteurs et les réseaux IoT
- Défini par le standard IETF: Internet Engineering Task Force (RFC 4919, RFC 4944)
- Le protocole utilise des techniques de compression et de fragmentation pour réduire la surcharge liée à la transmission des paquets IPv6 sur des liens à faible débit.
- Les objets ont globalement une adresse unique
- Paquets de faibles taille.
- Les paquets IPv6 peuvent être envoyés ou reçus via le protocole de communication IEEE 802.15.4.



1 undecillion = 10^{36}
1 billion (milliard) = 10^9



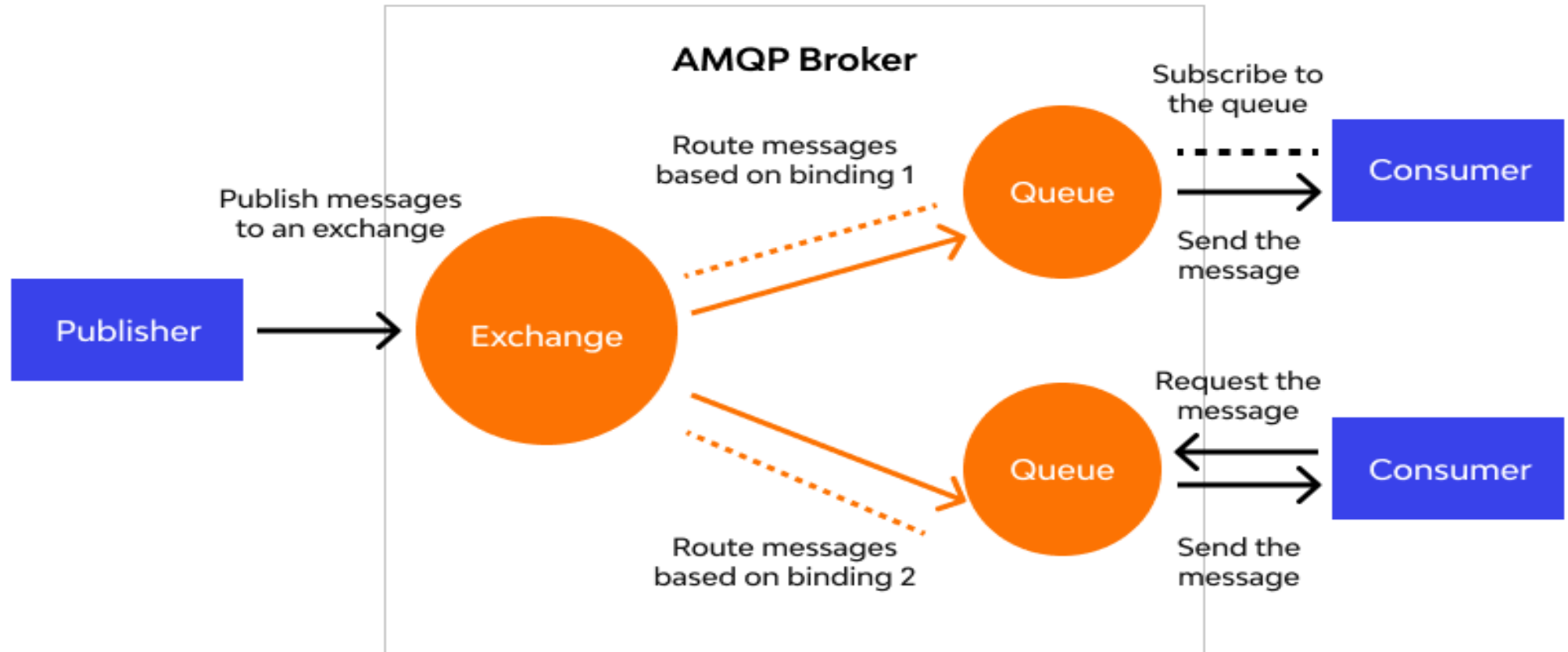
4. Protocoles de données IoT (IoT Data Protocols)

4.1. Le protocole AMQP (Advanced Message Queuing Protocol):

- Protocole de communication orienté messages, conçu pour faciliter le transfert de messages entre des applications ou des services distribués.
- Créée pour la première fois par John O'Hara en 2003.
- AMQP 1.0 a été lancé en octobre 2011
- En octobre 2012, AMQP est devenu le standard OASIS autorisé
- Fonctionnalités clés: le routage, l'orientation des messages et la file d'attente.



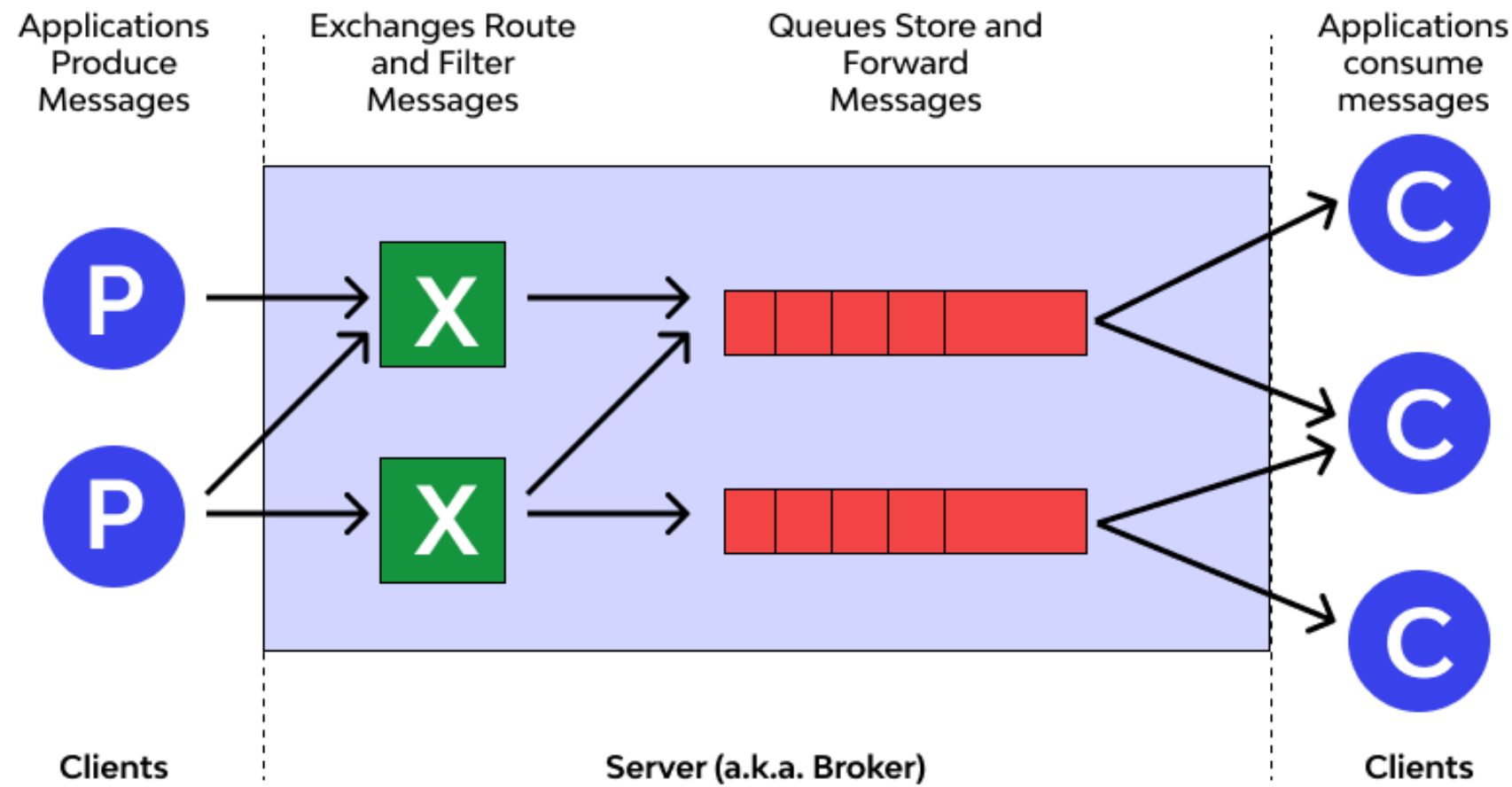
Terminologie AMQP:



Terminologie AMQP:

- **Broker (Courtier) :**
 - Serveur qui agit comme un intermédiaire entre les producteurs de messages (producers) et les consommateurs de messages (consumers).
 - Le broker AMQP gère les files d'attente (queues) dans lesquelles les messages sont stockés et distribués aux consommateurs appropriés en fonction des règles de routage définies.
 - Il assure la fiabilité de la livraison des messages, la gestion des transactions, la sécurité, etc.
- **Producer (Producteur) :**
 - Composant qui crée et envoie des messages vers le broker.
 - Les producteurs sont responsables de la création des messages, de leur encodage conformément au format AMQP, de leur envoi au broker et de la gestion des éventuelles réponses ou confirmations de livraison.
- **Consumer (Consommateur) :**
 - Composant qui reçoit et traite les messages à partir du broker.
 - Les consommateurs sont responsables de la réception des messages depuis les files d'attente du broker, de leur décodage, de leur traitement et de l'envoi éventuel de réponses ou de confirmations au broker.

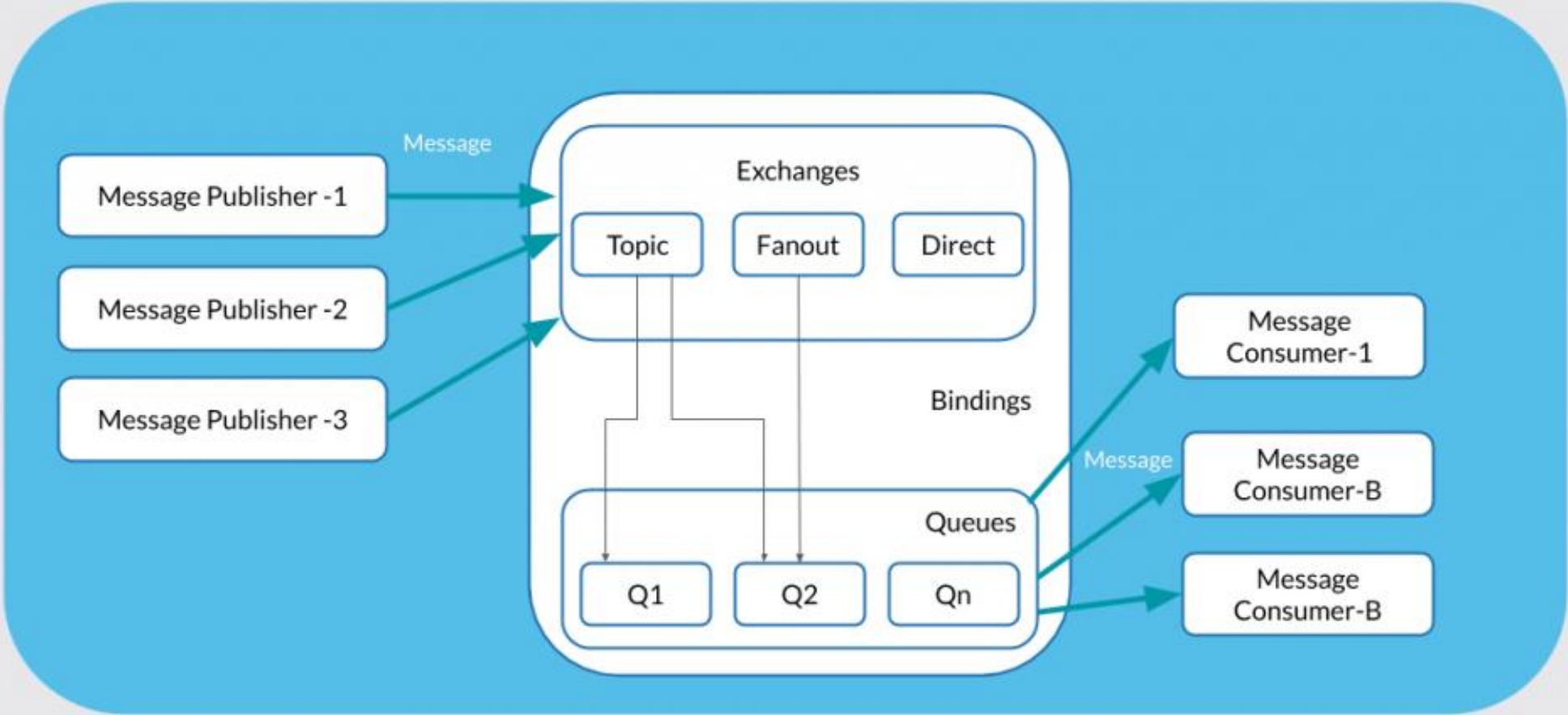
L'échange AMQP:



L'échange AMQP:

- **Publication de messages par les producteurs** : Les producteurs AMQP créent et publient des messages vers l'échange sur le broker. Chaque message est accompagné d'une clé de routage (routing key) qui indique à quelles files d'attente l'échange doit envoyer le message
- **Routage des messages** : L'échange utilise les règles de routage pour acheminer les messages reçus des producteurs vers les files d'attente appropriées en fonction de la clé de routage. Il existe différents types d'échanges dans AMQP, tels que direct, topic, fanout, headers, qui déterminent le comportement de routage.
- **Consommation des messages par les consommateurs** : Les consommateurs AMQP se connectent aux files d'attente pour recevoir et traiter les messages qui y sont stockés. Chaque consommateur peut être lié à une file d'attente spécifique ou à plusieurs files d'attente, en fonction de ses besoins de consommation de messages

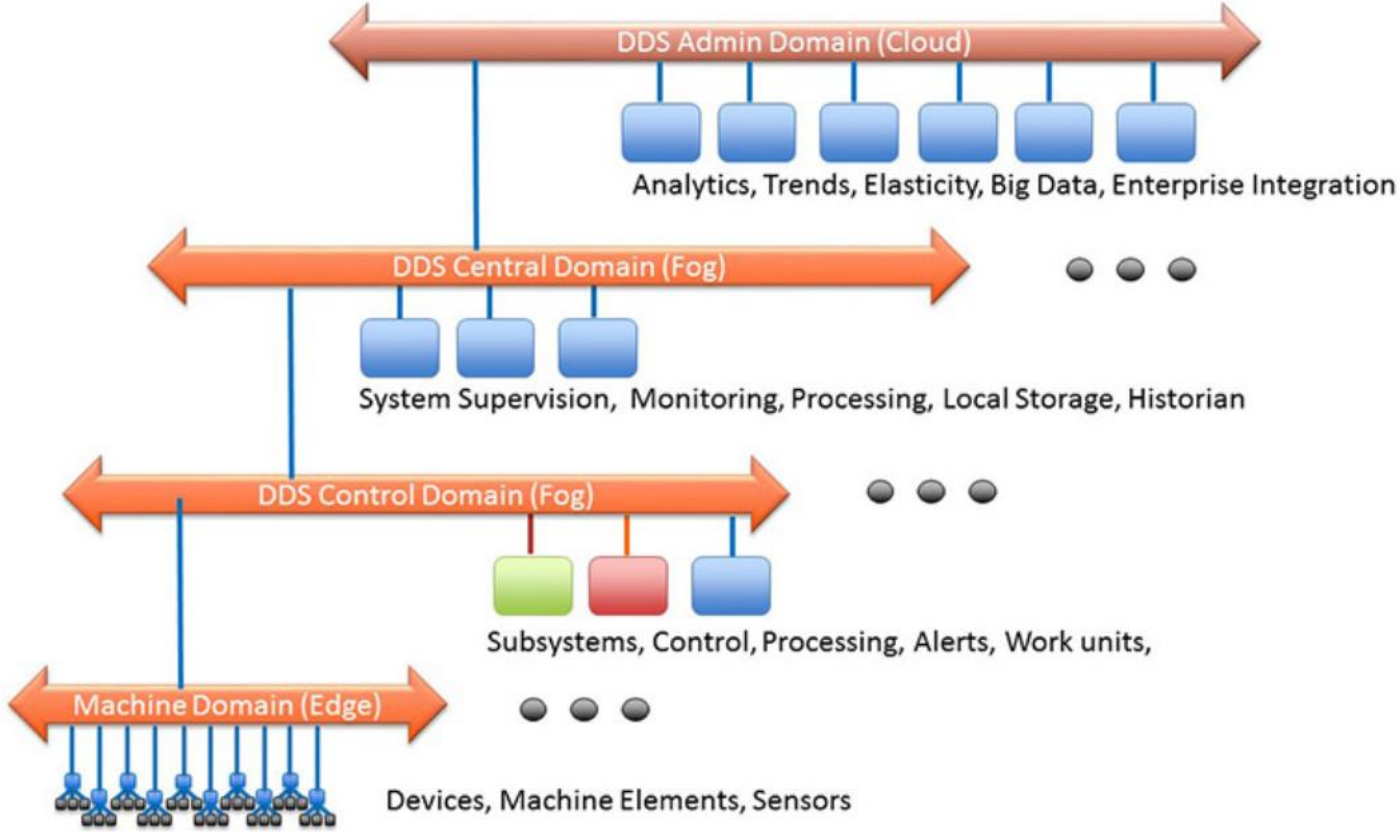
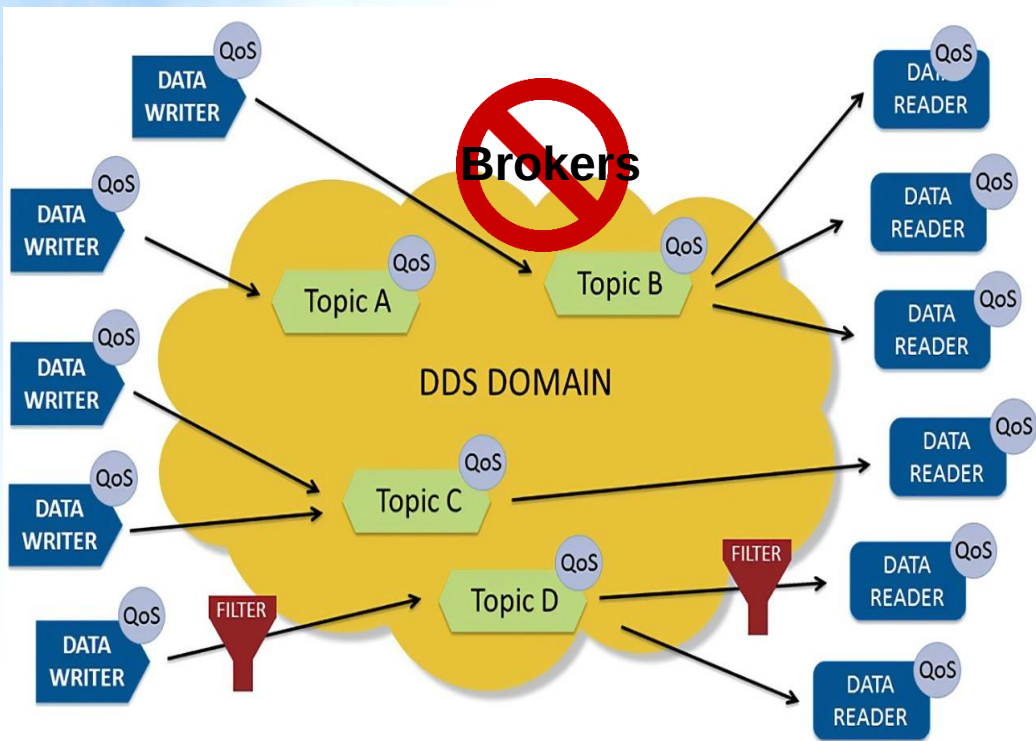
AMQP Elements



4.2. Le protocole DDS (Data Distribution Service):

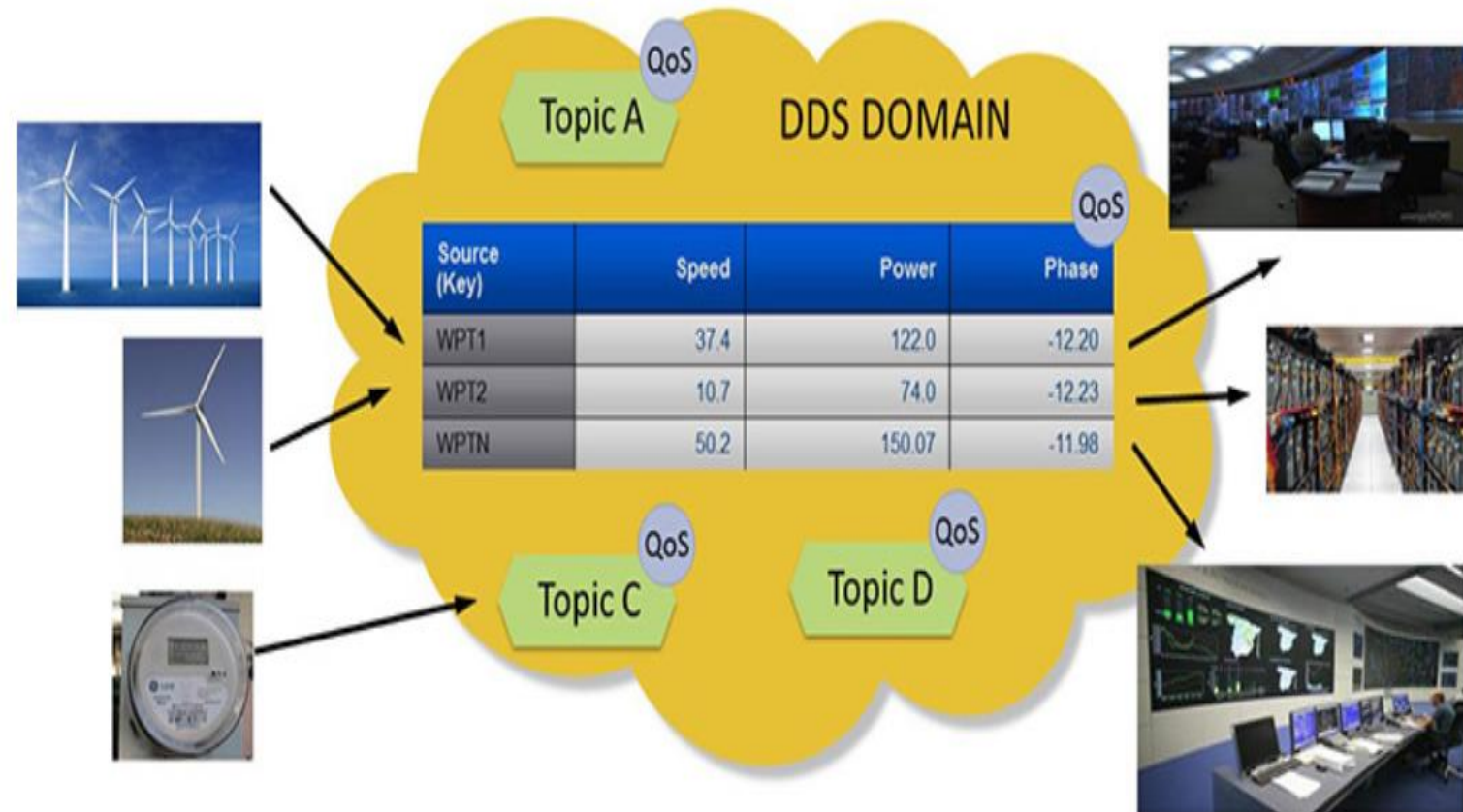
- Le protocole DDS est un standard de communication utilisé principalement dans les systèmes distribués en temps réel pour la diffusion et l'échange de données entre des composants logiciels hétérogènes.
- Quelques points clés sur le protocole DDS :
 - Communication en Temps Réel
 - Communication peut se faire de manière peer-to-peer (P2P) entre les nœuds du système distribué (**pas de broker: brokerless**)
 - Modèle de Publication/Abonnement (publish/subscribe)
 - QoS (Quality of Service) Paramétrable
 - Interopérabilité : Conçu pour être interopérable entre différents systèmes et plateformes
 - Capable de gérer des données complexes et structurées, telles que des données en temps réel, des événements, des états, des commandes
 - Intègre des fonctionnalités de sécurité telles que l'authentification, le chiffrement des données, le contrôle d'accès

Architecture DDS:



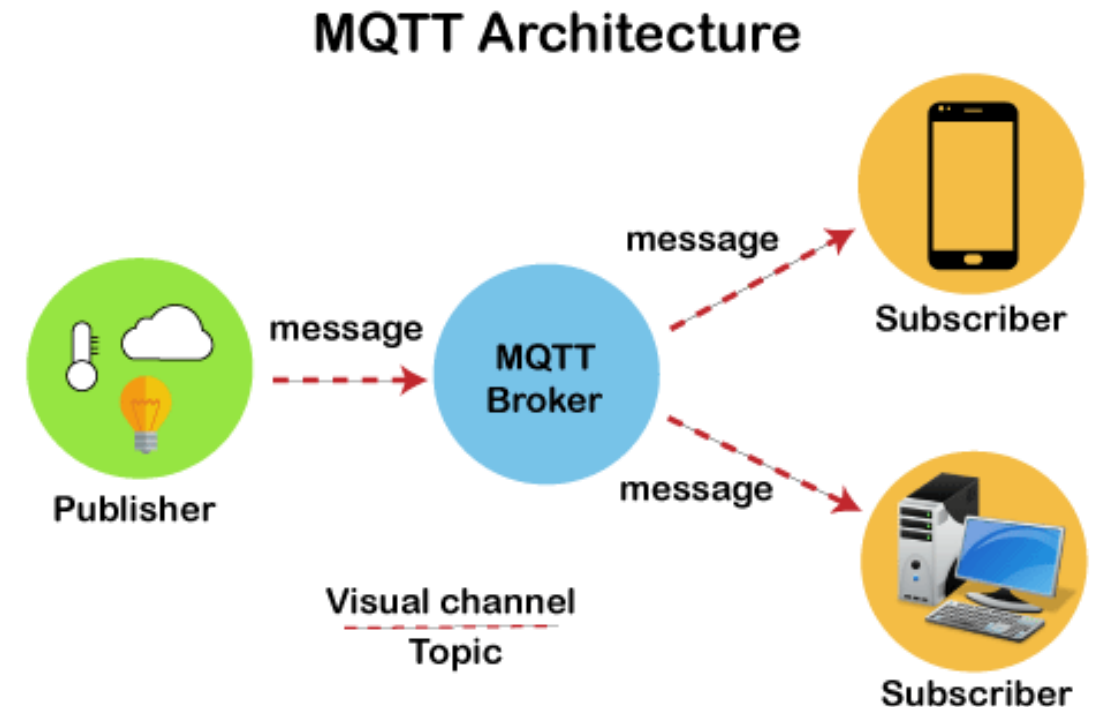
Applications:

En raison de sa fiabilité, de sa performance et de sa capacité à gérer des volumes élevés de données en temps réel, DDS est souvent utilisé dans des applications critiques telles que le contrôle industriel, les systèmes embarqués, la santé, la défense, etc.



4.3. Le protocole MQTT (Message Queuing Telemetry Transport):

- **MQTT utilise un modèle de publication/abonnement**
 - Les appareils clients (abonnés: Subscribers) s'abonnent à des sujets (topics) spécifiques pour recevoir des messages, tandis que les appareils ou les serveurs (éditeurs: Publishers) publient des messages sur ces sujets.
 - Cela permet une communication flexible et évite le besoin de communications directes entre chaque paire d'appareils.
- **MQTT est un protocole open-source.**



- Apparu en 1999, standardisé depuis 2014, il devient désormais incontournable (2019)
- Utilisé par de nombreux acteurs dans le monde, Facebook, OpenStack, Geospatial, Bosch, IBM, Adafruit, EVERYTHING IoT, Amazon IoT, Google Home Assistant, Pimatic, MS Azure, certains systèmes de signalisation, systèmes d'alarme, industrie du Gaz, de l'électricité et bien plus encore.
- Les composantes principales du protocole MQTT sont:



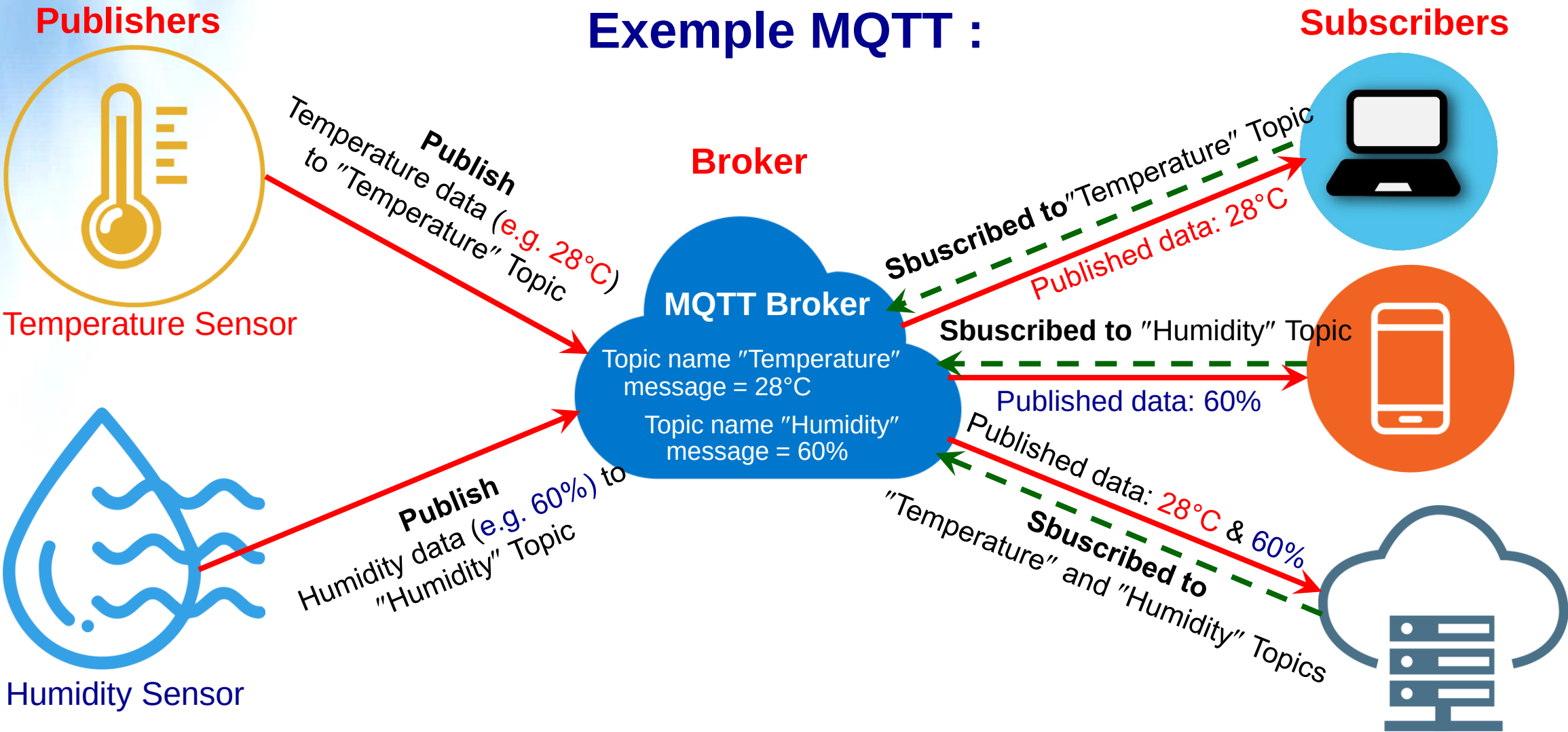
BROKER (Courtier):

- Le broker MQTT reçoit les messages des appareils connectés et les route vers les destinataires appropriés.
- La plupart des brokers MQTT sont publics (open source):
 - Mosquitto
 - EMQ X Broker
 - VerneMQ
 - RabbitMQ
 - ActiveMQ
 - JoramMQ
 - EMQTT (ou EMQ X)

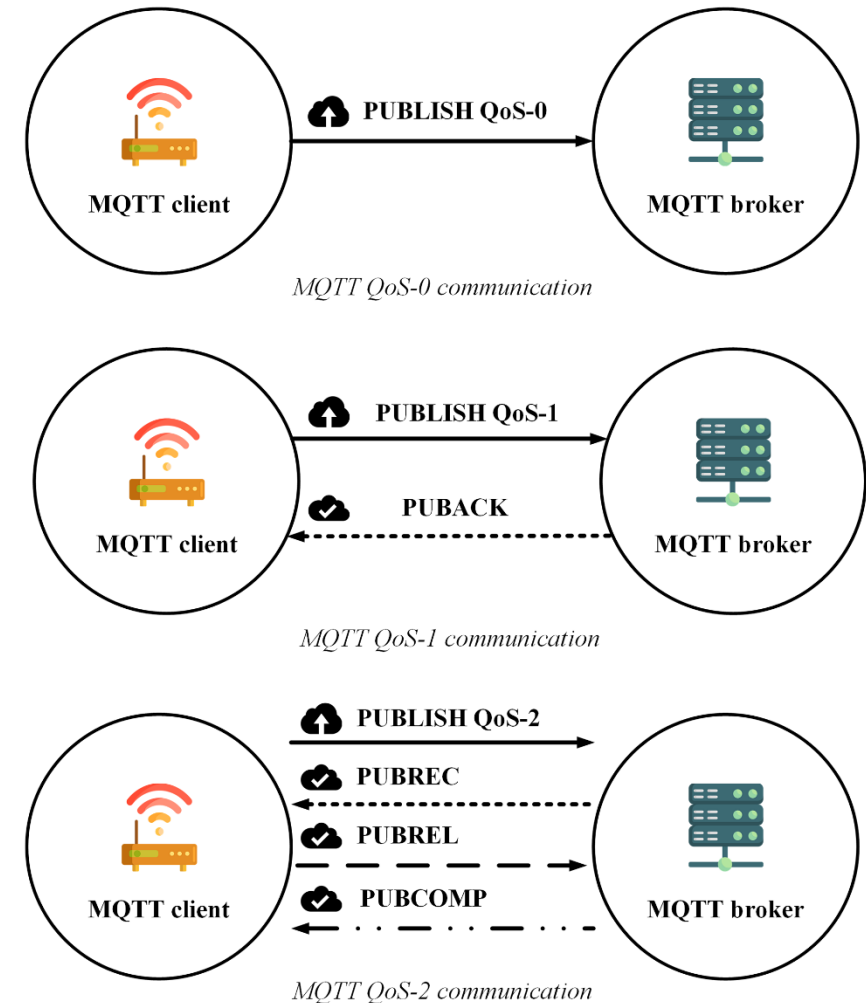
TOPICS (Sujets):

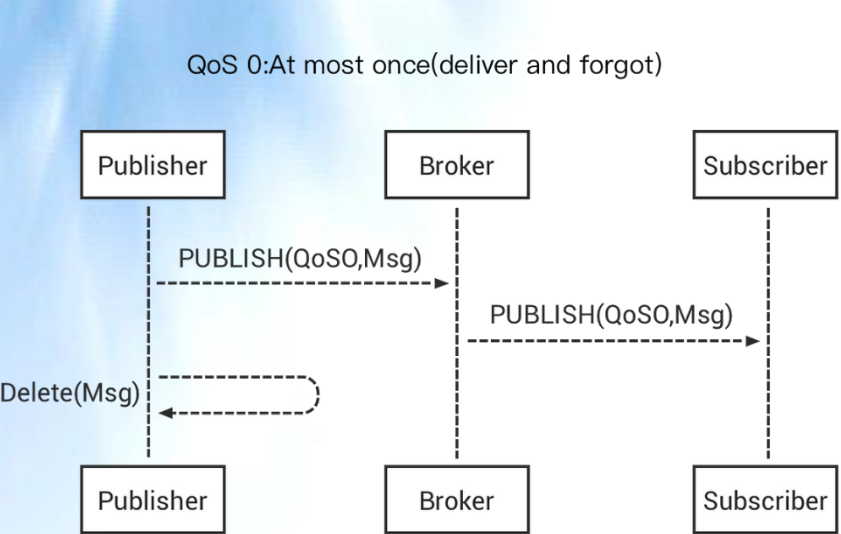
- Les topics sont construits de manière hiérarchique un peu comme les url:
 - Maison/chambre1/temperature
 - Maison/chambre1/lampe
 - Maison/chambre1/#
 - Maison/#

Le symbole dièse "#" est appelé le caractère wildcard multi-level, et il est utilisé dans un topic MQTT pour s'abonner à tous les sous-topics correspondants à un niveau donné dans la hiérarchie. Par exemple, si vous vous abonnez à « Maison/chambre1/#", cela signifie que vous recevrez tous les messages publiés sur des topics commençant par « Maison/chambre1/", quelle que soit la profondeur des sous-niveaux (par exemple, « Maison/chambre1/lampe", « Maison/chambre1/température", etc.).

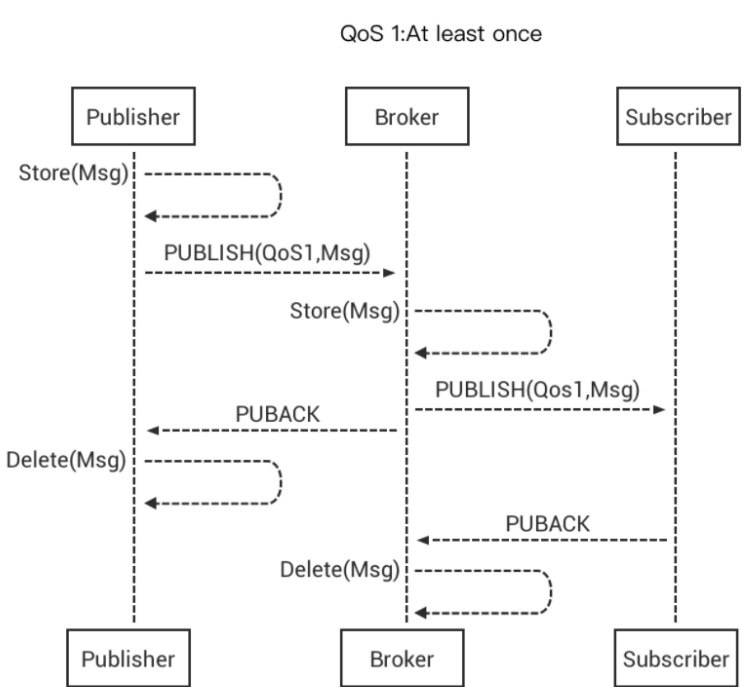


- **QoS: Quality of Service:** MQTT prend en charge plusieurs niveaux de qualité de service (QoS) pour la livraison des messages :
 - QoS 0 : Au plus une fois (at most once) - Les messages sont envoyés sans garantie de livraison.
 - QoS 1 : Au moins une fois (at least once) - Les messages sont envoyés avec garantie de livraison, mais peuvent être reçus en double.
 - QoS 2 : Exactement une fois (exactly once) - Les messages sont envoyés et livrés exactement une fois, garantissant une livraison sans doublon.

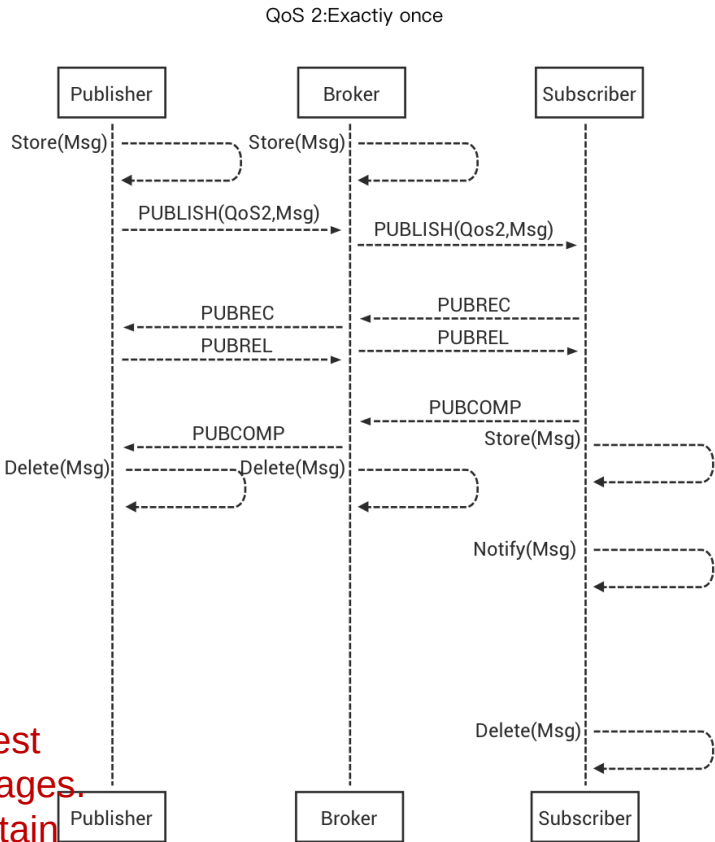




QoS0: utilisé lorsque la perte de certains messages est acceptable: données qui ne nécessitent pas une garantie de livraison absolue.



QoS1: utilisé lorsque la garantie de livraison au moins une fois est nécessaire, même si cela peut entraîner des doublons de messages. Si le Publieur ne reçoit pas de PUBACK du Broker après un certain temps, il renvoie la publication pour garantir que le message est livré au moins une fois.



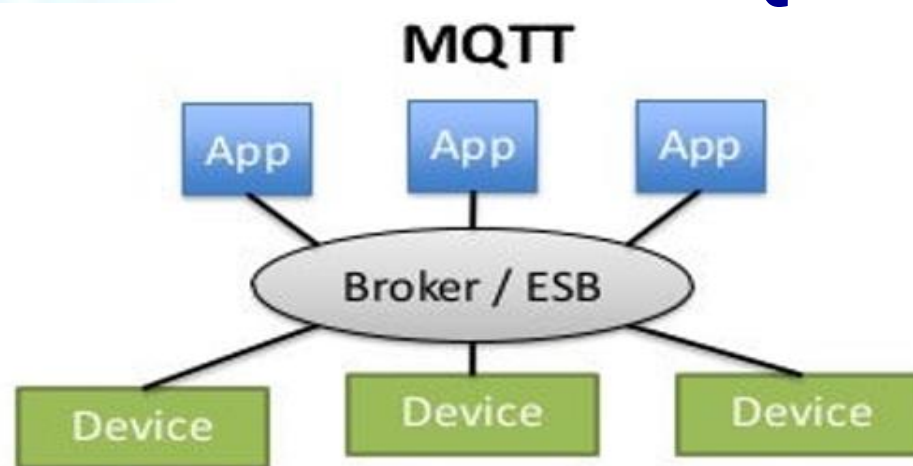
QoS2: utilisé lorsque la garantie de livraison exactement une fois est essentielle: commandes critiques ou des mises à jour de données sensibles où la duplication de messages est indésirable

- Pubrec: Publication Received
- Pubrel: Publication Release
- Pubcomp: Publication Complete
- Puback: Publication Acknowledgment

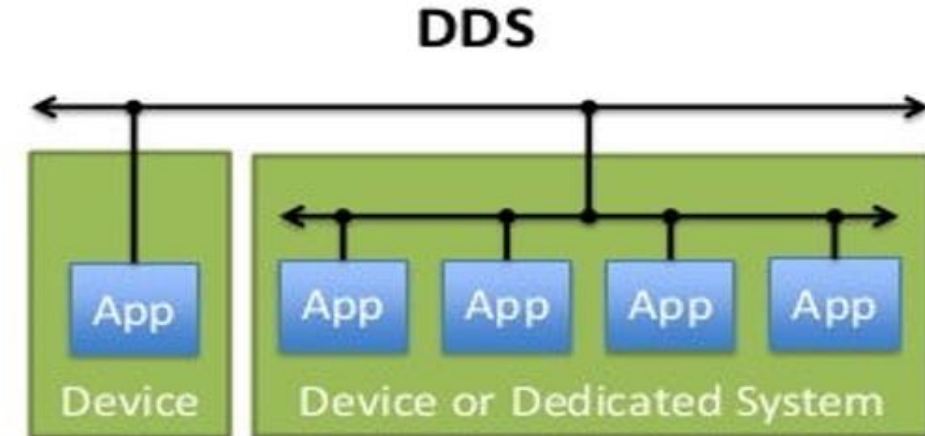
- **Session persistante** : MQTT prend en charge les sessions persistantes, ce qui signifie que les abonnés peuvent recevoir des messages même après une interruption de connexion. Cela garantit une communication fiable et continue, même dans des environnements où la connectivité peut être intermittente.
- **Sécurité** : MQTT offre des mécanismes de sécurité pour protéger la confidentialité et l'intégrité des données, y compris l'authentification des clients, le chiffrement des données (TLS/SSL), et la gestion des autorisations d'accès aux sujets.

TLS: Transport Layer Security SSL: Secure Sockets Layer

MQTT vs. DDS :



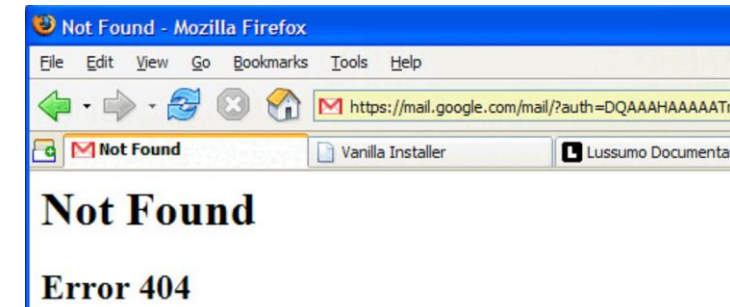
- **Centralized**
 - All comms route through broker
 - Typically TCP
 - Broker queues messages
 - Some service interruption when broker fails over
- **Administered**
 - Broker itself
 - Clients configured with broker/server address

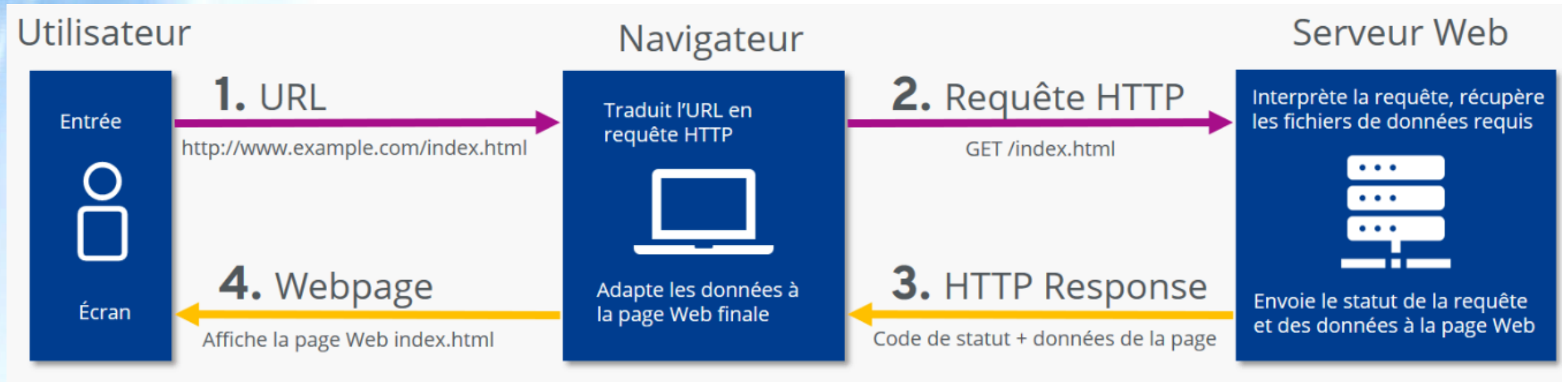


- **Decentralized**
 - Peer-to-peer communication
 - Typically UDP; multicast for one-to-many
 - Fully embeddable: no external s/w
 - Keeps latency and jitter low: no intermediary, bottleneck
 - No single point of failure or service interruptions
- **No admin/config required at deployment**
 - Automatic discovery → plug-and-play
 - Self-forming and self-healing

4.4. Le protocole HTTP (Hypertext Transfer Protocol):

- **Communication Client-Serveur** : HTTP suit un modèle de communication client-serveur, où le client envoie une requête au serveur et attend une réponse.
- **Méthodes HTTP** : Les méthodes HTTP définissent l'action à effectuer sur la ressource identifiée par l'URL dans la requête. Les principales méthodes incluent:
 - GET (pour obtenir des données),
 - POST (pour envoyer des données au serveur),
 - PUT (pour mettre à jour une ressource),
 - DELETE (pour supprimer une ressource), etc.
- **Codes de Statut** : Les réponses HTTP incluent des codes de statut qui indiquent le résultat de la requête. Par exemple,
 - le code 200 signifie "OK" (la requête a réussi),
 - le code 404 indique "Not Found" (la ressource demandée n'a pas été trouvée),
 - le code 500 signifie "Internal Server Error" (erreur interne du serveur), etc.





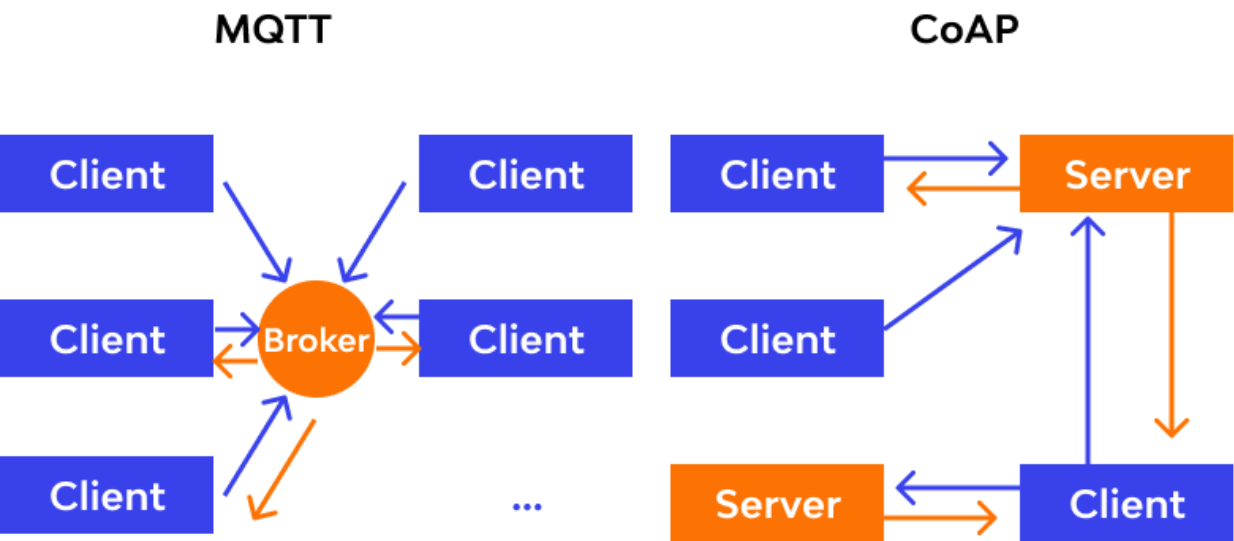
Exemples de Navigateurs:
Google Chrome,
Mozilla Firefox,
Microsoft Edge,
Safari (développé par Apple)

Exemples de Serveurs Web :
Apache HTTP Server;
Nginx;
Microsoft Internet Information
Services (IIS) ;
LiteSpeed Web Server

4.5. Le protocole CoAP (Constrained Application Protocol)

- **Objectif** : CoAP a été développé pour fournir une alternative légère et efficace à HTTP pour les appareils IoT, qui peuvent avoir des ressources limitées en termes de mémoire et de puissance de traitement.
- **Caractéristiques principales** :
 - **RESTful** : CoAP suit le modèle architectural REST (Representational State Transfer), ce qui le rend similaire à HTTP en termes de style d'architecture. Cela permet une interaction simple et cohérente avec les ressources sur le réseau.
 - **UDP** : Contrairement à HTTP qui utilise TCP comme protocole de transport, CoAP utilise UDP (User Datagram Protocol) pour réduire la surcharge liée à la gestion de la connexion.
 - **Méthodes similaires à HTTP** : CoAP utilise des méthodes similaires à celles d'HTTP, telles que GET, POST, PUT, DELETE, pour effectuer des opérations sur les ressources.

MQTT vs. CoAP



Positionnement de HTTP et CoAP dans le modèle OSI

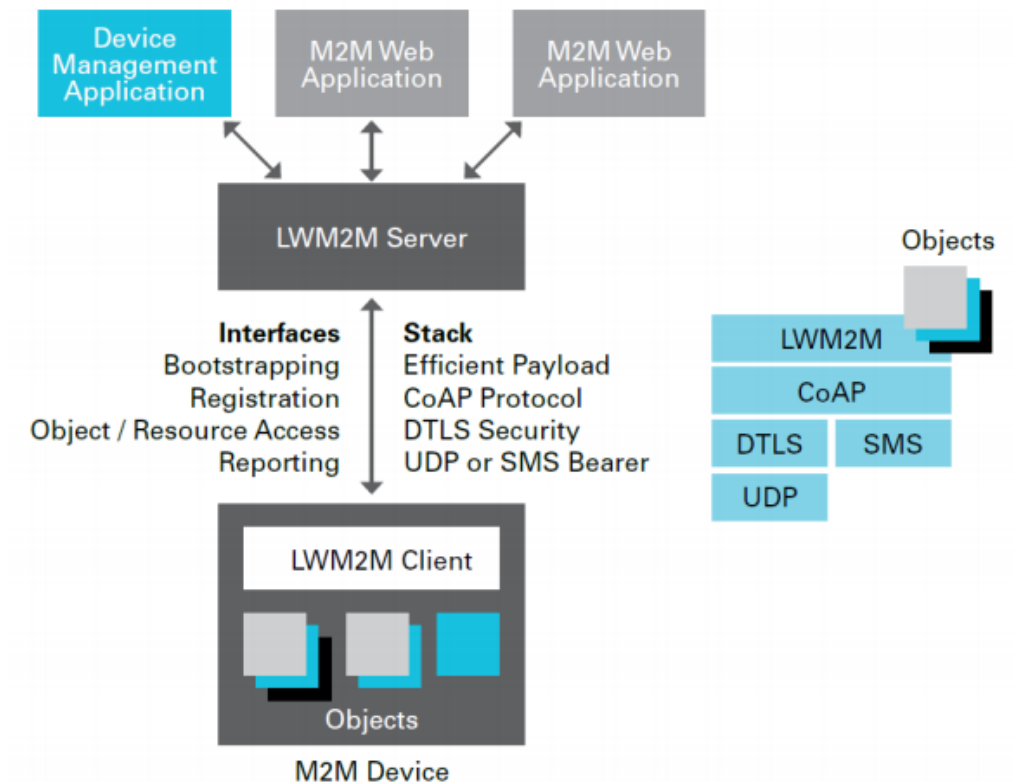
Navigateur Web / Applications M2M				Application
HTTP		CoAP		
TCP		UDP		Transport
IPv4 / IPv6			IPv6	Réseau
			6LoWPAN	
UMTS / GPRS	802.3 Ethernet	802.11 Wifi	802.15.4 LoWPAN	Physique et Liaison de Données

Voici quelques-unes des principales bibliothèques et frameworks qui permettent de mettre en œuvre le protocole CoAP dans le développement d'applications IoT:

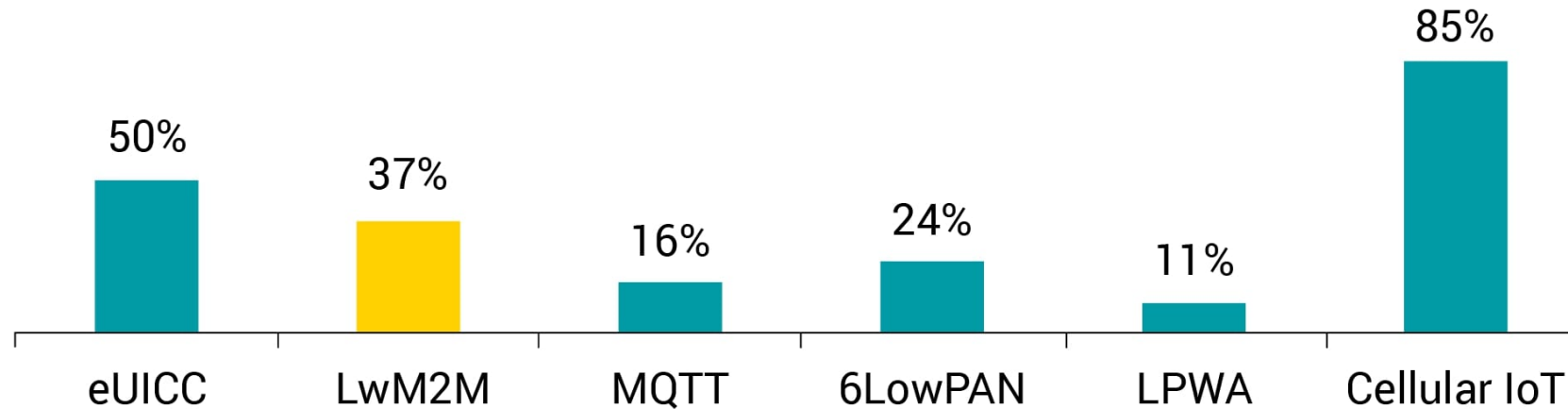
- Californium (Java)
- libcoap (C)
- CoAPthon (Python)
- node-coap (Node.js)
- Microcoap (C)

4.6. Le protocole LwM2M (Lightweight Machine-to-Machine)

- Conçu pour être léger, efficace et adapté aux appareils IoT à faible puissance, LwM2M offre des fonctionnalités de gestion à distance et de communication entre les appareils et les serveurs IoT.
- Repose sur une architecture client/serveur où les appareils IoT (clients LwM2M) communiquent avec des serveurs LwM2M pour échanger des informations.
- LwM2M utilise le protocole CoAP (Constrained Application Protocol) comme protocole de transport pour la communication entre les clients et les serveurs.



The Lightweight M2M architecture with LwM2M Server and LwM2M Client

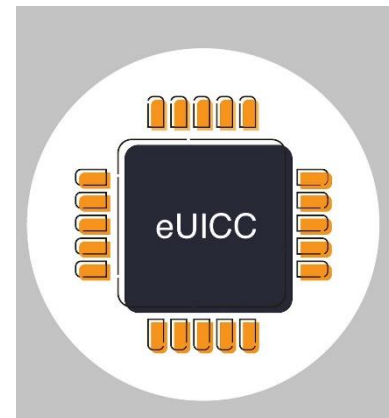


Source: IDATE DigiWorld - Key IoT Technologies 2017

eUICC: embedded Universal Integrated Circuit Card.

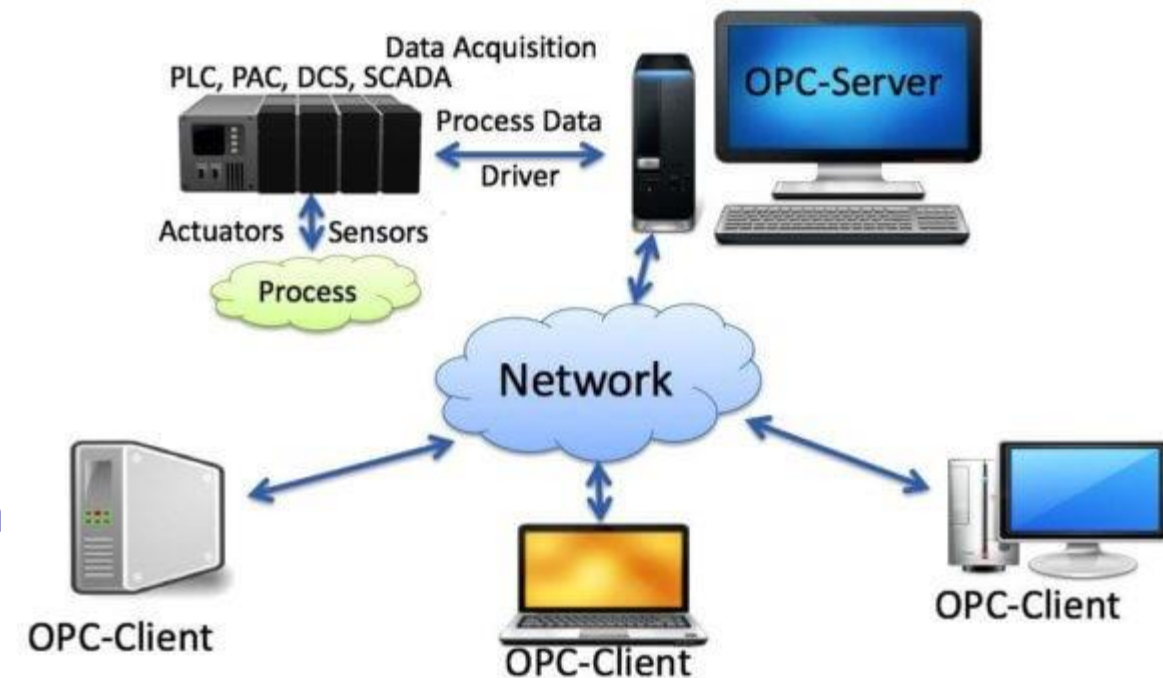
Il s'agit d'une technologie de carte SIM embarquée dans des appareils électroniques, tels que les smartphones, les tablettes, les montres connectées, les véhicules connectés, etc.

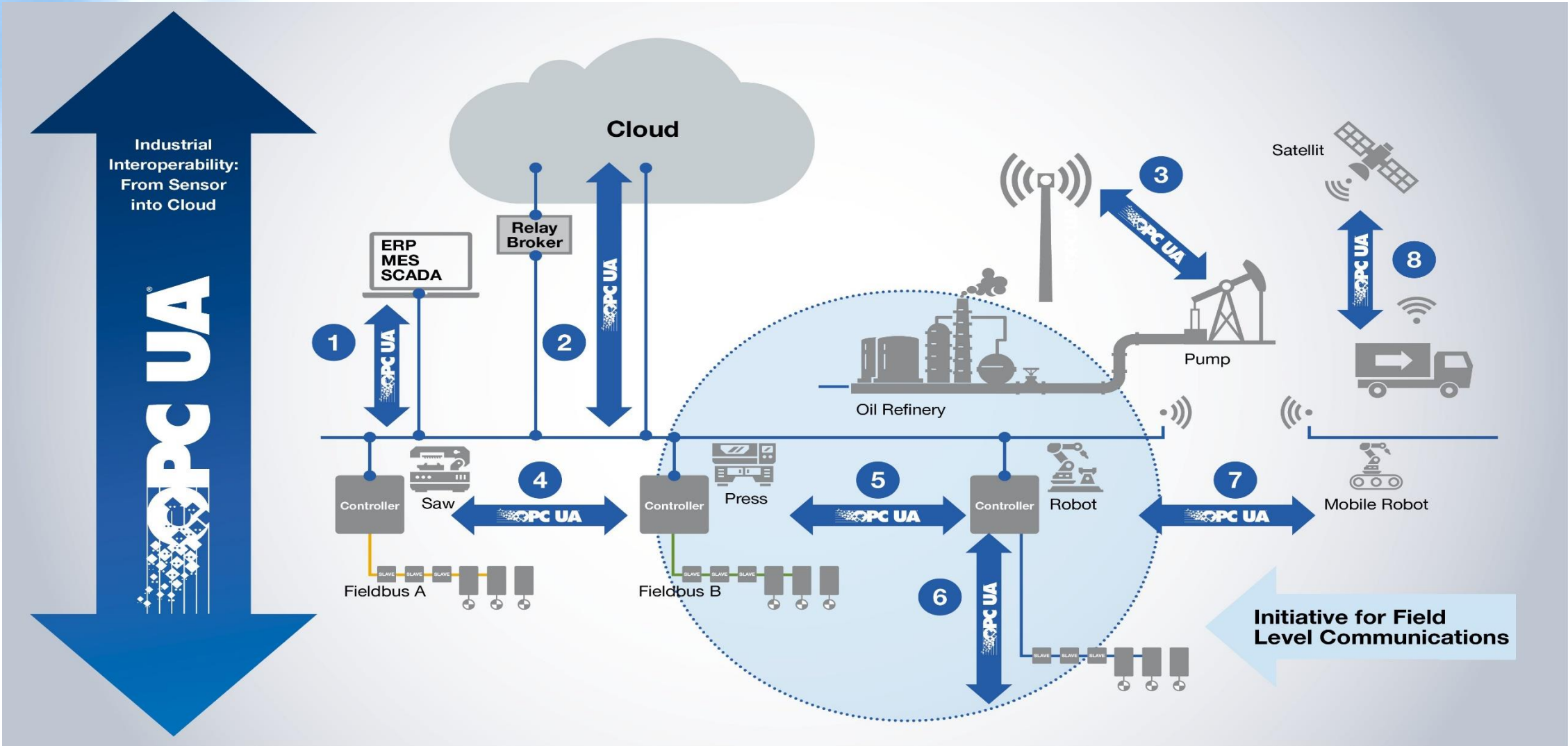
Peuvent être programmées à distance pour changer de réseau mobile sans nécessiter de remplacement physique de la carte.



4.7. Le protocole OPC UA (Open Platform Communication Unified Architecture)

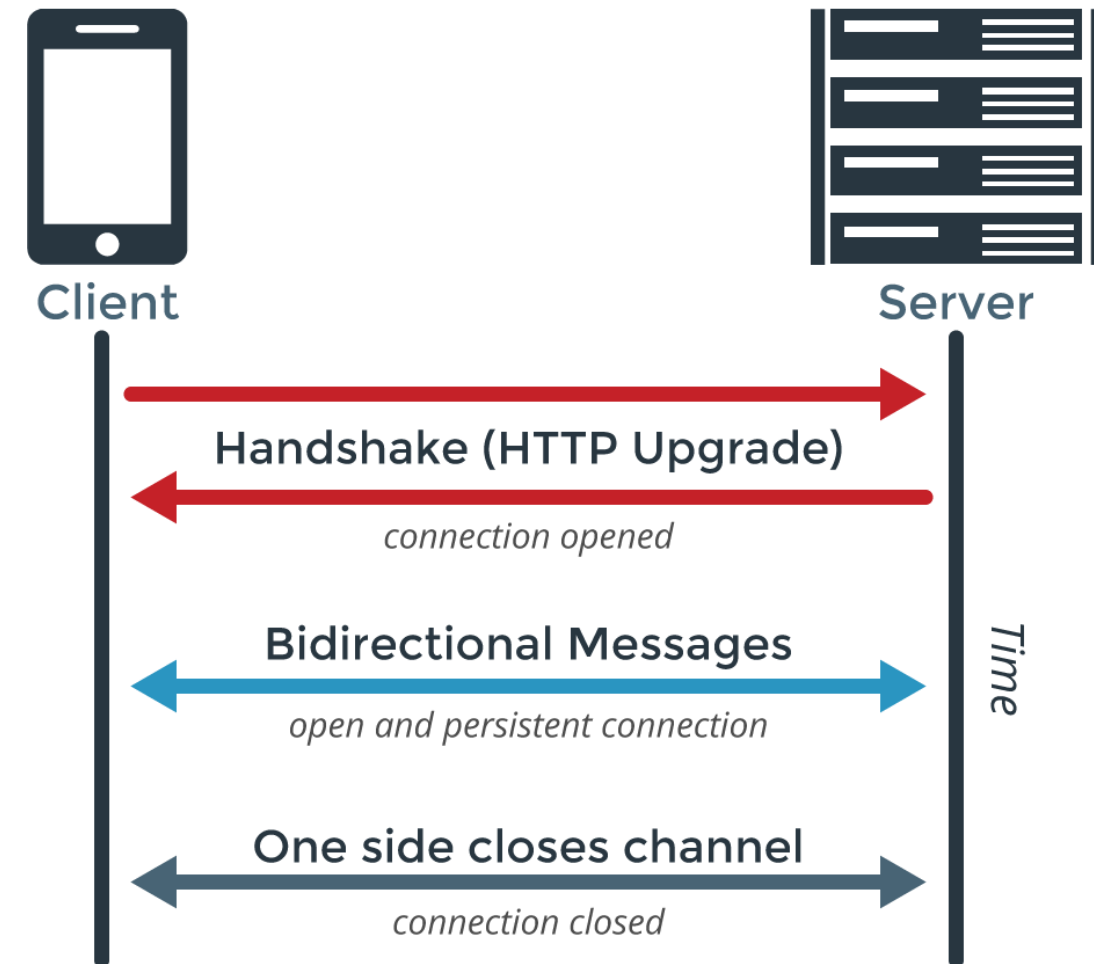
- L'OPC UA est un standard de communication industrielle qui facilite l'échange de données entre les systèmes informatiques utilisés dans les environnements industriels.
- OPC UA vise à améliorer l'interopérabilité entre les différents systèmes industriels, qu'ils proviennent de différents fabricants ou qu'ils utilisent des technologies et des protocoles de communication variés
- OPC UA offre une architecture unifiée qui prend en charge divers types de données, de services et de fonctionnalités, ce qui le rend adapté à une large gamme d'applications industrielles, y compris la surveillance en temps réel, la gestion des actifs, la maintenance prédictive, etc

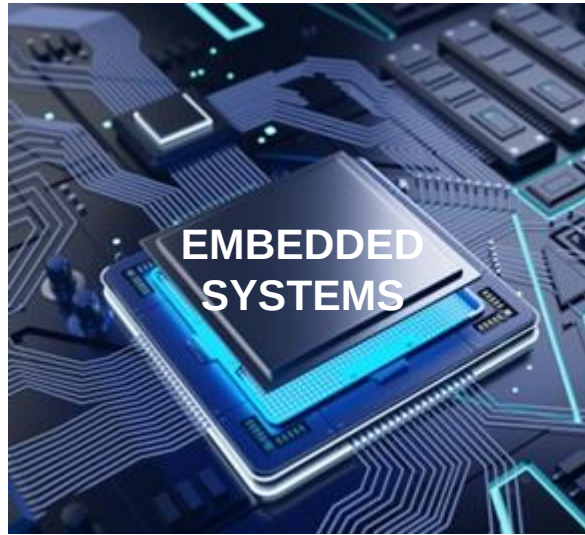




4.8. Le protocole WebSocket

- Le protocole WebSocket est un protocole de communication bidirectionnelle et full-duplex qui permet une communication interactive en temps réel entre un navigateur web (client) et un serveur.
- Contrairement au protocole HTTP traditionnel qui suit le modèle de requête-réponse, WebSocket permet une communication continue et simultanée, ce qui le rend particulièrement adapté aux applications nécessitant des mises à jour en temps réel, telles que les applications de chat, les jeux en ligne, les tableaux de bord en direct, etc





FIN !
Questions ?