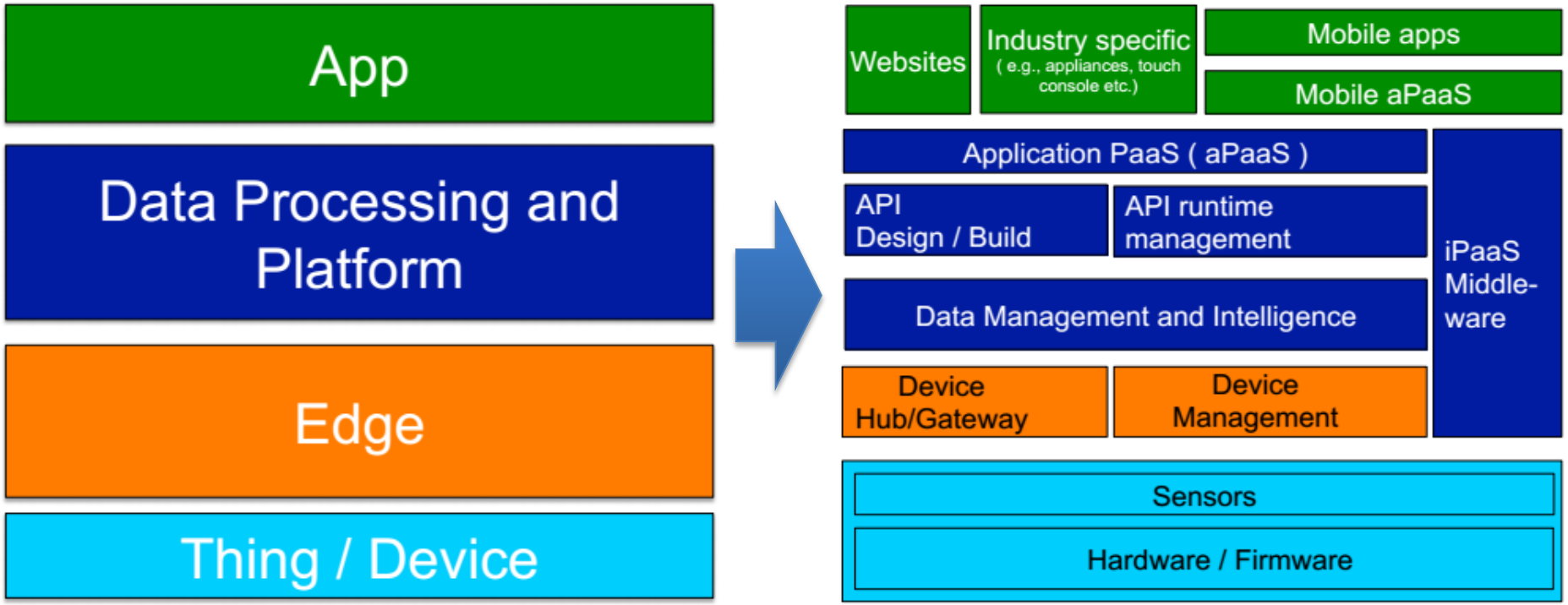
Arquitecturas de referencia y protocolos de comunicaciones en IoT

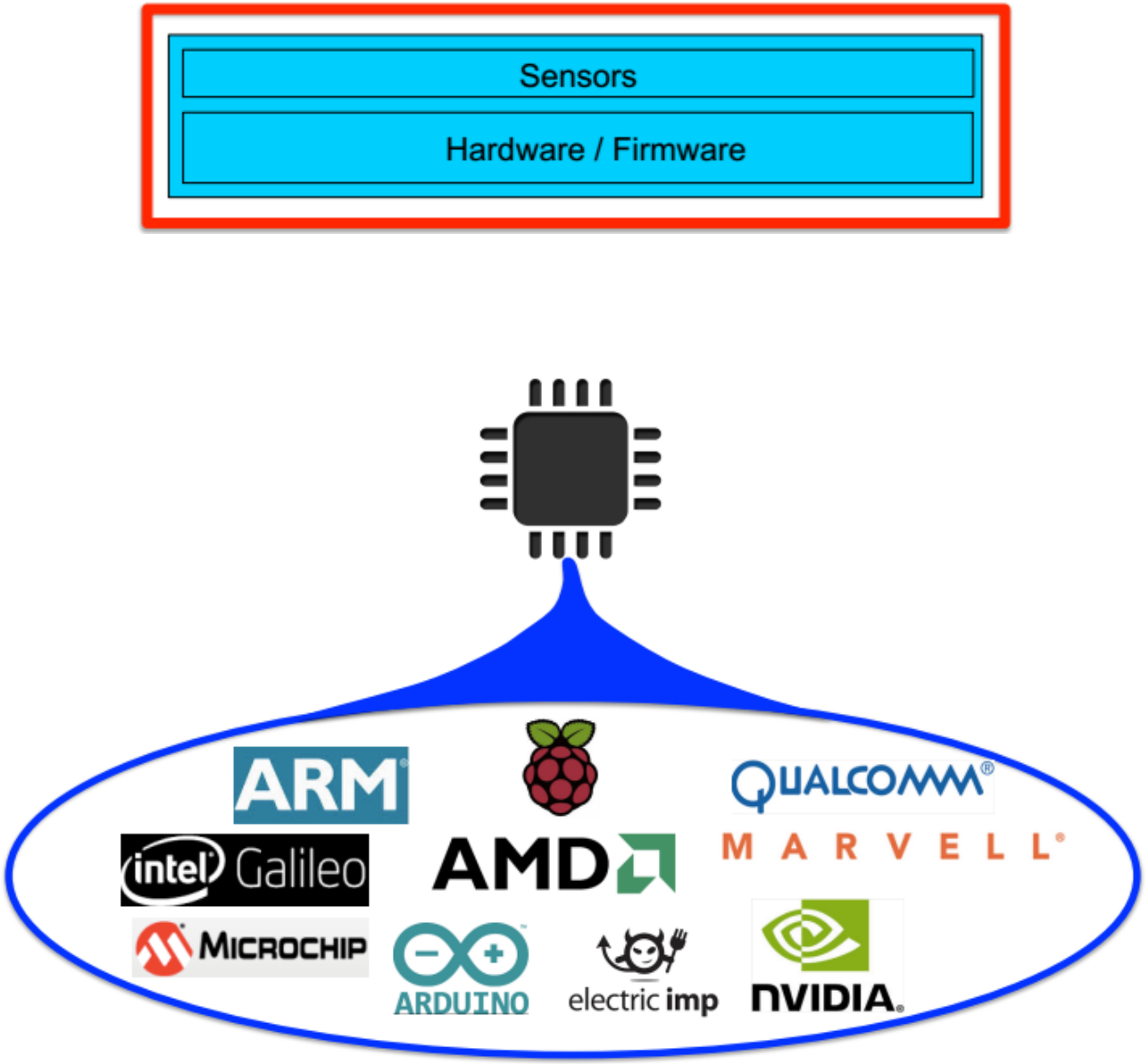
Internet de las cosas en el contexto de Big Data

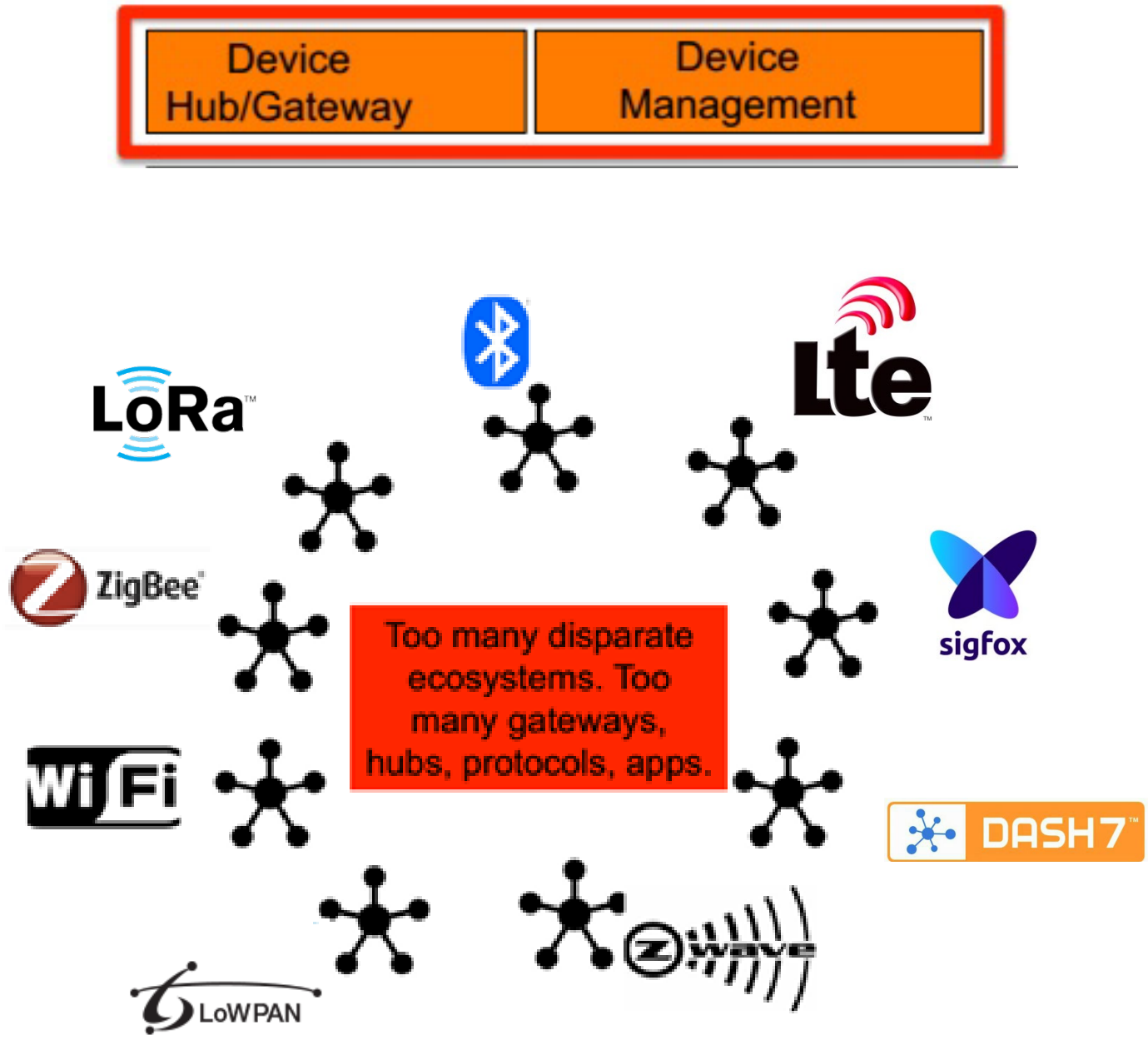
Máster Interuniversitario en Big Data: Tecnologías de Análisis de Datos Masivos

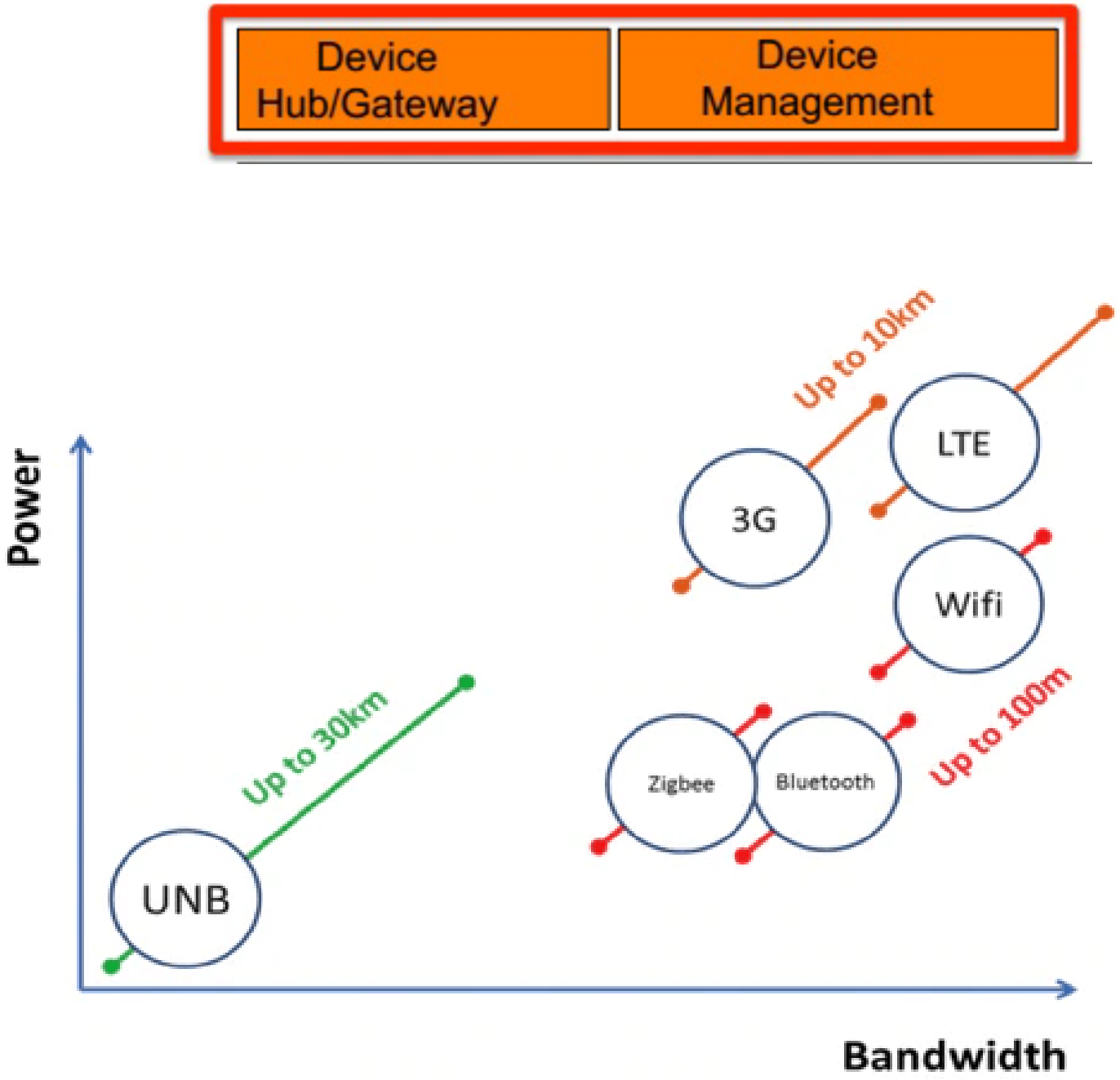
Universidade de Santiago de Compostela (USC)

Arquitectura de referencia en IoT




Sensors
Hardware / Firmware
ARM
QUALCOMM
MARVELL
intel Galileo
AMD
MICROCHIP
ARDUINO
electric imp
NVIDIA


Device Hub/Gateway
Device Management
LoRa
Lte
ZigBee
sigfox
Too many disparate ecosystems. Too many gateways, hubs, protocols, apps.
WiFi
DASH7
LoWPAN
Z-Wave


Device
Hub/Gateway
Device
Management
Power
Bandwidth
Up to 10km
LTE
3G
Wifi
Up to 100m
Zigbee
Bluetooth
Up to 30km
UNB

Data Processing and Platform

Google app engine

Application PaaS (aPaaS) </>

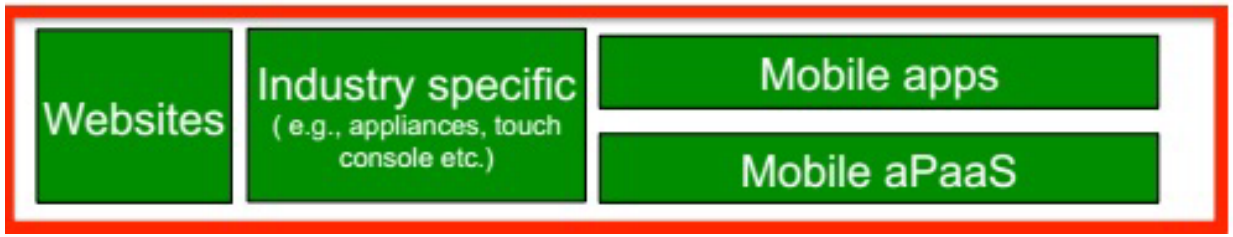
- OS/DB, Storage, Server, Network
- Design and Development tooling
- Management and analytics tooling
- Routing, transform, orchestration services
- Web, Database, Application Server
- Administrative portal

API Design / Build

- API design lifecycle
- API spec creation
- Reusable API patterns
- API mocking/ modelling
- Deployment automation

API runtime management

- Rate limiting / Throttling
- Multi-tenant org / RBAC support
- API SLA management
- Deployment automation
- Custom policy engine
- API and data security



IBM amazon Jasper GE thinger.io platform Blynk

icontrol NETWORKS xively ThingWorx BlackBerry

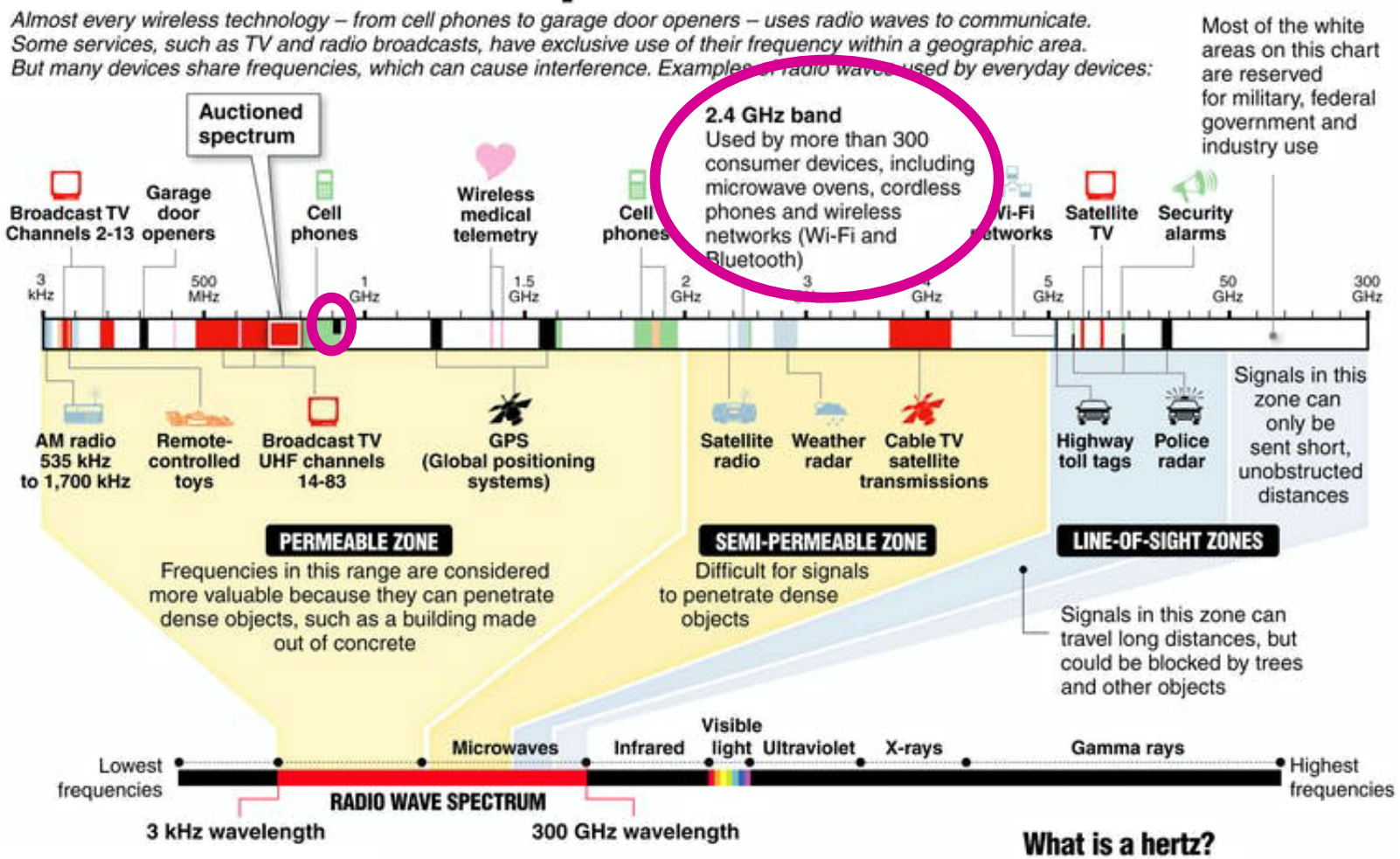
Ayla Networks

ZATAR PubNub SAMSUNG SmartThings

ANDROID iOS

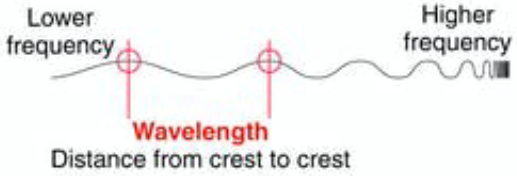
Inside the radio wave spectrum

Almost every wireless technology – from cell phones to garage door openers – uses radio waves to communicate. Some services, such as TV and radio broadcasts, have exclusive use of their frequency within a geographic area. But many devices share frequencies, which can cause interference. Examples of radio waves used by everyday devices:



The electromagnetic spectrum

Radio waves occupy part of the electromagnetic spectrum, a range of electric and magnetic waves of different lengths that travel at the speed of light; other parts of the spectrum include visible light and x-rays; the shortest wavelengths have the highest frequency, measured in hertz



What is a hertz?

One hertz is one cycle per second. For radio waves, a cycle is the distance from wave crest to crest

1 kilohertz (kHz) = 1,000 hertz

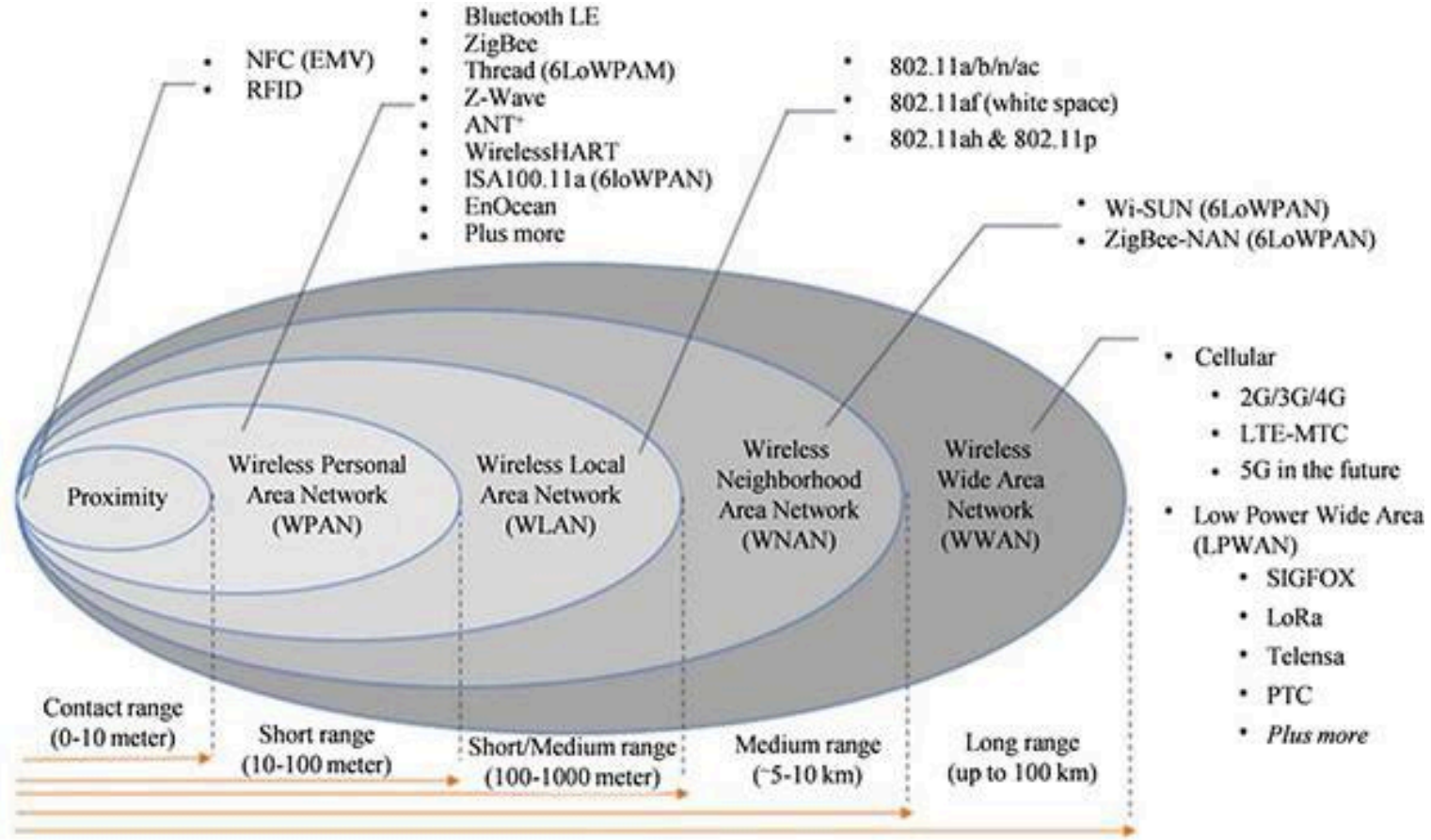
1 megahertz (MHz) = 1 million hertz

1 gigahertz (GHz) = 1 billion hertz

Source: New America Foundation, MCT, Howstuffworks.com
Graphic: Nathaniel Levine, Sacramento Bee

Source: https://theconversation.com/wireless-spectrum-is-for-sale-but-what-is-it-11794

Sub-GHz technologies



* Source: https://www.digikey.com.br/pt/articles/wireless-modules-operating-in-the-sub-ghz-bands

Protocolos de comunicaciones en IoT

- Multitud de protocolos:

- Nivel enlace y red:
  - **802.15.4**
    - **6LoWPAN**
    - **Zigbee**
  - **LoRaWAN**
  - Bluetooth
  - WiFi
  - Weightless protocol
  - Proveedores:
    - Ingenu (M2M)
    - **Sigfox**

- Nivel de aplicación:
  - Constrained Application Protocol (**CoAP**)
  - MQ Telemetry Transport (**MQTT**)
  - Lightweight M2M (LWM2M)
  - REST API
  - XMPP (Extensible Messaging and Presence Protocol)

Estandarización

- **Internet Engineering Task Force (IETF):**
  - 6LoWPAN Working Group (IPv6 global)
  - CoRE Working Group (Rest for IoT, CoAP , Resource Directory)
- **OMA SpecWorks:**
  - Lightweight M2M (LWM2M), basado en CoAP, DTLS, REST
- **ETSI**: Estandarización en comunicaciones M2M, CoAP, HTTP binding…
  - NGSI-LD, context management (Fiware)
- **W3C** : Efficient XML Interexchange (EXI), estándares web
- **ZigBee Alliance**
- **IEEE**: IEEE 802.XX.YY
- **DASH7 Alliance**: Dash7 protocol (bi-directional, sub-Ghz medium range wireless communication)
- **OASIS**: Message Queuing Telemetry Transport (MQTT)

IPv6

- IPv6 permite que un dispositivo IoT obtenga de forma sencilla una dirección IP global, facilitando la comunicación peer-to-peer
- Comunicación usando tecnologías inalámbricas que requieran menos consumo energético por parte de los dispositivos.
- Las redes 6LoWPAN proporcionan mecanismos de encapsulado y compresión de cabeceras lo que reduce los tiempos de transmisión y ofrece conectividad a Internet sin un overhead excesivo.

Diferencias entre IPv4 e IPv6

- **Tamaño de la dirección IP:**
  - IPV4: 32 bits
  - IPv6: 128 bits
- **Método de direccionamiento:**
  - IPV4: numérico y bits binarios separados por un punto
  - IPv6: alfanumérico y bits separados por dos puntos (:)
- **Clases de direcciones IP:**
  - IPv4: cinco clases de direcciones IP diferentes
  - IPv6: número casi ilimitado de direcciones IP. Soporte para rangos privados

Diferencias entre IPv4 e IPv6

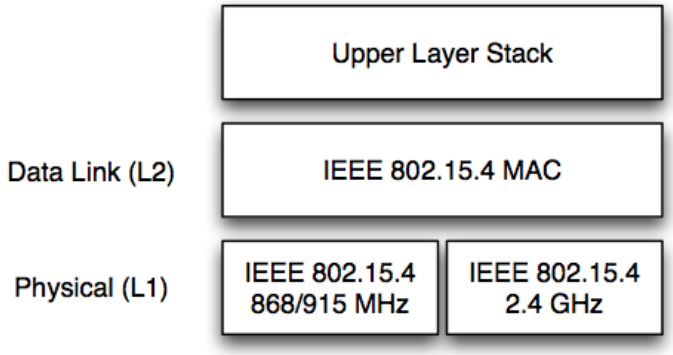
- **Configuración**:
  - IPV4: cada sistema debe ser configurado para poder comunicarse con otros. La red también se configura de manera manual o con DHCP.
  - IPv6: configuración opcional según las funciones. Soporta la autoconfiguración entre dispositivos IPv6
- **Interoperabilidad**
  - IPV4: topologías de red relativamente restringidas, con capacidad limitada de interoperabilidad y movilidad
  - IPv6: capacidad de interoperabilidad y movilidad incluida en los dispositivos de red

IPv6

- **Otras ventajas**
  - Jerarquía estructurada para disminuir tamaño de tablas de enrutamiento. Desacopla prefijo (64bits) del identificador del host (64 bits)
  - Puede ser mejorado con IPsec (Internet Protocol Security, en inglés) para gestionar la encriptación y autenticación entre hosts
  - Soporta el protocolo IPv6 móvil, MIPv6, que permite a los dispositivos móviles cambiar de una red a otra y recibir notificaciones itinerantes

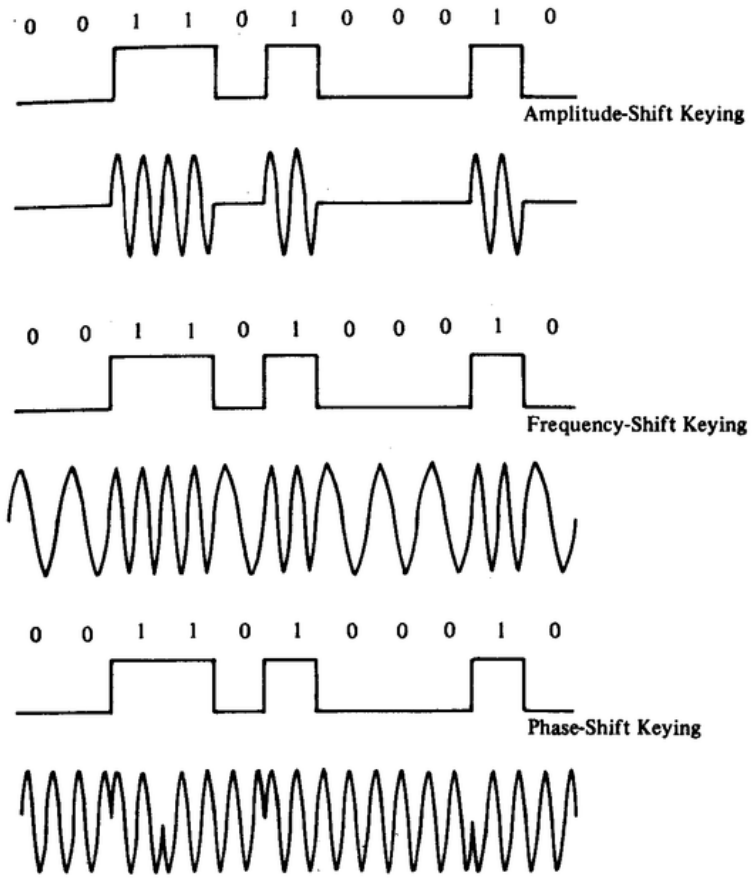
IEEE 802.15.4

- Estándar muy empleado de redes inalámbricas de área personal (WPAN). 1ª versión: 2003
- Utilizado en redes domésticas, control industrial, automatización edificios, WSN…→ corto alcance
- Define control físico y control de acceso al medio (MAC)
- Tres bandas de frecuencias: 868 MHz, 915 MHz, 2.4 GHz
- Tasas bajas de transferencia: 20kbps - 250kbps
- Baja potencia de emisión: 0.5-1 mW
- Rango de entre 10m a 100m
- Modulación: DSSS



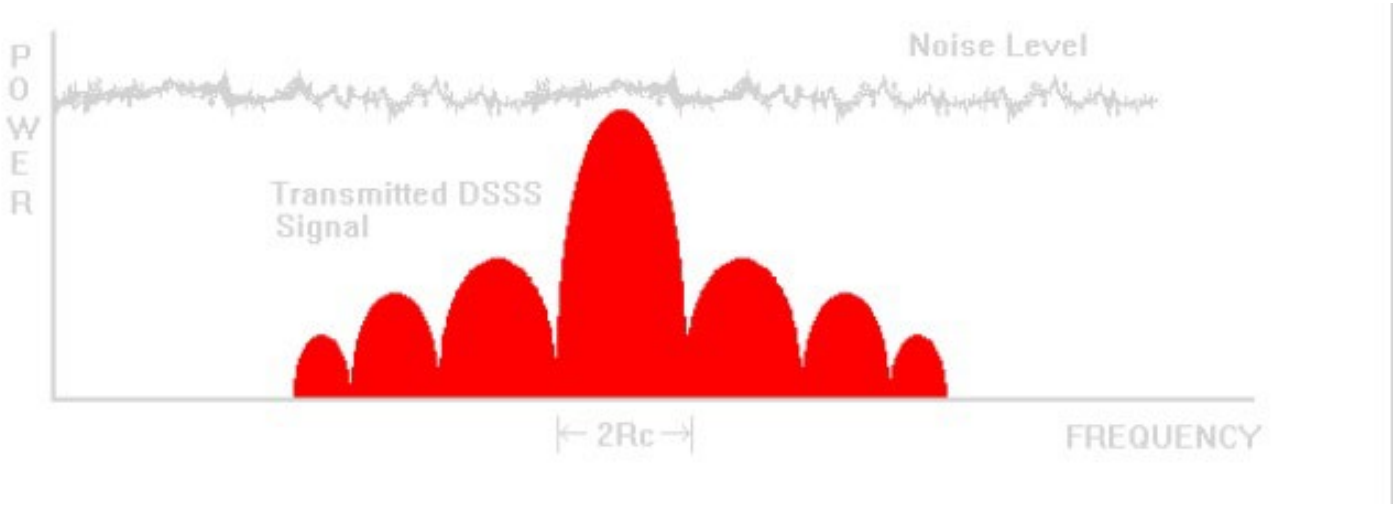
IEEE 802.15.4

- Modulación:
  - DSSS: Direct-Sequence Spread Spectrum
  - PSK: Phase-Shift-Keying. Modulación por desplazamiento de fase

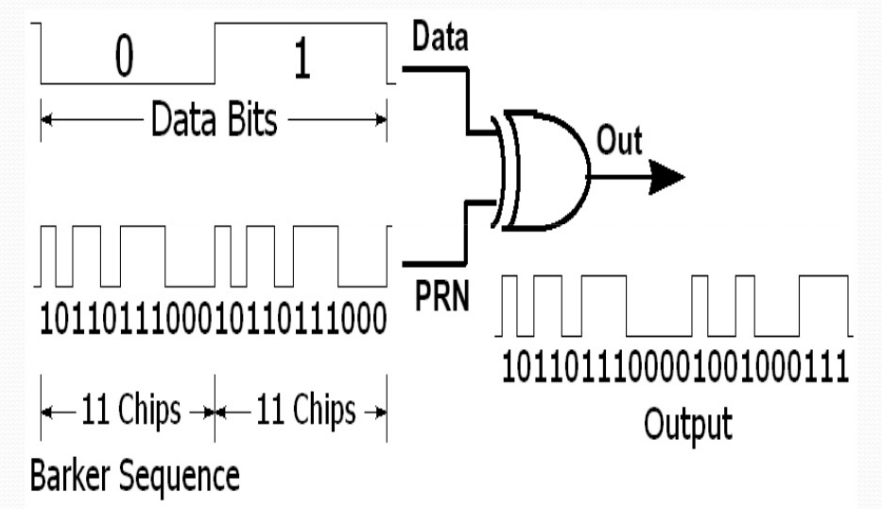


IEEE 802.15.4

- Modulación DSSS:
  - Primero se modula digitalmente una señal de pseudo-ruido (PRN) con la señal de información.
  - Después, se multiplica la portadora RF y la señal PN modulada. De esta forma la señal de RF se transforma en una señal con un gran ancho de banda y un espectro equivalente al de una señal de ruido.
  - En el receptor, se recupera la señal original y se elimina la interferencia.
  - GPS, Galileo, GLONASS, IEEE 802.11b, IEEE 802.15,4, WiFi, ….



IEEE 802.15.4



La salida de la XOR es modulada en una portadora usando BPSK o QPSK

BPSK Encoding

XOR Output	Phase Change
0	0
1	π

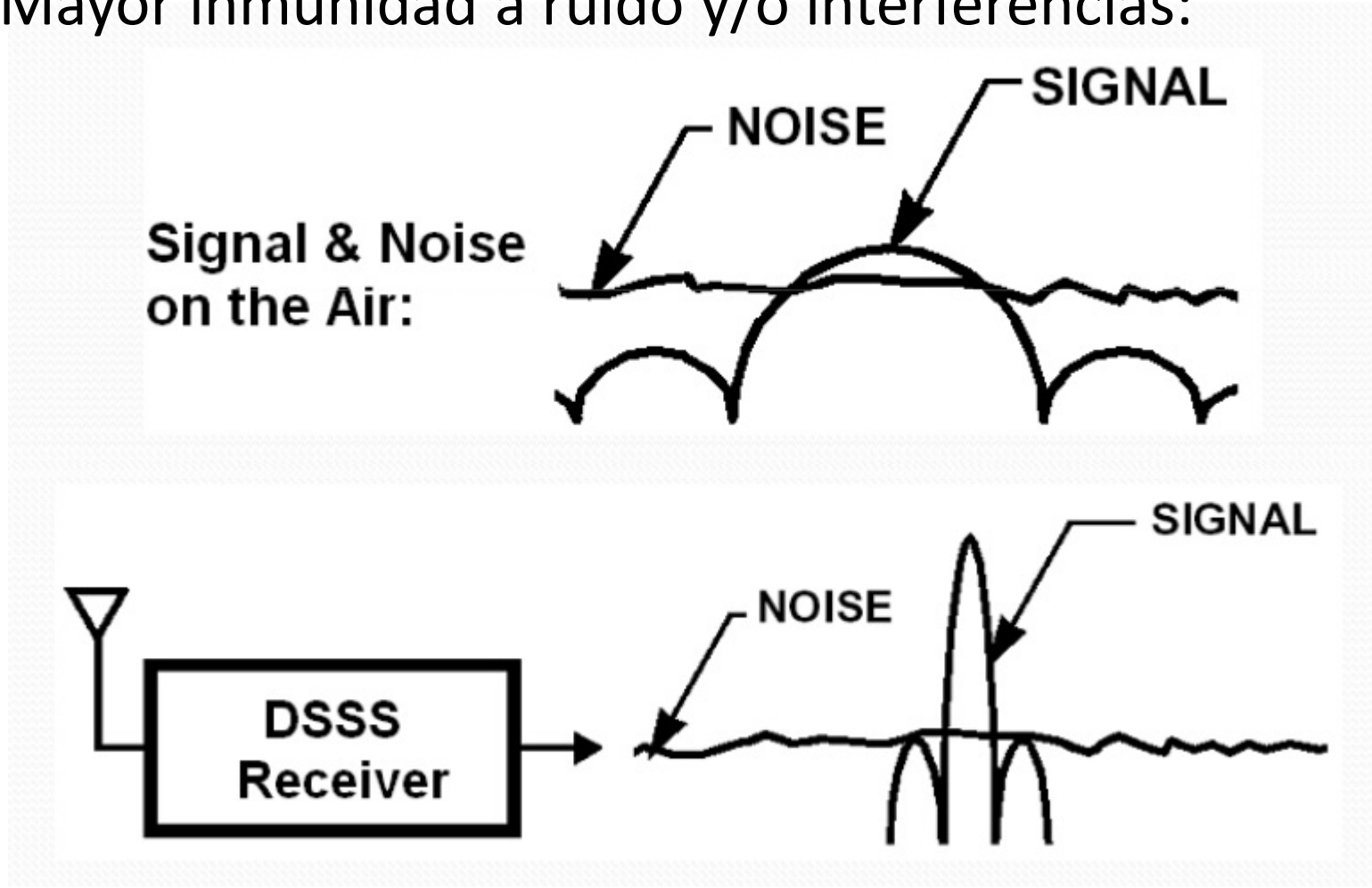
QPSK Encoding

2-Bit (d0,d1) XOR Output (d0 is the first bit in time)	Phase Change
00	0
01	π/2
11	π
10	3π/2

(*) Spread Spectrum and Wi-Fi Basics by Syed M. Mahmu

IEEE 802.15.4

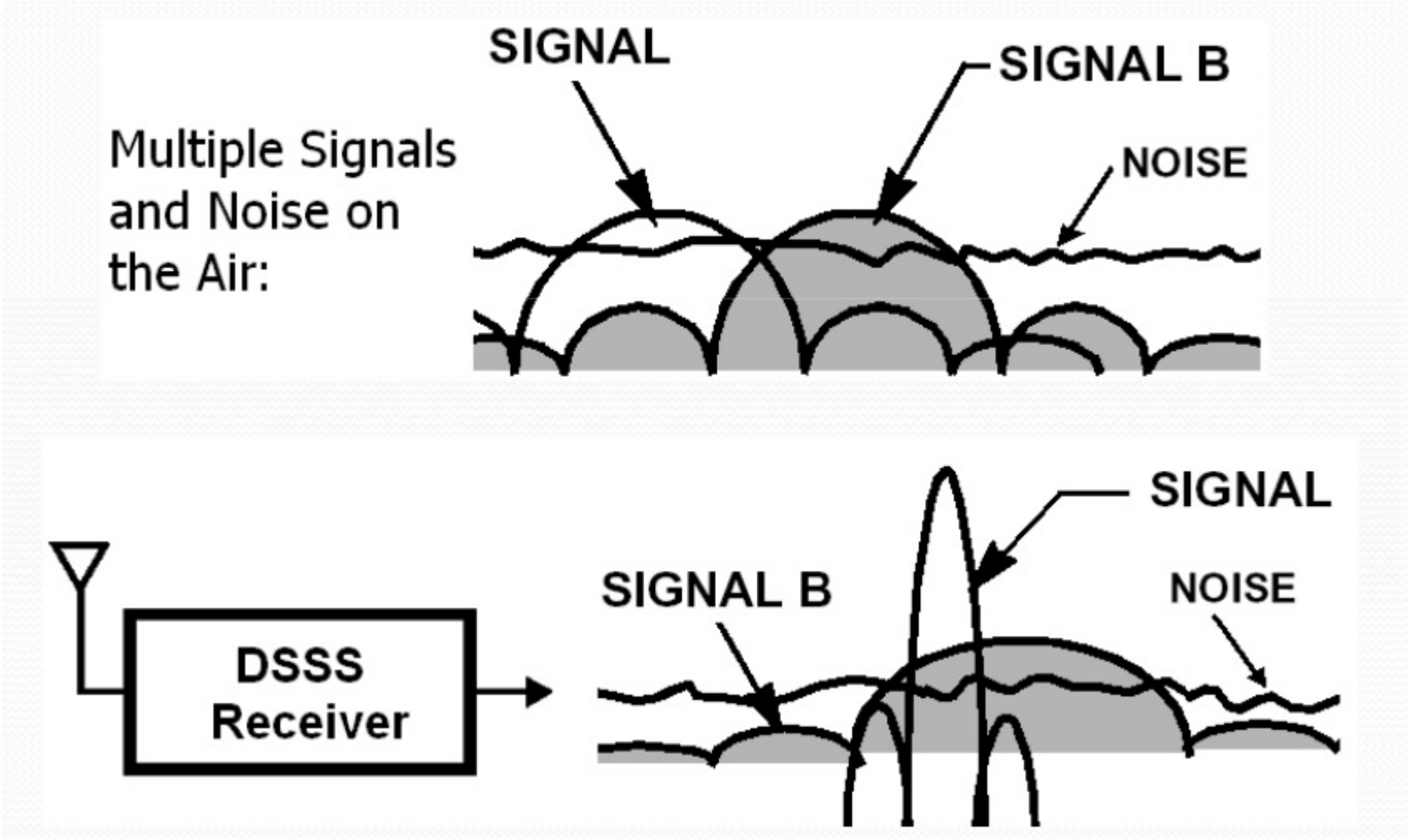
- Mayor inmunidad a ruido y/o interferencias:



(*) Spread Spectrum and Wi-Fi Basics by Syed M. Mahmu

IEEE 802.15.4

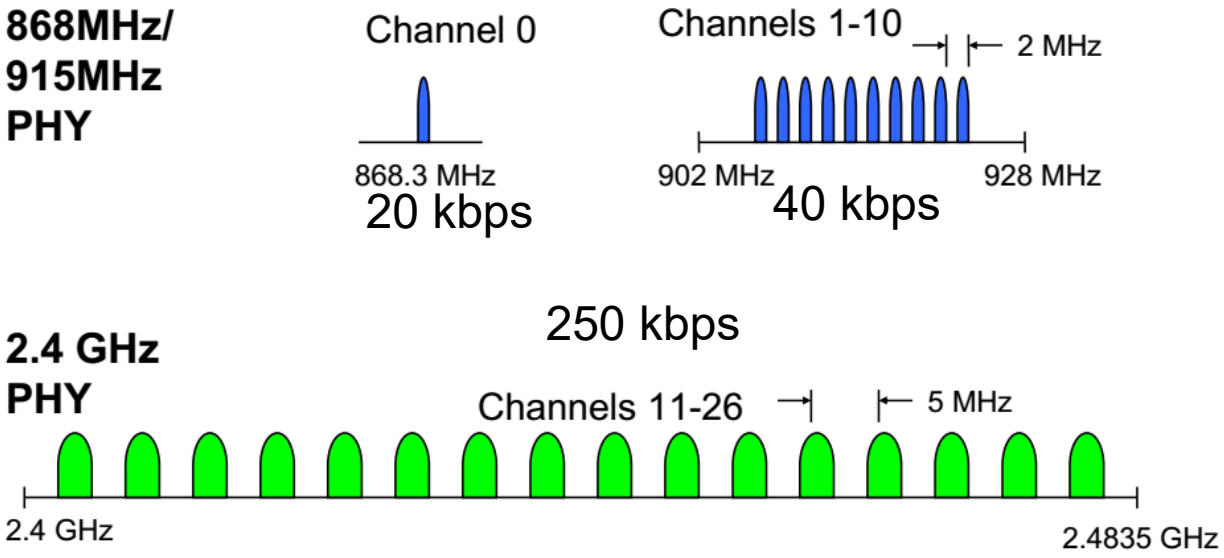
- Acceso múltiple usando diferentes códigos PRN:



(*) Spread Spectrum and Wi-Fi Basics by Syed M. Mahmu

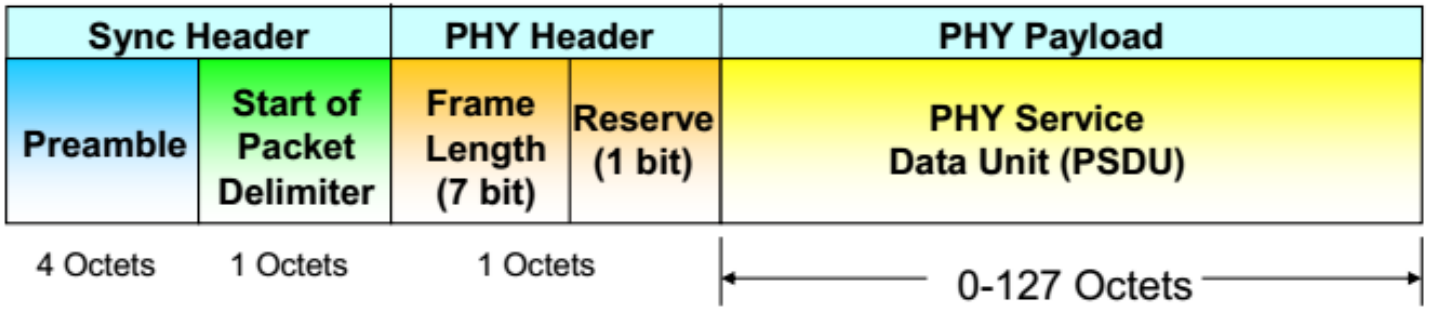
IEEE 802.15.4

- Nivel físico. Funciones:
  - Activación/desactivación del módulo radio
  - Detección de ocupación del canal para Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - Indicador de calidad del enlace en la recepción de paquetes
  - Selección de canal de frecuencia (27 canales)



IEEE 802.15.4

- Nivel físico. Formato de trama:
  - Preámbulo: sincronización
  - Indicador de comienzo de paquete: “11100101”
  - Cabecera de nivel físico: tamaño de la trama
  - *Payload*: hasta 127 bytes

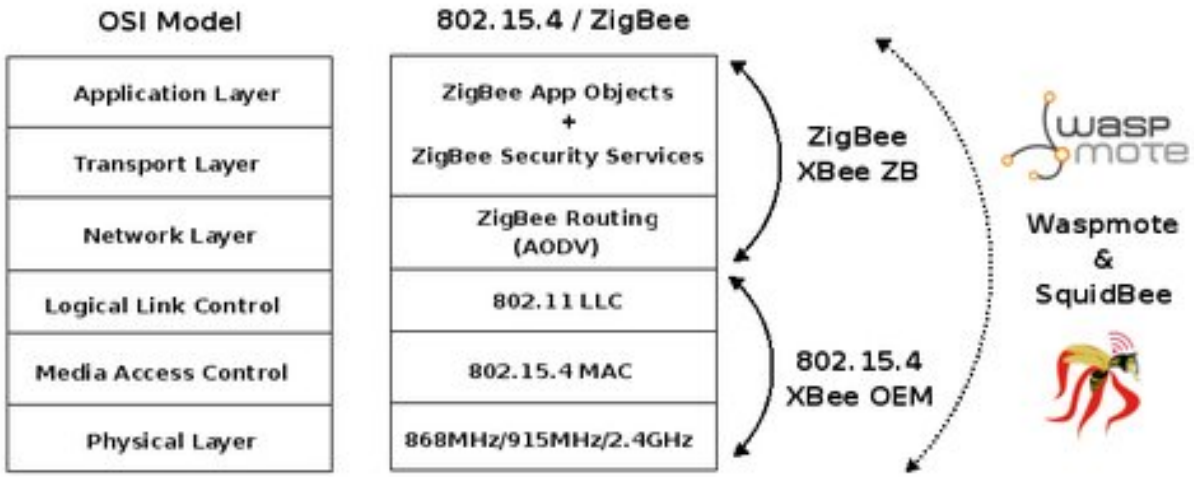


IEEE 802.15.4

- Nivel de enlace:
  - Algoritmo MAC (Media Access Control) basado en el protocolo de acceso a redes CSMA (Carrier Sense Multiple Access)
  - Primero espera hasta que el canal esté inactivo.
  - Una vez que el canal esté libre, comienza a enviar los data frames.
  - El receptor reconoce la correcta recepción de un data frame .
  - Si el remitente no recibe un acuse de recibo, se reintenta la transmisión de datos.

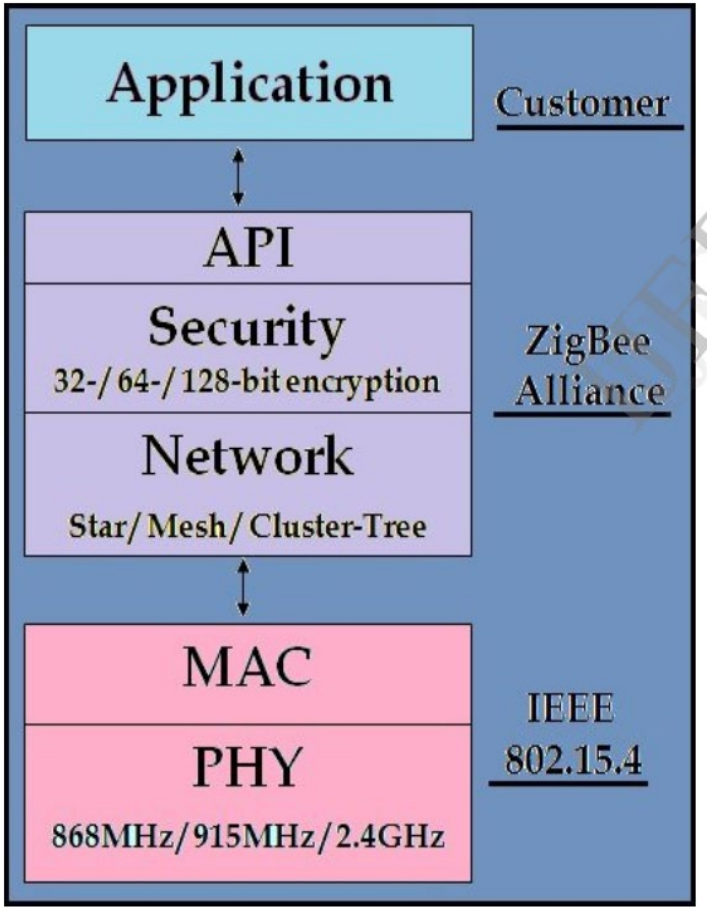
Zigbee

- Protocolo estándar abierto que provee funcionalidad y características adicionales sobre 802.15.4
- Promovido por la *Zigbee Alliance* desde 2002.



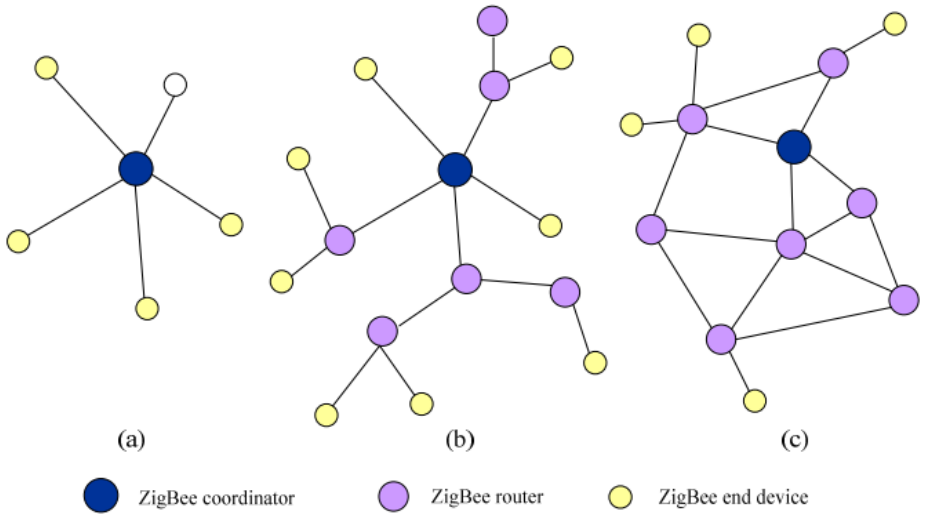
Zigbee

- Características adicionales a IEEE 802.15.4
  - Servicios añadidos de cifrado: a nivel de red y aplicación
  - Asociación y autenticación: durante el proceso de asociación a la red
  - Direccionamiento a nivel de red
  - Enrutamiento: basado en árbol o protocolo reactivo basado en AODV



Zigbee: Topologías

- Topología en estrella
  - Comunicación a través del coordinador PAN
  - Pueden ser una combinación de FFD (Full Functional Device) y RFD (Reduced Functions Device).
  - Coordinador PAN suele ser un dispositivo confiable conectado a la red eléctrica



Tipos de nodos lógicos

- Dispositivo final
  - RFD o FFD sin tareas de control
- Router Zigbee
  - FFD con tareas de gestión y control de la red
- Coordinador Zigbee
  - Controlador principal de la red. Una red solo puede tener uno

Zigbee: Topologías

- Topología peer-to-peer (mesh)
  - Extensión de la topología en estrella para comunicación directa entre dispositivos
  - Enrutamiento
- Topología en árbol clusterizada
  - Varios coordinadores conectados entre sí dan servicio a nodos finales
  - Un coordinador es designado coordinador PAN

6LoWPAN

- Capa de adaptación para transportar paquetes IPv6 sobre Low-Power Wireless Personal Area Networks (LP-WPAN)
  - Definido sobre el estándar IEEE 802.15.4
  - Está siendo adaptado también para otros protocolos a nivel de enlace (Bluetooth Smart, Low-power Wi-Fi, *Power Line Control* (PLC))
- Interoperabilidad con otras tecnologías
- Integración con Internet transparente
  - Permite el uso de API de sockets estándar
- Uso mínimo de código y memoria

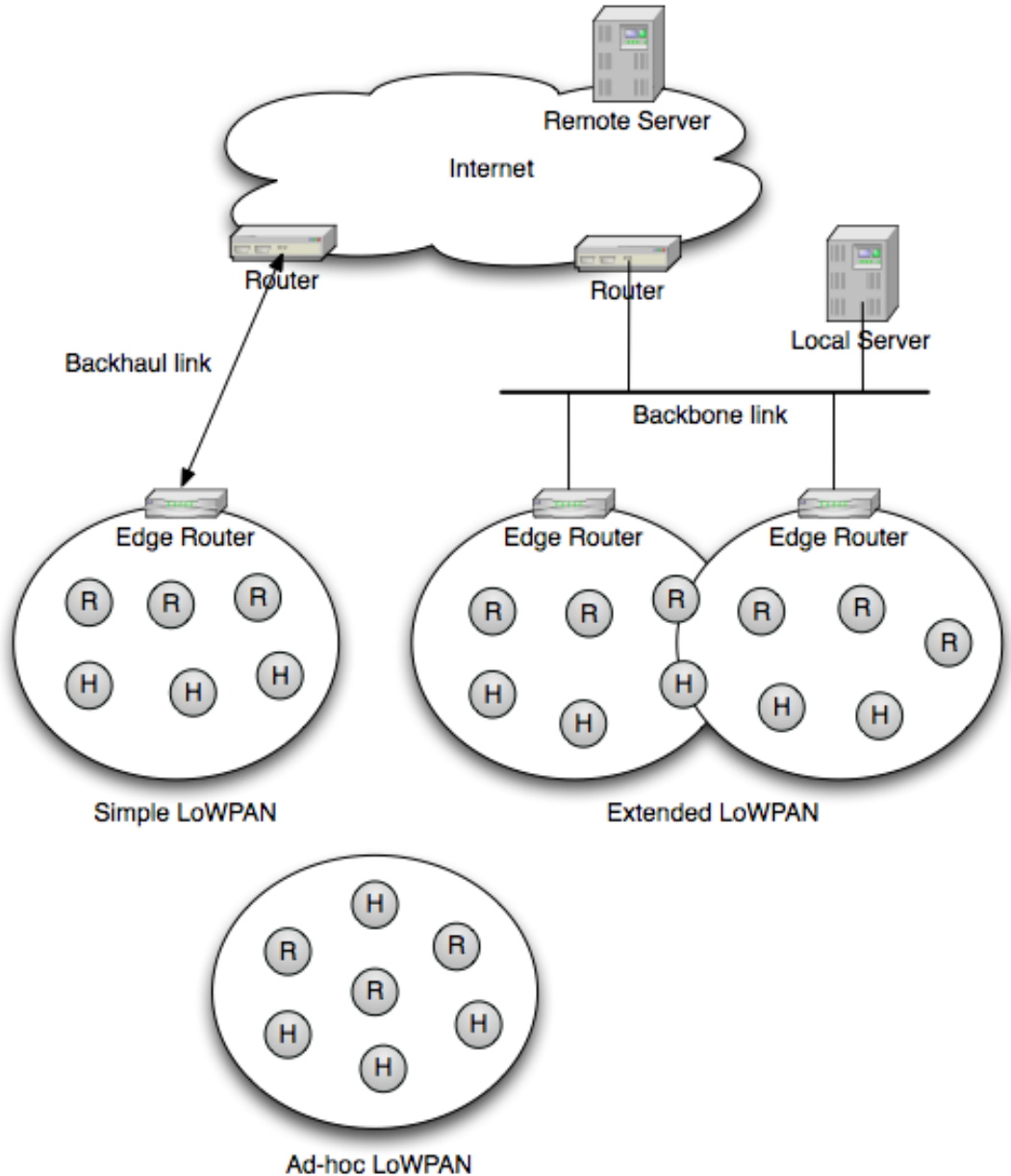
6LoWPAN

- Problemas de IPv6 para trabajar en WSN:
  - Direcciones IPv6 muy largas (128 bits): soporte para direcciones de 64 bits y 16 bits 802.15.4
  - Cabecera IPv6 muy larga: compresión eficiente de cabeceras
    - Compresión IPv6
    - Compresión cabeceras de extensión IPv6
    - Compresión cabecera UDP
  - Autoconfiguración de red → uso de *network Discovery* con intensos envíos multicast

6LoWPAN

- Los protocolos de enrutamiento ad-hoc suelen introducir mucho overhead → 6LoWPAN emplea su propio protocolo de enrutamiento eficiente (RPL)
- Estándares del IETF sobre 6LoWPAN:
  - RFC 4944 - cabeceras
  - RFC 6282 - formato de compresión
  - RFC 6550 - *routing* (RPL)
  - RFC 6775 - *neighbour discovery*

6LoWPAN: Arquitectura



- *Edge router*:
  - Intercambio de datos entre dispositivos 6LoWPAN e Internet (otras redes IPv6)
  - Intercambio de datos entre dispositivos 6LoWPAN
  - Opcional: soporte para conectar redes 6LoWPAN a redes IPv4

IPv6	
Ethernet MAC	LoWPAN Adaptation
	IEEE 802.15.4 MAC
Ethernet PHY	IEEE 802.15.4 PHY

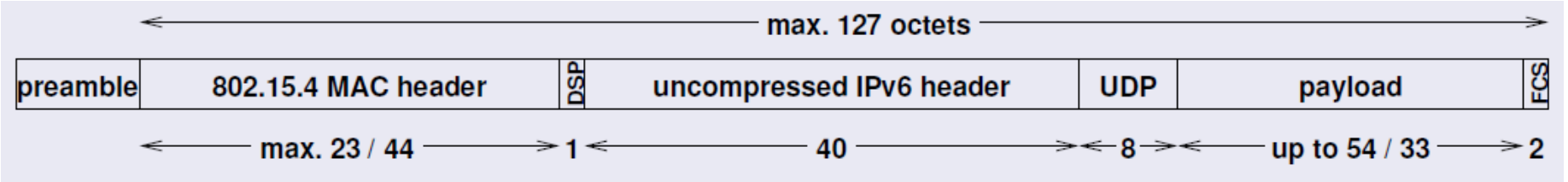
IPv6-LoWPAN Router Stack

6LoWPAN: Resolución de direcciones

- A los nodos IPv6 se le asignan direcciones IP de 128 bits
- Los dispositivos IEEE 802.15.4 pueden usar direcciones IEEE de 64 bits o, después de un evento de asociación, direcciones de 16 bits que son únicas dentro de una Personal Area Network.
- 6LoWPAN comprime las direcciones IPv6
  - Quitando el prefijo de IPv6 (primeros 64 bits)
    - El prefijo global ya es conocido por todos los nodos de la red
  - Comprimiendo el identificador de la interfaz (IID)
    - Se quita para comunicaciones locales
  - Compresión utilizando un “contexto” bien conocido (RFC-6282)
  - Compresión de direcciones multicast

6LoWPAN – Adaptación de los tamaños de paquetes

- Peor escenario: sin compresión



- Cálculo de la cabecera.
  - Cabecera IPv6 → 40 octetos
  - Cabecera UDP → 8 octetos
  - Cabecera MAC de 802.15.4
    - 23+2=25 octetos (sin seguridad)
    - 44+2=46 octetos (si se utiliza seguridad AES-CCM-128)

6LoWPAN - Fragmentación

- IPv6 tiene un límite inferior en MTU de 1280 octetos. Es decir, IPv6 no fragmenta los paquetes por debajo de este límite. Para enviar IPv6 a través de un enlace con una MTU de menos de 1280 octetos, la capa de enlace debe fragmentar y desfragmentar con transparencia los paquetes IPv6.
- Tamaño trama 802.15.4 es 127 octetos, queda para datos:
    - 127-25-40-8 = **54 octetos** (sin seguridad)
    - 127-46-40-8 = **33 octetos** (usando AES-CCM-128)
- Se necesita fragmentación y reensamblado para encajar los 1280 octetos IPv6 en los 33 (o 54) octetos de 802.15.4

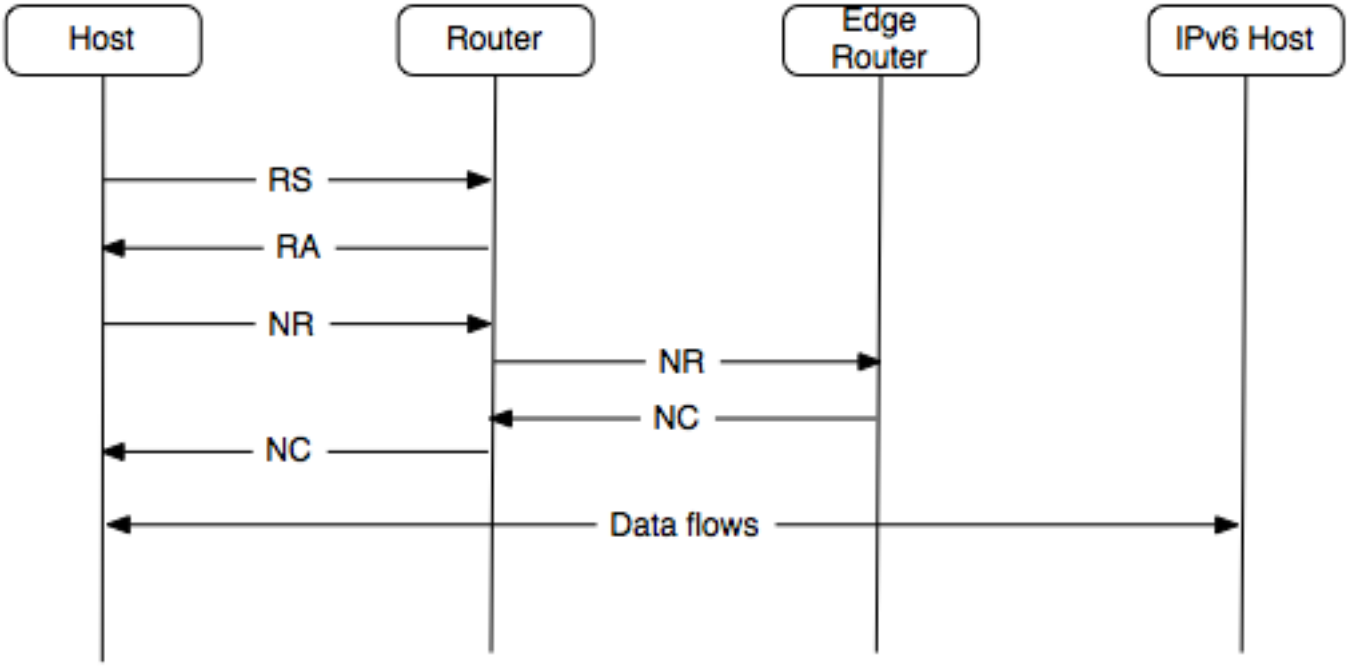
6LoWPAN - Fragmentación

- Bajo rendimiento de paquetes grandes IPv6 fragmentados sobre redes LoWPAN
  - La pérdida de fragmentos causa que los paquetes se retransmitan
  - Bajo ancho de banda y alto retardo del canal inalámbrico
  - Los protocolos de aplicación sobre 6LoWPAN deben evitar fragmentación
  - Los protocolos de aplicación deberían aplicar compresión cuando se usan en 6LoWPAN

6LoWPAN – Neighbor Discovery

- El standard de *Neighbor Discovery* para IPv6 no es apropiado para 6LoWPAN:
  - Asume que los nodos están operativos
  - Uso intensivo de multicast
- 6LoWPAN *Neighbor Discovery* proporciona:
  - Un enlace adecuado y modelo para comunicaciones inalámbricas de baja potencia
  - Minimiza el tráfico de control requerido por los nodos
  - Node Registration (NR) and Confirmation (NC)
  - Duplicate Address Detection (DAD) and *recovery*
  - Soporte para infraestructuras *extended Edge Router*
- RFC 6775 → Define el *Neighbor Discovery* para 6LoWPAN

6LoWPAN – Network Discovery



RS → *Router Solicitation*. Búsqueda de *router*
RA → *Router Advertisement*. Respuesta de *router*
NR → *Node Registration*. Registro de un nodo
NC → *Node Confirmation*. Confirmación de registro

6LoWPAN - Routing

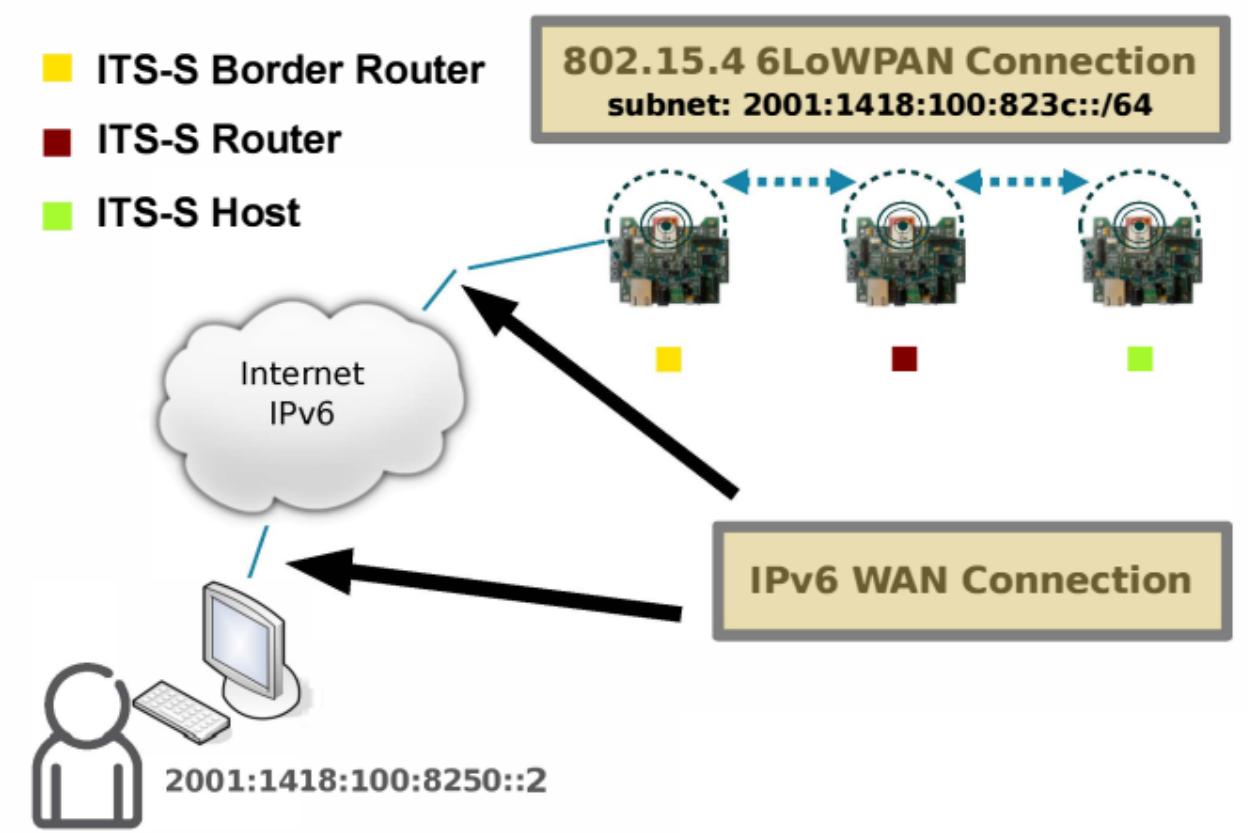
- *Routing Over Low power and Lossy networks* (ROLL)
  - Grupo de trabajo del IETF
- Protocolo RPL “Ripple”
  - *IPv6 Routing Protocol for Low-Power and Lossy Networks*
  - RFC 6550
  - Cada *router* envía información a sus vecinos sobre toda la red, para calcular el camino más corto al destino
  - Utiliza varias métricas. Diferentes función objetivo
  - Detección de inconsistencias: evitar bucles, mantener convergencia, etc.
- Otros protocolos ad-hoc: AODV, OLSR, BATMAN, JOKER…

6LoWPAN - Seguridad

- En redes inalámbricas el canal es muy vulnerable
- Nivel 2: Mecanismos de IEEE 802.15.4
  - Basado en 128-bit Advanced Encryption Standard (AES)
  - Muchos dispositivos incluyen chips para procesamiento AES128
- Nivel 3: IPSec standard [RFC4301] seguridad IP, *end-to-end*
  - Dos formatos de cabecera
    - Authentication Header (AH) in [RFC4302]
      - Sólo integridad y autenticación
    - Encapsulating Security Payload (ESP) [RFC4303] (más usado)
      - También cifra para conseguir confidencialidad

6LoWPAN: Caso de uso

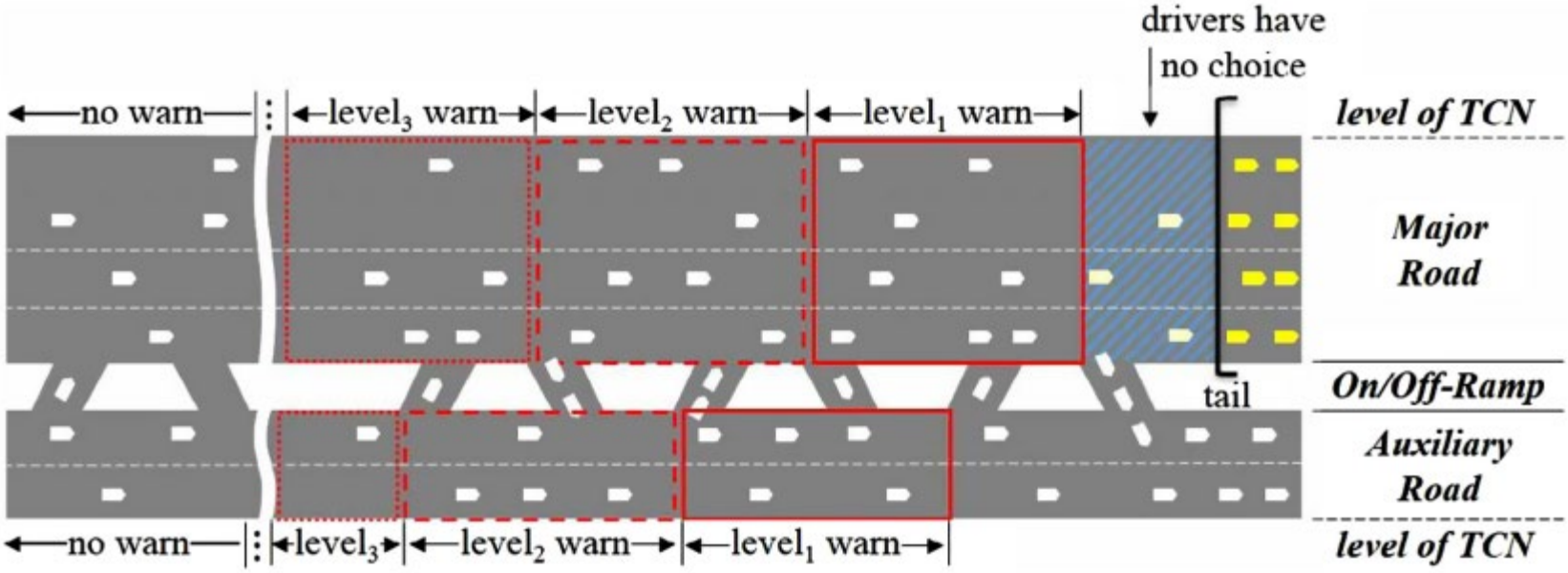
- ***Intelligent Transportation Systems*** **(ITS)**



G. Pellerano, M. Falcitelli, M. Petracca and P. Pagano, "6LoWPAN conform ITS-Station for non safety-critical services and applications," *2013 13th International Conference on ITS Telecommunications (ITST)*, Tampere, 2013, pp. 426-432. doi: 10.1109/ITST.2013.6685584

6LoWPAN: Caso de uso

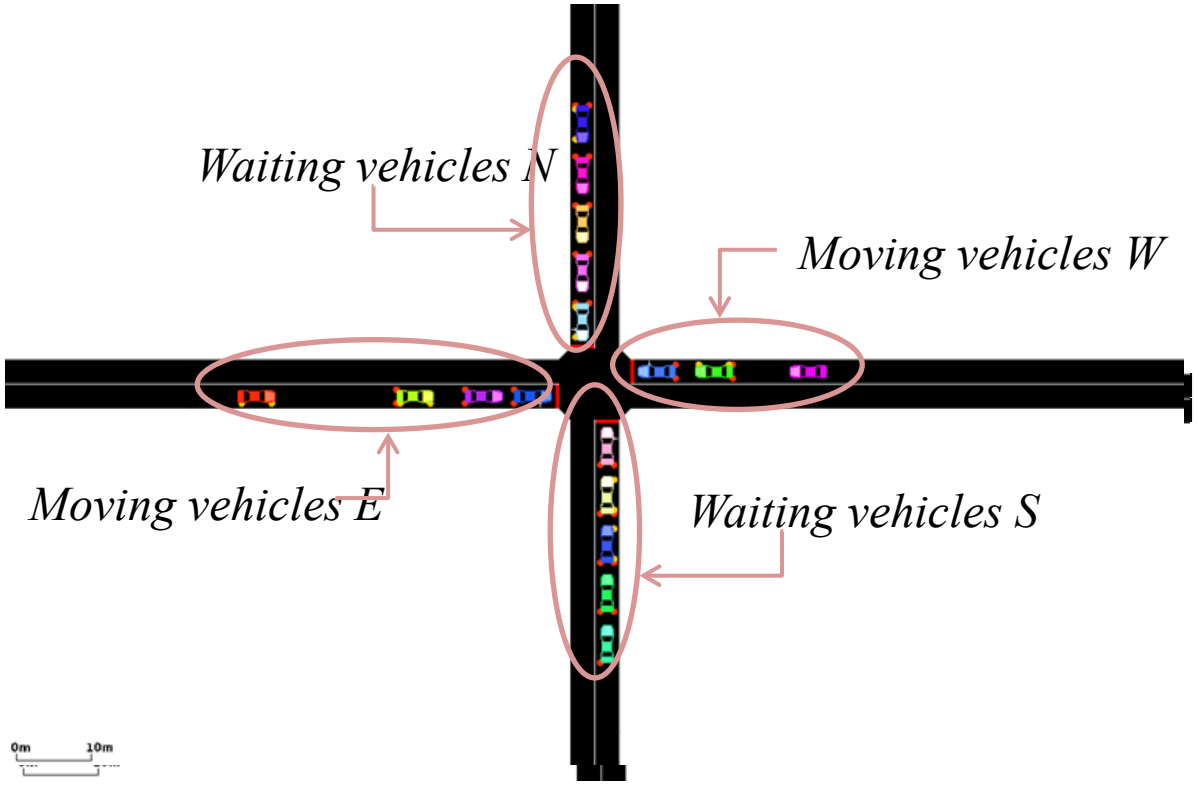
- **ITS: redistribución de tráfico**



Q. Yuan, Z. Liu, J. Li, J. Zhang, and F. Yang, "A traffic congestion detection and information dissemination scheme for urban expressways using vehicular networks," *Transp. Res. Part C Emerg. Technol.*, vol. 47, pp. 114–127, Oct. 2014.

6LoWPAN: Caso de uso

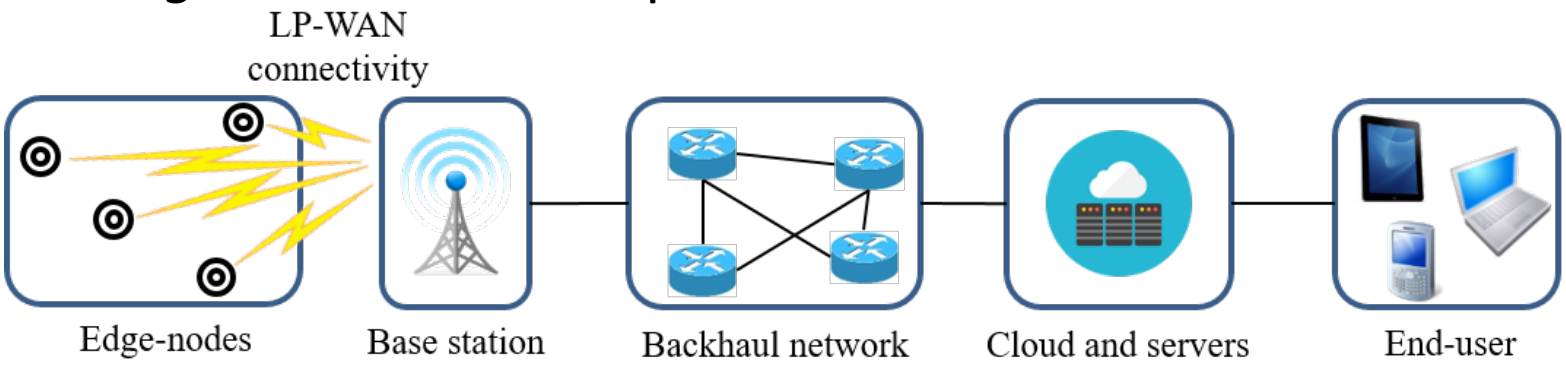
- **ITS: ajuste tiemo semáforos**



R. Sanchez-Iborra, J. F. Ingles-Romero, G. Domenech-Asensi, J. L. Moreno-Cegarra, and M.-D. Cano, "Proactive intelligent system for optimizing traffic signaling," in Proc. *14th IEEE International Conference on Pervasive Intelligence and Computing (PICom-2016)*, 2016, pp. 544–551.

LP-WAN

- Características
  - Largo alcance como las redes celulares (o más)
  - Bajo consumo como las redes de sensores
  - Alta escalabilidad
  - Topología en estrella o estrella de estrellas
  - Uso de frecuencias libres ISM sub-GHz (868 MHz o 902 MHz)
  - Dispositivos de bajo coste
  - Enlaces asimétricos: mayor valor al *uplink*
  - *Roaming:* conexión del dispositivo a distintas estaciones base



LP-WAN: Sigfox

- Protocolo propietario
- Modulación Ultra Narrow Band (200 Hz). Differential Binary Phase Shift Keying (DBPSK)
- Tasa de transmisión muy limitada: 100 bps
- Utilización de bandas libres ISM (Industrial, Scientific and Medical) sub-GHz: 868 MHz (Europa) y 902 MHz (EEUU)
- Largos alcances y penetración (10 km en campo abierto y 2-3 km en zona urbana) y muy bajo consumo de energía

LP-WAN: Sigfox

- Limitaciones técnicas:
  - Límite de mensajes: 140 mensajes al día (*duty cycle*)
  - Tamaño máximo de *payload*: 12 bytes
  - Seguridad: no ofrece ni cifrado ni seguridad extremo a extremo. Se asume que sólo el usuario conoce el contenido y significado del *payload*. Saltos en frecuencia
- Éxito: modelo de negocio
  - Muy **buena cobertura** y escalabilidad
  - **Amplio despliegue**: varios países europeos cubiertos, mediante convenios con operadores de servicios móviles. España: Cellnex
  - Instalación muy simple
  - **Alta eficiencia energética**: las baterías duran más de 10 años
  - Ejemplo: securitas direct

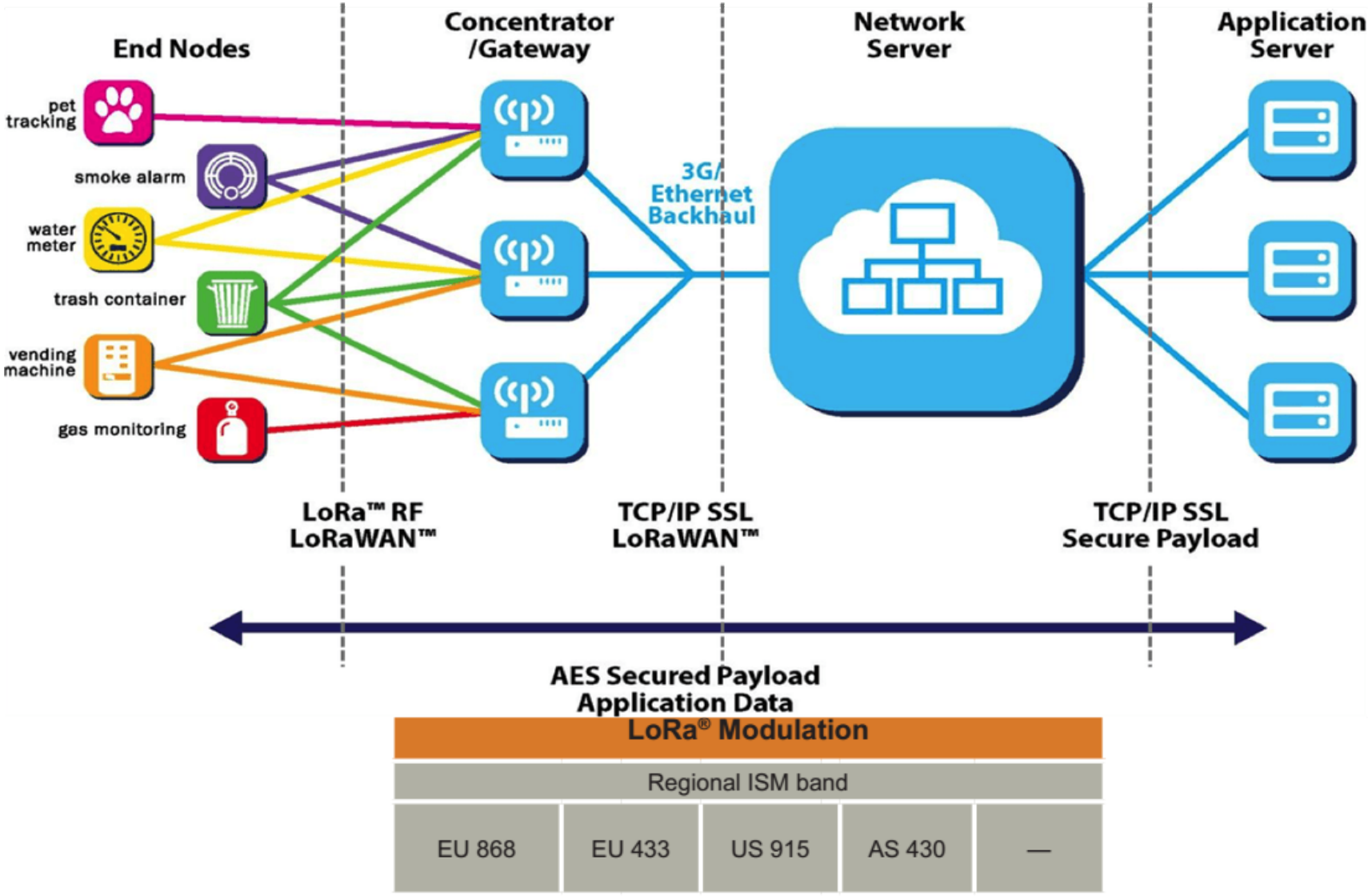
LP-WAN: Sigfox

Estaciones base Sigfox en España

LP-WAN: LoRaWAN

- Conectividad de largo alcance (similar a Sigfox), tanto en uplink como en downlink:
  - Nodos Clase A: después de cada transmisión en uplink, el nodo abre dos ventanas de escucha para recibir: menor consumo energético
  - Nodos Clase B: misma funcionalidad que Clase A, pero además, los nodos abren unas ventanas de escucha de forma programada: consumo energético medio
  - Nodos Clase C: ventana de escucha siempre abierta: dispositivos conectados a alimentación
- LoRa: Long Range.

LP-WAN: LoRaWAN



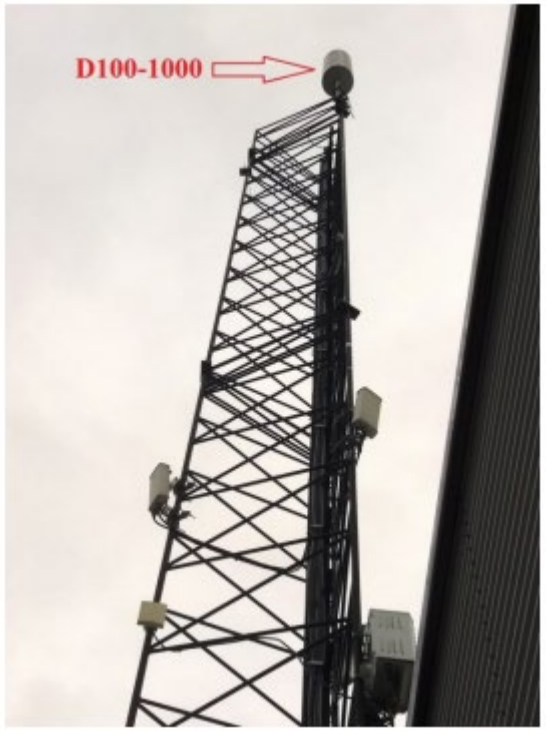
LP-WAN: LoRaWAN

	Europe	North America	China	Korea	Japan	India
Frequency band	867-869MHz	902-928MHz	470-510MHz	920-925MHz	920-925MHz	865-867MHz
Channels	10	64 + 8 +8	In definition by Technical Committee	In definition by Technical Committee	In definition by Technical Committee	In definition by Technical Committee
Channel BW Up	125/250kHz	125/500kHz				
Channel BW Dn	125kHz	500kHz				
TX Power Up	+14dBm	+20dBm typ (+30dBm allowed)				
TX Power Dn	+14dBm	+27dBm				
SF Up	7-12	7-10				
Data rate	250bps- 50kbps	980bps-21.9kpbs				
Link Budget Up	155dB	154dB				
Link Budget Dn	155dB	157dB				

LP-WAN: LoRaWAN

LP-WAN: LoRaWAN Caso de uso

- E-health



J. Petäjäjärvi, K. Mikhaylov, M. Hämäläinen and J. Iinatti, "Evaluation of LoRa LPWAN technology for remote health and wellbeing monitoring," *2016 10th International Symposium on Medical Information and Communication Technology (ISMICT)*, Worcester, MA, 2016, pp. 1-5.

Sigfox vs. LoRaWAN

- LoRaWAN es una solución tecnológicamente más avanzada
- LoRaWAN presenta mejores prestaciones y parámetros de configuración adaptables a los distintos entornos de transmisión
- Sigfox tiene una arquitectura de red más amigable para el usuario final que no quiere invertir en infraestructura ni sabe como gestionar sus datos en la nube

CoAP: Constrained Application Protocol

- IETF CoRE Working Group: RFC 7252 (2014); RFC 7641: extensión OBSERVE (2015)
- Protocolo eficiente modelo cliente-servidor basado en RESTful
- Soporta operaciones GET / PUT / POST / DELETE (como HTTP)
- Aparentemente sencillo, pero muy potente

CoAP: Constrained Application Protocol

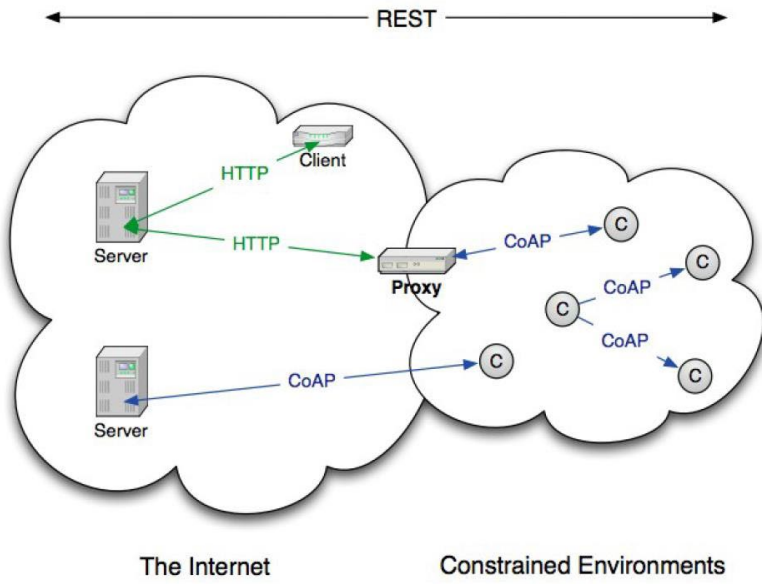
- Usuarios CoAP:
  - Usuarios de servicios web: CoAP implementa un protocolo para servicios web
  - Otros dispositivos CoAP (máquinas)
  - Servidores de gestión, p.e., uso de LWM2M, para acceder y gestionar un dispositivo restringido usando CoAP
- CoAP es un rediseño (no una simple compresión) de HTTP. CoAP puede ser traducido a HTTP para interoperabilidad e integración con la WEB
- CoAP se ha definido sobre UDP como protocolo de transporte

CoAP: Constrained Application Protocol

- Emplea recursos limitados:
  - Tamaño mensajes reducido (cabecera 4 bytes)
  - Redes *constrained,* ej. Low-Power and Lossy Networks (LLN)
  - Soporta nodos inactivos, uso de *proxies*
- Reduce las ineficiencias de operaciones REST
  - No codifica en texto plano, y reduce el tamaño de los mensajes
  - No utiliza TCP que añade overhead, sino UDP
- Permite operaciones *Machine to Machine* (M2M)
  - Descubrimiento de recursos
  - publicación / subscripción / notificación
  - *multicast*

CoAP: Constrained Application Protocol

The CoAP Architecture



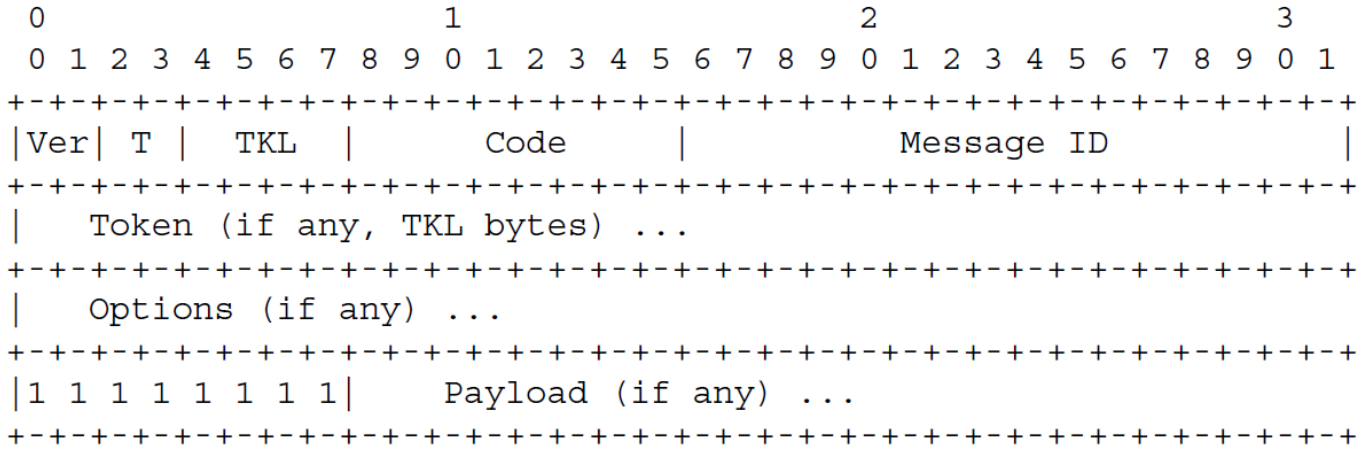
	Traditional IP	IoT protocols
Application protocol	HTTP (and related protocol, eg SMTP)	CoAP
Transport layer	TCP (or UDP)	UDP only
Network layer	IPv4 / IPv6	6LoWPAN
Link layer	802.11n (or ethernet)	802.15.4e

Mensajes CoAP

- Se utiliza UDP (no orientado a la conexión, no garantía entrega)
- Control de entrega realizado a nivel de aplicación por el protocolo CoAP. Cada mensaje se marca como “confirmable” o “no confirmable”:
  - Mensajes confirmables: requiere de un ACK
  - Mensajes no-confirmables: *fire and forget*
- Seguridad → DTLS (Datagram Transport Layer Security)

Mensajes CoAP

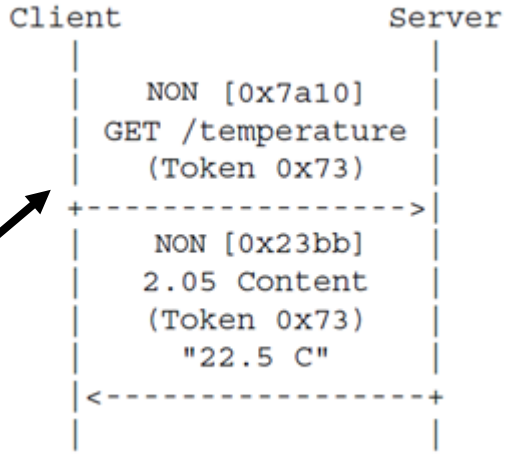
- Formato:



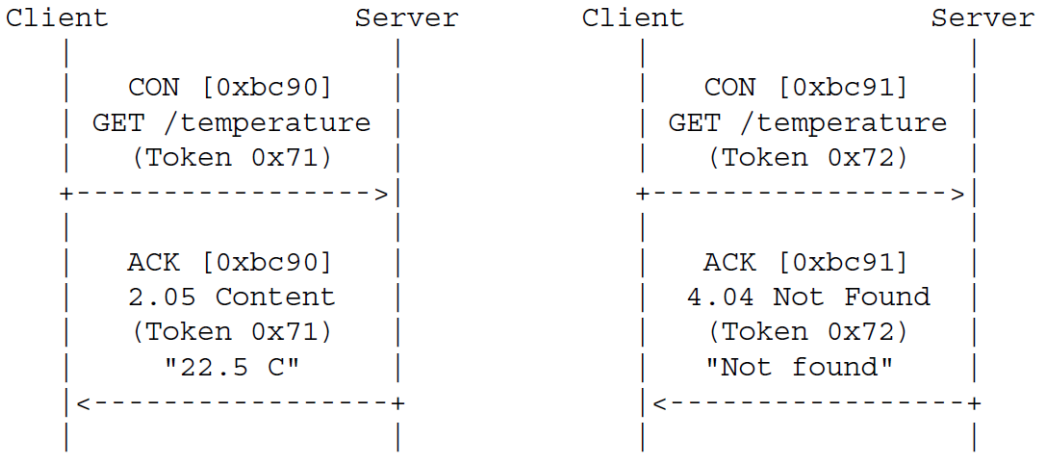
- **type** → indica el rol del mensaje como parte de la transacción. CON / ACK / NON / RST
- **TKL** → token length
- **code** → da información adicional sobre el propósito del mensaje:
  - *Request* o *response*. GET, POST, PUT, DELETE
- **Message id** → valor único a la transacción
- **token** → para especificar el concepto de "*topic*"
- **options** → para incluir parámetros y mecanismos de gestión de mensajes

Mensajes CoAP

- Tipos Mensajes
  - **CON** →Confirmable
  - **NON** →Non-Confirmable
  - **ACK** → acknowledge CON +piggyback
  - **RST**→ reset interaction
- Ej. Mensaje no-confirmable



- Ej. Mensajes confirmables con ACK



CoAP

- Implementaciones
  - Contiki-2.6: Erbium. http://www.contiki-os.org
  - C: libcoap http://sourceforge.net/projects/libcoap/develop
  - .NET (C#) CoAPSharp http://www.coapsharp.com
  - Phython. http://sourceforge.net/projects/coapy
  - Java. Californium https://github.com/mkovatsc/californium
  - Firefox Javascript browser plugin: Cooper https://github.com/mkovatsc/Copper
- Proxies:
  - Squid 3.1.9 with transparent HTTP-CoAP mapping module http://telecom.dei.unipd.it/pages/read/90/
  - jcoap Proxy https://code.google.com/p/jcoap/
  - Californium cf-proxy https://github.com/mkovatsc/Californium
  - CoAPthon https://github.com/Tanganelli/CoAPthon

MQTT (Message Queue Telemetry Transport)

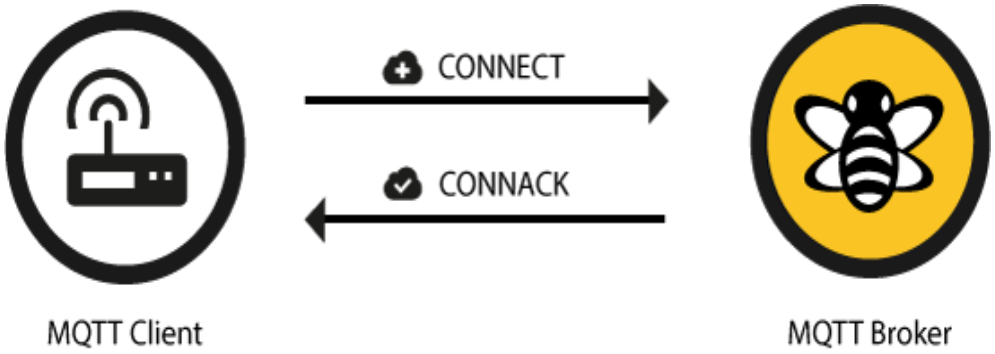
- Protocolo ligero de publicación/subscripción **sobre TCP/IP** para sensores, dispositivos y redes "*constrained*".
- Estándar de OASIS para IoT (2014), pero diseñado por IBM para conectar instalaciones petrolíferas vía satélite (1999)
- Ideal para situaciones con comunicaciones M2M e IoT:
  - Simple de implementar
  - Provee una capa de QoS
  - Requiere de poco ancho de banda
  - Agnóstico a las aplicaciones de capa superior
  - Permite el establecimiento continuo de una conexión (TCP)
- Amplio grado de desarrollo y despliegue: Arduino, Android/iOS, C/C++/C#, Java/JavaScript

MQTT

- El productor publica el mensaje solo una vez (al servidor/*broker*)
- Múltiples consumidores (aplicaciones/dispositivos) reciben el mensaje a través del *broker*
- Desacopla al productor y al consumidor.
- El productor manda el mensaje con un *topic*
- Los consumidores se han suscrito previamente a ese *topic*
- El servidor/*broker* realiza la asociación entre publicaciones y suscripciones: recibe→filtra→asocia→re-envía
  - Si no hay ninguna asociación, el mensaje se descarta
  - Si uno o más mensajes cumplen la asociación, el mensaje se entrega al consumidor correspondiente

MQTT

MQTT Connection



MQTT-Packet:

CONNECT

contains:	Example
clientId	"client-1"
cleanSession	true
username (optional)	"hans"
password (optional)	"letmein"
lastWillTopic (optional)	"/hans/will"
lastWillQos (optional)	2
lastWillMessage (optional)	"unexpected exit"
lastWillRetain (optional)	false
keepAlive	60

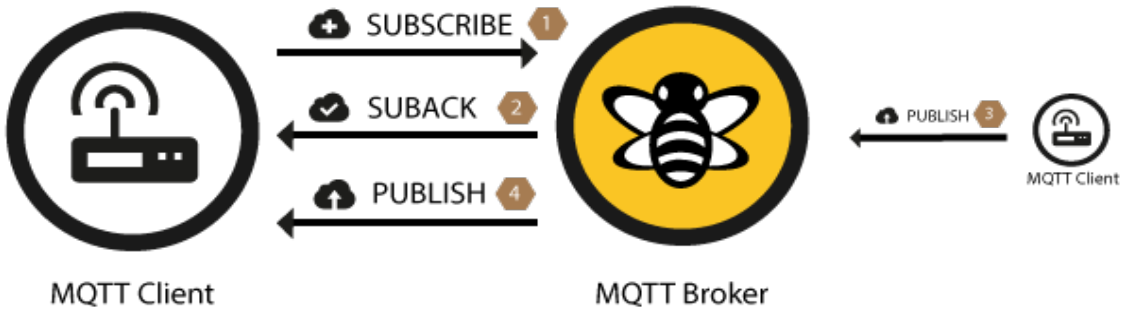
MQTT-Packet:

CONNACK

contains:	Example
sessionPresent	true
returnCode	0

MQTT

Subscription/publishing



MQTT-Packet:

SUBSCRIBE

contains:		Example
packetId		4312
qos1	} (list of topic + qos)	1
topic1		"topic/1"
qos2	}	0
topic2		"topic/2"
...		...

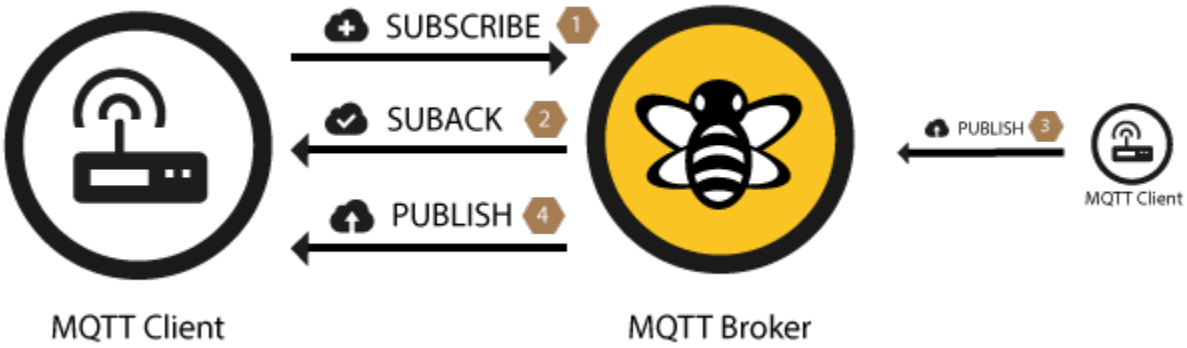
MQTT-Packet:

SUBACK

contains:		Example
packetId		4313
returnCode 1	(one returnCode for each topic from SUBSCRIBE, in the same order)	2
returnCode 2		0
...		...

MQTT

Subscription/publishing



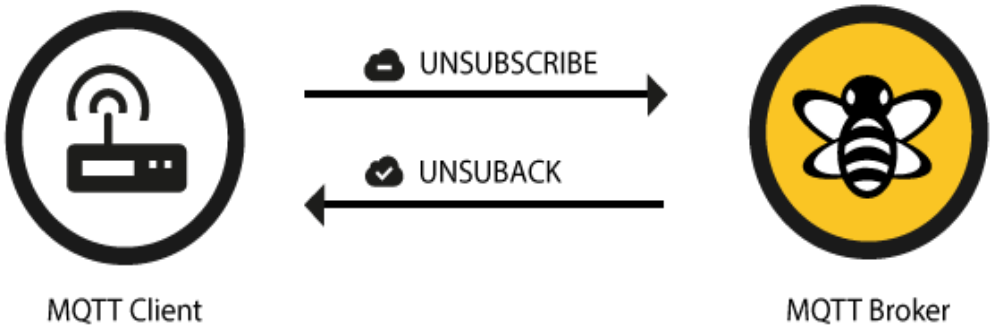
MQTT-Packet:

PUBLISH

contains:	Example
packetId (always 0 for qos 0)	4314
topicName	"topic/1"
qos	1
retainFlag	false
payload	"temperature:32.5"
dupFlag	false

MQTT

Unsubscribe



MQTT-Packet:

UNSUBSCRIBE

contains:	Example
packetId	4315
topic1 } (list of topics)	"topic/1"
topic2	"topic/2"
...	...

MQTT-Packet:

UNSUBACK

contains:	Example
packetId	4316

MQTT

- *Topics* con estructura jerárquica. Cada jerarquía se separa con ‘/’. Por ejemplo:
  - **“edificio1/planta3/sala1/raspberry0/temperatura”**
  - **“edificio1/planta1/sala0/arduino0/ruido”**
  - Suscripción agregada (no la publicación) ej.“edificio1/planta2/#”

MQTT

- Ejemplo de *topic*: Una casa que publica información sobre si misma:
  - *<country>/<region>/<town>/<postcode>/<house>/energyConsumption*
  - *<country>/<region>/<town>/<postcode>/<house>/fireAlarm*
  - *<country>/<region>/<town>/<postcode>/<house>/floodingAlarm*
- Un suscriptor se puede suscribir a un *topic* concreto usando un valor absoluto o *wildcards*
  - Single-level *wildcards* "+" → puede aparecer en cualquier lugar del nombre
  - Multi-level *wildcards* "#" → deben aparecer al final del *namespace*
  - Los *wildcards* se deben poner a continuación del separador
  - Ejemplos:
    - *Spain/Murcia/Espinardo/30110/1/energyConsumption*
      - Consumo de energia para una casa concreta en Espinardo
    - *Spain/Murcia/Espinardo/+/+/energyConsumption*
      - Consumo de energía para todas las casas de Espinardo
    - *Spain/Murcia/Espinardo/30110/#*
      - Consumo de energía y alarmas (2) para todas las casas con el código postal:30110

MQTT

- Diseñado para dispositivos *constrained*:
  - Recursos limitados en cuanto a memoria, batería y CPU
  - Implementaciones de clientes MQTT para diferentes lenguajes
- Diseñado para redes *constrained*:
  - El protocolo comprime las cabeceras y tiene campos variables para reducir tamaño
  - Menor tamaño posible de paquete: 2 bytes
  - Testado en diferentes tipos de redes VSAT, GPRS, 2G….
- Soporta Calidad de servicio QoS para asegurar la entrega de mensajes de forma determinista. Niveles QoS:
  - 0 – mensaje enviado como mucho una vez (*fire and forget*) → entrega garantizada por TCP
  - 1 – mensaje entregado al menos una vez
  - 2 – mensaje entregado exactamente una vez
  - Productor y consumidor pueden tener niveles de QoS diferentes

MQTT-SN

- MQTT-SN: MQTT for Sensor Networks
- Aunque diseñado para dispositivos muy limitados, MQTT aún puede ser demasiado pesado para ciertos casos específicos:
  - Mantener conexión TCP
  - *Topics* excesivamente largos para algunos protocolos de capas inferiores (ej. 802.15.4)
- MQTT-SN: para dispositivos embebidos, sobre UDP
- Rediseño de algunos mensajes, predefinición (indexado) de algunos *topics*

MQTT – Caso de uso

- Facebook messenger: