UNIVERSIDAD
DE BURGOS

# Internet de las cosas

José M. Cámara 2018

# ¿IoT?

- Qué: Cosas de cualquier tipo con conexión a Internet
- Para qué: múltiples motivos. Veamos una clasificación:
  - Para proporcionar información
  - Para recibir información
  - Para aceptar órdenes
  - Para ser localizado
- Cómo: múltiples formas:
  - Wifi
  - LAN
  - Red telefónica celular: GPRS-UMTS-LTE
  - LPWAN

# IPv4

- Direcciones IP de 32 bits -> 2.800 millones de direcciones únicas.
- Hay más de 10.000 millones de dispositivos conectados -> las direcciones IPv4 ya no son únicas.
- Los dispositivos que no son identificados de forma única no pueden ser encontrados -> no es posible un intercambio directo entre el dispositivo y el usuario final.
- Aparece la necesidad de un intermediario.
- Los dispositivos no pueden ser interrogados -> ellos deciden cuándo contactar con el intermediario.
- Contactar demasiado a menudo supone muchos datos y mucho consumo.
- Contactar con poca frecuencia supone que datos y eventos importantes se pueden perder. Las actualizaciones tampoco son inmediatas.

# NAT (Network Address Translation)

- Los dispositivos IPv4 no suelen tener una IP fija.
- Esto no significa que no tengan una dirección.
- Las hay de dos tipos: pública / privada.
- Los dispositivos tienen una dirección privada para ser reconocidos dentro de su red local.
- Para acceder al resto del mundo necesitan una una dirección pública única.
- NAT garantiza una correcta traslación entre direcciones privadas y públicas.
- Varios dispositivos se pueden mostrar a través de una misma dirección pública pero el proveedor NAT es capaz de distinguirlos gracias a su IP privada y el puerto que utilizan para conectarse.

# IPv6

- Direcciones de 128 bits -> $2^{128}$ dispositivos = un número inimaginable de cosas que se pueden conectar.
- Todos los objetos pueden ser encontrados en Internet.
- Los dispositivos pueden subir información pero también pueden ser interrogados a través de la red.
- No se necesita NAT.

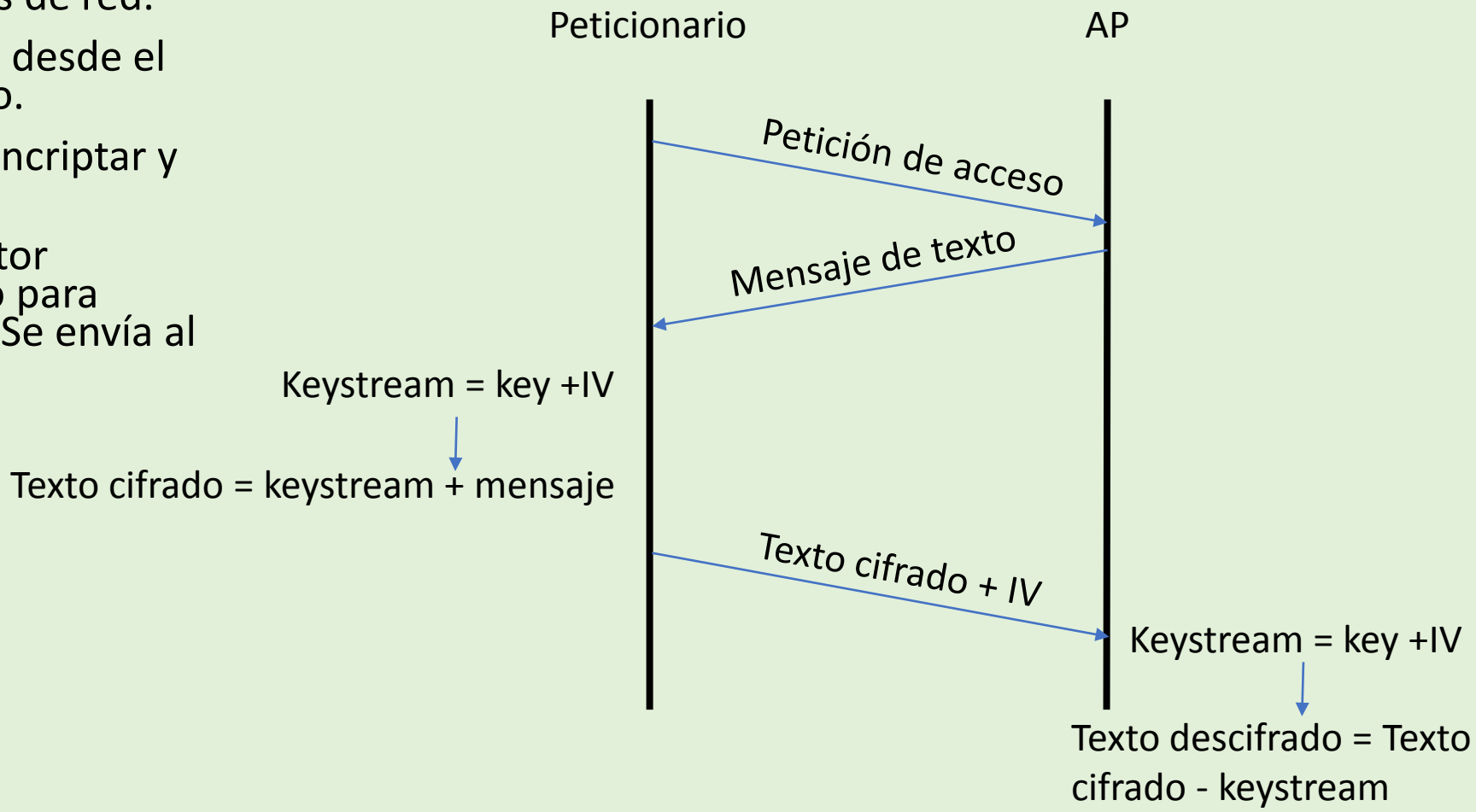
# Wifi

- Alto ancho de banda, alto consumo
- Autenticación y encriptación:
  - WEP
  - WPA/WPA-2:
    - Personal
    - Enterprise

UNIVERSIDAD DE BURGOS

# WEP (Wired Equivalent Privacy)

- Master key: debe ser configurada en AP (Access points) y dispositivos de red.
- Challenge message: enviado desde el AP al dispositivo peticionario.
- RC4: algoritmo usado para encriptar y des-encriptar mensajes.
- Initialization vector (IV): vector aleatorio o pseudo-aleatorio para combinar con la clave (key). Se envía al receptor.



UNIVERSIDAD DE BURGOS

# WPA (Wi-Fi Protected Access)

- Personal: PKS (Pre-Shared Key)
- Enterprise (802.1x): usuario + clave

# Encriptación

- **TKIP (Temporal Key Integrity Protocol):**
  IV más largo – clave más larga – la clave cambia dinámicamente a lo largo del tiempo
  más seguro que WEP pero bajo el mismo principio
- **AES (Advanced Encryption Standard):**
  Introducido para WPA2 – mecanismo de cifrado de bloques frente a mecanismo de stream (WEP & TKIP)

# 802.1x

- EAP (Extensible Authentication Protocol):
  - TLS: requiere la presencia de certificados tanto al lado del cliente como del servidor.
  - TTLS: requiere certificado solo en el lado del servidor.
  - PEAP: requiere certificado solo en el lado del servidor.
  - Otros: MD5, LEAP, FAST.

- TTLS y PEAP requieren configuración de “usuario” + “contraseña” en el dispositivo IoT.

UNIVERSIDAD DE BURGOS

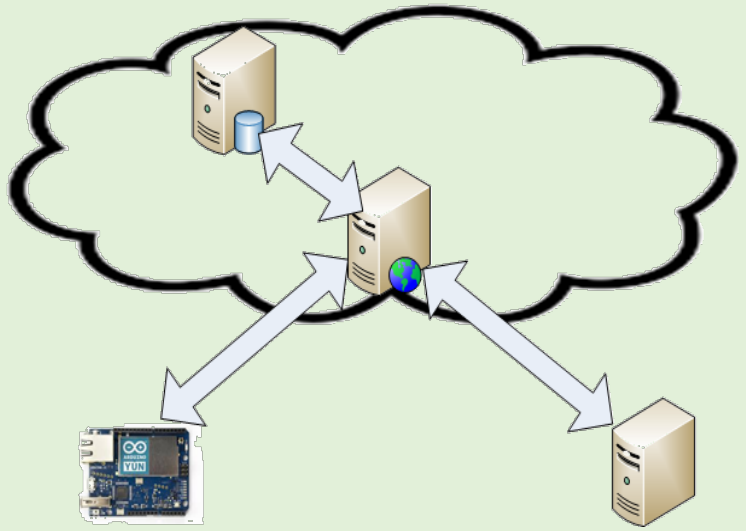
# Prototipado IoT basado en Wifi

- Características del Arduino YUN:
  - Wifi integrada
  - Ethernet integrada
  - Acceso API REST
  - Procesador ATmega32U4 para aplicaciones Arduino
  - Procesador Atheros AR9331 corriendo Linux y pila OpenWrt Wireless
  - Micro SD
  - No soporta 802.1x

UNIVERSIDAD DE BURGOS

# Escenario Wifi IoT

- Lado del dispositivo: Arduino Yun
- Lado del usuario: navegador Web
- Cloud:
  - Servidor Web: recibe y transmite información y control
  - Servidor de base de datos: almacena información y órdenes
- La información se envía desde Arduino a la base de datos vía servidor Web
- Las órdenes se envían desde el usiario a la base de datos a través del servidor Web



Una gúia completa sobre cómo implementar este escenario se puede encontrar en: http://hdl.handle.net/10259/4308

# Red celular (GMS/GPRS/3G/4G)

- Las redes telefónicas celulares proporcionan cobertura casi ilimitada para conexiones de datos.
- Los dispositivos necesitan un adaptador, una tarjeta SIM y, obviamente, un ISP.
- Se conectan al ISP y están listos para enviar información a través de la red.
- Los dispositivos se pueden conectar prácticamente en cualquier parte y disfrutar de un elevado ancho de banda pero…
- … el coste y el consumo de energía son habitualmente inasumibles.
- La vida de las baterías debe estar próxima, si no por encima de 10 años. Esto supone una importante desventaja.

# LPWAN (Low Power Wide Area Network)

- Se trata también de redes celulares.
- Sus demandas de energía son mucho menores que las de las redes telefónicas. También lo es el ancho de banda disponible.
- Los principales parámetros a observar son: disponibilidad, coste, vida de las baterías. El ancho de banda no es una gran restricción en muchos casos.
- Hasta el momento, las principales tecnologías son:
  - Sigfox
  - LoRa (Long Range)
  - NB-IoT (Narrow Band-Internet of Things)

# Comparativa LPWAN

| | Sigfox | LoRa | NB-IoT |
|---|---|---|---|
| Disponibilidad | Alto alcance: (40 km)<br>Depende del estado de despliegue | Alcance medio: (20 km)<br>Depende del estado de despliegue | Alcance bajo: 10 km<br>Se soporta en la infraestructura LTE/4G (urbano). |
| Coste | Coste de infraestructura medio.<br>Coste de los dispositivos bajo. | Coste de infraestructura bajo.<br>Coste de los dispositivos medio. | Coste de infraestructura alto.<br>Coste de los dispositivos alto. |
| Uso de batería | Bajo | Bajo | Medio |
| Ancho de banda | 100 bps | 300 – 50k bps dependiendo del rango seleccionado | 200 kbps |

# Estado del despliegue en España

## Sigfox

- Áreas urbanas y zonas rurales llanas (<90%, 2017)
- https://www.sigfox.com/en/coverage
- Securitas Direct, Correos, Starbucks, DAM,…

## LoRa

- No está disponible comercialmente
- Posible despliegue por parte de Orange a corto plazo
- Open source -> cualquiera puede crear la infraestructura

## NB-IoT

- En despliegue
- Soportado por Vodafone
- https://www.vodafone.es/c/statics/narrowband-iot.pdf

UNIVERSIDAD DE BURGOS

# Prototyping Sigfox


Arduino MKRFOX1200


Pycom sipy

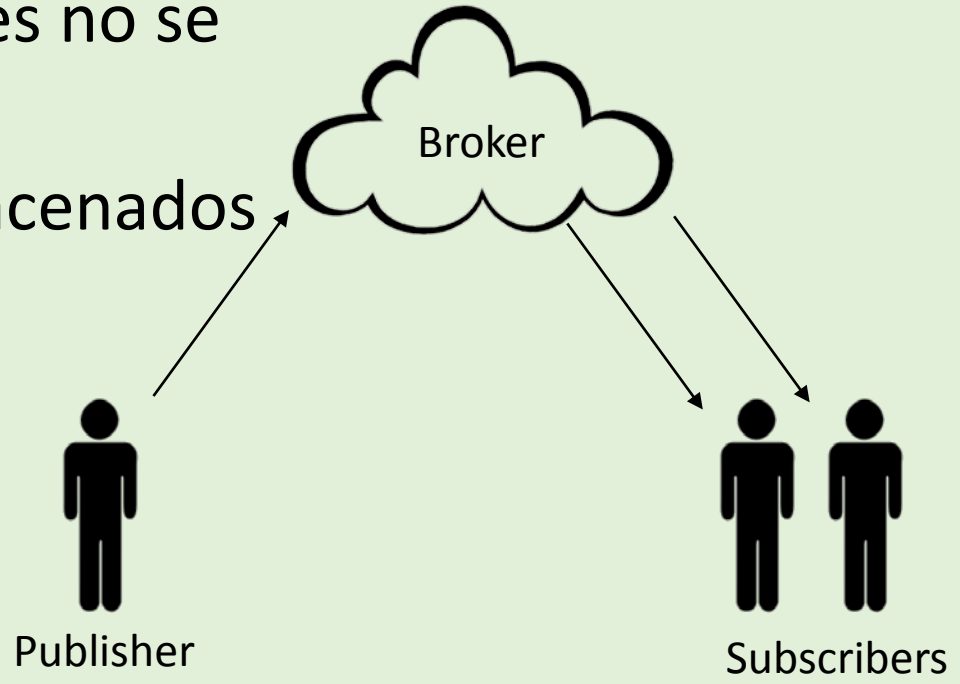
Nemeus XM001

# Application Layer Protocols

- FTP (File Transfer Protocol): no es la mejor opción para IoT. Destinado a transferencias infrecuentes de grandes volúmenes de información.
- HTTP (Hypertext Transfer Protocol): protocolo de petición-respuesta (cliente-servidor). Los mensajes contienen texto plano y están compuestos pro:
  - Línea inicial (especifica el método, la URL y la versión de protocolo)
  - Cabecera (compuesta por metadatos)
  - Cuerpo (datos)
- CoAP (Constrained application protocol): modelo petición / respuesta. Basado en HTTP.
- SCHC (Static Context Header Compression, Sigfox): basado en CoAP. Esquema de compresión que reduce las cabeceras de CoAP.
- MQTT (Message Queue Telemetry Transport, LoRa): modelo publicador/subscriptor.
- LwM2M (Lightweight M2M, NB-IoT): construido sobre CoAP.
- AMQP (Advanced Message Queuing Protocol): modelo publicador/subscriptor encolado.
- XMPP (Extensible Messaging and Presence Protocol): modelo publicador/subscriptor.
- REST (Representational State Transfer): más que un protocolo es un estilo de arquitectura para implementar servicios web. Es posible implementarlo mediante diferentes protocolos como HTTP o CoAP.

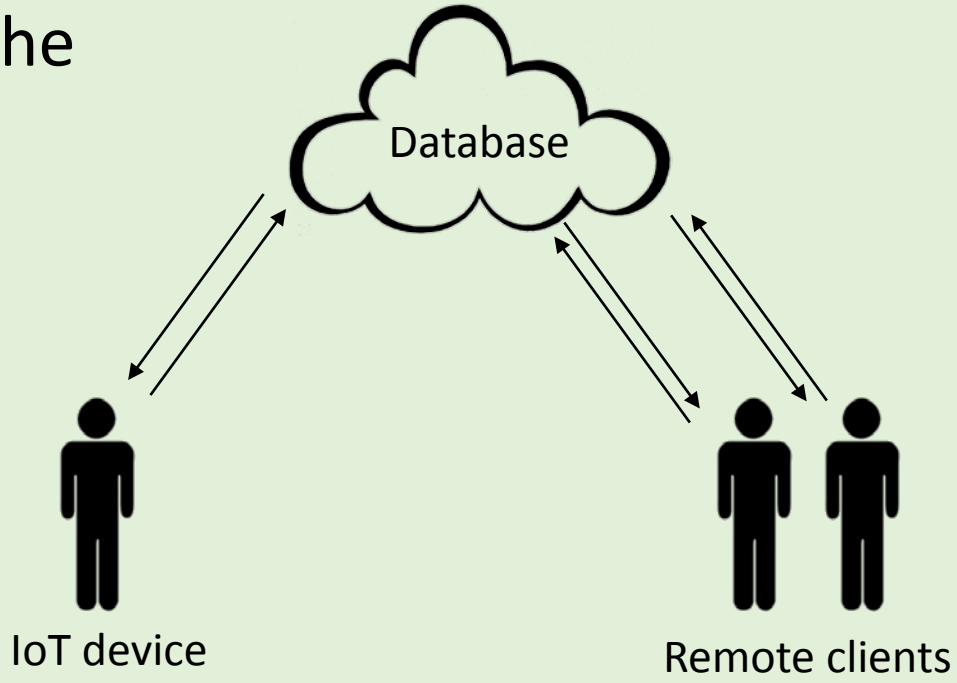
# Modelo publicador / subscriptor

- Dos tipos de clientes:
  - Publicadores: publican información (envían mensajes)
  - Subscriptores: solicitan información (reciben mensajes)
- Broker: recibe y envía mensajes. Los clientes no se conocen entre sí.
- Los mensajes no suscritos pueden ser almacenados en una base de datos.



# Request / response model

- Client IoT devices upload data onto the database posting a request.
- The can also get information from the database.
- Client remote devices can request data to the database
- They can also post information for the IoT device to the database.



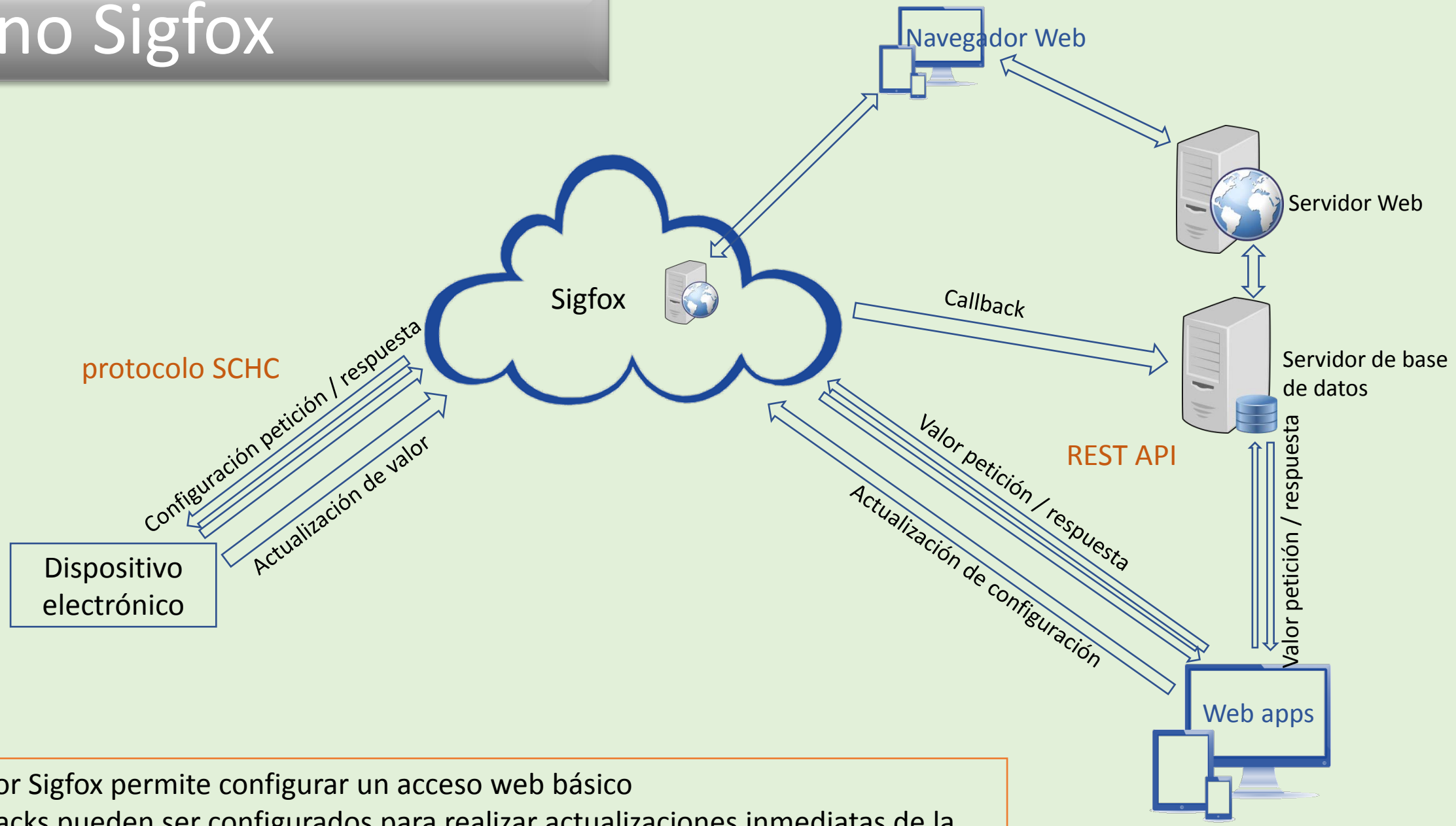
# Configuración de inicio

| | | |
|---|---|---|
| Los dispositivos basados en WAN necesitan una dirección Ip para acceder al exterior. | A diferencia de la dirección MAC, la IP no puede ser preconfigurada en firmware. | Los dispositivos tienen que darse de alta. |
| Cuando se utiliza la red telefónica es necesario disponer de tarjeta SIM | Se asigna una IP dinámica | Hay que darse de alta en la red. |
| Los dispositivos basados en LpWan necesitan otro tipo de ID | El procedimiento de alta depende de la tecnología | Habitualmente se requiere un registro en la web del proveedor. NB-IoT resulta similar a la red telefónica. |

# Referencias


- K. Mekki, et al., A comparative study of LPWAN technologies for large-scale IoT deployment, ICT Express (2018), https://doi.org/10.1016/j.icte.2017.12.005.
- https://www.intel.es/content/www/es/es/support/articles/000006999/network-and-i-o/wireless-networking.html

# Entorno Sigfox




- El servidor Sigfox permite configurar un acceso web básico
- Los callbacks pueden ser configurados para realizar actualizaciones inmediatas de la base de datos del usuario en una operativa de pseudo – tiempo real