UNIVERSIDAD
DE BURGOS

Internet of Things

José M. Cámara 2018

¿IoT?

- What: Things of any kind are connected to the Internet
- What for: a number of reasons. They can be classified:
  - To provide information
  - To receive information
  - To accept orders
  - To be localized
- How: a number of ways:
  - Wifi
  - LAN
  - Cellular telephone network: GPRS-UMTS-LTE
  - LPWAN

IPv4

- 32 bit IP address -> 2.8 billion unique addresses.
- More tan 10 billion connected devices-> IPv4 addresses are no longer unique.
- Devices not uniquely identified can not be found -> no direct Exchange between device and final user is achievable.
- The need for an intermediate host arises at this point.
- Devices can not be polled -> they will decide when to contact the host.
- Too often means too much data and power
- Not frequent enough means important data and events can be missed. Updates are not immediate either.

NAT (Network Address Translation)

- IPv4 devices don’t usually have a unique IP address.
- This doesn’t mean they don’t have an address.
- There are two types of them: public / private.
- Devices have a private address to be recognized within their own local network.
- To gain access to the rest of the world they need a unique public address.
- NAT guarantees a correct translation between private and public addresses.
- Several devices show themselves under the same public address but the NAT provider knows them individually thanks to their private IP and the port they use to connect.

IPv6

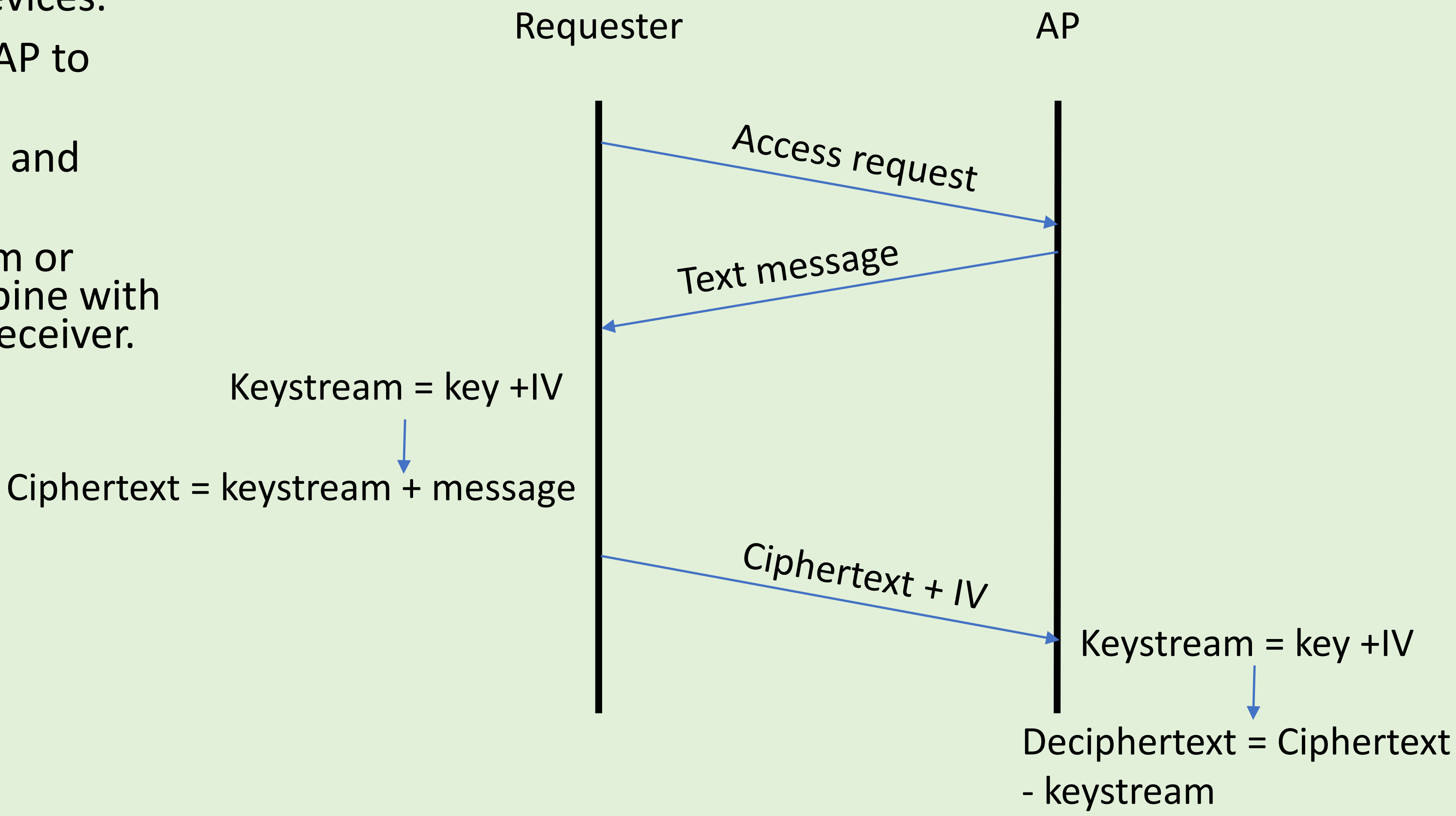
- 128 bit addresses-> 2^{128} devices = unimaginable number of things.
- All objects can be found on the Internet.
- Devices can push information but can also be polled throughout the network.
- No need for NAT.

Wifi

- High bandwidth, high power
- Authentication & encryption:
  - WEP
  - WPA/WPA-2:
    - Personal
    - Enterprise

WEP (Wired Equivalent Privacy)

- Master key: must be configured on AP (Access points) and network devices.
- Challenge message: sent from AP to requesting device.
- RC4: algorithm used to encrypt and decrypt messages.
- Initialization vector (IV): random or pseudo-random vector to combine with the key. It is forwarded to the receiver.



Requester

AP

Access request

Text message

Keystream = key +IV

Ciphertext = keystream + message

Ciphertext + IV

Keystream = key +IV

Deciphertext = Ciphertext - keystream

WPA (Wi-Fi Protected Access)

- Personal: PKS (Pre-Shared Key)
- Enterprise (802.1x): user + key

Encryption

- TKIP (Temporal Key Integrity Protocol):
  Longer IV – longer key – key dynamically changed over time
  safer than WEP but same principle
- AES (Advanced Encryption Standard):
  Introduced for WPA2 – block ciphering mechanism vs stream (WEP & TKIP)

802.1x

- EAP (Extensible Authentication Protocol):
  - TLS: requires the presence of certificates both at client and server sides.
  - TTLS: requires only server side certificate.
  - PEAP: requires only server side certificate.
  - Others: MD5, LEAP, FAST.

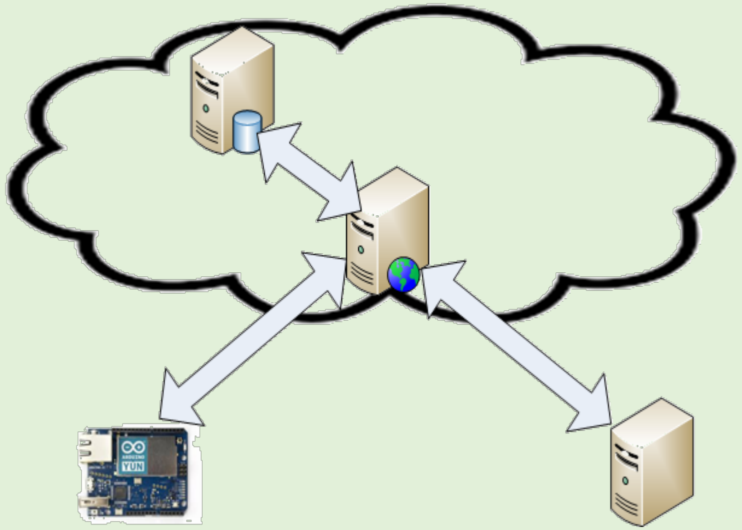
- The TTLS and PEAP require “user” + “password” configuration on the IoT device.

Prototyping Wifi based IoT

- Arduino YUN features:
  - Integrated Wifi
  - Integrated Ethernet
  - REST API access
  - ATmega32U4 processor for Arduino applications
  - Atheros AR9331 running Linux and OpenWrt Wireless stack
  - Micro SD card slot
  - No 802.1x capable

Wifi IoT scenario

- Device side: Arduino Yun
- User side: Web browser
- Cloud:
  - Web server: receives and delivers information and control
  - Database server: stores information and orders
- Information sent by Arduino to the database via Web server
- Orders sent by user to the database via Web server



A complete guide on how to setup an IoT scenario based on Wifi connections can be found at: http://hdl.handle.net/10259/4308

Cellular network (GMS/GPRS/3G/4G)

- Cell phone networks provide almost unlimited coverage for data connections.
- Devices need an adapter, a SIM card and, obviously, an ISP.
- They connect to the ISP and then are ready to deliver information across the network.
- Devices can be connected almost anywhere and enjoy high bandwidth but…
- … cost and energy consumption are usually unaffordable.
- Battery life should be close, if not above, 10 years. This is a significant drawback.

LPWAN (Low Power Wide Area Network)

- These are also cellular networks.
- Their power demands are much lower tan those of the phone networks. So does their bandwidth.
- The three major parameters to be observed are: availability, cost, battery lifetime. Bandwidth is not an issue in most cases.
- Most successful technologies so far are:
  - Sigfox
  - LoRa (Long Range)
  - NB-IoT (Narrow Band-Internet of Things)

LPWAN comparison

	Sigfox	LoRa	NB-IoT
Availability	High range: (40 km) Depends on deployment status	Mid range: (20 km) Depends on deployment status	Low range: 10 km Relies on LTE/4G infrastructure (urban).
Cost	Medium infrastructure cost. Low cost of end devices.	Low infrastructure . Medium cost of end devices.	High infrastructure. High cost of end devices.
Battery usage	Low	Low	Medium
Bit rate	100 bps	300 – 50k bps depending on selected range	200 kbps

Deployment status in Spain

Sigfox

- Urban areas and flat rural areas (<90%, 2017)
- https://www.sigfox.com/en/coverage
- Securitas Direct, Correos, Starbucks, DAM,…

LoRa

- Not present commercially
- Possibly deployed by Orange in the short term
- Open source -> anyone can create the infrastructure

NB-IoT

- Under roll-out
- Supported by Vodafone
- https://www.vodafone.es/c/statics/narrowband-iot.pdf

Prototyping Sigfox

Arduino MKRFOX1200

Pycom sipy

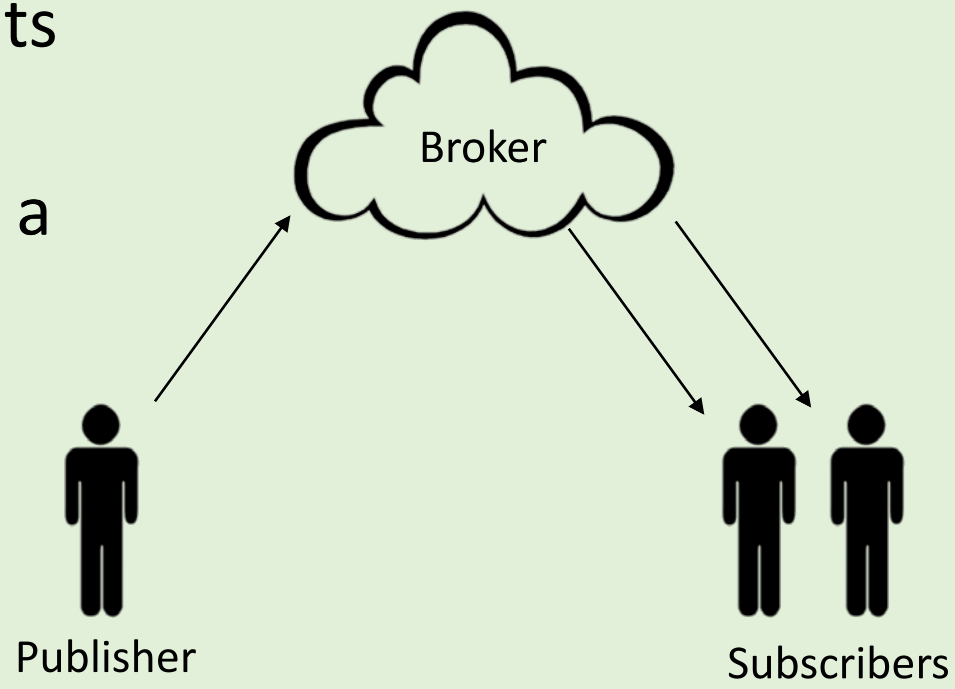
Nemeus XM001

Application Layer Protocols

- FTP (File Transfer Protocol): not the best option for IoT. Meant to transfer big chunks of information rather unfrequently.
- HTTP (Hypertext Transfer Protocol): request-response (client-server) protocol. Messages are made of plain text and composed of:
  - Initial line (where the method, URL and protocol version are specified)
  - Header (composed by metadata)
  - Message body (data)
- CoAP (Constrained application protocol): request / response model. HTTP based.
- SCHC (Static Context Header Compression, Sigfox): based on CoAP. Compression scheme that reduces CoAP headers.
- MQTT (Message Queue Telemetry Transport, LoRa): publish/subscribe model.
- LwM2M (Lightweight M2M, NB-IoT): built on CoAP.
- AMQP (Advanced Message Queuing Protocol): publish /subscribe queuing model.
- XMPP (Extensible Messaging and Presence Protocol): publish/subscribe model.
- REST (Representational State Transfer): not quite a protocol but rather an architecture style to implement web services. Different protocols can be used to implement RESTful services, such as HTTP and CoAP.

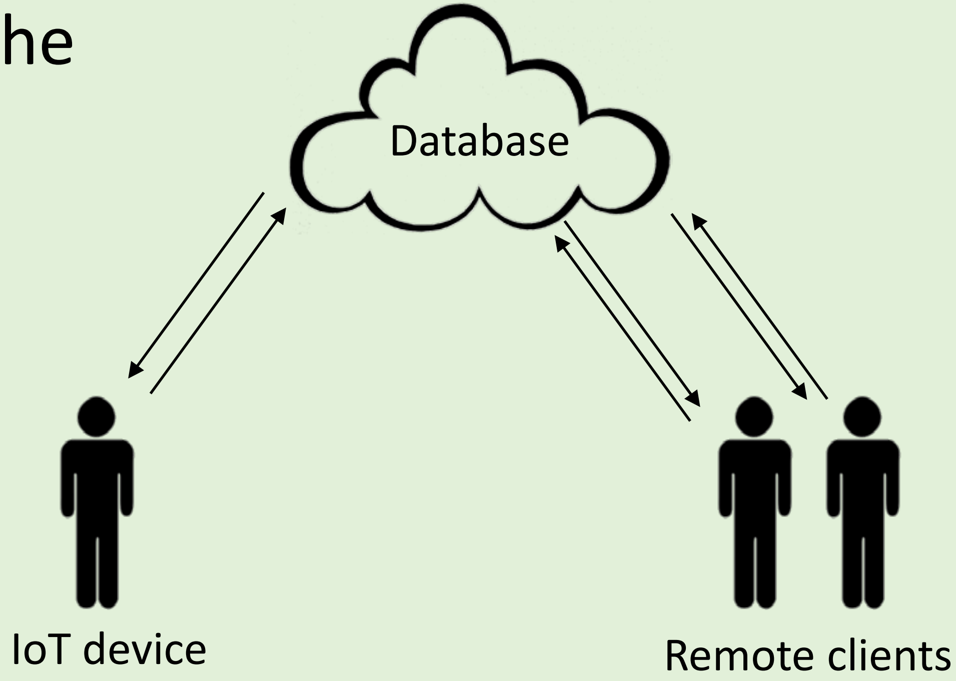
Publish / subscribe model

- Two types of clients:
  - Publishers: post information (send messages)
  - Subscribers: request information (receive messages)
- Broker: receives and sends messages. Clients don’t know one another.
- Unsubscribed messages can be logged into a database.

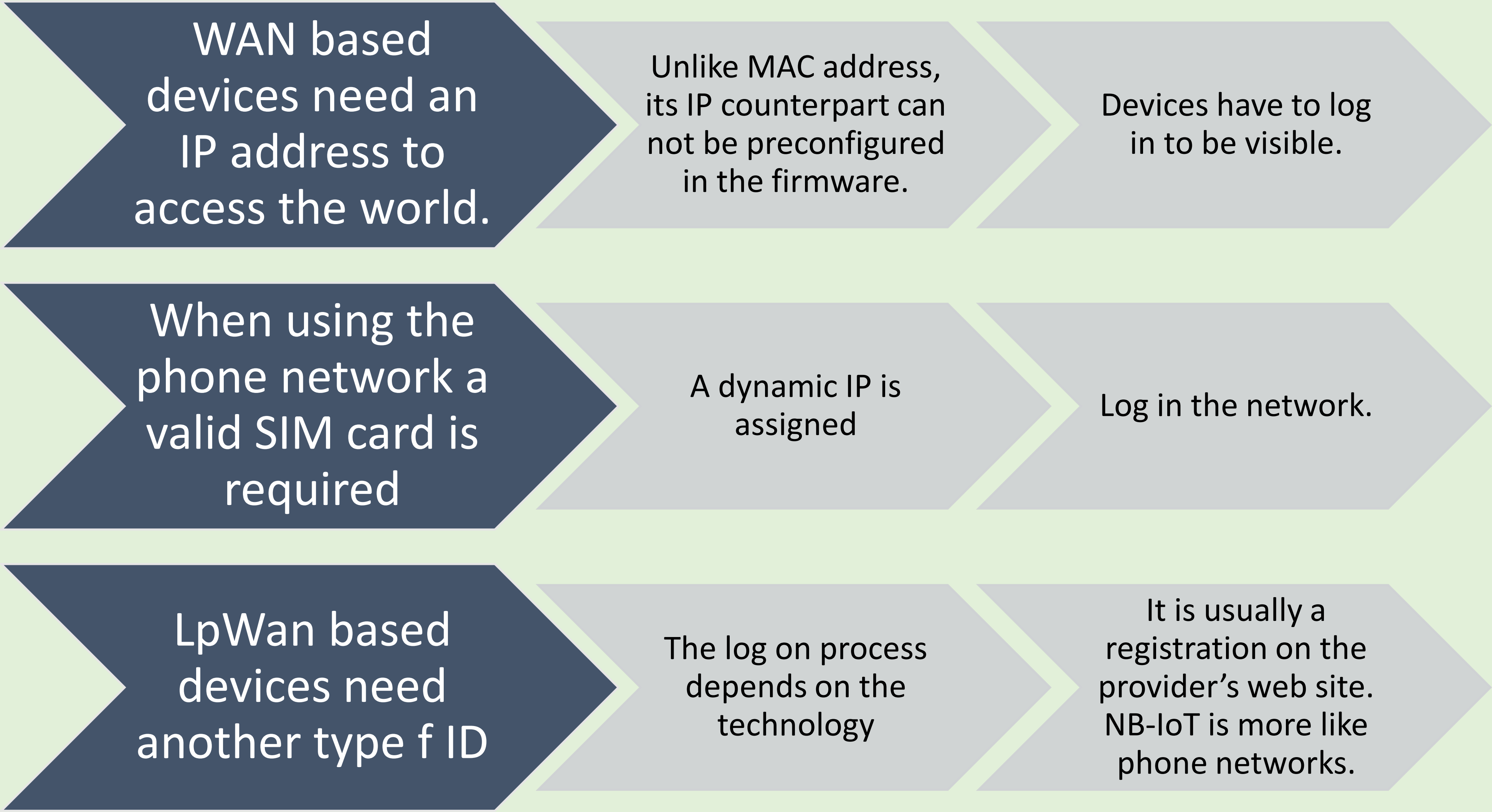


Request / response model

- 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.



Power-up configuration



WAN based devices need an IP address to access the world.

Unlike MAC address, its IP counterpart can not be preconfigured in the firmware.

Devices have to log in to be visible.

When using the phone network a valid SIM card is required

A dynamic IP is assigned

Log in the network.

LpWan based devices need another type f ID

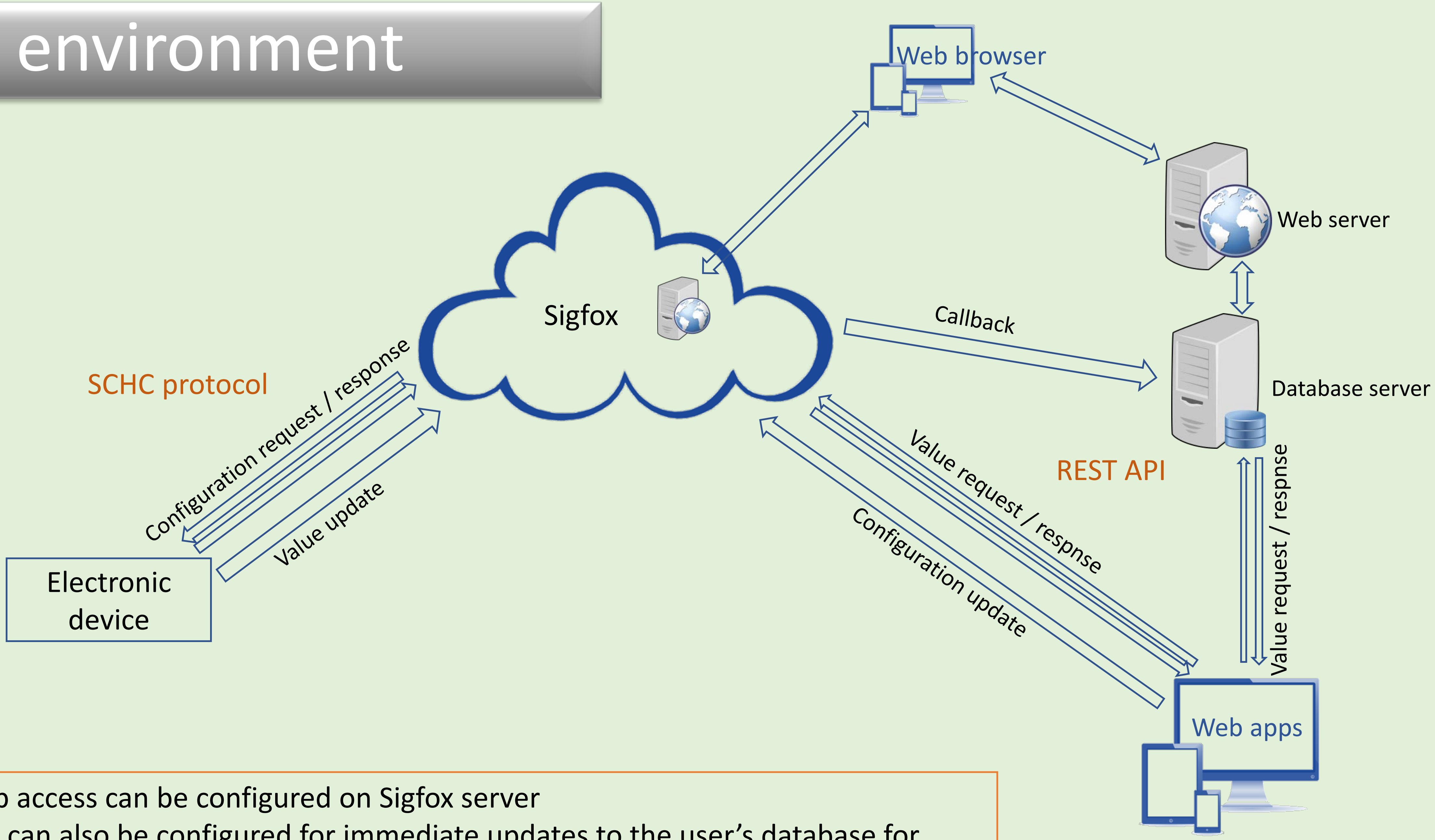
The log on process depends on the technology

It is usually a registration on the provider's web site. NB-IoT is more like phone networks.

References

- 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

Sigfox environment



- Basic web access can be configured on Sigfox server
- Callbacks can also be configured for immediate updates to the user’s database for pseudo – real time operation