

Chapter 6

Protocols

ADVANCED TOPICS IN DATA SCIENCE



Outline

Introduction to non-IP based protocols

- I. Bluetooth wireless protocol
- II. Zigbee
- III. Z-Wave

Introduction to IP based protocols

- IV. 6LoWPAN
- V. Wi-Fi

Long-range protocols

- VI. 5G

MQTT protocol

Non-IP Based WPAN

- Sensors, and other things connected to the internet, need a method of transmitting and receiving information. This is the topic of **personal area network (PAN)** and near-range communication.
- A personal area network, or PAN, is a network that enables communication between devices near a person. PANs can be wired, such as USB, or they can be **wireless (WPAN)**, such as ZigBee, Bluetooth, ... The range of a PAN typically is a few meters.

Non-IP Based WPAN

Bluetooth 5.0

- Bluetooth 5 is revolutionizing the Internet of Things (IoT), allowing design engineers to pioneer innovative solutions while advancing the field of design engineering itself.
- With up to 4x the range, 2x the speed, 8x the broadcasting message capacity, and improved coexistence with other cellular and wireless technologies, the enhancements of Bluetooth 5 open more possibilities than before. And the **best advantage of 5 is Bluetooth Low Energy specification.**
- BLE is more prominent in applications where power consumption is crucial (such as battery powered devices) and where small amounts of data are transferred in frequently (such as in sensor applications). BLE remains in sleep mode constantly except for when a connection is initiated. The BLE guarantees about 4/5 years of battery life of an IoT device.

Non-IP Based WPAN

Bluetooth 5 – Increased speed

- Bluetooth 5 increases the bandwidth of data transfer from 1Mbps to 2Mbps without increasing power consumption. By doubling the amount of data that devices can transfer, Bluetooth 5 reduces the time required for transmitting and receiving data.
- This enhancement empowers engineers to design solutions that redefine the way information is sent to devices, particularly in solutions where speed is a priority, like medical devices and security systems.

Non-IP Based WPAN

Bluetooth 5 – Increased range

- Quadrupling the range from about 50 meters to approximately 200 meters delivers robust, reliable connections that make full-home or building coverage and more outdoor use cases a reality.
- So if you want to connect the smart home with other technology in the garden and beyond, you can use Bluetooth 5 and employ much further ranges while still maintaining that low power envelope that Bluetooth low energy is known for.
- However, extended range and higher speed cannot be used at the same time while still hitting a low power consumption envelope; as a design engineer, you can choose one or the other.

Non-IP Based WPAN

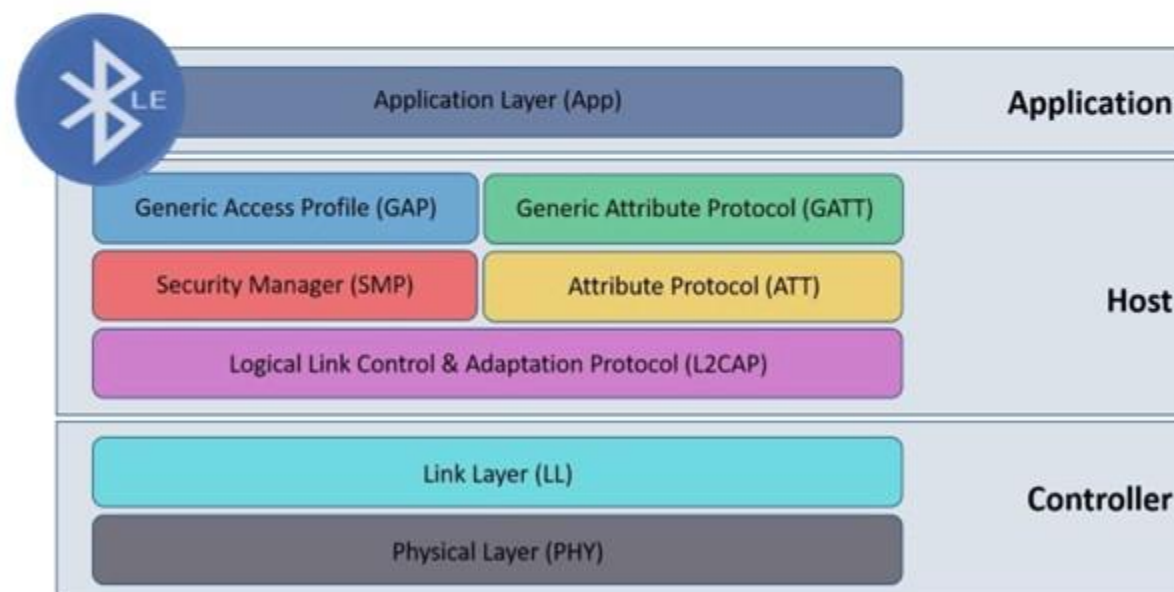
Bluetooth 5 – 8x data

- Increased broadcasting message capacity with support for larger data packets up to 255-octet
- More efficient use of advertising channels

Non-IP Based WPAN

Bluetooth 5 -Protocols stack

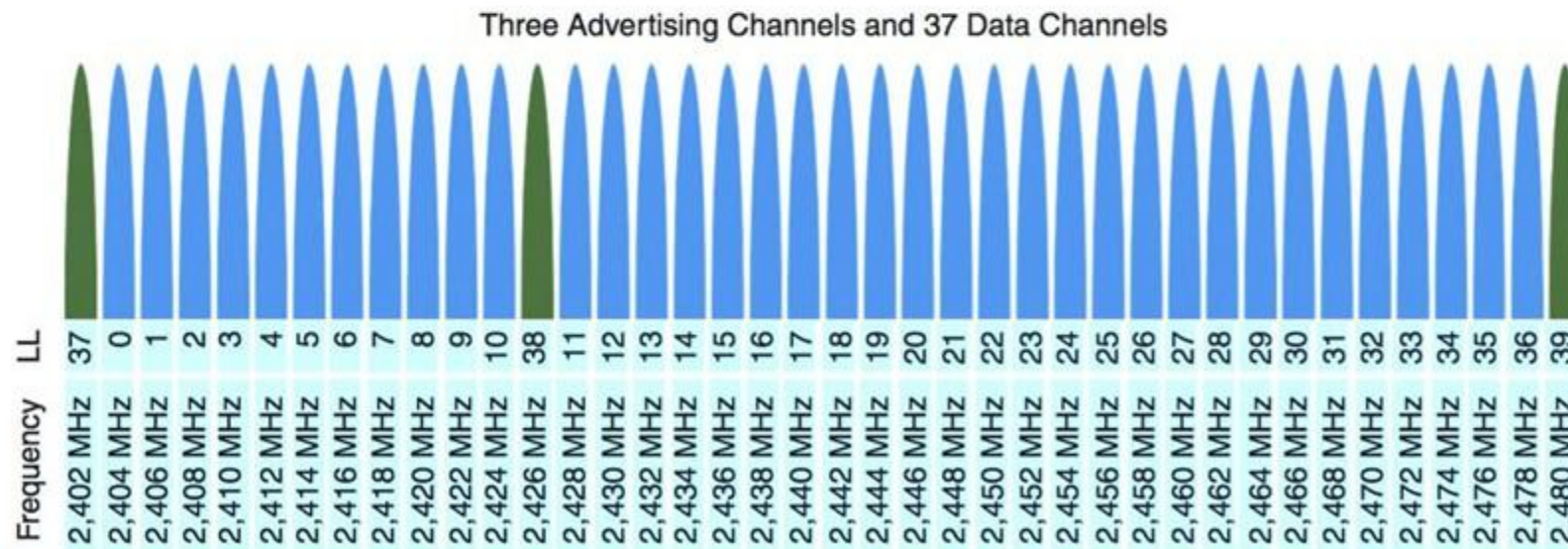
- **Controller — Physical Layer (PHY)**
- The physical (PHY) layer handles the operation involving analog communications. Specifically, it defines the modulation and demodulation of analog signals and applies source coding to transform the signals into digital symbols.
- The BLE radio uses the 2.4 GHz ISM band — it is a licensed free band. There are 40 channels — 3 for advertising channels and 37 for data channels. Each channel is 2 MHz width.



Non-IP Based WPAN

Bluetooth 5 - Advertising channels

- In the Advertising state, a device sends out packets containing useful data for others to receive and process. The packets are sent at a fixed interval defined as the Advertising Interval. There are 40 RF channels in BLE, each separated by 2 MHz (center-to-center), as shown in the following figure. Three of these channels are called the Primary Advertising Channels, while the remaining 37 channels are used for Data Packet transfer during a Connection.



Non-IP Based WPAN

Bluetooth 5 -Link Layer

- Link layer (LL) directly interfaces with the physical layer (PHY), and is usually implemented as a combination of custom hardware and software.
- The hardware part of LL defines a certain automated functionalities to avoid overloading the central processing unit that runs all of the software layers in the stack. These functionalities includes CRC generation and verification, and manages the link state of the radio to define the role of a device as master, slave, advertiser, or scanner.

Non-IP Based WPAN

Bluetooth 5 -BLE operation

- In Bluetooth Low Energy mode, there are five link states that are negotiated by the host and device:
- **Advertising:** Devices that transmit the advertising packets on the advertising channels.
- **Scanning:** Devices that receive advertising on the advertising channels without intention to connect. Scanning can be active or passive:
 - **Active scanning:** Link layer listens for advertising PDUs. Depending on the received PDU, it may request an advertiser to send additional information.
 - **Passive scanning:** Link layer will only receive packets, transmission disabled.
- **Initiating:** Devices that need to form a connection to another device listen for connectable advertising packets and initiate by sending a connect packet.
- **Connected:** There is a relationship between master and slave in the connected state. The master is the initiator and the slave is the advertiser.
- **Standby:** Device in the unconnected state.

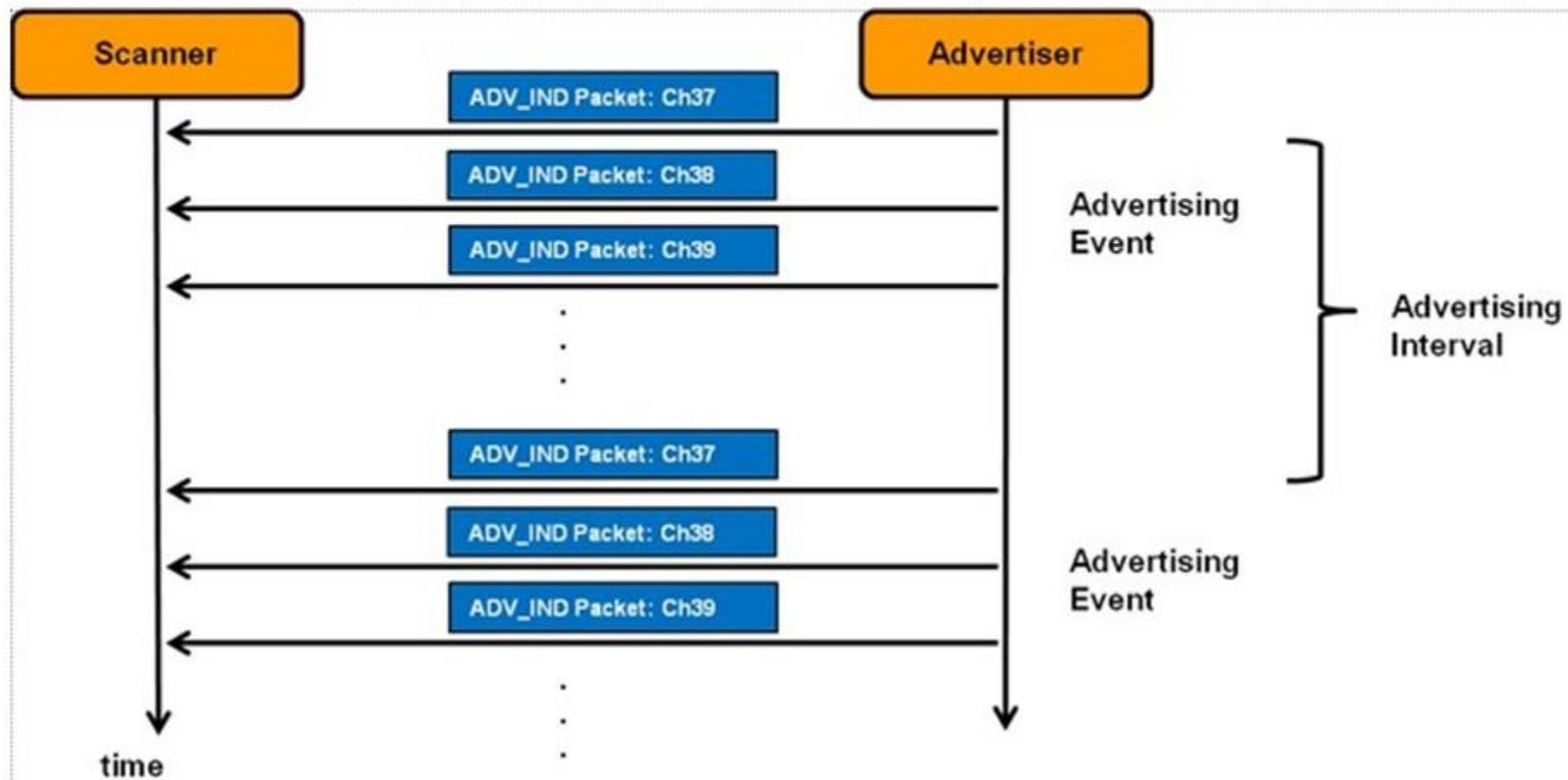
Non-IP Based WPAN

Bluetooth 5 -Bluetooth Low Energy Discovery Process

- The Bluetooth Low Energy (BLE) Link Layer discovery process consists of devices that use advertising channels to find each other, with one device advertising and another device scanning.
- Each time a device advertises, it transmits the same packet in each of the three advertising channels. This sequence of events is called an advertising event. The following example shows general advertising using ADV_IND Advertising Packets.

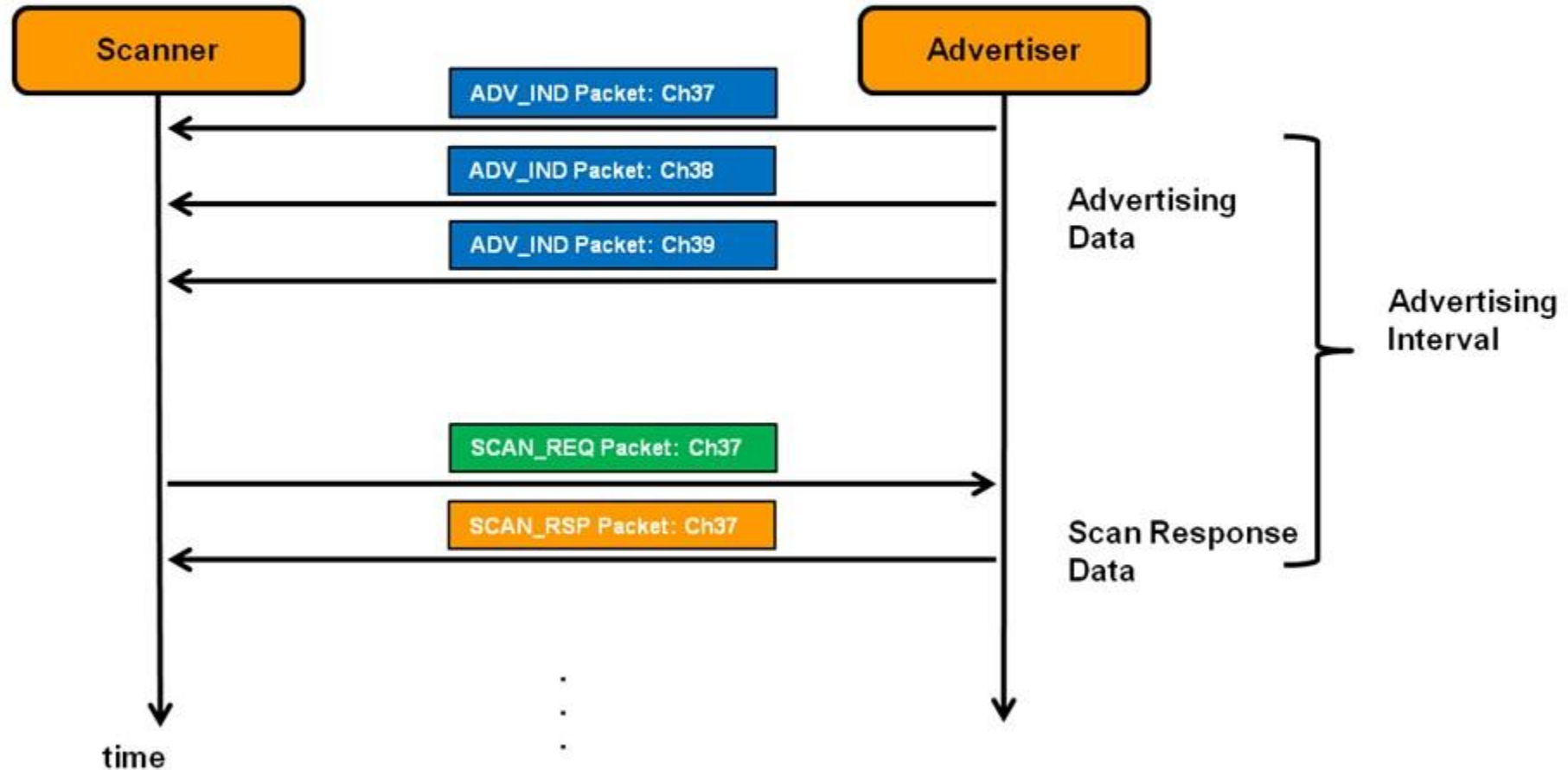
Non-IP Based WPAN

Bluetooth 5 -Advertising



Non-IP Based WPAN

Bluetooth 5 -Scanning



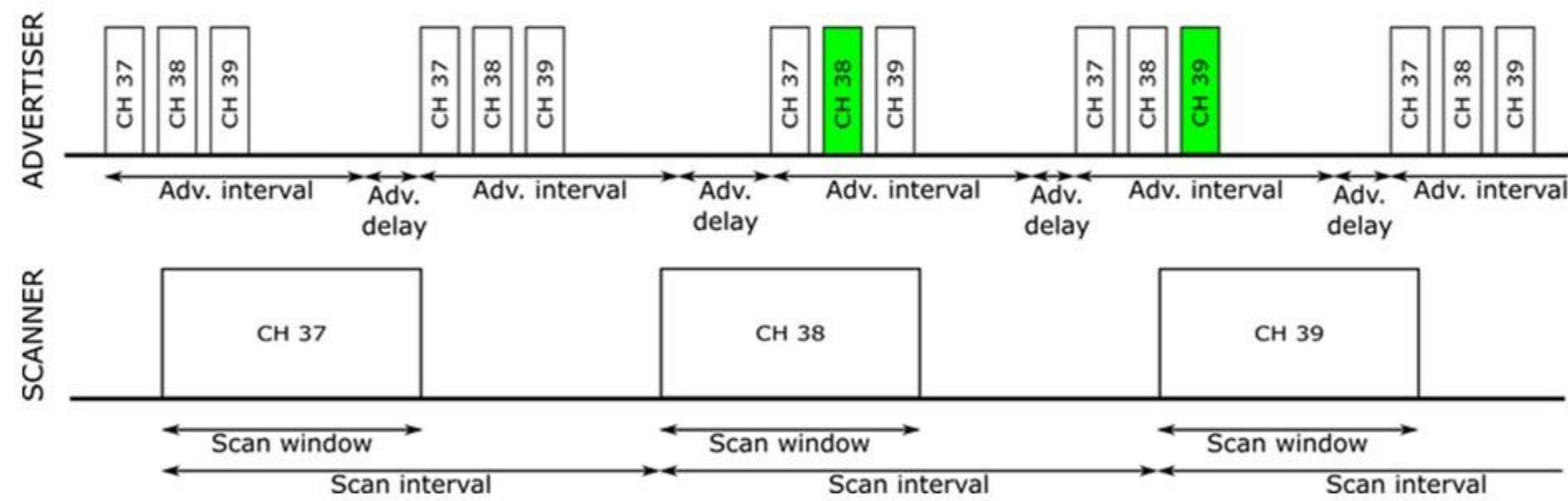
Non-IP Based WPAN

Bluetooth 5 -Advertising and scanning

- Advertising and scanning activities occur at regular intervals. Note, however, that Advertisers and Scanners are not synchronized.
- The black dotted rectangles above indicate potential time positions where advertising and scanning activities overlap, enabling discovery to take place.

Non-IP Based WPAN

advertising and scanning



Bluetooth Low Energy (BLE) advertisement and scanner operation in connectionless mode. The green color denotes advertisements that are coincidentally received, i.e., when the hub happens to scan the same channel as the one the tag uses for transmission.

Non-IP Based WPAN

Bluetooth 5.0

- In BLE, there are three main states a device can operate in. It can either be Advertising, Scanning or Connected.
- To get two BLE devices connected, one device has to advertise and the other has to scan for it, and then initiate the connection. Advertising essentially involves broadcasting packets which allow another scanning device to discover them. The scanning device may then decide to initiate a connection if the advertisement packets indicate that the advertising device allows it.

Non-IP Based WPAN

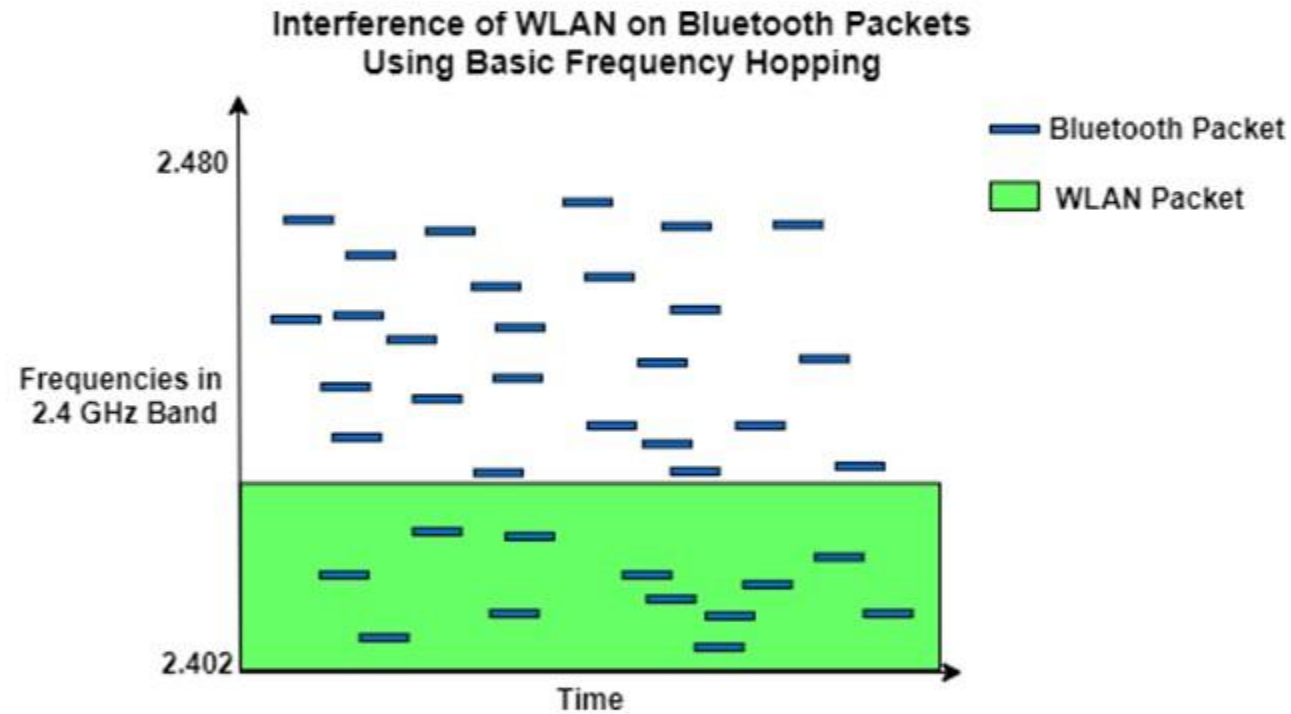
Bluetooth 5 -wireless coexistence

- Bluetooth 5 was marketed as improving wireless coexistence and interoperability, a statement that can easily be misunderstood as enhanced coexistence with a Wi-Fi device.
- The real improvement in coexistence is with other nearby BLE devices. The random frequency-hopping scheme of Bluetooth 5 decreases the chance of a neighboring BLE device transmitting on the same radio-frequency (RF) channel at the same time, thus increasing the overall robustness of each connection.
- Bluetooth 5 allows a user to control multi-devices from Bluetooth-equipped smartphones, headphones, and other devices.

Non-IP Based WPAN

Bluetooth hopping

- **Bluetooth** utilizes frequency-hopping spread spectrum technology to avoid interference problems: the data channels that **Bluetooth** technology is "**hopping**" over. The signal switches carrier channels rapidly, at a rate of 1600 **hops** per second, over a determined pattern of channels.
- The benefits of Hopping is that it reduces the possibility of interference



Non-IP Based WPAN

Zigbee

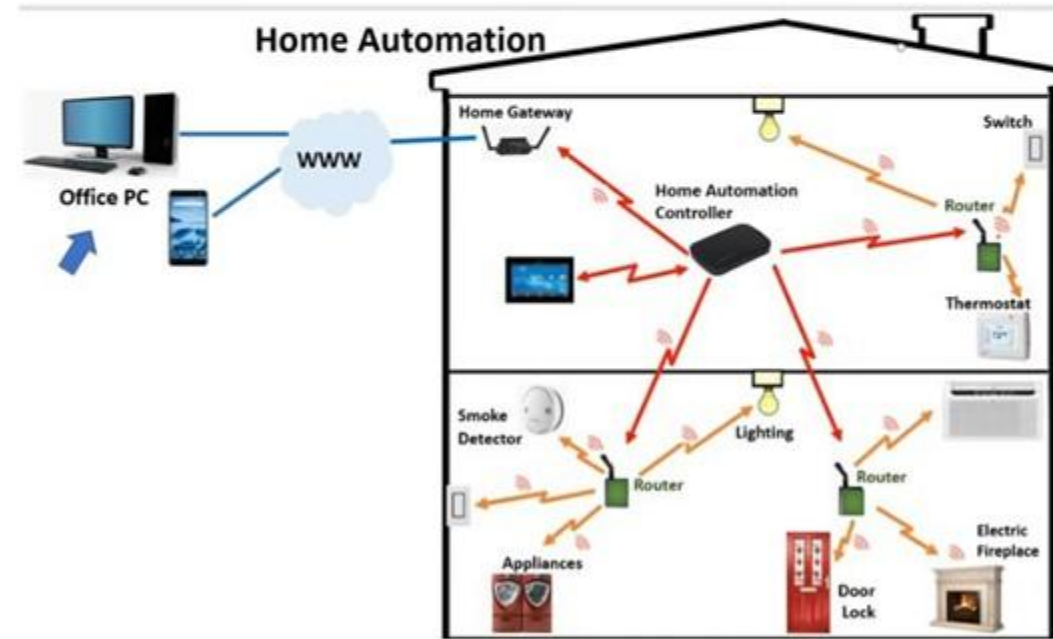
- Zigbee is a Wireless technology standard that defines a set of communication protocols for short range communications.
- Why another short-range communication standard ?
 - Zigbee standard is specially build for control and sensor networks
 - It addresses the need for very low-cost implementation of low power devices with low data rate for short range wireless communications.
- The Zigbee standard operates in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz.



Non-IP Based WPAN

Zigbee Applications

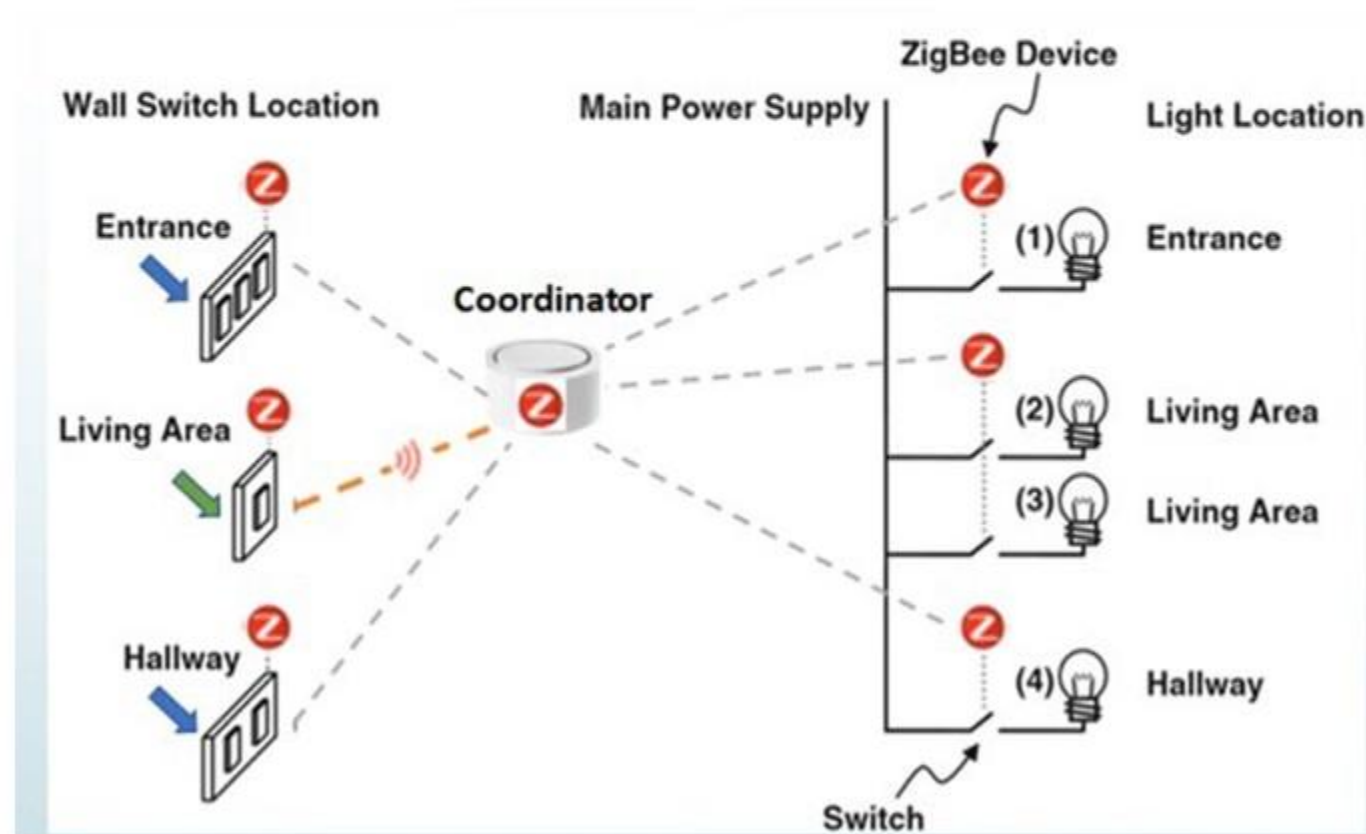
- Home automation: In home automation, basically a home automation controller with a software application that controls smart devices. The controller is also called a central hub or simply a hub
 - Medical data collection
 - Industrial control systems
- 
- The diagram, titled "Home Automation", illustrates the system architecture. It shows an "Office PC" and a smartphone connected to a "WWW" cloud. The "WWW" cloud is connected to a "Home Gateway" located inside a house. Inside the house, the "Home Gateway" is connected to a "Home Automation Controller" (the central hub). The controller is then connected to various smart devices: a light bulb, a "Switch", a "Router", and a "Thermostat". Red arrows indicate the primary control path from the gateway to the controller and then to the devices. Orange arrows show secondary or data paths, such as from the controller to the router and then to the thermostat, or from the router to the switch.



Non-IP Based WPAN

Zigbee- Home automation

- Perform control tasks inside a building example



Non-IP Based WPAN

Zigbee

There are three principal components in a Zigbee network.

- **Zigbee controller (ZC):** Highly capable device on a Zigbee network that is used to form and initiate network functions. Each Zigbee network will have a single ZC. It is a special router. In addition to all of the router capabilities, the coordinator is responsible for forming the network. To do that, it must select the appropriate channel, and other parameters. It is also responsible for selecting the security mode of the network. The trust center is responsible for authenticating new nodes & distributing network keys to new nodes as they join the network. After the network is formed, the ZC can behave as a ZR (Zigbee router).
- **Zigbee router (ZR):** Routers are responsible for routing traffic between different nodes. Routers may not sleep. As such, routers are not a suitable choice for battery operated devices. Routers are also responsible for receiving and storing messages intended for their children. In addition to this, routers are the gate keepers to the network. They are responsible for allowing new nodes to join the network.
- **Zigbee end device (ZED):** This is usually a simple endpoint device such as a light switch. It contains enough functionality to communicate with the coordinator. It has no routing logic; therefore, any messages arriving at a ZED that are not targeted to that end device are simply relayed.

Non-IP Based WPAN

Zigbee -Channel access

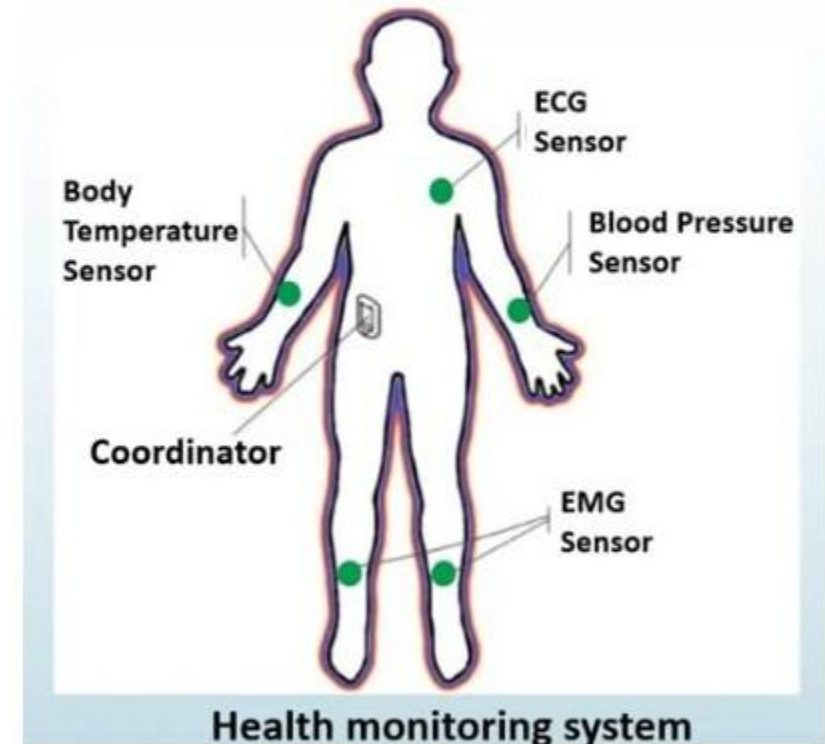
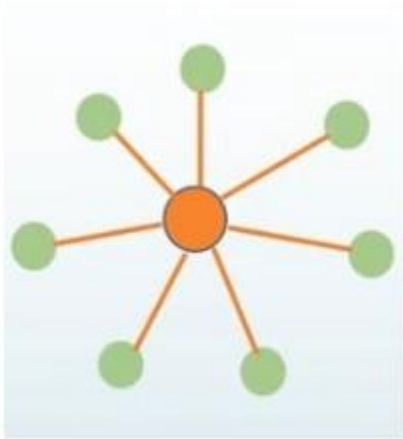
- The coordinator assigns only one channel to the network → all devices have to share this single channel to communicate
- Channel access methods:
 - Contention-free method** : The coordinator dedicates a specific time slot to each device. This is called a guaranteed time slot (GTS).
 - Contention based method** : Devices do not need to be synchronized. CSMA(collision avoidance mechanism) is used :
 - Each time a device wants to transmit.
 - It first goes into receive mode
 - Detect if there is any signal in the channel
 - Device will only transmit the data if the channel is clear. If the channel is not clear, the device backs off for a random period of time and tries again.

Non-IP Based WPAN

Zigbee topologies

- **Star topology**

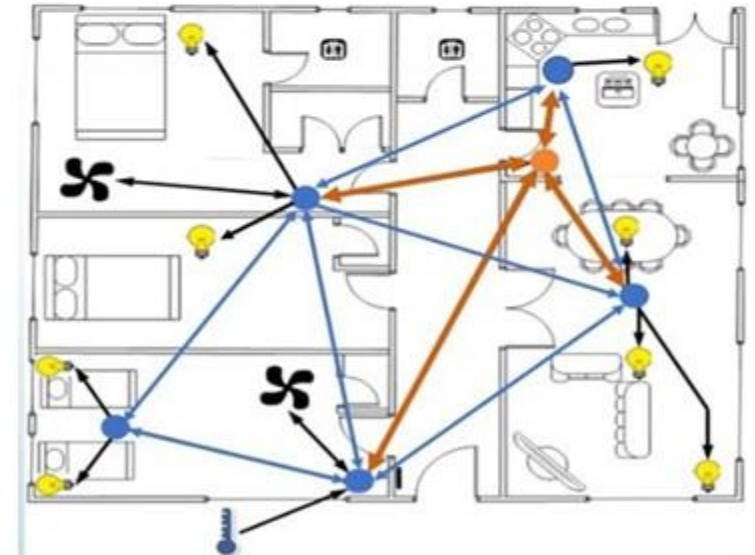
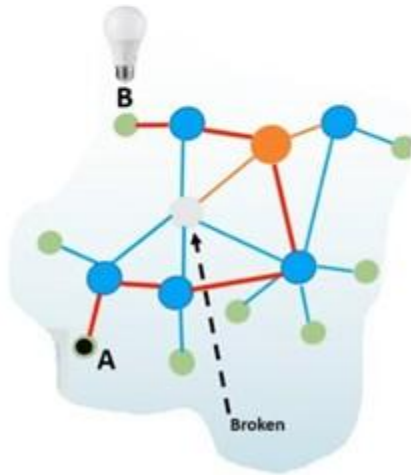
- Simplest / less expensive
- No routers in this architecture
- End devices cannot communicate directly



Non-IP Based WPAN

Zigbee topologies

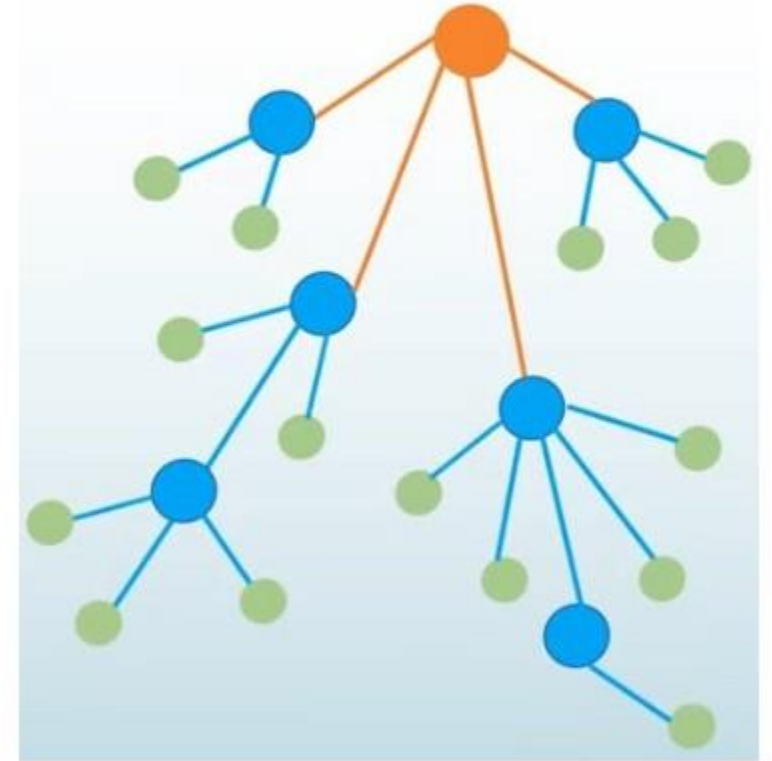
- **Mesh topology**
 - Every node is connected with the neighboring node (except for the end devices)
 - A message hops from one device to another to reach its destination
 - If a node fails, data can be re-routed using another path



Non-IP Based WPAN

Zigbee topologies

- **Tree topology**
 - not very different from a mesh configuration
 - Routers are not interconnected



Non-IP Based WPAN

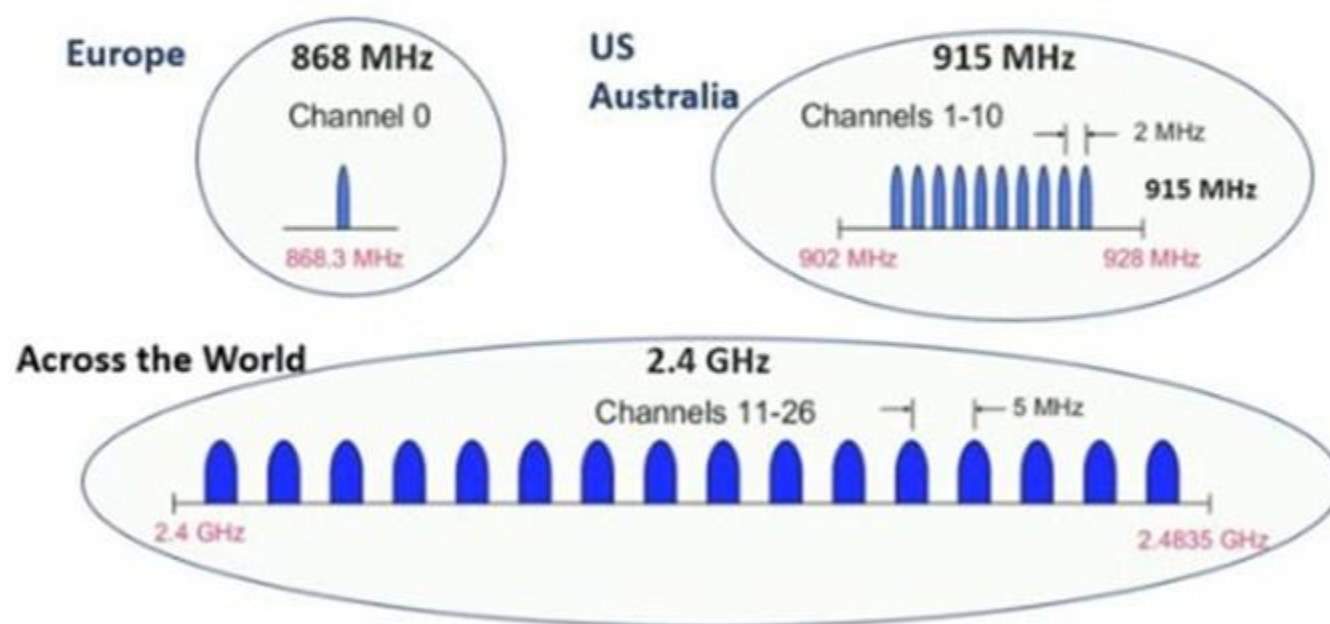
Zigbee – characteristics

- The Zigbee wireless connection protocol is intended for applications that require low power consumption and do not require large data transfer speeds. The most common application areas are home automation, wireless network sensors, smoke or motion sensors, medical data collection and even specific industrial control systems.
- Among the most notable features of Zigbee :
 - The devices do not connect individually to the Internet.
 - It offers **low energy consumption** .
 - **Up to 75-100 meters indoor and up to 300+ meters (line of sight).**
 - Very low data transfer speeds, defined speed of **250 kbit / s.**
 - Network join time: ~ 30 msec (Wifi: up to 3 s , Bluetooth up to 10 s)
 - Number of devices: Up to 65 000 in theory / 240 in practice (very high)
 - Low cost products and cheap implementation
 - AES cryptographic algorithm

Non-IP Based WPAN

Zigbee- F bands

- There are 3 different bands currently assigned to Zigbee



- Only one channel will be selected for use in a network.

Non-IP Based WPAN

Zigbee benefits

- Self forming: Zigbee network can configure itself automatically.
- Self healing: Zigbee can reconfigure itself dynamically in situations that Zigbee nodes become faulty, removed or disabled.
- Interoperability: Different Zigbee modules from many different manufacturers in home automation and industrial devices can operate together.

Non-IP Based WPAN

Z-wave

- Z-Wave is together with Zigbee the two wireless communication protocols alternative to WiFi or Bluetooth.
- Although both function as a mesh network system, there are certain differences between the two. The first difference is that Zigbee is an open protocol managed by the Zigbee Alliance, while **Z-Wave is private**.
- And the fact that it is closed guarantees that all compatible devices can function without any problem between them. However, with Zigbee it can be given that certain manufacturers can only allow the compatibility of devices of the manufacturer itself.
- Z-Wave has a greater range than Zigbee (**up to 100m**) and usually offers greater stability in connections, while Zigbee supports more connected devices, 65000 compared to just over 200.

Non-IP Based WPAN

Z-wave

- Like Zigbee, Z-Wave also requires the use of a hub or bridge to connect and manage the IoT devices we use. As far as compatibility is concerned, the fact that Zigbee uses the 2.4GHz frequency means that if at any time we want to take our devices to another country, we will have no problem using it. However, Z-Wave uses different radio frequencies in different countries, which means we cannot use them in countries where different frequencies are used.
- As main features of Z-Wave, it should be noted:
 - It requires the use of a **bridge or hub** device .
 - **Mesh network** system .
 - The devices do not connect individually to the Internet.
 - It offers **low** energy **consumption** .
 - Maximum reach 100m.
 - Very low data transfer speeds, maximum speed of **100 kbit / s**.
 - Mainly for home use, control of household items, sensors, electronic security elements, start-up of electronic devices or entertainment.
 - It is a closed protocol.

IP-based protocols

Why do we need IP-based protocols for PAN?

- Use of existing infrastructure
- IP based networks can readily be connected to other IP-based networks without the need for gateways

IP-based protocols

6LoWPAN

- 6LoWPAN is a somewhat acronym that combines the latest version of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN). 6LoWPAN, therefore, allows for the smallest devices with limited processing ability to transmit information wirelessly using an internet protocol. It's the newest competitor to ZigBee.
- A secondary effect is that IPV6 provides significant theoretical addressability of 2^{128} or 3.4×10^{38} unique addresses. This covered the estimates of 50 billion internet-connected devices by 2021 and continued to cover those devices well beyond that. Therefore, IPV6 is well-suited for IoT growth.

IP-based protocols

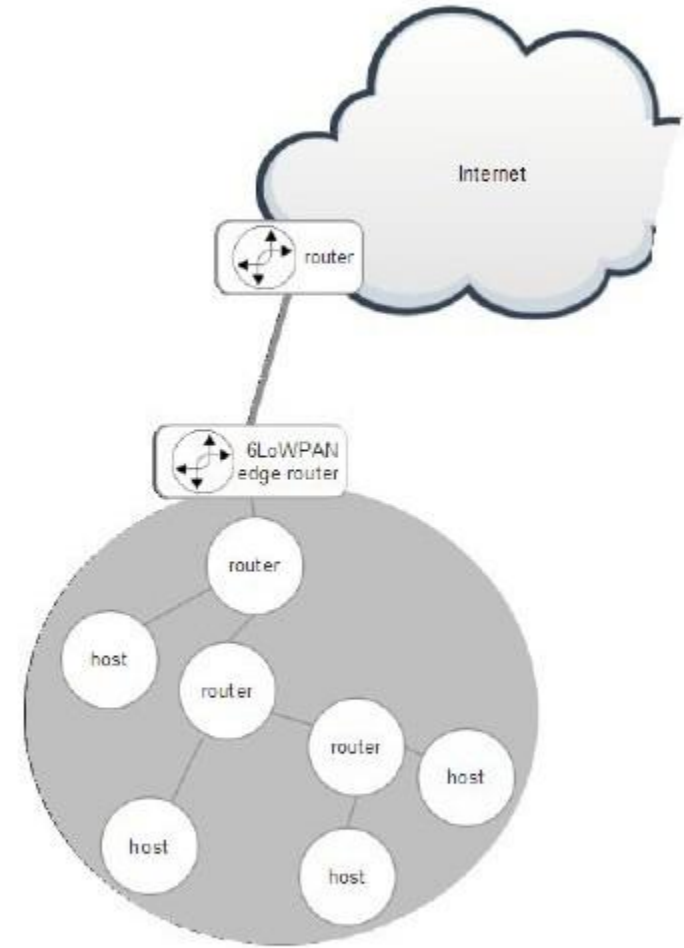
6LoWPAN

- Acronym: IPv6 over Low-Power Wireless PAN
- It is a networking technology or adaptation layer allowing to transport IPv6 packets over small link layer frames, such as those defined by 802.15.4
- Why IPv6 ?
 - More suitable for high density
 - No Intermediate gateway

IP-based protocols

6LoWPAN topology

6LoWPAN networks are mesh networks residing on the periphery of larger networks. The topologies are flexible, allowing for ad hoc and disjointed networks without any binding to the internet or other systems, or they can be connected to the backbone or the internet using edge routers. Additionally, ad-hoc networks can form without requiring an Internet connectivity of an edge router.



IP-based protocols

6LoWPAN topology

An edge router (also known as border router) is necessary for a 6LoWPAN architecture as it has four functions:

- Handles the communication to the 6LoWPAN devices and relays data to the internet.
- Performs compression of IPv6 headers by reducing a 40-byte IPv6 header and 8-byte UDP headers for efficiency in a sensor network. A typical 40-byte IPv6 header can compress to two to 20-bytes depending on usage.
- Initiates the 6LoWPAN network.
- Exchanges data between devices on the 6LoWPAN network.

IP-based protocols

Thread

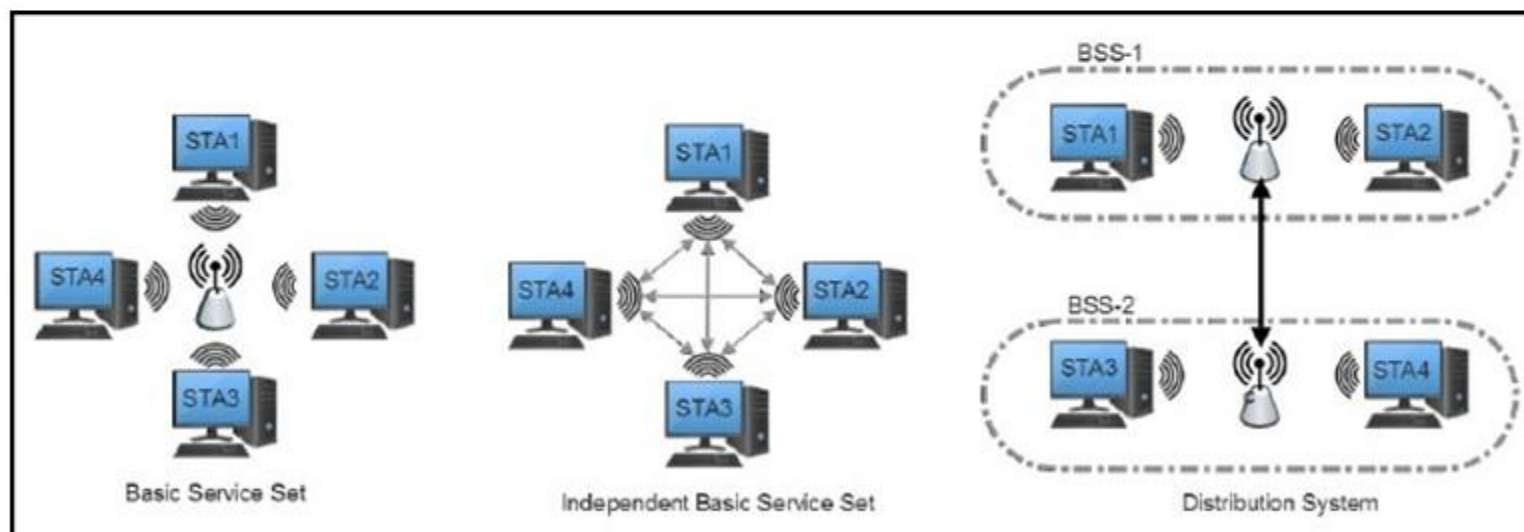
- Thread is a relatively new networking protocol for IoT and is based on IPV6 (6LoWPAN). Its principal target is home connectivity and home automation. Thread was launched in July of 2014.
- Based on the IEEE 802.15.4 protocol and 6LoWPAN, it has commonality with Zigbee and other 802.15.4 variants, but with a significant difference: Thread is IP addressable. This IP protocol builds on the data and physical layers provided by 802.15.4 and the features such as security and routing from 6LoWPAN. Thread is also mesh-based, making it attractive for home lighting systems with up to 250 devices in a single mesh. The philosophy with Thread is that by enabling IP addressability in the smallest of sensors and home automation systems, one can reduce power because it doesn't need to persist application state since the protocol uses datagrams at the network layer. This also implies that the edge router hosting a Thread mesh network doesn't need to process application layer protocols and can lower its power and processing needs.
- Finally being IPV6 compliant, it is inherently secure with all communications being encrypted using the Advanced Encryption Standard (AES). Up to 250 nodes can exist on a Thread mesh all with fully encrypted transport and authentication. A software upgrade allows a pre-existing 802.15.4 device to be Thread compatible.

IP-based protocols

IEEE 802.11

- IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high-frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

- Architectures



IP-based protocols

IEEE 802.11

802.11 systems support three basic topologies:

- **Infrastructure:** In this form, a **Station (STA)** refers to an 802.11 endpoint device (like a Smartphone) that communicates with a central **access point (AP)**. An AP can be a gateway to other networks (WAN), a router, or a true access point in a larger network. This is also known as **Infrastructure Basic Set Service (BSS)**. This topology is a star topology.
- **Ad hoc:** 802.11 nodes can form what is called an **Independent Basic Set. Service (IBSS)** where each station communicates and manages the interface to other stations. No access point or a star topology is used in this configuration. This is a peer-to-peer type of topology.
- **Distribution system (DS):** The DS combines two or more independent BSS networks through access point interconnects.

5G

- 5G is the 5th generation of mobile networks, a significant evolution of today's 4G LTE networks. 5G has been designed to meet the very large growth in data and connectivity of today's modern society, the internet of things with billions of connected devices, and tomorrow's innovations. 5G will initially operate in conjunction with existing 4G networks before evolving to fully standalone networks in subsequent releases and coverage expansions. Initial 5G services commenced in many countries in 2019.
- In addition to delivering faster connections and greater capacity, a very important advantage of 5G is the fast response time referred to as latency. Latency is the time taken for devices to respond to each other over the wireless network. 3G networks had a typical response time of 100 milliseconds, 4G is around 30 milliseconds and 5G will be as low as 1 millisecond. This is virtually instantaneous opening up a new world of connected applications.

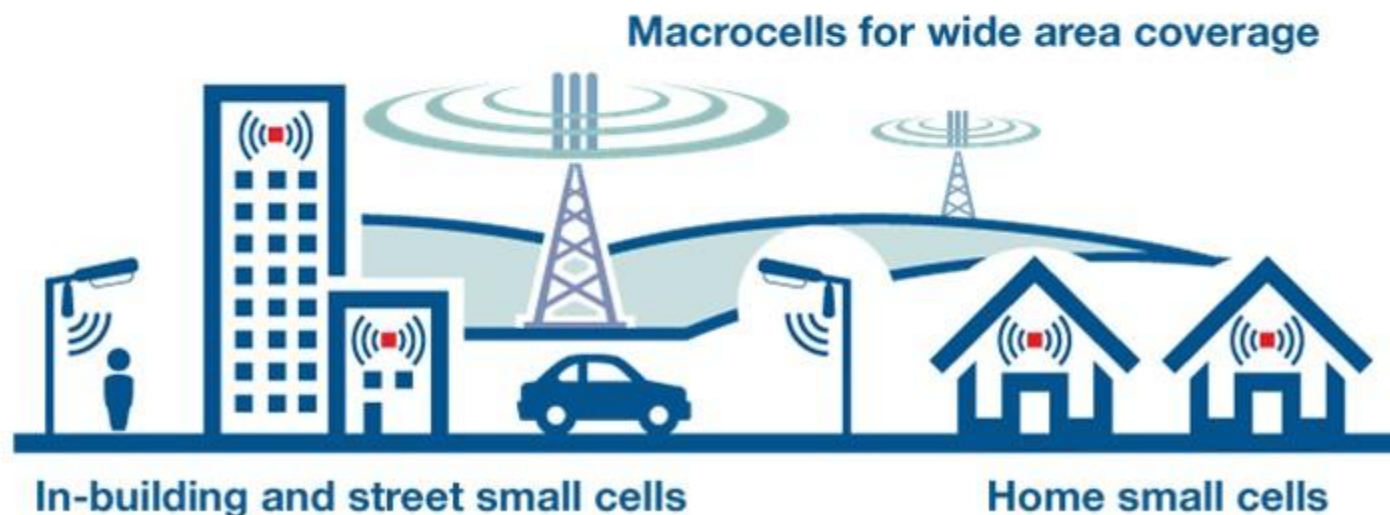


5G

How does 5G deliver continuous connection, greater capacity, and faster speed and response times?

Better Connection - always connected

5G networks are designed to work in conjunction with 4G networks using a range of macro cells, small cells and dedicated in-building systems. Small cells are mini base stations designed for very localized coverage typically from 10 meters to a few hundred meters providing in-fill for a larger macro network. Small cells are essential for the 5G networks as the mmWave frequencies have a very short connection range.



5G

- Increased Spectrum – greater capacity, more users and faster speed
- In many countries the initial frequency bands for 5G are below 6 GHz (in many cases in the 3.3-3.8 GHz bands) and similar frequencies to existing mobile and Wi-Fi networks. Additional mobile spectrum above 6 GHz, including the 26-28 GHz bands often referred to as millimeter (mm) Wave, will provide significantly more capacity compared to the current mobile technologies. The additional spectrum and greater capacity will enable more users, more data and faster connections.

5G

- **Massive MIMO**
- multiple element base station - greater capacity, multiple users, faster data
- 5G will use 'massive' MIMO (multiple input, multiple output) antennas that have very large numbers of antenna elements or connections to send and receive more data simultaneously. The benefit to users is that more people can simultaneously connect to the network and maintain high throughput. The overall physical size of the 5G massive MIMO antennas will be similar to 4G, however with a higher frequency, the individual antenna element size is smaller allowing more elements (in excess of 100) in the same physical case. 5G User Equipment including mobile phones and devices will also have MIMO antenna technology built into the device for the mmWave frequencies.

5G

- MIMO - Beam Steering
- Beam steering is a technology that allows the massive MIMO base station antennas to direct the radio signal to the users and devices rather than in all directions. The beam steering technology uses advanced signal processing algorithms to determine the best path for the radio signal to reach the user. This increases efficiency as it reduces interference (unwanted radio signals).



MQTT protocol

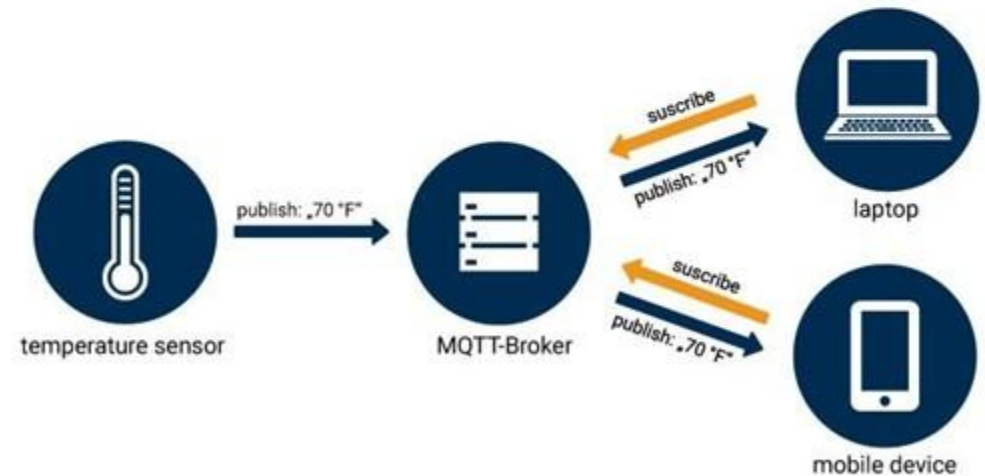
- The Message Queuing Telemetry Transport (MQTT) is a lightweight, publish- subscribe network protocol that transports messages between devices.



- MQTT is a simple messaging protocol, designed for constrained devices with low-bandwidth. It's the perfect solution for Internet of Things applications. MQTT allows you to send commands to control outputs, read and publish data from sensor nodes and much more.

MQTT advantages

- Distribute information more efficiently.
- Increase scalability.
- Reduce network bandwidth consumption dramatically.
- Reduce update rates to seconds.
- Very well-suited for remote sensing and control.
- Maximize available bandwidth.



MQTT broker

- The broker is software that is primarily responsible for **receiving** all messages, **filtering** the messages, **decide** who is interested in them and then **publishing** the message to all subscribed clients.
- There are several brokers you can use. you can use a cloud MQTT broker.
- It is a software that could be installed on computers, servers or others

MQTT broker benefits

- Eliminate insecure Connections
- Easily scales (from few devices to thousands)
- Manages the clients easily
- It is like a post-office, instead of sending messages peer to peer, all messages are sent/received by the broker.



MQTT broker benefits

- publish/subscribe models



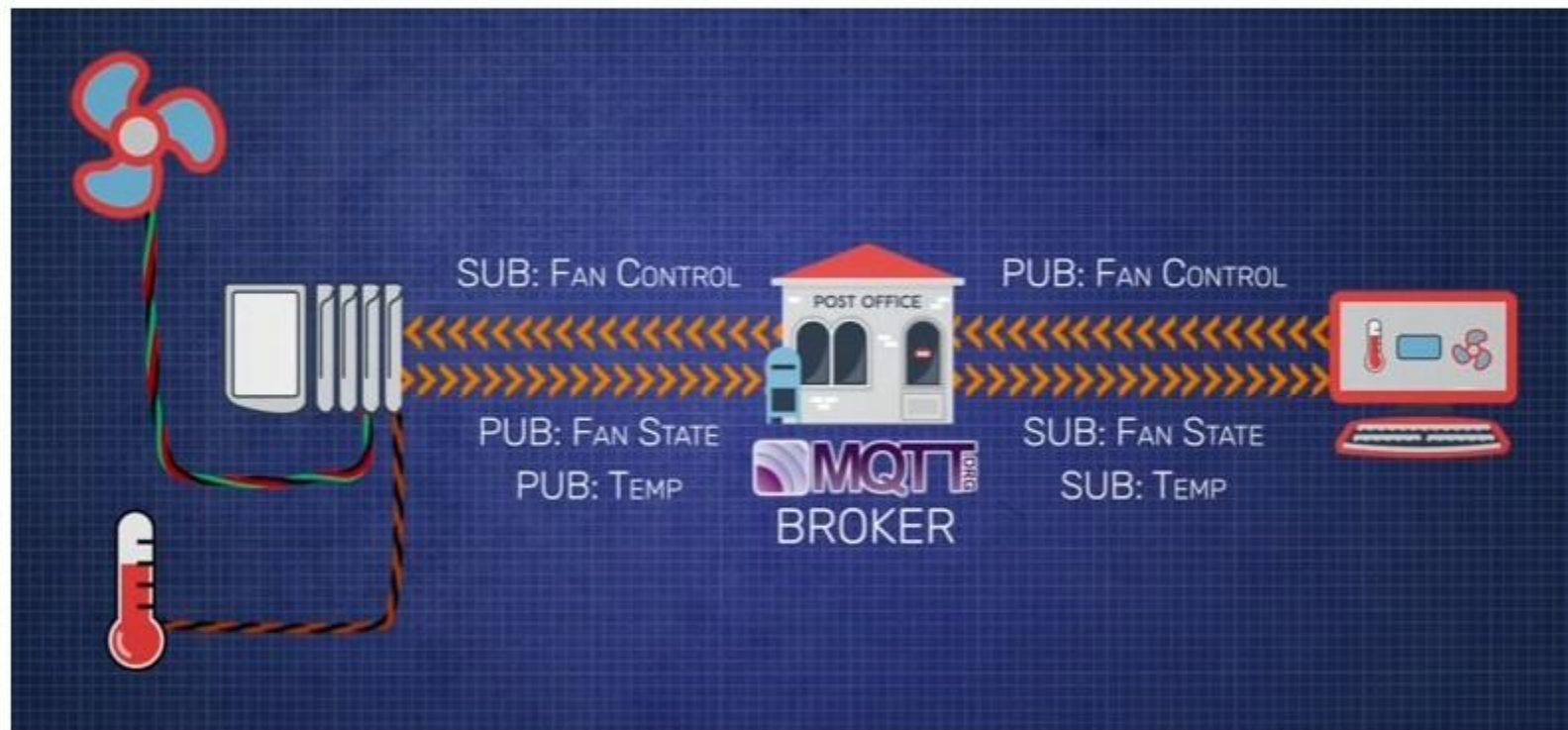
One to many model : when several clients subscribe to the same topic. Of course the publisher publishes the message one time.



Many to one model : when several clients publish over the same topic, but only one subscriber.

MQTT broker benefits

- MQTT is a bidirectional messaging protocol, due to the broker role.



MQTT broker benefits

- All devices in MQTT architecture are less coupled and more secured. The broker is the central location for security.
- TLS Encryption
- Username/ password
- Each client is unaware of other clients
- Automatic redundant Backup broker
- All MQTT implementations have their clients published data only when there is change in value.

MQTT broker benefits

- New subscribers got the last data published. So the broker retains the last value published about a topic.
- The broker keeps track of all sessions. So if a device loses the connection temporarily, it can easily reconnect with the broker without having to resubscribe to topics. The broker remembers its clients and when they left off.

MQTT broker benefits

- The broker handles 3 types of messages :
 - Birth
 - Death
 - Last Will and Testament (when something is wrong with a connection)
- These messages are sent to the broker.

MQTT

