

Chapter 6: Protocols

1- Non-IP Based WPAN

Sensors and other internet-connected devices require methods for transmitting and receiving information, focusing on personal area networks (PANs). PANs facilitate communication between nearby devices and can be either wired (e.g., USB) or wireless (e.g., WPANs like ZigBee and Bluetooth), typically covering a range of a few meters.

2- Bluetooth 5.0

- Bluetooth 5.0 is transforming the Internet of Things (IoT) by enabling new innovative solutions and advancing design engineering.
- Bluetooth 5.0 provides up to four times the range, double the speed, and eight times the message capacity. It also improves compatibility with other wireless technologies and emphasizes the significant benefit of Bluetooth Low Energy (BLE).
- BLE is ideal for applications that require low power consumption, such as battery-powered devices and sensors with infrequent data transfers, ensuring up to 4-5 years of battery life for IoT devices.

3- Bluetooth 5.0 - Increased Speed

- Bluetooth 5 boosts data transfer bandwidth from 1 Mbps to 2 Mbps without raising power consumption, effectively doubling the data transfer rate and reducing transmission and reception time.
- This upgrade enables engineers to create solutions that improve data delivery speed, crucial for applications like medical devices and security systems. For instance, Bluetooth 5 allows faster software updates for medical wearables at 2 Mbps over short distances without compromising battery life for users.

4- Bluetooth 5.0 - Increased Range

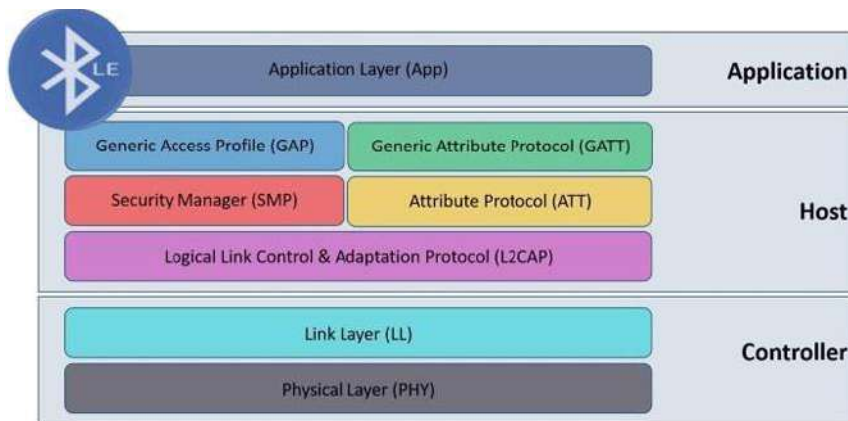
Bluetooth 5 increases range from 50 to 200 meters, enabling robust connections for full-home and outdoor use while maintaining low power consumption. However, it cannot simultaneously maximize range and speed within the low power framework, requiring a choice between these benefits. This flexibility allows for customized Bluetooth optimization.

5- Bluetooth 5.0 - 8x Data

- Bluetooth 5 enhances broadcasting by supporting larger data packets, up to 255 octets.
- It optimizes the use of advertising channels for better efficiency.

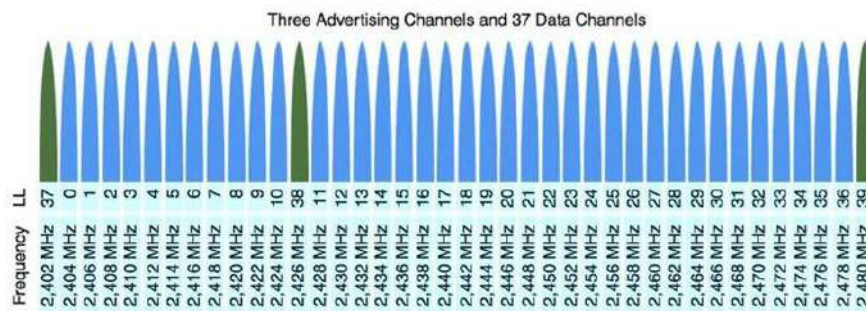
6- Protocol Stack

- The physical layer manages analog communications, including the modulation and demodulation of signals and converting them to digital symbols.
- BLE operates on the 2.4 GHz ISM band, which is a free, unlicensed band. It includes 40 channels: 3 for advertising and 37 for data, each with a 2 MHz width.



7- Advertising Channels:

In the advertising state, a device broadcasts data packets at fixed intervals called the Advertising Interval. Bluetooth Low Energy (BLE) uses 40 RF channels, each 2 MHz apart. Three channels are designated as Primary Advertising Channels, while the other 37 are used for data packet transfer during active connections.



8- Link Layer (LL)

- The link layer interfaces with the physical layer (PHY) and typically involves a combination of hardware and software.
- Its hardware component automates functions to reduce CPU load, such as CRC generation and link state management, determining if a device acts as a master, slave, advertiser, or scanner.

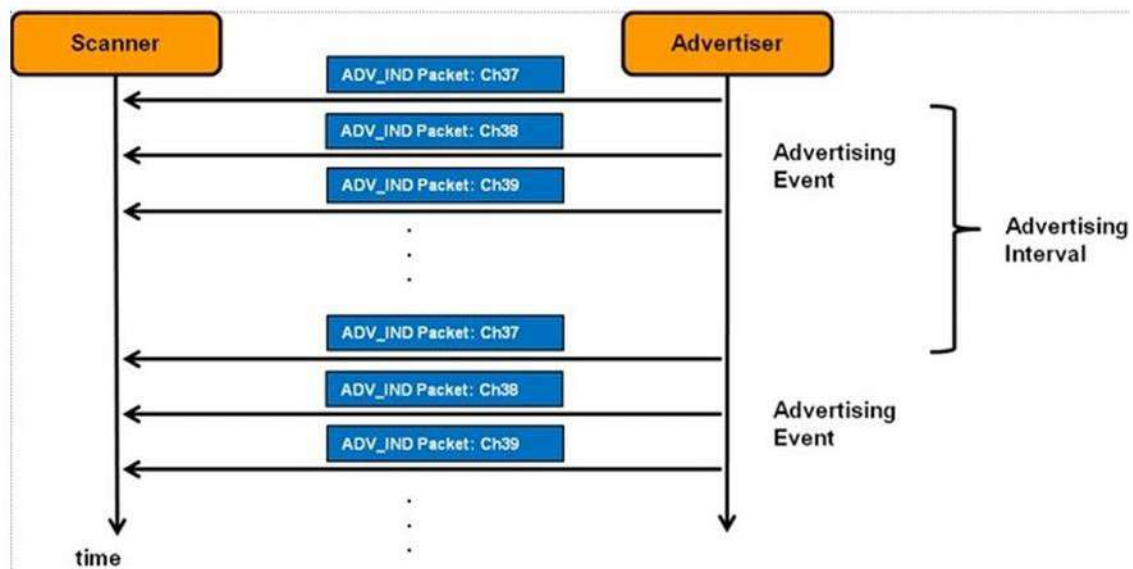
9- BLE operations

- Advertising: Devices broadcast advertising packets on specific channels.
- Scanning: Devices listen for advertising packets; scanning can be:
 - Active: Devices request additional information by listening for PDUs.
 - Passive: Devices only listen without sending requests.
- Initiating: Devices send connection requests to establish links.
- Connected: A state where a master and slave device maintain a relationship.
- Standby: Devices are not connected and not performing any operations.

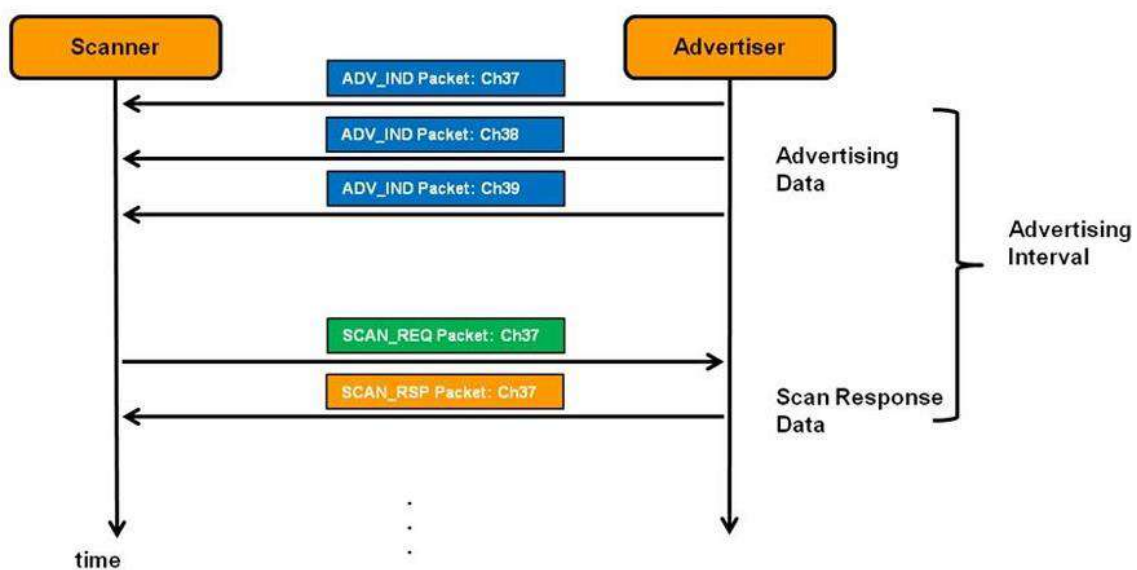
10- Bluetooth Low Energy Discovery Process

- **Discovery Process:** Bluetooth Low Energy (BLE) devices discover each other using advertising channels, with one device sending out advertising packets and the other scanning for them.
- **Advertising Events:** Each time a device advertises, it sends the same packet on all three advertising channels. This sequence is known as an advertising event, typically using ADV_IND packets for general advertising.

Advertising:



Scanning



11- Advertising and Scanning

- Advertising and scanning occur at regular intervals, but they are not synchronized. Therefore, these activities must overlap for device discovery to happen.

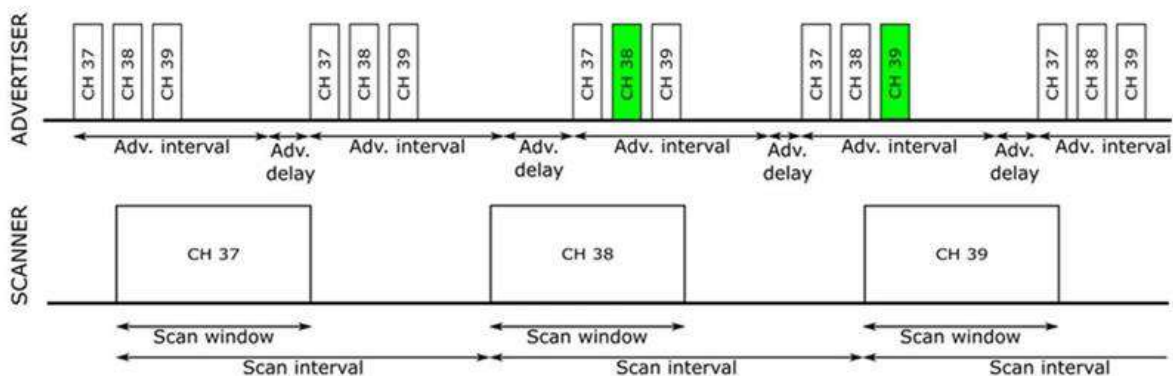
- Advertiser Settings:

- Advertising Interval: 20 milliseconds (ms)
- Advertising Delay: Random

- Scanner Settings:

- Scan Interval: 50 milliseconds (ms)
- Scan Window: 25 milliseconds (ms)

- The black dotted rectangles represent times when advertising and scanning overlap, which is necessary for successful device discovery.



- In Bluetooth Low Energy (BLE) connectionless mode, advertisements are received by a scanner when it happens to be scanning the same channel that the advertiser is using for transmission. The green color indicates when advertisements are successfully received by coincidence.

12- Bluetooth 5.0

- Bluetooth Low Energy (BLE) devices operate in three main states: Advertising, Scanning, and Connected.

- To connect, one device must advertise while another scans for it. Advertising sends out packets that scanning devices can detect. If the scanning device finds the advertisement suitable, it can initiate a connection.

13- Wireless Coexistence

Bluetooth 5 enhances coexistence and interoperability, specifically with other nearby BLE devices, not Wi-Fi. It uses a random frequency-hopping scheme to minimize interference, improving connection robustness. This allows users to effectively control multiple Bluetooth-equipped devices like smartphones and headphones.

14- Bluetooth Hopping *fig 14*

Bluetooth uses frequency-hopping spread spectrum technology to minimize interference by rapidly switching carrier channels 1,600 times per second over a set pattern of channels. The main advantage of frequency hopping is the significant reduction in the likelihood of interference.

15- Zigbee

fig 15

- Zigbee is a wireless technology standard for short-range communications, particularly for control and sensor networks.
- It provides a low-cost, low-power solution for devices needing short-range wireless communication with low data rates.
- Zigbee operates on unlicensed frequency bands including 2.4 GHz, 900 MHz, and 868 MHz.

16- Zigbee Applications

fig 16

- Home Automation: Uses a central controller to manage smart devices through a software app *fig 16.1*
- Medical Data Collection
- Industrial Control Systems
- Purpose: collect information and perform control tasks within a building

17- Zigbee

3 Zigbee Network Components

- **Zigbee Controller (ZC):** A key device that initiates and manages the network, forms it, and handles security and network functions. Each Zigbee network has one ZC, which can also function as a router.
- **Zigbee Router (ZR):** Responsible for routing data between nodes and ensuring network connectivity. Routers maintain network operation and are key for adding new nodes.
- **Zigbee End Device (ZED):** A basic endpoint like a light switch that communicates with the controller but doesn't route data. It's simple and relies on other devices to relay messages.

18- Channel Access

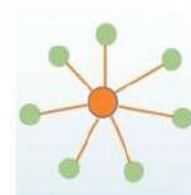
- The network coordinator assigns only one channel for all devices to share for communication.
- Channel Access Methods:
 - **Contention-Free Method:** The coordinator allocates a specific time slot, known as a guaranteed time slot (GTS), for each device to transmit data without contention.
 - **Contention-Based Method:** Devices use CSMA (Carrier Sense Multiple Access) to avoid collisions by:
 - Switching to receive mode.
 - Checking if the channel is clear.
 - Transmitting only if the channel is free, if not they wait for a random time and retry

19- Zigbee Topologies

- Star topology:

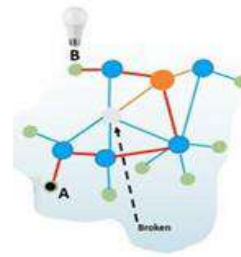
fig 19

- Simplest/Less Expensive
- no routers in this architecture
- End devices cannot communicate directly



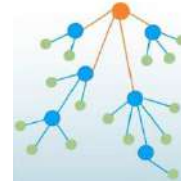
- Mesh topology:

- In a mesh network, each node is connected to its neighboring nodes, except for end devices.
- Messages are relayed from one device to another until they reach their destination.
- If a node fails, data can be rerouted through other available paths, ensuring reliable communication.



- Tree Topology:

- Not very different from mesh configuration
- Routers are not interconnected



20- Zigbee Characteristics

- Zigbee is ideal for low-power, low-data applications like home automation, sensor networks, smoke detectors, and industrial systems.

- Key features:

- Devices don't connect directly to the internet.
- Low energy consumption.
- Effective range: 75-100 meters indoors, 300+ meters line-of-sight outdoors.
- Low data transfer speed of 250 kbit/s.
- Quick network join time (around 30 milliseconds).
- Supports up to 65,000 devices theoretically, 240 practically.
- Cost-effective with low implementation costs.
- Uses AES cryptographic algorithm for security.

- **RF Bands:** There are 3 different bands currently assigned to Zigbee (Europe-US-Across the world)

fig 20

21- Zigbee Benefits

- **Self-Forming:** Zigbee networks can automatically configure themselves.
- **Self-Healing:** The network can dynamically reconfigure when nodes fail, are removed, or become disabled.
- **Interoperability:** Different Zigbee modules from various manufacturers can work together in home automation and industrial devices.

22- Z-wave

- Z-Wave Overview:

Z-Wave and Zigbee are alternatives to WiFi or Bluetooth, both functioning as mesh networks.

Zigbee: An open protocol managed by the Zigbee Alliance.

Z-Wave: A private, closed protocol, ensuring compatibility but limiting flexibility with different manufacturers.

- Advantages and Disadvantages:

Zigbee: Offers flexibility but may have compatibility issues due to manufacturer-specific adaptations.

Z-Wave: Ensures full compatibility among devices but restricts integration with non-Z-Wave products.

- Range and Device Support:

Z-Wave: Has a greater range (up to 100 meters) and provides more stable connections.

Zigbee: Supports a higher number of connected devices (up to 65,000), but this is less relevant for domestic use.

- Z-Wave Requirements:

Similar to Zigbee, Z-Wave needs a hub or bridge to connect and manage IoT devices.

Zigbee's use of the 2.4 GHz frequency allows global compatibility, while Z-Wave's varying frequencies restrict its use in different countries.

- Main Features of Z-Wave:

- Requires a bridge or hub.
- Functions as a mesh network.
- Devices do not connect individually to the internet.
- Low energy consumption.
- Maximum range of 100 meters.
- Low data transfer speed, up to 100 kbit/s.
- Primarily for home use, controlling household items, sensors, security elements, and entertainment devices.
- Closed protocol, ensuring compatibility within its ecosystem.

23- IP-Based Protocol

- 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 gateway

24- 6LoWPAN

fig 24

- Definition:

- 6LoWPAN combines IPv6 with Low-power Wireless Personal Area Networks, enabling small devices to transmit data over the internet.

- Competes with Zigbee, providing similar functions.

- Benefits of IPv6:

- Offers a big number of unique addresses, making it suitable for the growing number of IoT devices.

- **Acronym:** IPv6 over Low-Power Wireless PAN.

- **Functionality:** Transports IPv6 packets over small link layer frames, such as those defined by IEEE 802.15.4.

- Advantages of IPv6:

- Suitable for high device density.

- Eliminates the need for intermediate gateways.

- Mesh Networks:

- 6LoWPAN networks operate as mesh networks at the periphery of larger networks.

- Supports flexible topologies, allowing for both ad-hoc and connected networks.

- Networks can operate independently or connect to the internet via edge routers.

- Edge Router:

- Connects 6LoWPAN devices to the internet and handles data relay.

- Compresses IPv6 headers to fit the small frame sizes of sensor networks.

- Initiates and manages the 6LoWPAN network.

- Facilitates data exchange within the 6LoWPAN network.

25- Thread

- **Thread Protocol Overview:** Thread is a new IoT networking protocol based on IPv6 (6LoWPAN), aimed at home connectivity and automation. It was launched in 2014 by the Thread Group Alliance, including major companies like Alphabet, Qualcomm, and Samsung.

- Key Features and Advantages:

IEEE 802.15.4 Foundation: Similar to Zigbee and other variants, but Thread supports IP addressing, allowing for better integration and reduced power consumption.

Mesh Network: Can support up to 250 devices per mesh, making it ideal for large home systems.

Efficiency: The protocol does not require state maintenance at the network layer, reducing processing needs for edge routers.

Security: Fully compliant with IPv6 and uses AES encryption, ensuring secure communication.

Compatibility: Existing IEEE 802.15.4 devices can be upgraded to support Thread.

26- IEEE 802.11 *fig 26*

- IEEE 802.11, commonly known as WiFi, defines the architecture and specifications for wireless local area networks (WLANs).
- WiFi uses high-frequency radio waves for device connectivity within a LAN, allowing users to move freely within the coverage area.
- **Infrastructure:** A station (STA), like a smartphone, communicates with a central access point (AP). APs can act as gateways, routers, or access points in larger networks, forming an Infrastructure Basic Set Service (BSS) with a star topology.
- **Ad hoc:** Nodes form an Independent Basic Service Set (IBSS) where each station communicates with others directly. This peer-to-peer topology doesn't require an access point.
- **Distribution System (DS):** Combines multiple BSS networks through interconnecting access points, allowing seamless data distribution across a wider area.

27- 5G *fig 27*

- **5G Definition:**
 - The 5th generation of mobile networks, evolving from 4G LTE, designed to support the massive growth in data and connectivity for IoT and other innovations.
 - Initial 5G services began in 2019, with widespread availability expected by 2025.
- **Benefits:**

Provides faster connections, greater capacity, and significantly lower latency, reducing response times to as low as 1 millisecond, compared to 30 milliseconds for 4G.
- **Continuous Connection:**
 - Works alongside 4G using a mix of macro cells, small cells, and in-building systems to ensure reliable and localized coverage.
 - Small cells provide coverage over shorter distances, essential for 5G networks due to the short range of mmWave frequencies.
- **Increased Spectrum:**

Utilizes frequency bands below 6 GHz and introduces higher frequencies like the 26-28 GHz bands (mmWave), offering more capacity, faster speeds, and support for a greater number of users and devices.
- **Massive MIMO:**
 - Uses multiple input, multiple output (MIMO) antennas with numerous elements to enhance data transmission and user capacity.
 - Allows simultaneous connections and high throughput with smaller antenna sizes, supporting over 100 elements in the same physical space.
- **Beam Steering:**

Technology that directs radio signals from MIMO antennas towards specific users and devices, optimizing the signal path and reducing interference, thereby increasing efficiency and network performance.

28- MQTT Protocol *fig 28*

- Message Queuing Telemetry Transport (MQTT) is a lightweight, publish-subscribe network protocol that facilitates message exchange between devices.
- Designed for low-bandwidth, constrained devices, making it ideal for IoT applications.
- Allows for command transmission, data reading, and publishing from sensor nodes.

29- MQTT Advantages *fig 29*

- Efficiently distributes information.
- Enhances scalability.
- Significantly reduces network bandwidth usage.
- Lowers update rates to mere seconds.
- Ideal for remote sensing and control.
- Maximizes the use of available bandwidth.
- Has very low overhead, making it lightweight and efficient.

30- MQTT Broker

- The broker is a software that handles receiving, filtering, and deciding the distribution of messages to subscribed clients.
- Multiple types of brokers are available, including cloud-based options.
- The broker can be installed on various devices such as computers or servers.

31- MQTT Broker Benefits *fig 31*

- Eliminates insecure connections.
- Easily scales from a few devices to thousands.
- Manages clients efficiently.
- Acts like a post office, centralizing message reception and distribution.
- Supports both one-to-many and many-to-one publish/subscribe models.
- Ensures bidirectional messaging due to the broker's role.
- Centralizes security with TLS encryption and username/password authentication.
- Clients are unaware of each other, enhancing security.
- Supports automatic redundant backup brokers.
- Clients publish data only when there is a change in value.
- New subscribers receive the latest published data.
- Tracks all sessions, allowing for easy reconnection without re-subscribing.
- Handles three types of messages: Birth, Death, and Last Will and Testament, ensuring robust connection management.

Fig 14

Interference of WLAN on Bluetooth Packets
Using Basic Frequency Hopping

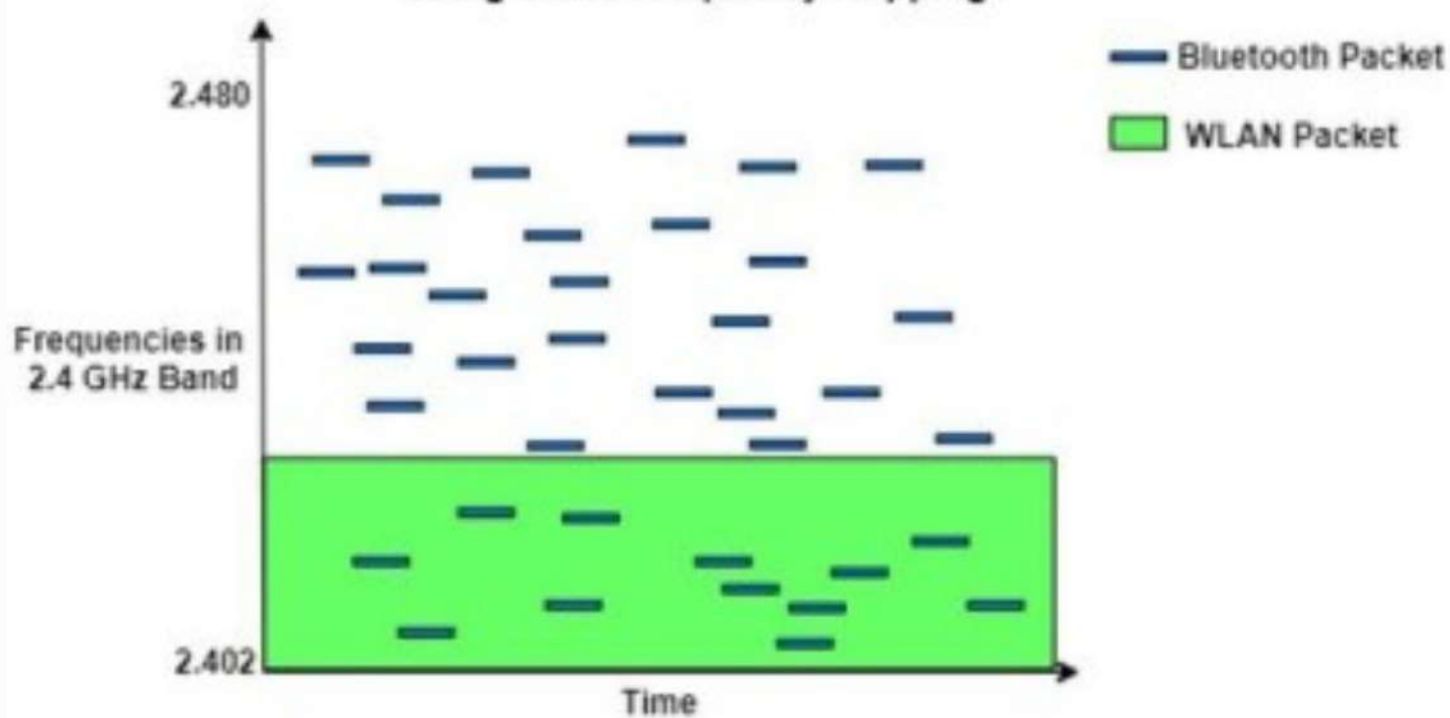
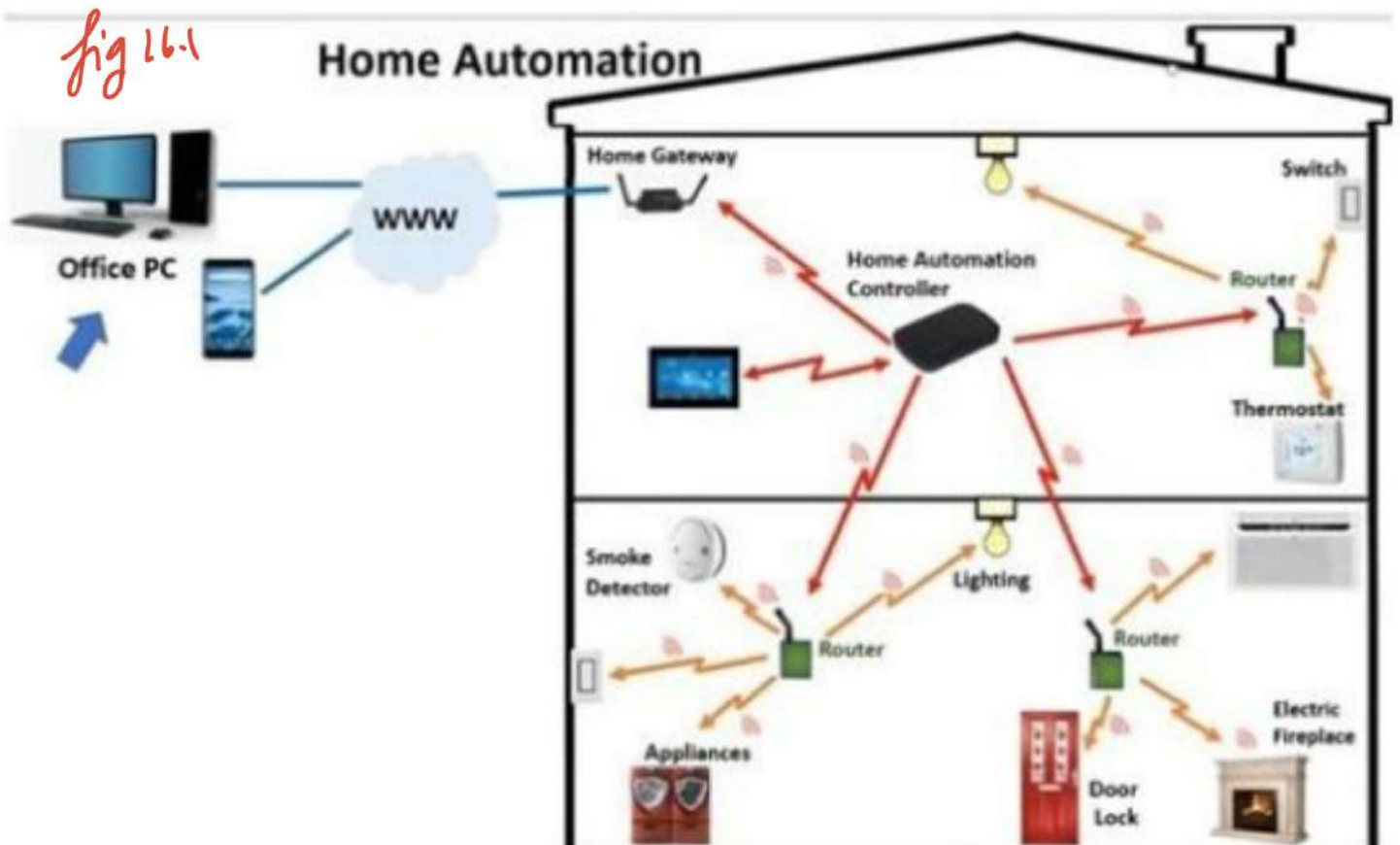


fig 15-



fig 16.1



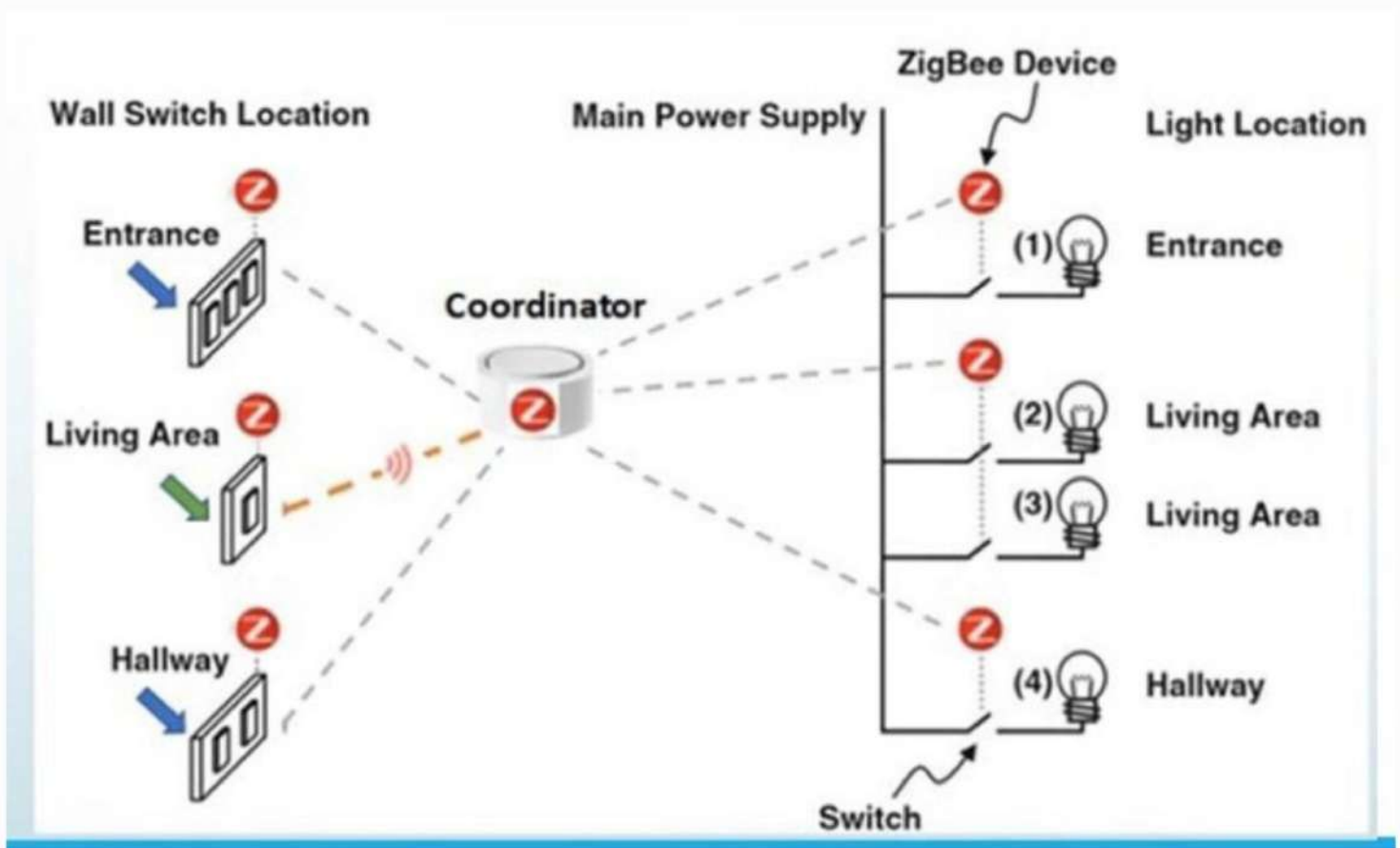
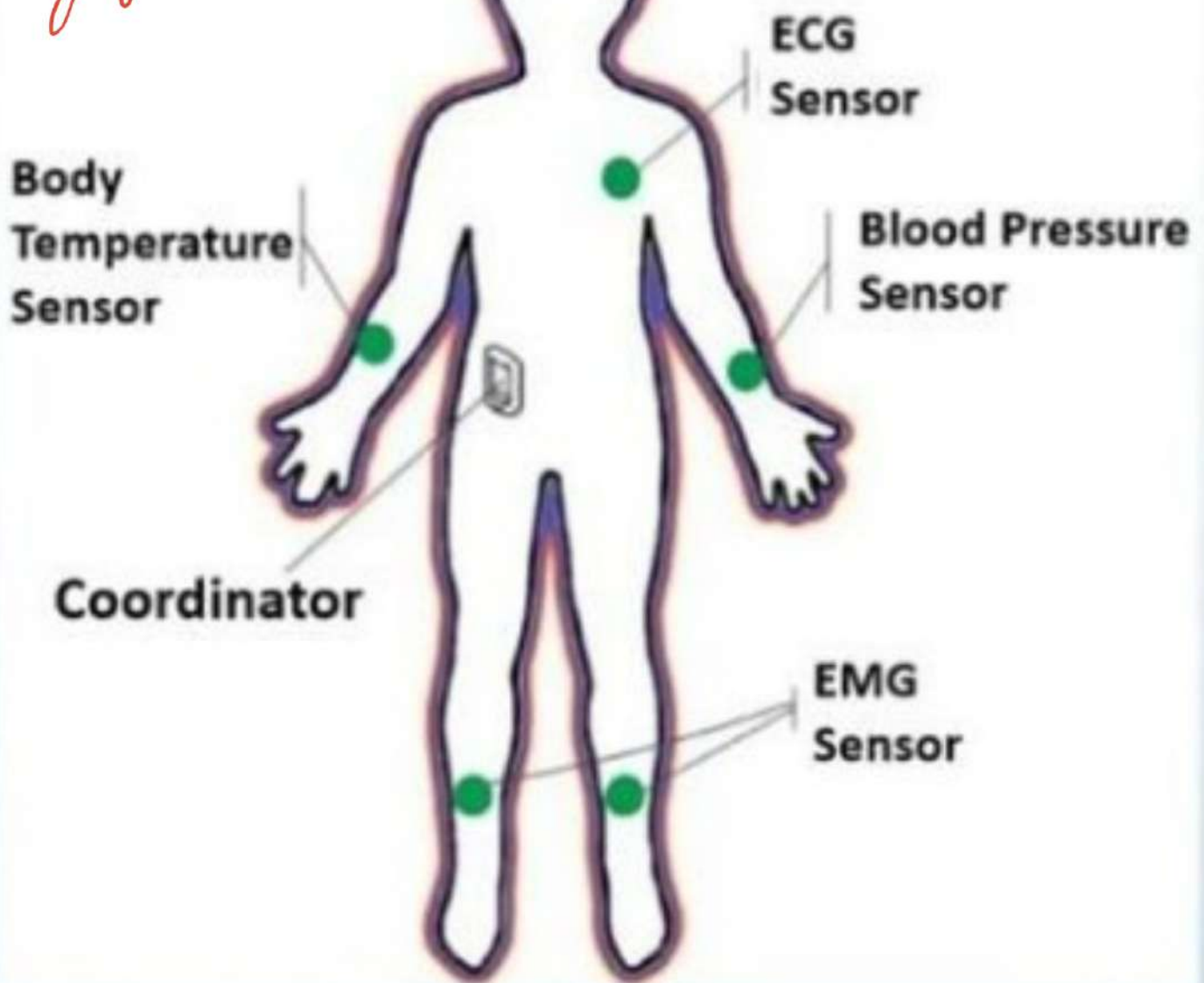
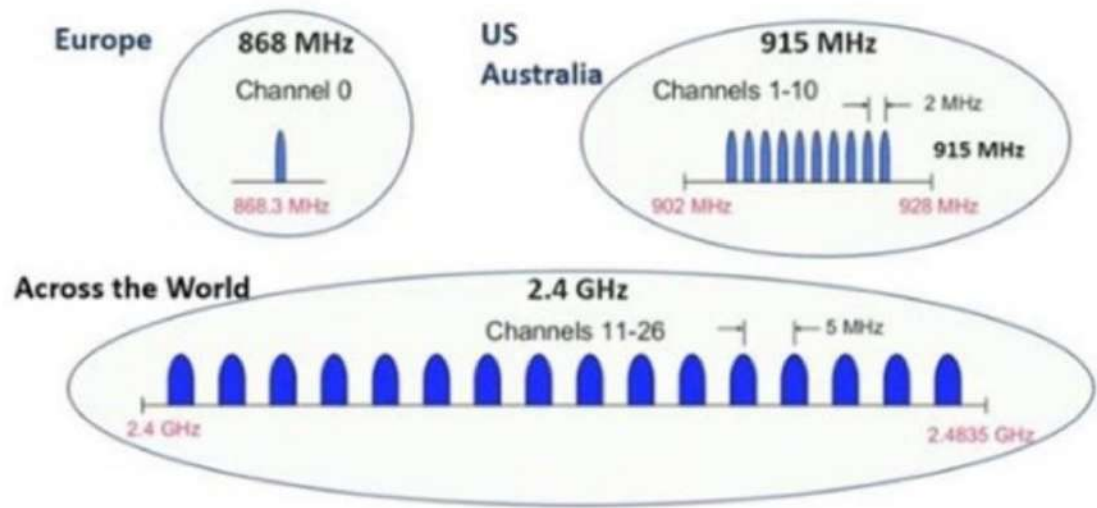


Fig 19



Health monitoring system

fig 20



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

fig 24

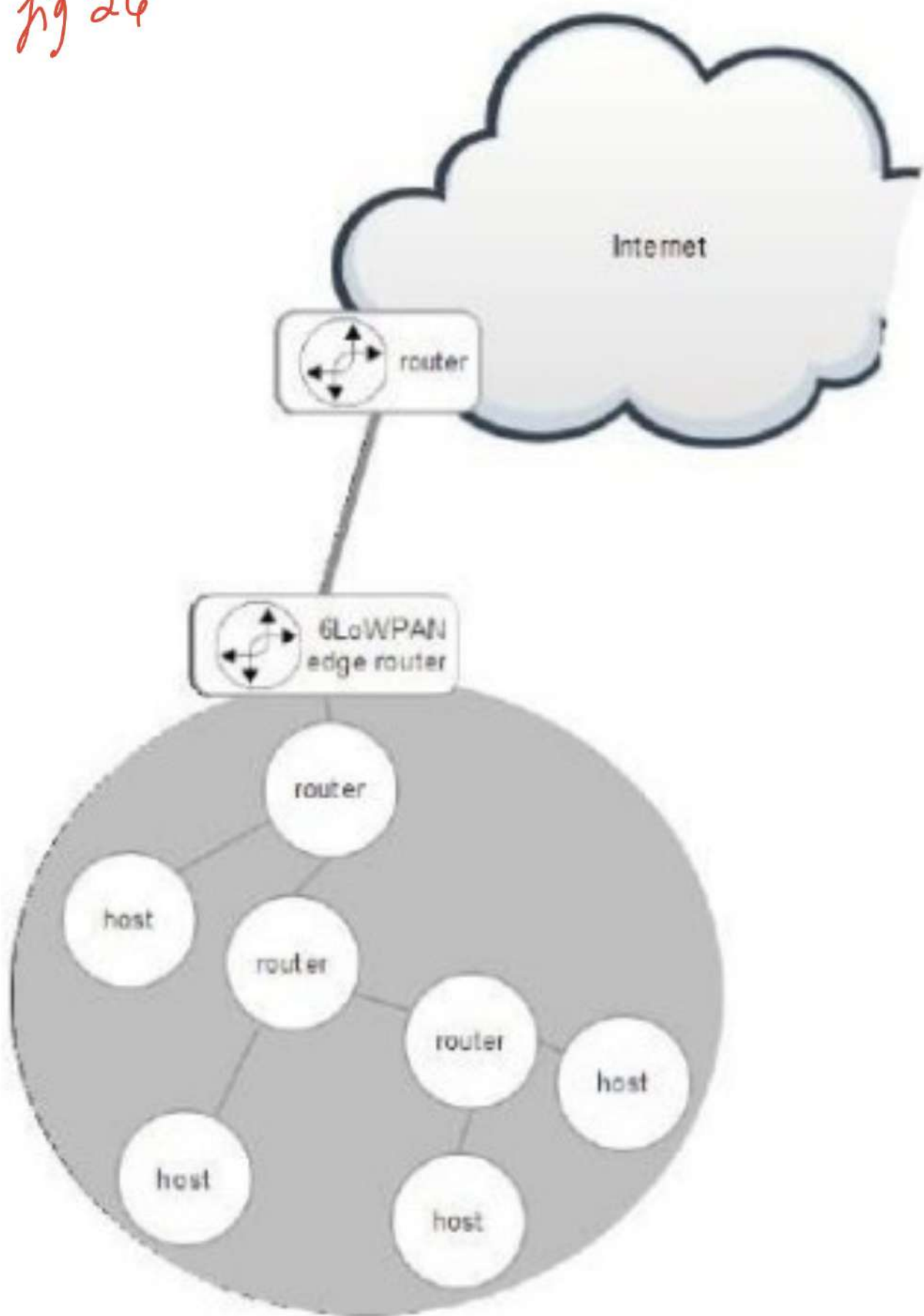
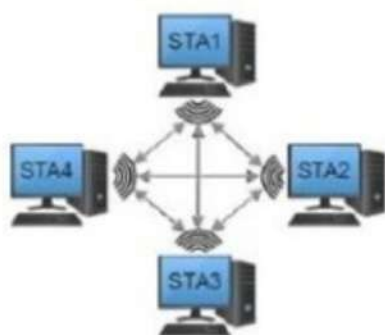


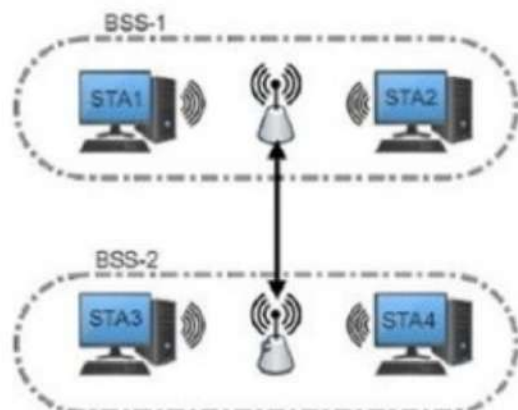
fig 26



Basic Service Set

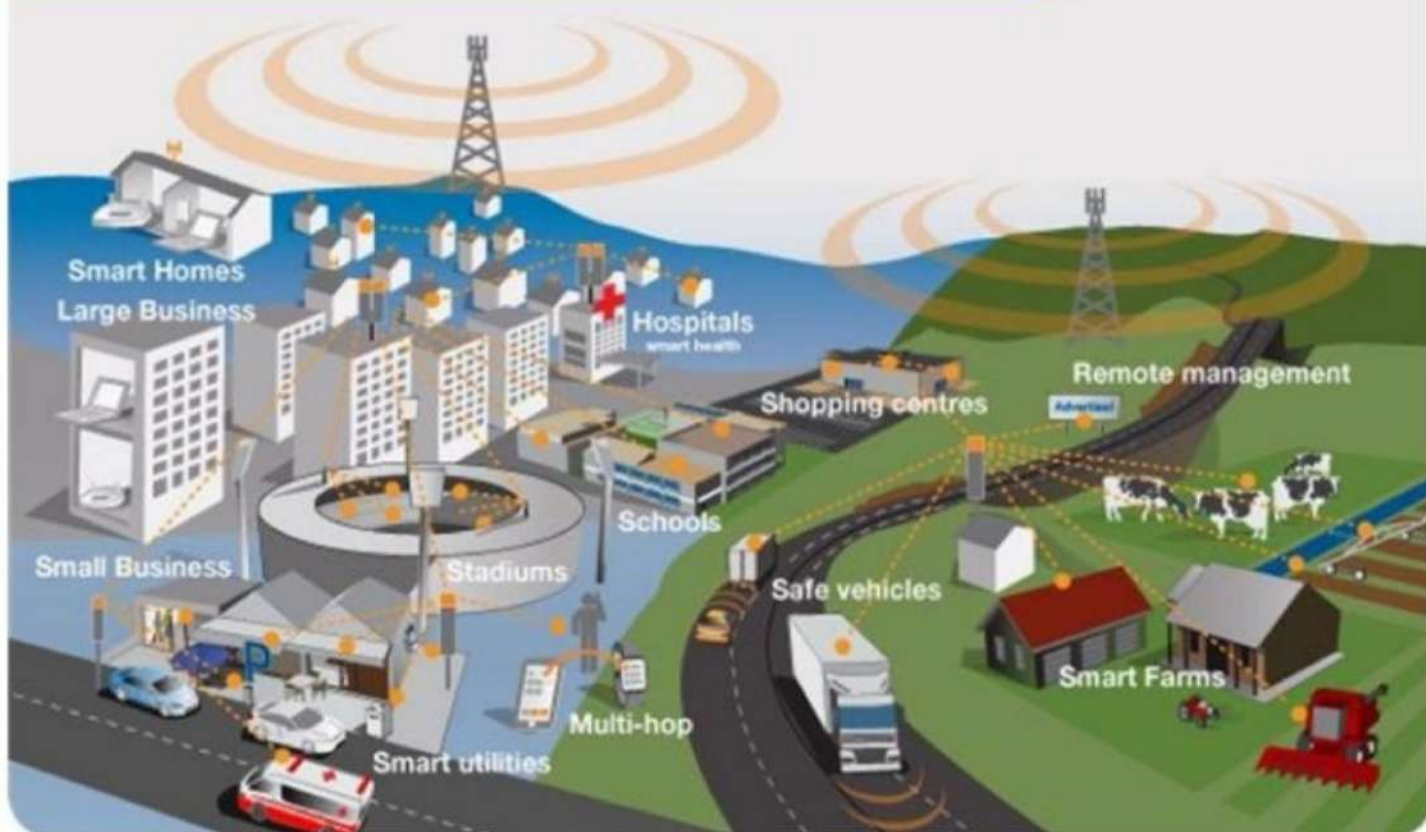


Independent Basic Service Set



Distribution System

THE CONNECTED COMMUNITY



Macrocells for wide area coverage



In-building and street small cells

Home small cells

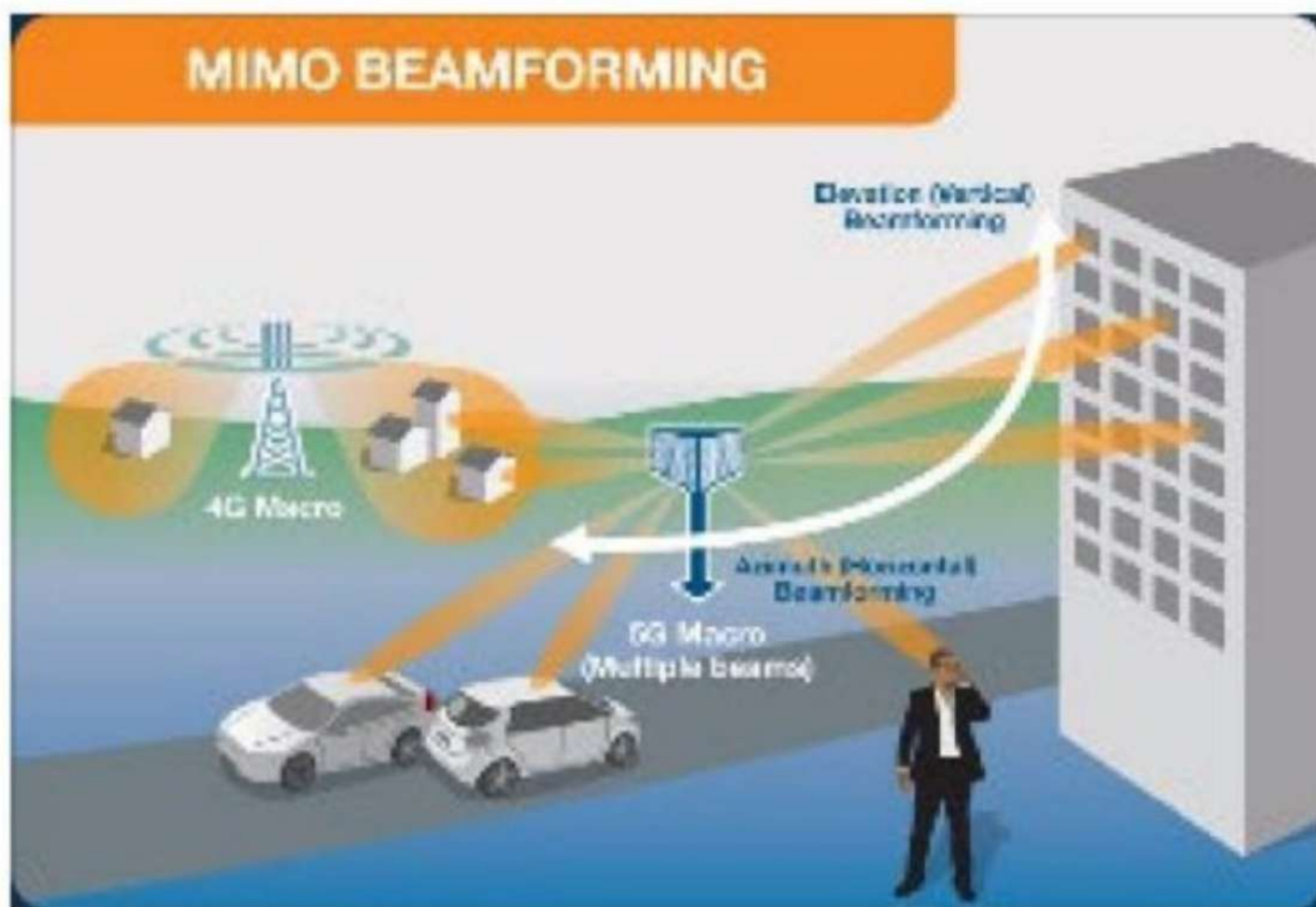


fig 2st

Publish



Subscribe



fig 29

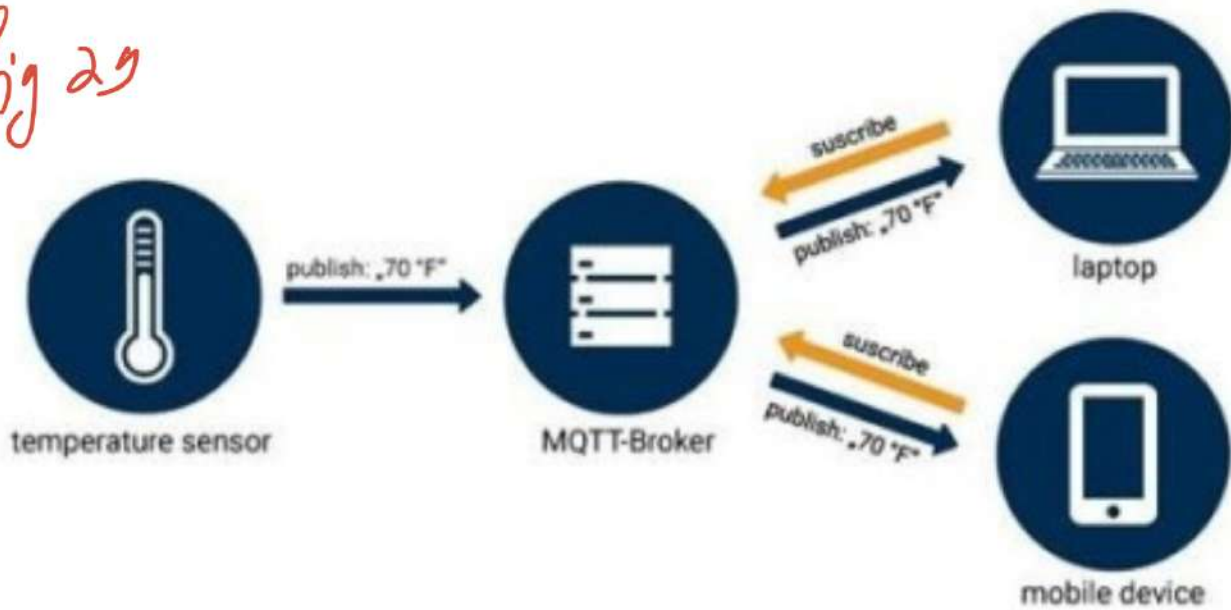


fig 31



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.

