Sunbeam Institute of Information Technology
Pune and Karad

Module – Internet of Things (IoT)

Trainer - Devendra Dhande

Email – devendra.dhande@sunbeaminfo.com

(wired / wireless)
Networks

PAN
(zigbee, bluetooth)

IoT Networks
(NB-IOT /
LoRAWAN /
6LOWPAN)

Security (Encryption/Decryption)

IoT

Cellular
Network
(1G/2G . . .)

Embedded (Microcontrollers)

Web Technologies
(Python, MERN, Enterprise Java, .NET)

Mobile Technologies
(Hybrid / Android / iOS)

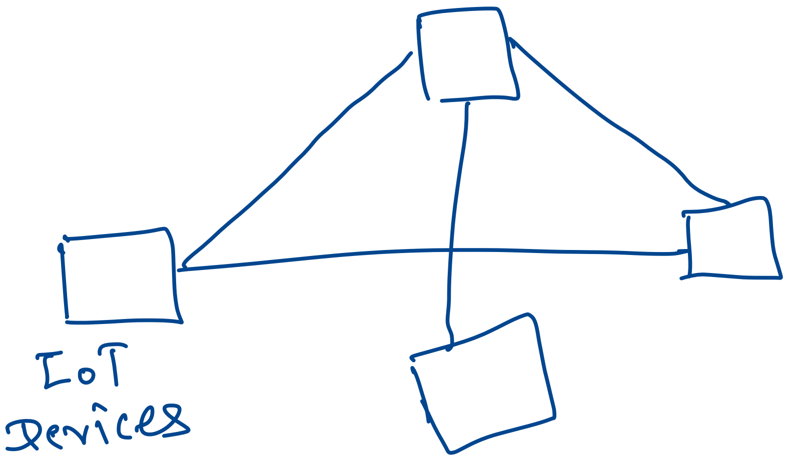
AI
(ML, NN, DL)

Databases (MySQL, MongoDB ...)
BigData (Hadoop . . .)

Internet of Things (IoT)

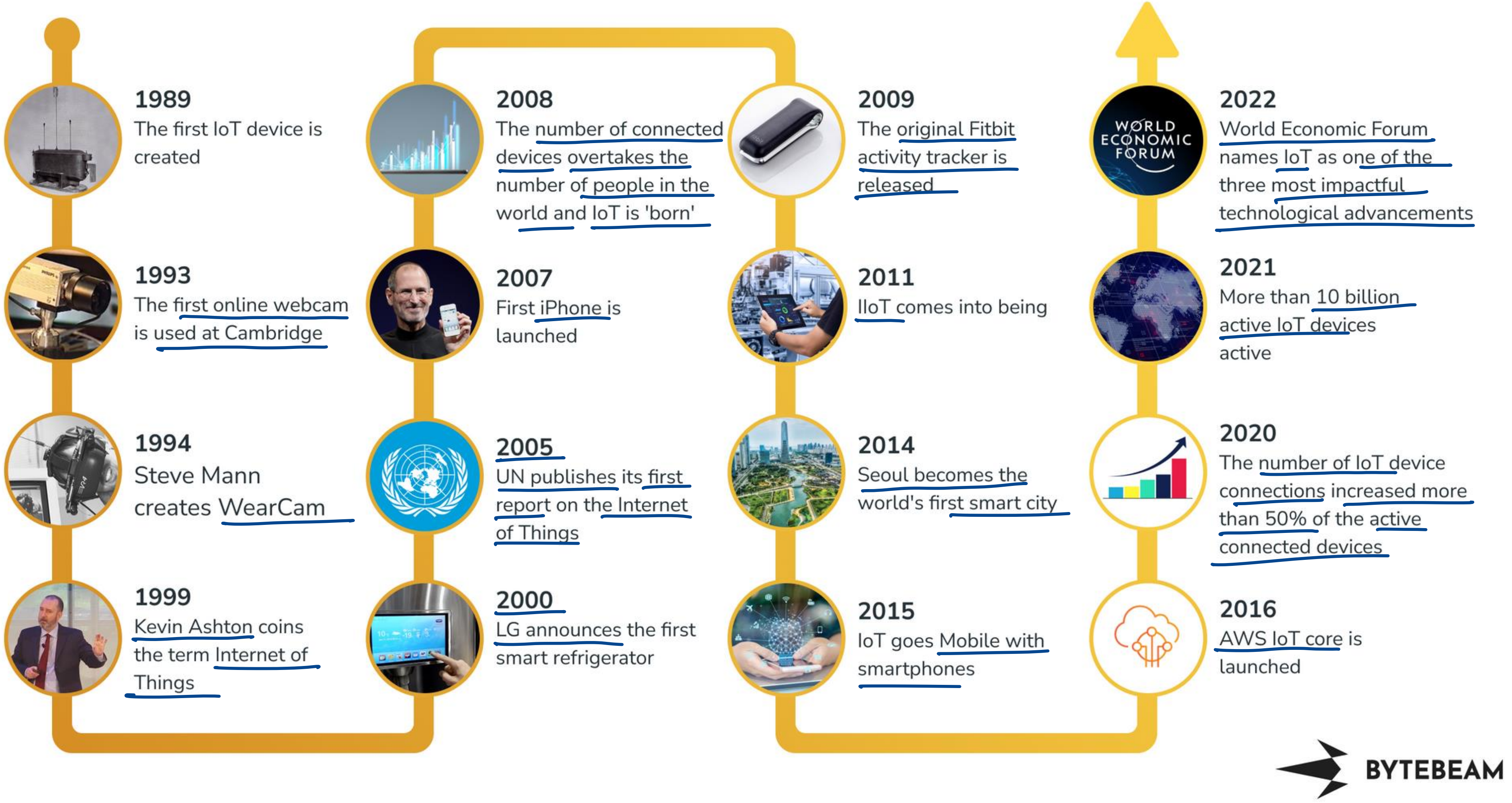
- **Internet of things** (**IoT**) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communication networks.

- **Internet of Things (IoT)** refers to a network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data.



Internet of Things (IoT) – Evolution and Growth

- Kevin Ashton, the co-founder of the Auto-ID Labs at MIT, coined the term ‘Internet of Things’ in 1999.



Benefits of Internet of Things (IoT)

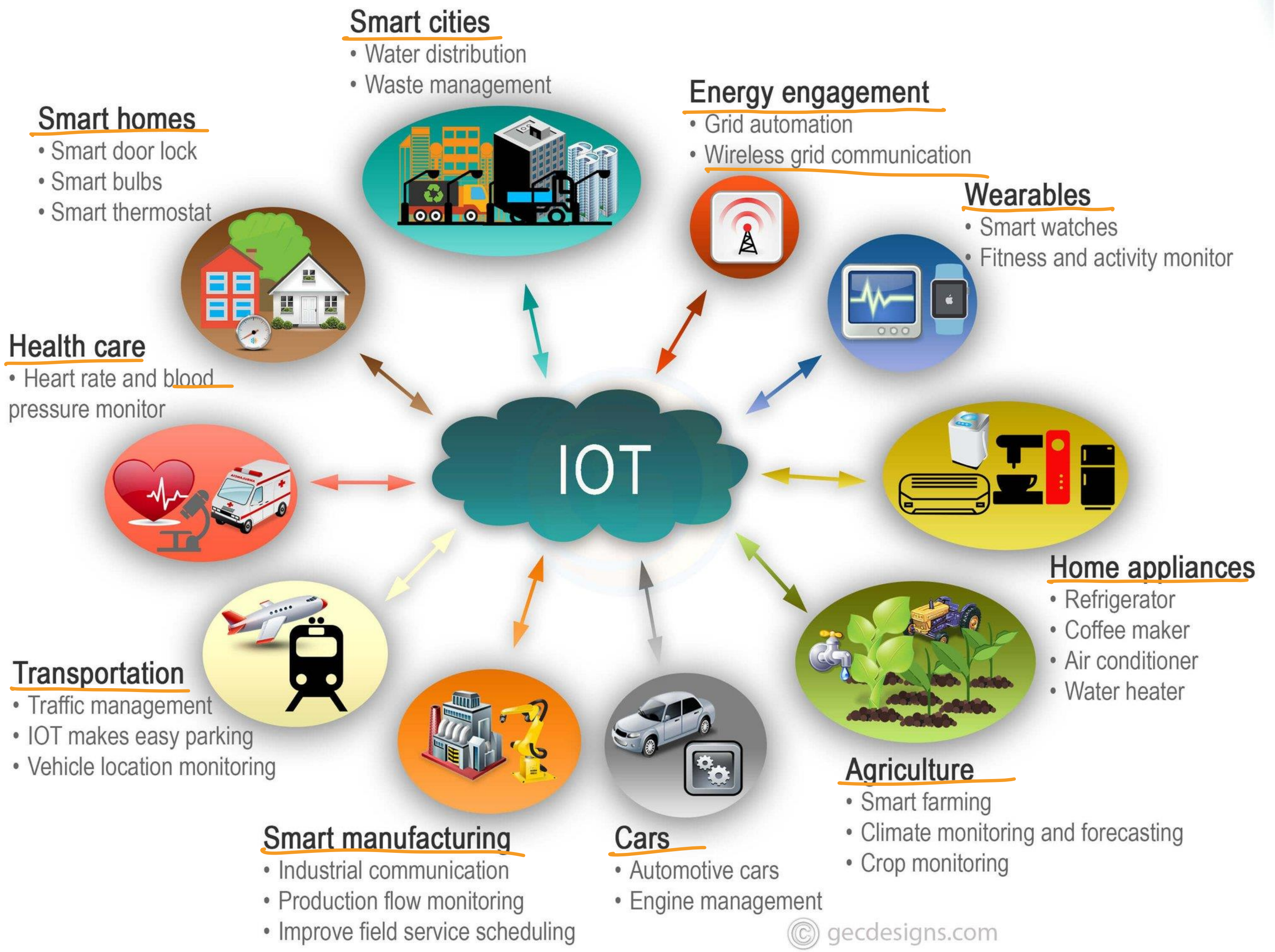
- **Improved efficiency**
  - IoT devices to automate and optimize processes, businesses can improve efficiency and productivity.
- **Data-driven decision-making**
  - IoT devices generate vast data that can be used to make better business decisions and new business models.
  - By analyzing this data, businesses can gain insights into customer behavior, market trends, and operational performance which helps to take decisions about strategy, product development, and resource allocation.
- **Cost-savings**
  - By reducing manual processes and automating repetitive tasks, IoT can help businesses reduce costs and improve profitability.
- **Enhanced customer experience**
  - By using IoT technology to gather data about customer behavior, businesses can create more personalized and engaging experiences for their customers.

Challenges in Internet of Things (IoT)

- **Security and privacy risks**
  - Many IoT devices are vulnerable to hackers and other cyber threats, which can compromise the security and privacy of sensitive data.
  - IoT devices can also collect vast amounts of personal data, raising concerns about privacy and data protection.
- **Interoperability issues**
  - IoT devices from different manufacturers often use different standards and protocols, making it difficult for them to perform “machine to machine” communication.
- **Data overload**
  - IoT devices generate vast data, which can overwhelm businesses that are not prepared to handle it.
  - Analyzing this data and extracting meaningful insights can be a significant challenge
- **Cost and complexity**
  - Implementing an IoT system can be costly and complex, requiring significant investments in hardware, software, and infrastructure.
  - Managing and maintaining an IoT system can also be challenging, requiring specialized skills and expertise.
- **Regulatory and legal challenges**
  - Businesses need to comply with various data protection, privacy and cybersecurity regulations, which can vary from country to country.

Internet of Things (IoT) Applications

- Healthcare
- Manufacturing
- Retail
- Agriculture
- Transportation
- Consumers
- Home automation
- Industrial
- Infrastructure
- Energy management
- Environmental monitoring



Internet of Things (IoT) Future / Trends

- **Growth**
  - number of IoT devices is expected to grow rapidly, with estimation of tens of billion IoT devices in use over the next few years
- **Edge computing**
  - important for IoT, as it allows data to be processed and analyzed closer to the source of the data, rather than in a centralized data center.
  - This can improve response times, reduce latency and reduce the amount of data that needs to be transferred over IoT networks.
- **Artificial intelligence and machine learning**
  - used to analyze vast amounts of data that is generated by IoT devices and extract meaningful insights.
  - This can help businesses make more informed decisions and optimize their operations.
- **Blockchain**
  - explored as a way to improve security and privacy in the IoT.
  - Blockchain can be used to create secure, decentralized networks for IoT devices, which can minimize data security vulnerabilities.
- **Sustainability**
  - IoT can be used to optimize energy usage, reduce waste and improve sustainability across a range of industries.

Internet of Things (IoT) Technologies

Several technologies come together to make IoT possible.

- **Sensors and actuators**
  - Sensors are devices that can detect changes in the environment, such as temperature, humidity, light, motion, or pressure.
  - Actuators are devices that can cause physical changes in the environment, such as opening or closing a valve or turning on a motor.
  - Automation is possible when sensors and actuators work to resolve issues without human intervention.

- **Connectivity technologies**
  - To transmit IoT data from sensors and actuators to the cloud, IoT devices need to be connected to the internet.
  - There are several connectivity technologies that are used in IoT, including wifi, Bluetooth, cellular, Zigbee, and LoRaWAN.

- **Cloud computing**
  - platforms provide the infrastructure and tools that are needed to store and analyze this data, as well as to build and deploy IoT applications.

Internet of Things (IoT) Technologies

Several technologies come together to make IoT possible.

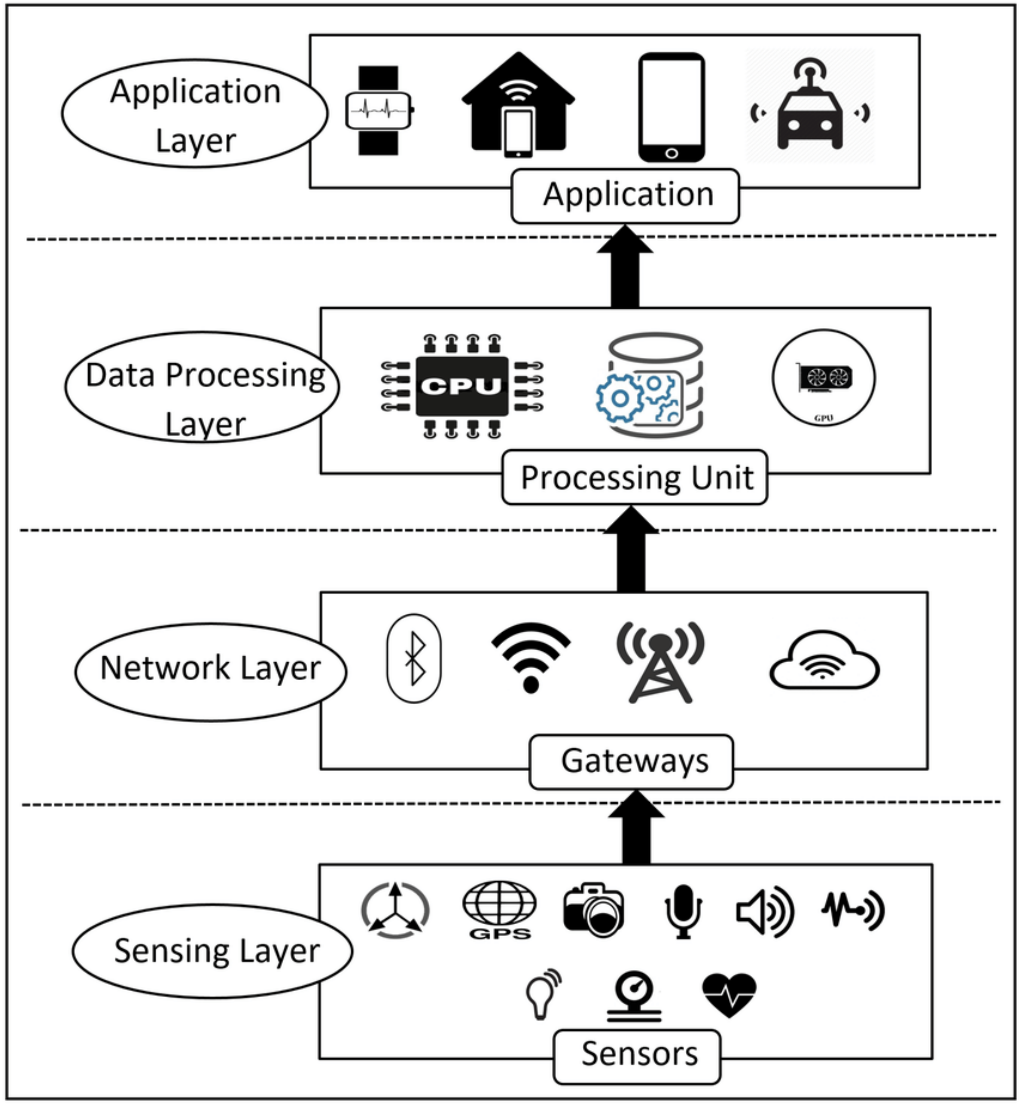
- **Big data analytics**
  - data generated by IoT devices need to use advanced analytics tools to extract insights and identify patterns.
  - These tools can include machine learning algorithms, data visualization tools and predictive analytics models.

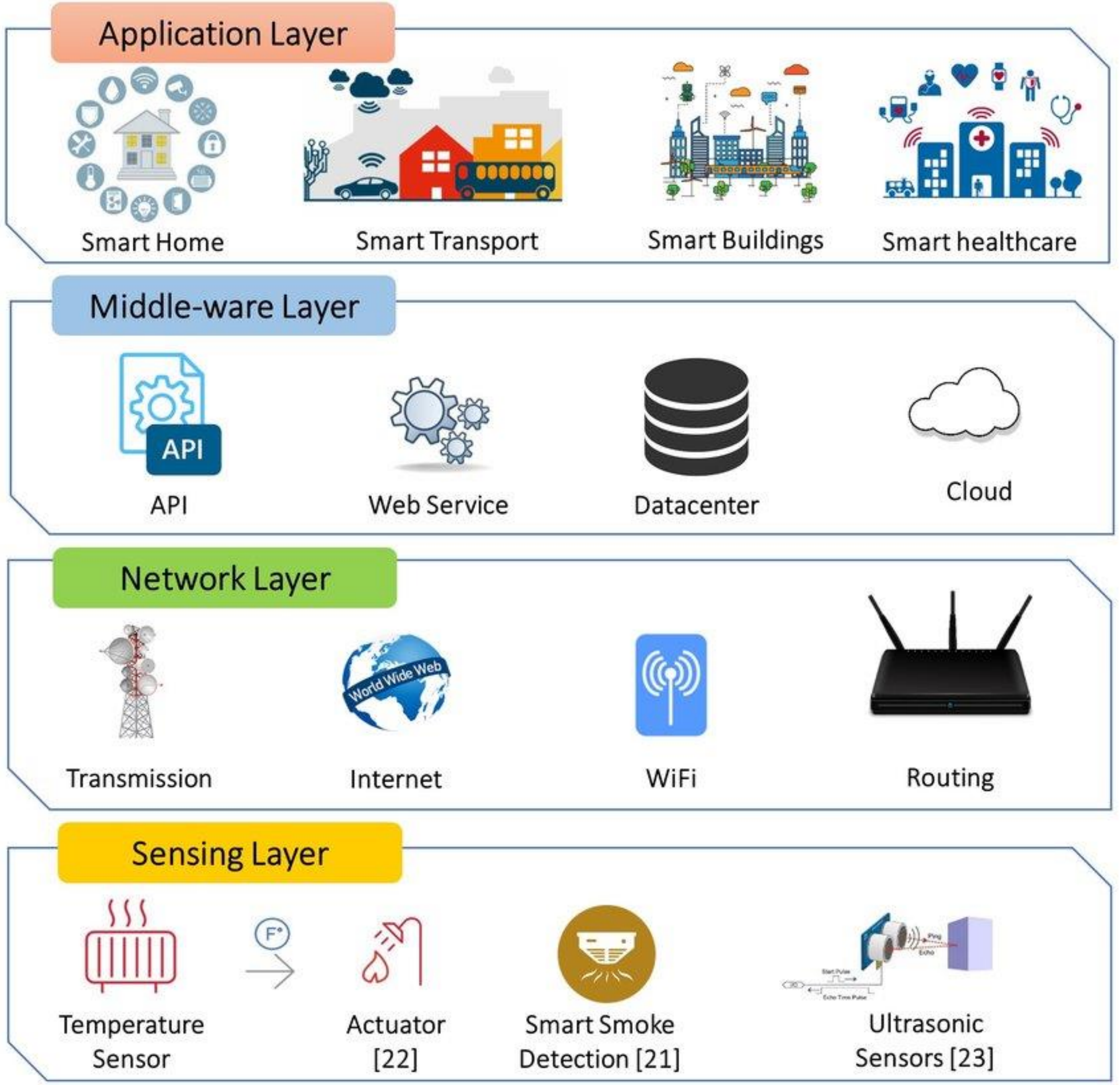
- **Security and privacy technologies**
  - Technologies such as encryption, access controls and intrusion detection systems are used to protect IoT devices

Internet of Things (IoT) Architecture

- **Perception/Sensing Layer**
  - Perception refers to the physical layer, which includes sensors and actuators that are capable of collecting, accepting, and processing data over the network.
  - Sensors and actuators can be connected either wirelessly or via wired connections.
- **Network Layer**
  - This layer contains Data Acquiring Systems (DAS) and Internet/Network gateways.
  - It is necessary to transmit and process the data collected by the sensor devices.
  - This layer allows these devices to connect and communicate with other servers, smart devices, and network devices.
- **Processing Layer**
  - The processing layer is the brain of the IoT ecosystem.
  - Data is analyzed, pre-processed, and stored here before being sent to the data center
  - Data is accessed by software applications that both monitor and manage the data as well as prepare further actions.
- **Application Layer**
  - User interaction takes place at the application layer, which delivers application-specific services to the user.

Internet of Things (IoT) Architecture





Networks

- Wired
  - Twisted pair cable
  - Coaxial cable
  - Fiber optic cable
- Wireless
  - WiFi
  - PAN
    - zigbee
    - bluetooth
  - Cellular Networks
  - LPWAN
    - Licensed
      NB-IoT
    - UnLicensed
      LoRaWAN

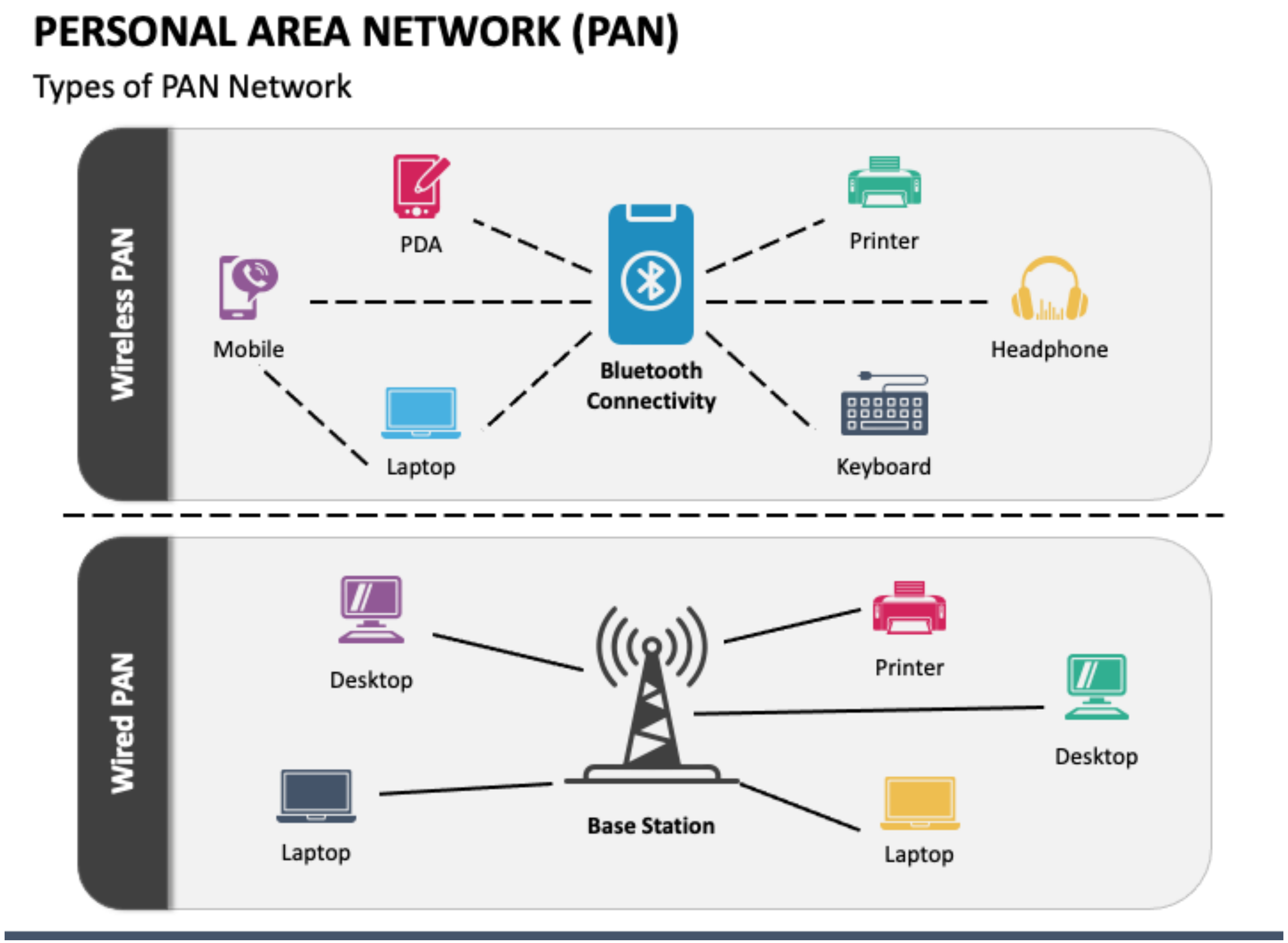
Radio wave

micro wave

infrared rays

Personal Area Network (PAN)

- A **personal area network** (**PAN**) is a computer network for interconnecting electronic devices within an individual person's workspace.
- A PAN provides data transmission among devices such as computers, smartphones, tablets and personal digital assistants.
- PANs can be used for communication among the personal devices themselves, or for connecting to a higher level network and the Internet where one master device takes up the role as gateway.



Personal Area Network (PAN)

- A PAN may be carried over wired interfaces such as USB, but is predominantly carried wirelessly, also called a **wireless personal area network** (**WPAN**).
- A PAN is wirelessly carried over a low-powered, short-distance wireless network technology such as IrDA, Wireless USB, Bluetooth or Zigbee.
- A wireless personal area network (WPAN) is a personal area network in which the connections are wireless.
- IEEE 802.15 has produced standards for several types of PANs operating in the ISM band

- IEEE (Institute of Electrical and Electronics Engineers)
- specifies wireless personal area network (WPAN) standards.
  - IEEE 802.15.1: WPAN / Bluetooth
  - IEEE 802.15.2: Coexistence
  - IEEE 802.15.3: High Rate WPAN
  - IEEE 802.15.4: Low Rate WPAN
  - IEEE 802.15.5: Mesh Networking
  - IEEE 802.15.6: Body Area Networks
  - IEEE 802.15.7: Visible Light Communication
  - IEEE P802.15.8: Peer Aware Communications
  - IEEE P802.15.9: Key Management Protocol
  - IEEE P802.15.10: Layer 2 Routing
  - IEEE 802.15.13: Multi-Gigabit/s Optical Wireless Communications

IEEE 802.15.4

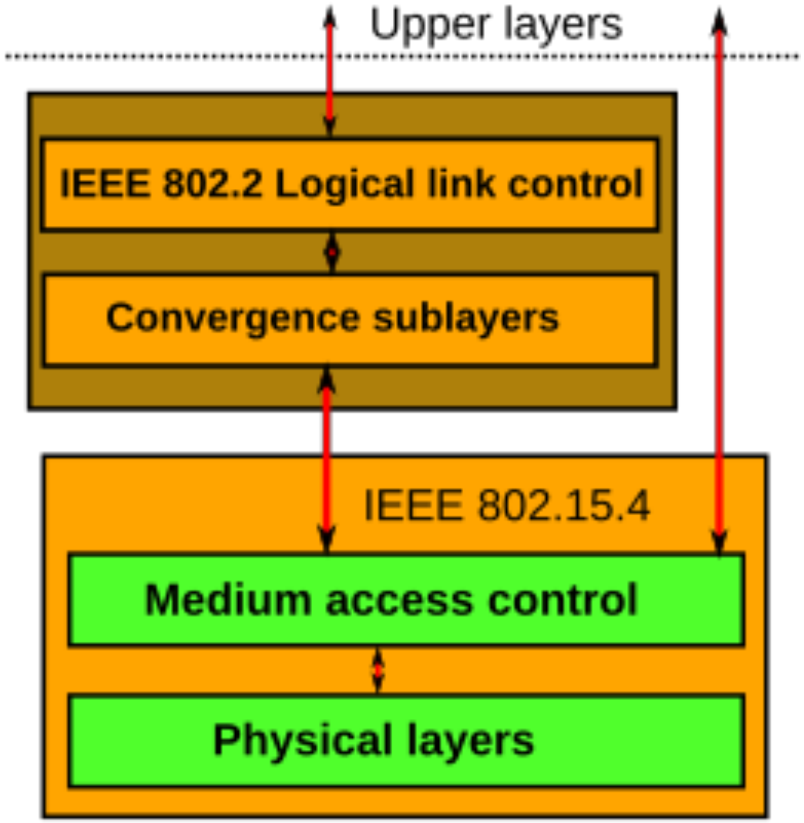
- **IEEE 802.15.4** is a technical standard that defines the operation of a **low-rate wireless personal area network** (**LR-WPAN**).
- It specifies the physical layer and media access control for LR-WPANs , which defined the standard in 2003.

- IEEE standard 802.15.4 focuses on low-cost, low-speed communication between devices and even low power consumption. (contrast with other approaches, such as Wi-Fi, which offers more bandwidth and requires more power.)

- Key 802.15.4 features include:
    - Suitability for real-time applications with reservation of Guaranteed Time Slots (GTS)
    - Collision avoidance through CSMA/CA
    - Integrated support for secure communications
    - Power management functions
    - Support for time- and data-rate–sensitive applications
    - IEEE 802.15.4 devices may use one of three possible frequency bands for operation (868/915/2450 MHz).

IEEE 802.15.4 - Protocol architecture

- only the lower layers are defined in this standard.
- interaction with upper layers is done using an IEEE 802.2 logical link control sublayer accessing the MAC through a convergence sublayer.



IEEE 802.15.4 Protocol stack

IEEE 802.15.4 - Protocol architecture

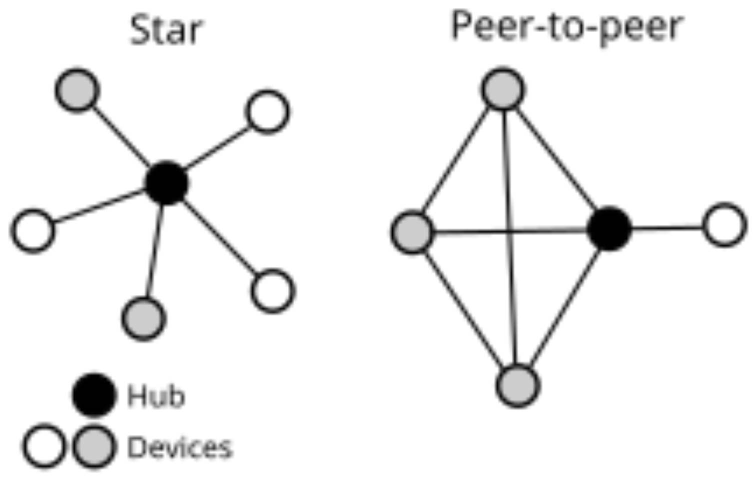
- **Physical Layer**
  - physical layer is the bottom layer in the OSI reference model
  - The *physical layer* (PHY) provides the data transmission service.
  - provides an interface to the *physical layer management entity*, which offers access to every physical layer management function maintains a database of information on related personal area networks.
  - the PHY manages the physical radio transceiver, performs channel selection along with energy and signal management functions.
  - It operates on one of three possible unlicensed frequency bands: (ISM band)
    - 868.0–868.6 MHz: Europe, allows one communication channel (2003, 2006, 2011)
    - 902–928 MHz: North America, originally allowed up to ten channels (2003), but since has been extended to thirty (2006)
    - 2400–2483.5 MHz: worldwide use, up to sixteen channels (2003, 2006)

- **MAC Layer**
  - enables the transmission of MAC frames through the use of the physical channel.
  - it offers a management interface and itself manages access to the physical channel and network beaconing.
  - It also controls frame validation, guarantees time slots and handles node associations.

IEEE 802.15.4 – Network Model

- **Node types**
  - The standard defines two types of network node.
    - **full-function device** (FFD) (mains powered)
      - It can serve as the coordinator of a personal area network
      - It implements a general model of communication which allows it to talk to any other device
    - **reduced-function devices** (RFD) (battery powered)
      - extremely simple devices with very modest resource and communication requirements
      - they can only communicate with FFDs and can never act as coordinators.

- **Topologies**
  - Networks can be built as either peer-to-peer or star networks.
  - However, every network needs at least one FFD to work as the coordinator of the network.
  - Networks are thus formed by groups of devices separated by suitable distances.
  - Each device has a unique 64-bit identifier, (sometimes, short 16-bit identifiers can be used within a restricted environment)



Zigbee

- **Zigbee** is an IEEE 802.15.4-based specification
- designed for small scale projects which needs wireless connection, low-power, low-bandwidth like low-power digital radios, home automation, medical device
- Hence, Zigbee is a low-power, low-data-rate, and close proximity (i.e., personal area)

- intended to be simpler and less expensive than other WPANs like Bluetooth, WiFi
- Zigbee was conceived in 1998, standardized in 2003, and revised in 2006.
- Zigbee is a low-power wireless mesh network standard targeted at battery-powered devices

- Zigbee operates in the industrial, scientific and medical (ISM) radio bands.
    - 2.4 GHz band being primarily used for lighting and home automation devices
- While devices for commercial utility use *sub-GHz* frequencies
    - 902-928 MHz in North America, Australia, and Israel
    - 868-870 MHz in Europe, 779-787 MHz in China

- data rates varying from around 20 kbit/s for sub-GHz bands to around 250 kbit/s for channels on the 2.4 GHz band range

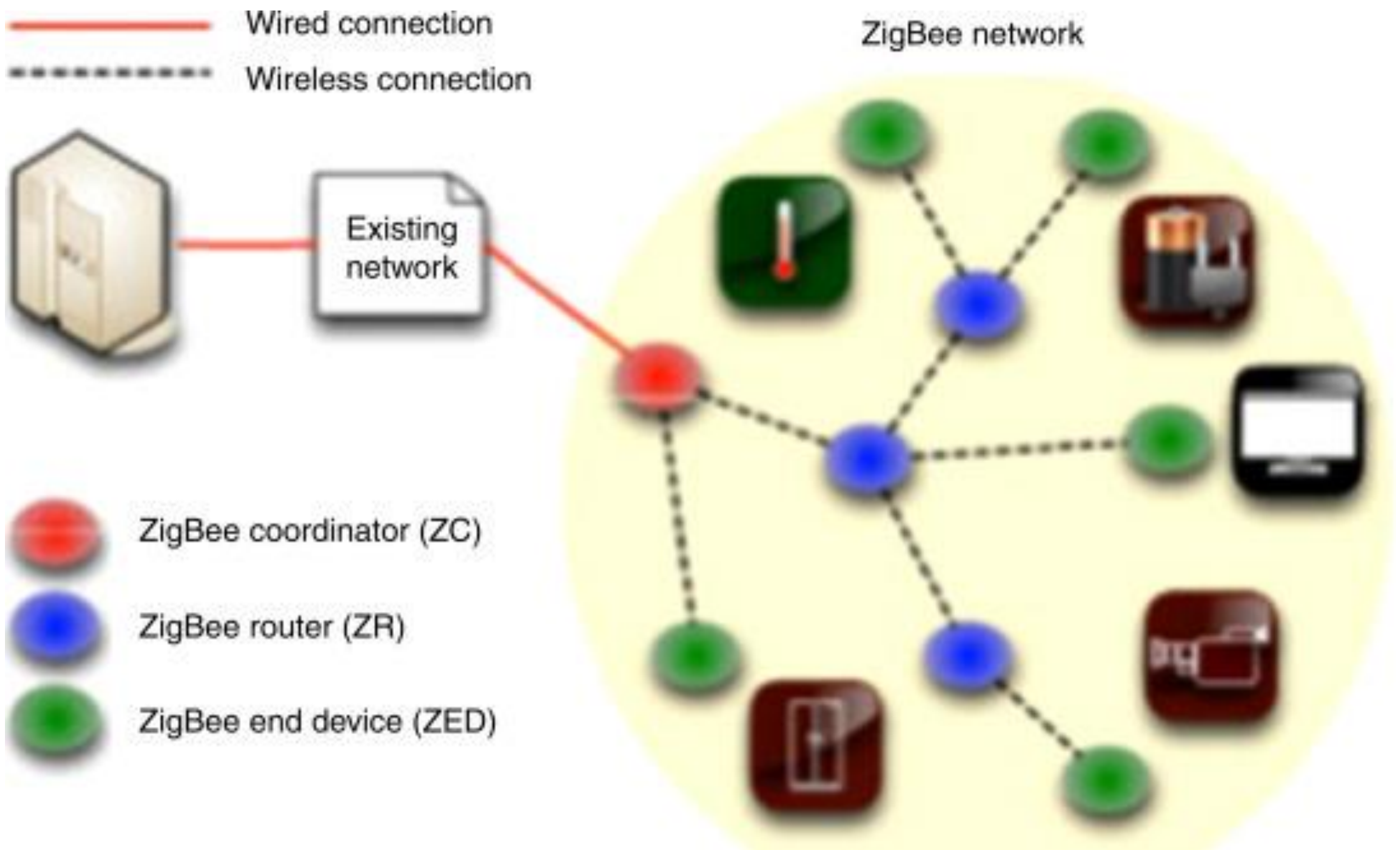
Zigbee – Device Types

- **Zigbee coordinator (ZC)**
  - The most capable device, root of the network tree and may bridge to other networks.
  - There is precisely one Zigbee coordinator in each network
  - It stores information about the network, including acting as the trust center and repository for security keys.

- **Zigbee router (ZR)**
  - router devices can act as intermediate routers, passing data on to other devices.
  - These types of Zigbee products are typically mains-powered so they are always available on the network.
  - Zigbee Router devices are sometimes called Zigbee repeaters or Zigbee range extenders.

- **Zigbee end device (ZED)**
  - Contains just enough functionality to talk to the parent node (either the coordinator or a router)
  - it cannot relay data from other devices.
  - This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life.
  - These types of Zigbee device products are often battery-powered.
  - A ZED requires the least amount of memory and thus can be less expensive to manufacture than a ZR or ZC.

Zigbee – Network



- The Zigbee network layer natively supports
  both star and tree networks, and generic mesh networking.

- Every network must have one coordinator device.
- Within star networks, the coordinator must be the central node.
- Both trees and meshes allow the use of Zigbee routers to extend communication at the network level.

Zigbee – Protocol Architecture

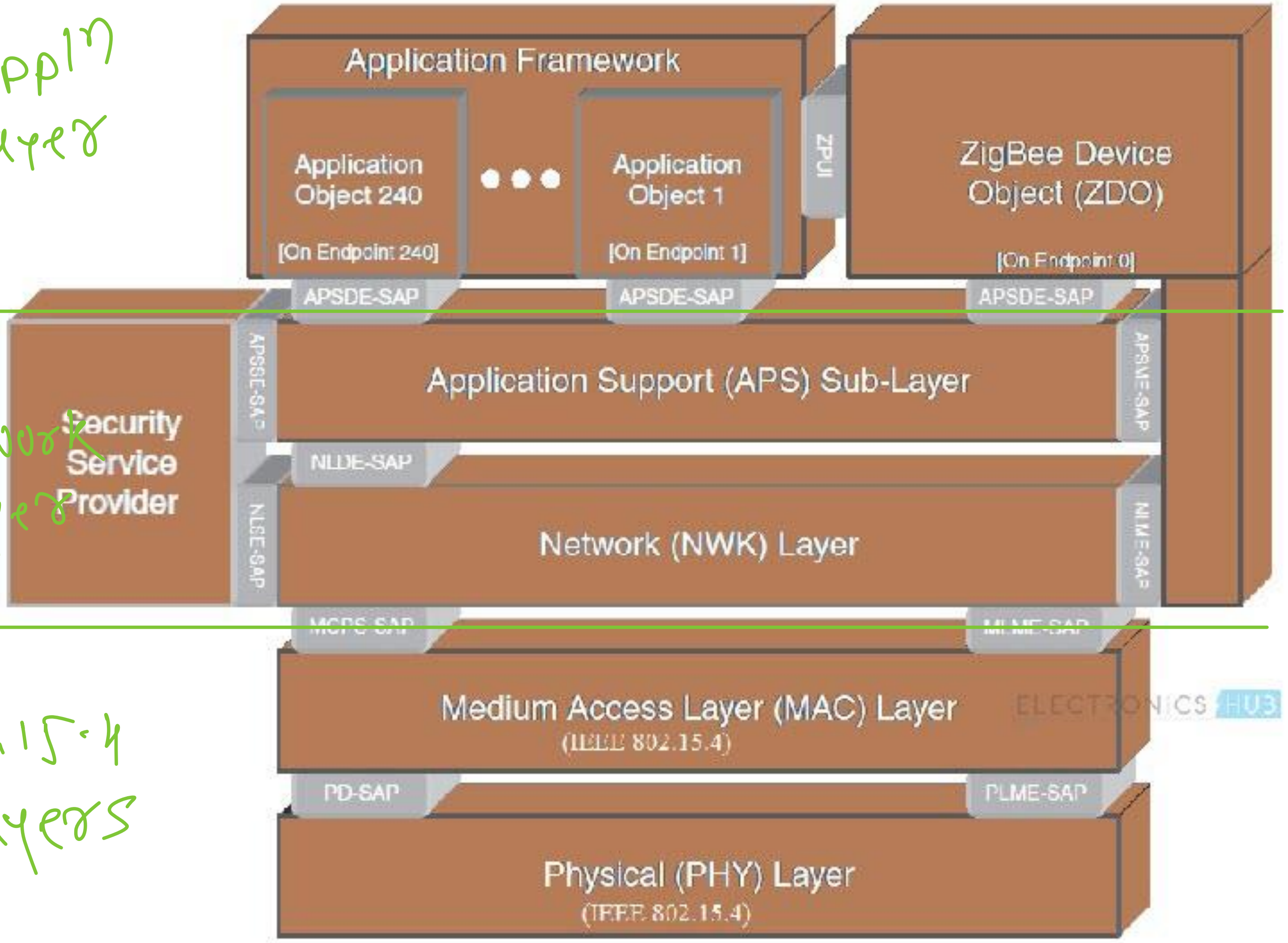
- Zigbee builds on the physical layer and media access control defined in IEEE standard 802.15.4

- The specification includes four additional key components
  - network layer
  - application layer
  - *Zigbee Device Objects* (ZDOs)
  - manufacturer-defined application objects

Appln layer

Network layer

802.15.4 layers



Zigbee – Protocol Architecture

- **Network Layer**
  - network layer ensure correct use of the MAC sublayer and provide a suitable interface for upper layer
  - It deals with network functions such as connecting, disconnecting, and setting up networks.
  - It can establish a network, allocate addresses, and add and remove devices.
  - This layer makes use of star, mesh and tree topologies.

- **Application layer**
  - It is the highest-level layer defined by the specification and is the effective interface of the Zigbee system to its end users.
  - It comprises the majority of components added by the Zigbee specification
    - ZDO (Zigbee device object) and its management procedures
    - application objects defined by the manufacturer
  - This layer binds tables, sends messages between bound devices, manages group addresses, reassembles packets, and transports data.

Zigbee – Protocol Architecture

- ***ZDO*** **(Zigbee device object)**
  - a protocol in the Zigbee protocol stack,
  - is responsible for
    - overall device management, security keys, and policies
    - defining the role of a device as either coordinator or end device
    - discovery of new devices on the network and the identification of their offered services
  - It may then go on to establish secure links with external devices and reply to binding requests accordingly.

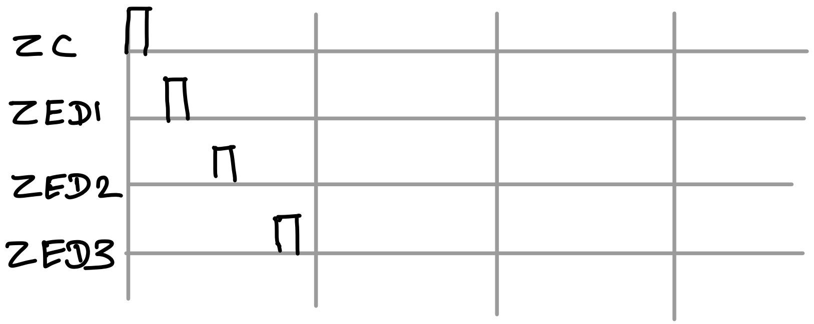
- **Application Support Sublayer (APS)**
  - main standard component of the stack, and it offers a well-defined interface and control services.
  - It works as a bridge between the network layer and the other elements of the application layer
  - it keeps up-to-date binding tables in the form of a database (used to find appropriate devices depending on the services that are needed)
  - As the union between both specified layers, it also routes messages across the layers of the protocol stack.

Zigbee – Applications

- Typical application areas include:
  - Home automation
  - Wireless sensor networks
  - Industrial control systems
  - Embedded sensing
  - Medical data collection
  - Smoke and intruder warning
  - Building automation
  - Remote wireless microphone configuration

① Beacaning

Garanteed time slot



② Nonbeacaning

Non Garanteed time slot

CSMA / CA

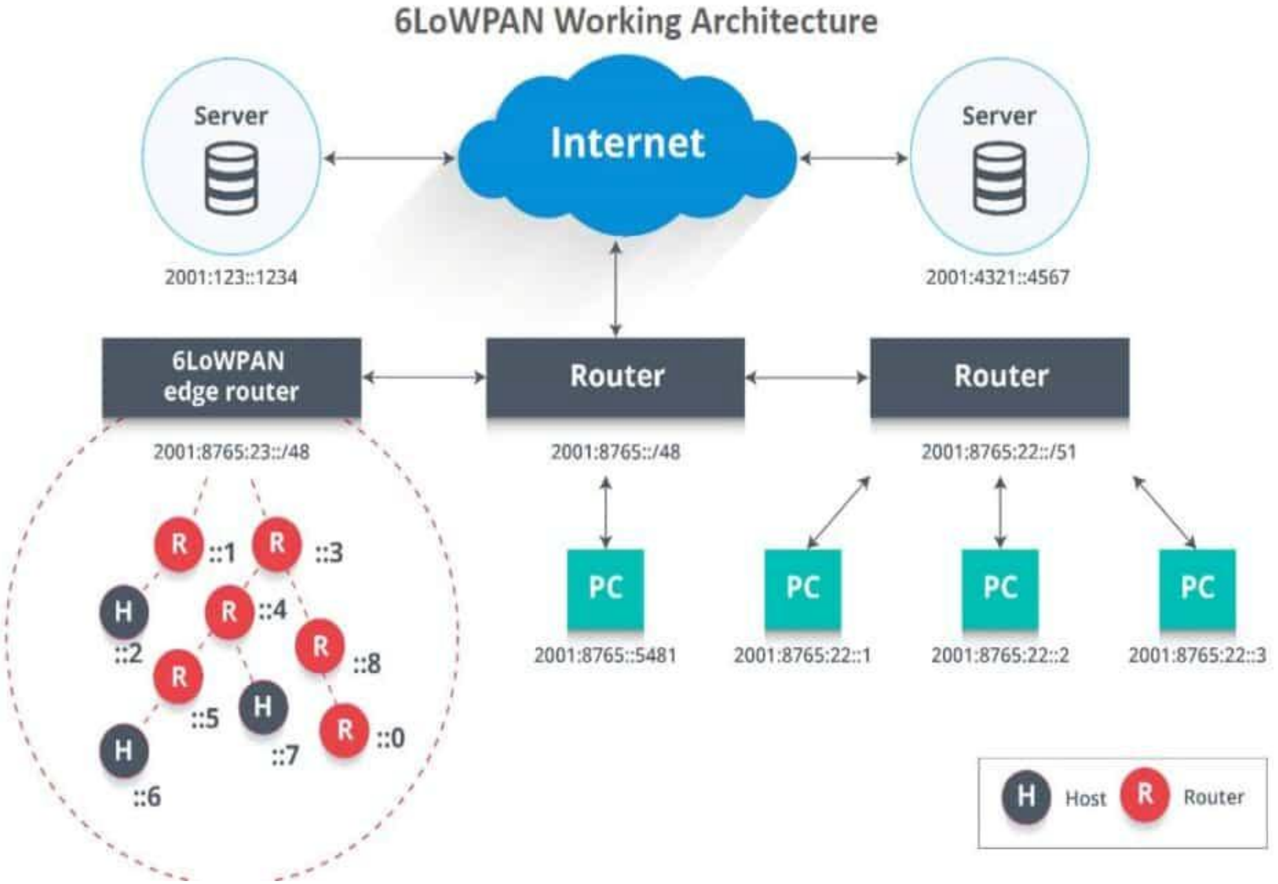
6LoWPAN

- **IPv6 over Low power Wireless Personal Area Networks**
- communication **protocol** specifically designed to **enable small, low-power devices to communicate** with each other over a **wireless network**.
- It allows these devices, such as sensors, smart home appliances, and wearable technology, to connect to the internet and exchange data.
- 6LoWPAN focuses on **connecting a larger number of devices to the cloud**.
- It is optimized for **small, resource-constrained devices, ensuring efficient communication** while conserving power.

- The fundamental **working principle** of 6LowPAN is the **encapsulation of IPv6 packets into smaller frames** that can be transmitted over a low-power wireless network.
- This encapsulation process allows small, low-power devices to send and receive data efficiently.
- 6LowPAN achieves this **by compressing the header of IPv6 packets**, reducing their size and making them suitable for transmission over low-power networks.
- 6LowPAN works with other IoT networking standards, **such as Bluetooth, Wi-Fi, and Zigbee**, enabling seamless communication between different devices.

6LowPAN

- In this architecture, the access point (AP) acts as an IPv6 router and handles the uplink to the internet.
- Various devices, such as PCs and servers, are connected to the AP.
- An edge router connects the 6LowPAN network to the IPv6 network, performing three key actions:
  - Facilitating data exchange between 6LowPAN devices and the internet or other IPv6 networks.
  - Enabling local data exchange between devices within the 6LowPAN network.
  - Generating and maintaining the radio subnet, which forms the 6LowPAN network.
- By communicating natively with IP, 6LowPAN networks can seamlessly connect to other networks using IP routers.



Advantages of 6LowPAN in IoT

- **Efficiency**: 6LowPAN is optimized for low-power devices, reducing the energy required for communication and extending the battery life of these devices.
- **Scalability**: With the increasing number of connected devices. 6LowPAN provides a more scalable and efficient communication protocol, allowing more devices to connect and interact with one another.
- **IP-based Connectivity**: 6LowPAN offers IP-based connectivity, enabling seamless integration with existing IP-based systems. This allows for the creation of large-scale, inexpensive IoT networks.
- **Interoperability**: 6LowPAN facilitates open standards and interoperability, making it easier to integrate devices from different manufacturers into an IoT ecosystem.
- **Cost-effectiveness**: By leveraging existing IP infrastructure, 6LowPAN offers a cost-effective solution for connecting many battery-operated or energy-harvesting IoT devices.
- **Robustness**: 6LowPAN provides a reliable communication infrastructure for IoT networks, ensuring robust connectivity and data exchange.

Thank you!!!

Devendra Dhande

devendra.dhande@sunbeaminfo.com