

COMMUNICATION PROTOCOLS:

Smart systems (IoT devices, sensors, actuators, smart grids, automation systems) need reliable communication to exchange data. The communication protocols define how devices talk to each other, how data is sent, received, formatted, and secured. Smart systems use wired protocols, wireless protocols, and application-level protocols depending on the requirement.

WIRED COMMUNICATION PROTOCOL:

UART (Universal Asynchronous Receiver-Transmitter):

- Simple serial communication. (Sending data one bit at a time, sequentially, over a single communication line.)
- Used for short-distance communication
- Transfers data bit by bit
- Common in microcontrollers, sensors, embedded systems
- Devices use TX (transmit) and RX (receive) pins

Applications: Sensor modules, GSM modules, GPS, microcontroller communication

SPI (Serial Peripheral Interface):

- High-speed, full-duplex communication
- Uses Master–Slave architecture
- Wires: MISO, MOSI, SCK, SS
- Faster than UART and I²C
- Used when large amounts of data must be exchanged quickly

Applications: SD cards, high-speed sensors, ADCs, displays

I²C (INTER-INTEGRATED CIRCUIT):

- Two-wire communication: SDA, SCL

- Supports multiple devices on the same bus
- Slower but simple and scalable
- Uses addressing system

Applications: Temperature sensors, EEPROMs, IMU sensors

CAN (CONTROLLER AREA NETWORK):

- Robust protocol used in harsh environments
- Supports long distances
- Used in automotive, industrial automation

Applications: Cars (engine control), factories, robotics systems

ETHERNET / INDUSTRIAL ETHERNET:

- High-speed wired communication
- Reliable, secure, supports large networks
- Variants: Ethernet/IP, PROFINET, Modbus TCP

Applications: Smart grids, factories, SCADA, PLC interconnections

Wireless Communication Technology:

Wireless communication technology refers to the transmission of data or information without using physical cables, by means of electromagnetic waves such as radio waves, infrared, or microwaves. It is a key part of smart systems, IoT, and automation, as it enables devices to communicate flexibly and remotely.

Basic Concept:

- Data is converted into electrical signals.
- These signals are transmitted through air using antennas.
- The receiving device captures the signal and converts it back into data.

RFID:

Radio Frequency Identification (RFID) is a technology used to identify and track objects automatically. It works using radio waves and is often connected to the Internet, so the information can be accessed from anywhere. In RFID, a small tag (label) is attached to an object. This tag stores data. When the tag comes near an RFID reader, the data is read without physical contact. The stored information can be sent, stored, or retrieved remotely through the Internet. Using RFID, we can track the movement of objects. The object can be anything like a parcel, a person, a bird, or an animal.



RFID Tag (or Smart Label):

- This is a small chip attached to an object (like a product, ID card, parcel, or animal).
- It stores information such as an ID number.
- It can be:
 - Passive (no battery, powered by scanner signal)
 - Active (has its own battery)

Example: The tag on a student ID card or on goods in a warehouse.

RFID Scanner (Reader / Antenna):

- This device sends radio waves.

- When the tag comes near, the scanner reads the information from the tag without touching it.
- It can also send data to the tag (in some systems).

Example: A handheld scanner used in stores or toll booths.

Database:

- The scanner sends the collected data to a computer/database.
- The database stores the information and connects it to applications.
- It helps in tracking, monitoring, and decision-making.

Example: A system that shows where a parcel is or whether a person is authorized.

In IoT applications, RFID is widely used in business and industry for:

- Parcel tracking
- Inventory control (Managing and monitoring stock)
- Sales record logging
- Supply chain management

RFID helps identify and track objects automatically and remotely, making business operations faster and more efficient.

BLUETOOTH:

Bluetooth is a short-distance wireless technology used to send and receive data between devices like mobile phones, laptops, headphones, keyboards, and smart devices. It works over small distances and is mainly used to create a Personal Area Network (PAN), which means connecting devices around one person (connecting personal devices that are close to a single user, usually within a few meters).

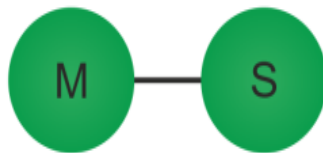
Bluetooth uses radio waves of Ultra High Frequency (UHF). These radio waves operate in a free-to-use frequency band called the ISM band, which lies between 2.402 GHz and 2.48 GHz. ISM band is a license-free frequency band used by many wireless devices.

The data speed of Bluetooth depends on its version:

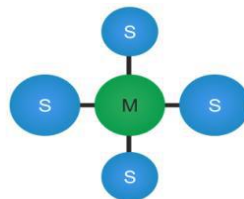
- The first-generation Bluetooth has a data rate of about 1 Mbps
- The second-generation Bluetooth increased the speed to about 2 Mbps
- When two devices are directly connected (one-to-one connection), the maximum practical data transfer speed is about 723 kbps.
- Bluetooth is designed to use very little power.
- In standby mode, it consumes only about 0.3 mA, which helps save battery life in devices like phones and wearables.

Functional modes:

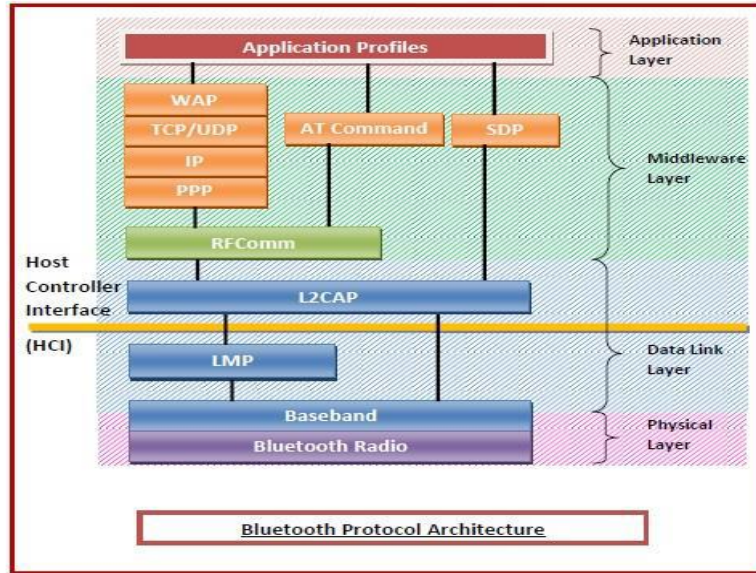
Bluetooth supports wireless point-to-point and point-to-multiple devices in Piconet (A Piconet is a small Bluetooth network formed when Bluetooth devices connect with each other). A point-to-point link has a master and slave relation and the Bluetooth function is also the same as a master and slave.



Point-to-multiple links is a network function. It functions like a master-to-one or more slaves, but the maximum number of slaves should be 7 .



BLUETOOTH ARCHITECTURE:



Physical Layer:

The physical layer of Bluetooth includes the Bluetooth Radio and the Baseband. These parts deal with actual wireless transmission.

1. Radio:

- The radio part is responsible for sending and receiving radio waves.
- It decides:
 - Which frequency band to use
 - How fast the frequency should hop
 - How the signal is modulated (converted into radio waves)
- It defines how Bluetooth signals travel through air.

2. Baseband:

- The baseband works using the radio.
- It controls:
 - How devices are identified (addressing)
 - How data is packed into frames

- Timing of data transmission
- Power control to save energy
- In simple words, it manages how data is organized and sent efficiently.

Data Link Layer:

The Data Link Layer in Bluetooth helps devices connect, stay connected, and exchange data safely. It includes Baseband, Link Manager Protocol (LMP), and L2CAP.

1. Link Manager Protocol (LMP):

- LMP is responsible for setting up and managing the connection between Bluetooth devices.
- It ensures:
 - Devices are authenticated (verified)
 - Data is encrypted (kept secure)
 - Both devices agree on packet size (It means that before sending data, both Bluetooth devices decide together how big each data packet should be)

2. Logical Link Control and Adaptation Protocol (L2CAP):

- L2CAP acts as a bridge between upper layers and the baseband.
- It:
 - Converts data from upper layers into a format suitable for baseband
 - Supports:
 - Connection-oriented services (reliable, continuous data transfer)
 - Connectionless services (data sent without a fixed connection)

Middleware Layer:

This includes Radio Frequency Communications (RFCOMM) protocol, adopted protocols, SDP, and AT commands.

1. RFComm – It is short for Radio Frontend Component. It provides a serial interface with WAP (Bluetooth uses a serial-type connection to carry WAP data between devices.)

2. Adopted Protocols:

- Adopted protocols are already available communication protocols that are reused in Bluetooth to save time and ensure compatibility.
- These are the protocols that are adopted from standard models.
- The commonly adopted protocols used in Bluetooth are Point-to-Point Protocol (PPP), Internet Protocol (IP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Wireless Application Protocol (WAP).

3. Service Discovery Protocol (SDP):

SDP takes care of service-related queries like device information so as to establish a connection between contending Bluetooth devices.

4. AT Commands:

Attention command set are text-based instructions used to control communication devices.

Applications Layer:

This includes the application profiles that allow the user to interact with the Bluetooth applications

Advantages of Bluetooth Protocols:

- Bluetooth offers economic wireless solutions (both data & voice) for short distances.
- It is used in the mobile and stationary environment.
- There is no setup file to install the Bluetooth; it is an inbuilt device.
- Global technology specifications are used.

ZIGBEE:

ZigBee is a **low-power, low-data-rate, wireless communication technology** designed for **short-range monitoring and control applications**. It is widely used in **smart automation systems, industrial monitoring, home automation, smart grids, and sensor networks**. ZigBee is based on the **IEEE 802.15.4 standard** and supports **reliable, secure, and scalable wireless networking** with minimal power consumption.

NEED FOR ZIGBEE IN SMART SYSTEM AUTOMATION:

In smart automation systems, multiple sensors and actuators need to communicate wirelessly with **low power, low cost, and high reliability**. ZigBee fulfills these requirements by:

- Supporting **mesh networking** (each node is connected to many other)
- Consuming **very low power**
- Allowing **large number of nodes** (network support many devices)
- Providing **secure communication**

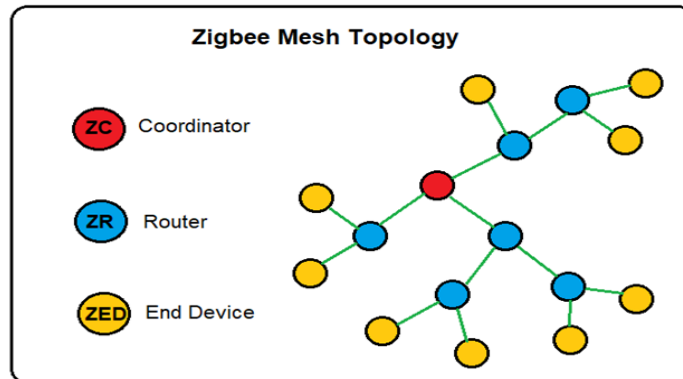
ZigBee network consists of three types of devices:

1. ZigBee Coordinator (ZC)

- Forms and manages the network
- Assigns addresses
- Stores network information

2. ZigBee Router (ZR)

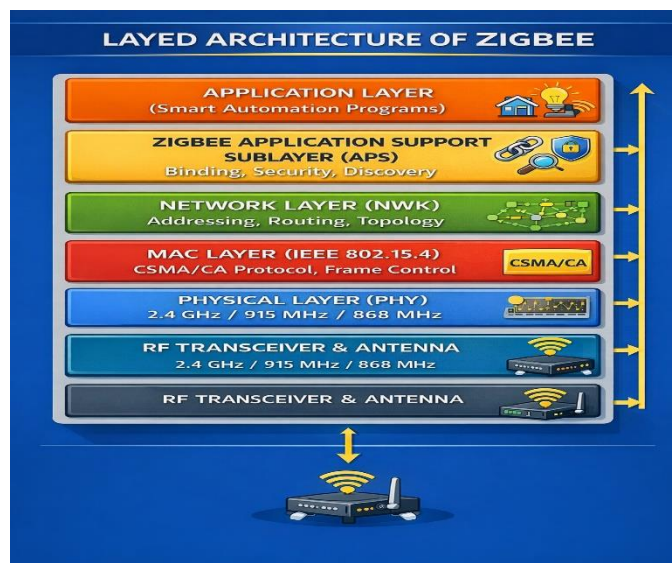
- Extends network coverage
- Routes data between nodes (receives data from one device and forwards it to another device)



3. ZigBee End Device (ZED)

- Low-power device
- Contains sensors/actuators
- Communicates only with parent node
- Battery-powered sensors or gadgets that connect to a parent (coordinator or router) but **cannot route** messages for others

BLOCK DIAGRAM OF ZIGBEE TECHNOLOGY:



APPLICATION LAYER:

- The **Application Layer** is the **topmost layer** of the ZigBee architecture.
- It is responsible for providing **user-specific automation applications** (behaves **according to what a specific user wants**).
- This layer enables **intelligent decision-making**, such as turning ON a motor or switching OFF a light based on sensor data.

FUNCTIONS:

- Defines **application objects** (A standard way to describe and control smart devices) for smart devices
- Implements automation logic such as:
 - Smart lighting control
 - Industrial monitoring
 - Home automation
- Interacts directly with sensors and actuators
-

ZIGBEE APPLICATION SUPPORT SUBLAYER (APS):

- The **APS layer** acts as an **interface between the Application Layer and the Network Layer**.

FUNCTIONS:

- **Data binding** (Creating a **logical link**) between devices
- **Device discovery** (locate another device) within the ZigBee network
- Provides **security services** such as authentication and encryption
- Manages message delivery between applications
- Ensures that the **right data reaches the correct application** securely.

NETWORK LAYER (NWK):

- The **Network Layer** is responsible for **network formation and management**.
- The **Network Layer** handles **creating the ZigBee network and controlling how devices join, communicate, and stay connected** within that network.
- This layer ensures **reliable communication** in large-scale automation systems.

FUNCTIONS:

- Assigns **network addresses** to devices
- Determines **routing paths** (electing the optimal path for data transmission)
- Supports network topologies:
 - Star
 - Tree
 - Mesh
- Enables **self-healing** by rerouting data when a node fails

MAC LAYER (IEEE 802.15.4):

- The **Medium Access Control (MAC) Layer** is defined by the **IEEE 802.15.4 standard**.
- Ensures **efficient and collision-free data transmission**.

FUNCTIONS:

- Controls access to the wireless channel
- Prevents data collision using **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance).
- Frame formatting and acknowledgment
- Synchronization between devices

PHYSICAL LAYER (PHY):

- The **Physical Layer** handles **actual transmission of data** over the wireless medium.

FUNCTIONS:

- Modulation and demodulation
- Signal transmission and reception
- Channel selection

OPERATING FREQUENCIES:

- **2.4 GHz** – Worldwide
- **915 MHz** – USA
- **868 MHz** – Europe

DATA RATE:

- Up to **250 kbps**

ADVANTAGES:

- Modular design
- Easy troubleshooting
- Scalable network
- Secure communication