

# Module 1

## Emergence of IoT

# Introduction

This Module explores the emergence and growth of the Internet of Things (IoT), showing how it evolved from technologies like M2M communication, wireless sensor networks, and cyber-physical systems into a global paradigm connecting billions of devices. It highlights the key enablers, networking paradigms, protocols, and addressing strategies that make IoT scalable and interoperable. The chapter emphasizes the complex interdependence of sensing, communication, processing, and application technologies, portraying IoT as an interdisciplinary ecosystem driving digital transformation across industries.

# Emergence of IoT - Introduction

## (4.1)

# Rapid Growth of IoT

- IoT has grown exponentially in the past decade.
- Present in households, industries, banking, logistics, education, and transportation.
- Adoption driven by automation, efficiency, and safety needs.
- Healthcare, agriculture, and transport rely heavily on IoT.

# Technological Foundations of IoT

## **Emerged from multiple paradigms and technologies:**

- Internet Computing – global connectivity.
- Cloud Computing – scalable processing & storage.
- Wireless Sensor Networks (WSN) – sensing capability.
- Cyber-Physical Systems (CPS) – linking computation with physical systems.
- Machine-to-Machine (M2M) Communication – automation.

# Networking Paradigms Supporting IoT

- Cloud Computing – large-scale affordable data storage and processing.
- Edge Computing – brings computation closer to devices, reduces latency.
- Fog Computing – intermediate layer between cloud and edge.
- Edge computing rise is directly attributed to IoT demands.

# IoT Communication & Protocols

## **IoT motivated new protocols and communication technologies:**

- IPv6 – expanded addressing for billions of devices.
- MQTT – lightweight messaging protocol.
- 6LoWPAN – IPv6 over low-power wireless networks.
- LoRa – long-range, low-power communication.

# Applications Across Domains

- **IoT is applied across multiple sectors:**
  - Consumer electronics & households.
  - Power & energy systems.
  - Healthcare, agriculture, environment.
  - Logistics, transport, military, and surveillance.
  - Analytics and decision-making.

# Evolution of IoT - Section 4.2

# The Evolutionary Path of IoT

- IoT did not emerge suddenly but as a culmination of decades of progress.
- It began with early computer networking and global Internet connectivity.
- Later, advances in wireless communication, embedded systems, sensors, and cloud computing shaped IoT.
- This evolutionary path gradually enabled massive IoT deployment.

# Technological Convergence

- IoT is built on multiple predecessor technologies:
  - Machine-to-Machine (M2M) – device-to-device communication.
  - Wireless Sensor Networks (WSNs) – real-time environmental data collection.
  - Cyber-Physical Systems (CPS) – integration of computational algorithms with physical processes.
  - IoT goes further by ensuring interoperability, scalability, and global connectivity.

# Timeline of Developments

- The sequence of developments leading to IoT includes:
    - Embedded electronics and miniaturization.
    - Mobile internet and wireless expansion.
    - IPv6 adoption – addressing billions of devices.
    - Cloud computing and big data analytics.
    - Edge and fog computing – real-time processing.
- These advances collectively shaped the modern IoT.

# Differences from Predecessors

- IoT vs M2M: IoT extends beyond communication to include analytics, cloud integration, and intelligent decision-making.
- IoT vs CPS: CPS is specific to systems integrating computation with physical processes, IoT is global and heterogeneous.
- IoT vs WoT: Web of Things integrates IoT devices via web standards, but is a subset of IoT.

# Industry-Wide Transformation

- The evolution of IoT has reshaped industries:
  - Smart Homes – interconnected appliances and automation.
  - Industry 4.0 – IoT-driven manufacturing and logistics.
  - Healthcare – from monitoring devices to predictive analytics and telemedicine.
  - Transportation – intelligent traffic and connected vehicles.
- IoT represents the mature stage of convergence in these domains.

# Conclusion

- IoT is the product of progressive integration of communication, sensing, and computing technologies.
- It surpasses predecessors by enabling global scalability, interoperability, and intelligence.
- The evolutionary journey of IoT reflects a timeline of breakthroughs that transformed industries and society.

## 4.3 – Enabling IoT and the Complex Interdependence of Technologies

# Multiple Enablers of IoT

- IoT is not a single technology but a convergence of many enablers.
- These include sensors, actuators, communication protocols, connectivity technologies, addressing mechanisms, processing paradigms (cloud/fog/edge), and interoperability frameworks.
- All these components collectively sustain the IoT ecosystem.

# Interdependence of Technologies

- IoT exhibits a complex web of interdependencies among technologies.
- Sensors generate data which is transmitted via communication protocols.
- Processing depends on cloud, fog, or edge computing, which in turn rely on networking technologies.
- Addressing strategies like IPv6 and 6LoWPAN ensure billions of devices can be uniquely identified.

# IoT Planes and Layers

- IoT can be viewed as multiple interconnected planes:
  - Perception Plane – sensors and actuators interacting with the physical world.
  - Network Plane – communication technologies and routing protocols.
  - Processing Plane – data analytics, edge/fog/cloud computing.
  - Application Plane – user interfaces and domain-specific applications.
- Each plane is dependent on the others for seamless functioning.

# Examples of Interdependence

- Healthcare IoT: Wearable sensors send patient data via Wi-Fi/LoRa (network plane) to fog nodes (processing plane) before showing insights to doctors (application plane).
- Smart Agriculture: Soil sensors use 6LoWPAN (network plane) to send data to cloud analytics (processing plane) that predict irrigation needs (application plane).
- These examples show how IoT enablers cannot function in isolation.

# Visualization of Interdependencies

- Figure 4.8 illustrates IoT planes, enablers, and their complex interdependencies.
- The diagram shows perception, networking, addressing, processing, and application layers interacting in a circular, mutually supportive way.
- This emphasizes the interdisciplinary and interconnected nature of IoT.

# 4.4 IoT Networking Components

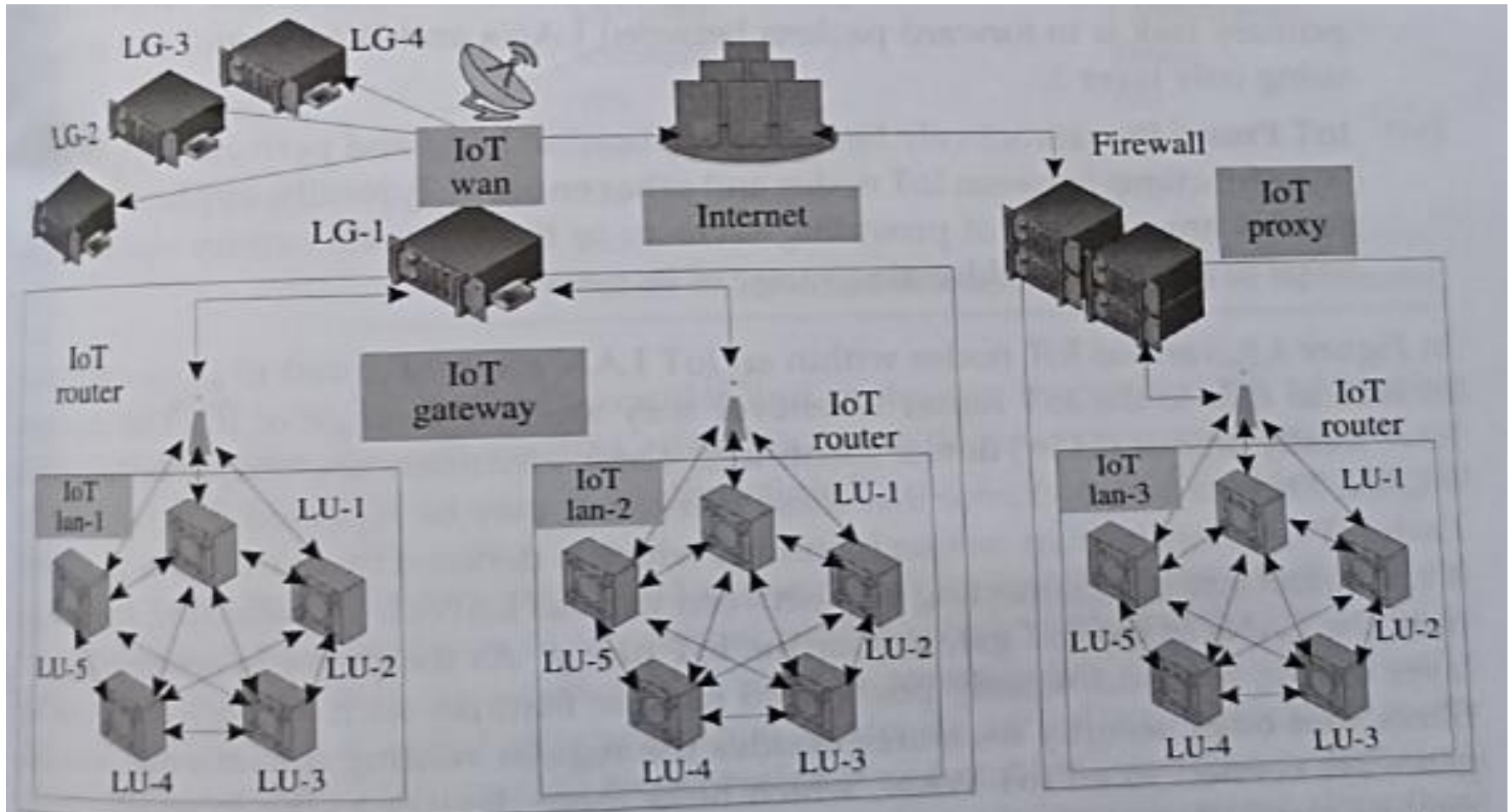


Figure 4.9 A typical IoT network ecosystem highlighting the various networking components—from IoT nodes to the Internet

# IoT Node

- Basic networking devices in an IoT LAN composed of sensors, processors, and radios.
- Collect data from the environment through sensors.
- Process data locally before sending to the network.
- Communicate either inside the LAN or with external networks.
- Support wired or wireless communication technologies.
- May connect directly to other nodes in the same LAN.
- Can communicate indirectly via an IoT gateway.
- Play a crucial role in edge computing scenarios.
- Have locally unique identifiers for network recognition.
- Enable real-time monitoring and control in IoT applications.

# IoT Router

- Directs data packets between devices in the IoT network.
- Ensures traffic flows correctly between endpoints.
- Supports network segmentation for security and efficiency.
- Can function as an IoT gateway with added configurations.
- Manages bandwidth allocation and traffic prioritization.
- Includes routing protocols tailored for IoT environments.
- Enables communication between different IoT subnets.
- Can handle both IPv4 and IPv6 addressing schemes.
- May include security features like packet inspection.
- Provides a stable backbone for IoT network traffic.

# IoT LAN

- Local Area Network confined to a specific location or building.
- Uses short-range technologies like Wi-Fi, Zigbee, or Bluetooth.
- Supports low-latency communication between IoT nodes.
- Often managed by a single IoT gateway.
- May operate in isolation from the Internet for security.
- Facilitates device discovery and local interactions.
- Enables centralized control for connected IoT devices.
- May connect to multiple IoT routers for redundancy.
- Supports both static and dynamic IP addressing.
- Acts as the foundation layer of most IoT deployments.

# IoT WAN

- Wide Area Network connecting multiple IoT LANs or networks.
- Spans large geographic areas, from kilometers to hundreds of kilometers.
- Links organizationally separate IoT deployments.
- Connects to the Internet for global accessibility.
- Can be implemented over cellular, satellite, or fiber networks.
- Provides redundancy and fault tolerance for IoT communication.
- Supports secure tunneling via VPNs for data protection.
- Enables real-time synchronization across distant locations.
- Integrates with cloud platforms for data storage and processing.
- Serves as the backbone for large-scale IoT infrastructures.

# IoT Gateway

- Connects IoT LANs to WANs or the Internet.
- Acts as a bridge between local devices and cloud services.
- Handles protocol translation between heterogeneous devices.
- Performs data aggregation and preprocessing before transmission.
- Implements security features such as encryption and authentication.
- Supports multiple communication standards simultaneously.
- Can host edge computing applications for faster processing.
- Monitors device health and network performance.
- Provides backup connectivity options in case of failure.
- Acts as the central management point for connected devices.

# IoT Proxy

- Application layer device facilitating communication between IoT nodes and other systems.
- Adds an additional security layer through authentication and filtering.
- Can cache frequently accessed data for faster retrieval.
- Extends the addressing range beyond local network limitations.
- Acts as a mediator between private IoT networks and public networks.
- Supports load balancing for application traffic.
- May perform protocol translation for interoperability.
- Filters malicious requests before reaching IoT nodes.
- Improves network performance through request optimization.
- Enhances scalability by managing application-level connections.

# Addressing Strategies in IoT

IPv4 vs IPv6, IPv6 Address Format,  
Types, and Multihoming

# IPv4 vs IPv6 Differences

- Developed: IPv4 – IETF 1974, IPv6 – IETF 1998
- Address length: IPv4 – 32 bits, IPv6 – 128 bits
- Number of addresses: IPv4 –  $2^{32}$ , IPv6 –  $2^{128}$
- Notation: IPv4 – Dotted decimal, IPv6 – Hexadecimal
- Dynamic allocation: IPv4 – DHCP, IPv6 – DHCPv6, SLAAC
- IPsec: IPv4 – Optional, IPv6 – Compulsory
- Header size: IPv4 – Variable, IPv6 – Fixed
- Header checksum: IPv4 – Yes, IPv6 – No
- Address types: IPv4 – Broadcast & Multicast, IPv6 – Multicast only
- Feature focus: IPv4 – Reliable transmission, IPv6 – Addressing capacity

# IPv6 Address Format

- IPv6 length: 128 bits, represented in hexadecimal.
- Global Prefix: First 3 blocks (48 bits) – globally unique.
- Subnet Prefix: Next block (16 bits) – identifies subnet of interface/gateway.
- Interface Identifier (IID): Last 64 bits – unique device/node identifier.

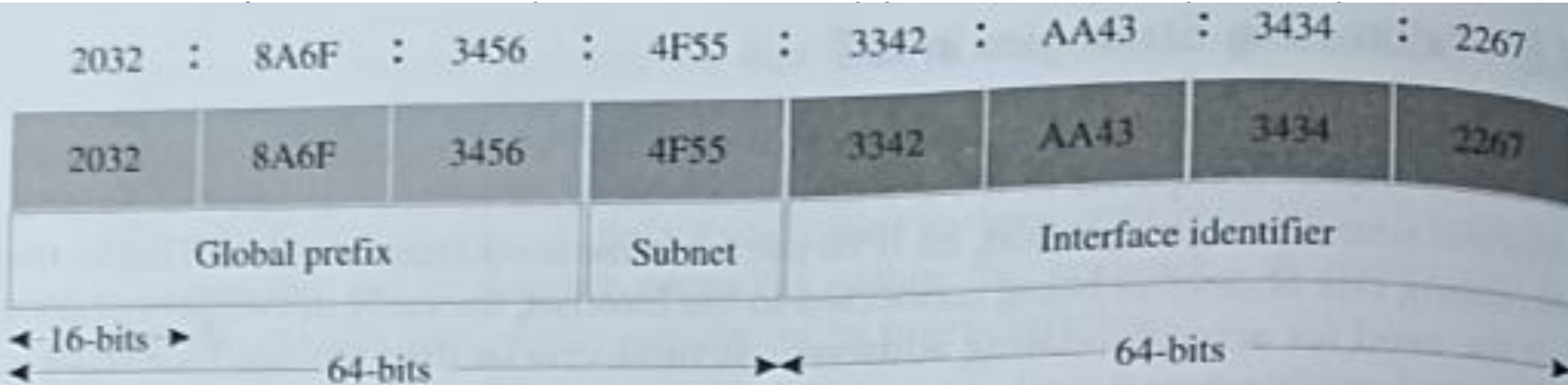


Figure 4.10 The IPv6 address format

# IPv6 Address Types in IoT

- Global Unicast (GUA): Unique Internet-routable addresses for IoT gateways, proxies, WANs.
- Multicast: Send messages to multiple destination entities simultaneously.
- Link Local (LL): Unique within LAN or network segment, not Internet-routable.
- Unique Local (ULA): Similar to LL, unique within segment, not routable on Internet.
- Loopback: Localhost address for diagnostics and testing.
- Unspecified: All bits set to zero, no specific destination.
- Solicited-node Multicast: Multicast based on IPv6 address of an IoT node.

# Multi-homing in IoT Networks

- Definition: Connecting a node/network to multiple networks simultaneously for reliability.
- Improves network fault tolerance and ensures continuous operation.
- Proxies manage multiple IPs and map them to LL addresses in small IoT deployments.
- Useful where direct address prefix allotment is not possible.
- Gateways may be used for assigning LL addresses to IoT nodes under their control.

# Enabling Technologies for the Internet of Things (IoT)

The Internet of Things (IoT) connects devices, sensors, actuators, and software into intelligent networks that communicate, process data, and make autonomous decisions. It is powered by communication protocols like Zigbee, BLE, Wi-Fi, LoRaWAN, NB-IoT, and 5G, along with networking standards such as MQTT, CoAP, and 6LoWPAN, and identification systems like RFID and NFC. Edge and cloud computing enhance performance by reducing latency, while blockchain ensures trust, immutability, and decentralized control. Artificial intelligence and analytics further enable predictive maintenance, anomaly detection, and automation, driving IoT adoption across industries from healthcare to smart cities.

# 1. Communication Technologies

## Zigbee

- Low-power, short-range mesh network standard for IoT.
- Operates on IEEE 802.15.4 standard at 2.4 GHz frequency.
- Supports mesh, star, and tree network topologies.
- Ideal for home automation, industrial monitoring, and sensor networks.
- Supports up to thousands of devices in one network.
- Low data rates (20–250 kbps) but high reliability.
- Battery life can last for years due to low power consumption.
- Interoperable between Zigbee-certified devices.
- Range typically 10–100 meters indoors, extendable via mesh.
- Examples: Philips Hue, smart switches, wireless sensors.

# Bluetooth Low Energy (BLE)

- Low-energy version of Bluetooth for short-range communication.
- Designed for low-power consumption and infrequent data transfer.
- Operates in the 2.4 GHz ISM band.
- Range is typically 10–50 meters.
- Ideal for wearables, fitness trackers, and health monitoring devices.
- Uses GATT (Generic Attribute Profile) for structured data exchange.
- Fast connection setup and low latency.
- Compatible with smartphones and tablets.
- Supports mesh networking for IoT use cases.
- Example devices: Smartwatches, BLE beacons, medical sensors.

# Wi-Fi

- High-speed wireless LAN technology for IoT.
- Operates on 2.4 GHz and 5 GHz frequency bands.
- Offers data rates from Mbps to Gbps.
- Ideal for high-bandwidth IoT devices like cameras.
- Supports direct Internet connectivity.
- Drawback: Higher power consumption than Zigbee/BLE.
- Commonly used in smart home appliances and routers.
- Supports WPA3 encryption for secure communication.
- Wide availability of infrastructure (routers, hotspots).
- Examples: Smart TVs, Wi-Fi cameras, home assistants.

# LoRaWAN

- Long Range Wide Area Network protocol for IoT.
- Operates in unlicensed ISM bands (EU 868 MHz, US 915 MHz).
- Supports long-range communication up to 15 km.
- Extremely low power consumption for battery devices.
- Ideal for rural and remote IoT applications.
- Low data rates (0.3–50 kbps) optimized for sensor data.
- Supports public and private network deployments.
- Scalable to millions of devices.
- Used in agriculture, smart metering, and environmental monitoring.
- Example: Smart irrigation systems, city-wide sensor networks.

# NB-IoT

- Narrowband IoT technology using cellular infrastructure.
- Optimized for low-power, low-bandwidth IoT communication.
- Operates in licensed LTE spectrum bands.
- Supports deep indoor coverage.
- Extremely power efficient, enabling years of battery life.
- Supports massive device connectivity.
- Ideal for smart meters, asset tracking, and healthcare.
- Low cost compared to traditional cellular IoT.
- No need for gateways; connects directly to cellular towers.
- Example: Smart parking sensors, water meters.

# 5G

- Next-generation cellular network for high-speed IoT.
- Supports ultra-low latency (as low as 1 ms).
- Handles massive IoT device connectivity.
- Operates in multiple frequency bands (sub-6 GHz, mmWave).
- Enables real-time applications like autonomous vehicles.
- High bandwidth for video streaming and AR/VR.
- Supports network slicing for dedicated IoT services.
- Energy-efficient modes for IoT sensors.
- Example: Remote surgery, smart factories.
- Integrates with edge computing for faster processing.

# RFID/NFC

- Radio Frequency Identification & Near Field Communication.
- RFID used for wireless identification and tracking.
- NFC is a short-range technology used for contactless communication.
- Operates at low frequencies (125 kHz), high frequencies (13.56 MHz), or ultra-high frequencies (860–960 MHz).
- Used in inventory management, access control, and payments.
- Low power, passive tags draw energy from readers.
- Can store small amounts of data.
- High security in NFC for transactions.
- Example: Metro cards, contactless credit cards.
- Common in logistics, retail, and security.

# Networking & Protocol Technologies

- These technologies control data transfer and define network architecture for IoT.
- MQTT (Message Queuing Telemetry Transport) – Lightweight messaging protocol for IoT devices.
- CoAP (Constrained Application Protocol) – Designed for devices with limited resources.
- HTTP/HTTPS – Standard web communication for IoT with security (TLS/SSL).
- 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) – Enables IPv6 over IEEE 802.15.4 networks like Zigbee.

# Introduction to Internet of Things (IoT)

Based Textbook 2 (Bahga & Madiseti)

# 1.1 Introduction

- IoT comprises things with unique identities connected to the Internet.
- Examples: thermostats, utility meters, irrigation pumps, sensors.
- Focus: configuration, control, networking of devices.
- Growth driven by sensors, mobile, wireless, networking, cloud.
- Forecast: 50 billion devices by 2020.
- Data → Information → Knowledge (processing & contextualization).

## **Data**

- Raw and unprocessed data obtained from IoT devices/systems.

## **Information**

- Information is inferred from data by filtering, processing, categorizing, condensing and contextualizing data.

## **Knowledge**

- Knowledge is inferred from information by organizing and structuring information and is put into action to achieve specific objectives.

**Figure 1.1: Inferring information and knowledge from data**

# From Data to Knowledge

- Data: Raw, unprocessed values from IoT systems.
- Information: Processed data (filtered, categorized, contextualized).
- Knowledge: Organized information applied to achieve objectives.

# Applications of IoT

- Home: Smart lighting, appliances, intrusion detection.
- Cities: Smart parking, smart roads, emergency response.
- Environment: Weather & pollution monitoring, forest fire detection.
- Energy: Smart grids, renewable integration, prognostics.
- Retail: Inventory management, smart payments.
- Logistics: Route scheduling, fleet tracking.
- Agriculture: Smart irrigation, greenhouse control.
- Industry: Machine diagnostics, air quality.
- Health & Lifestyle: Wearables, health monitoring.

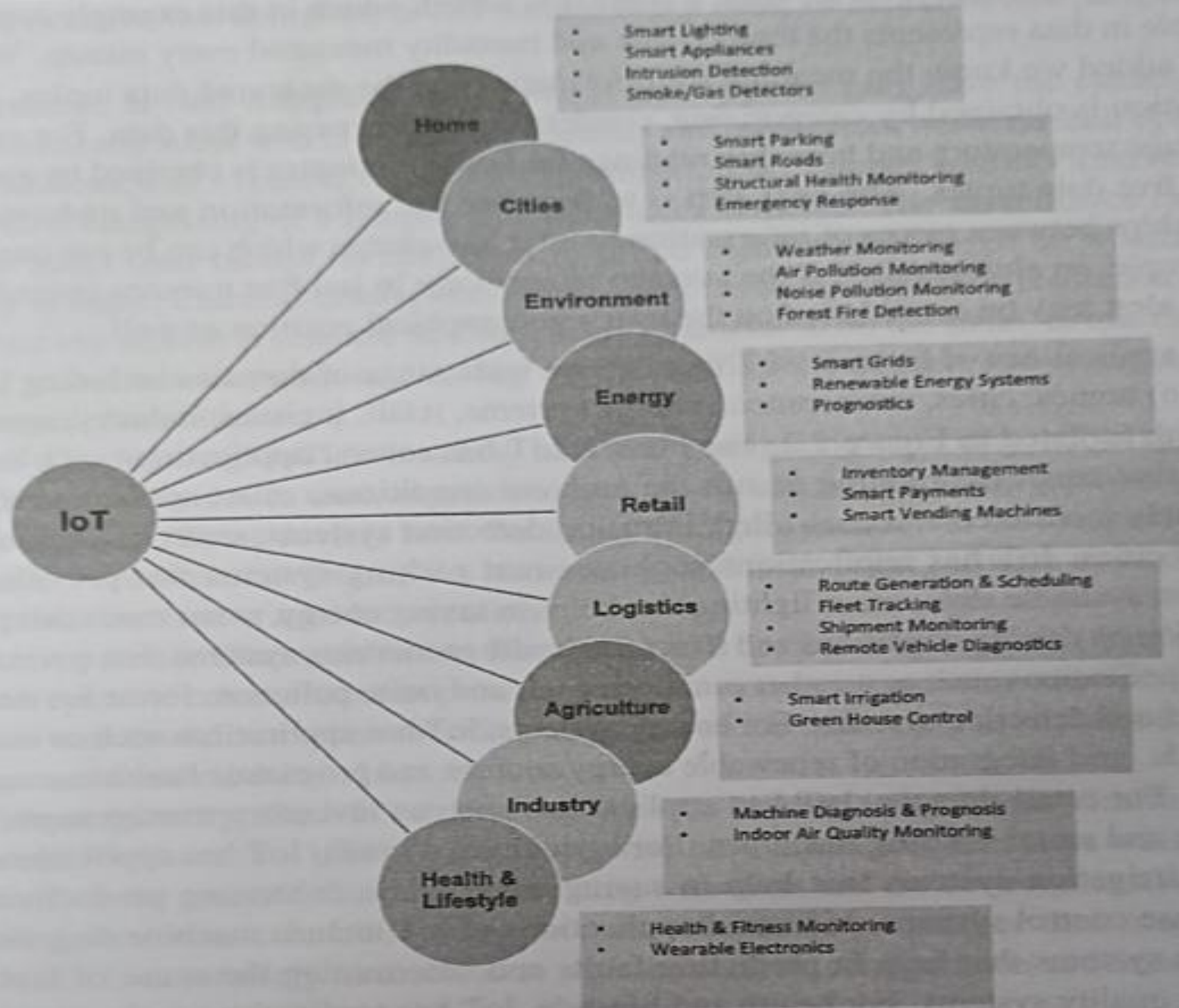


Figure 1.2: Applications of IoT

# 1.1.1 Definition of IoT

- “A dynamic global network infrastructure with self-configuring capabilities based on interoperable communication protocols, where physical and virtual ‘things’ have identities, attributes, and intelligent interfaces, seamlessly integrated into information networks.”

# Characteristics of IoT

1. Dynamic & Self-Adapting: Devices adapt to context (e.g., surveillance cameras).
2. Self-Configuring: Devices auto-configure, update, and coordinate.
3. Interoperable Protocols: Communicate via Wi-Fi, ZigBee, Bluetooth, etc.
4. Unique Identity: Each device has unique ID (IP, URI).
5. Integrated into Information Network: Devices exchange and share intelligence.

# Summary

- IoT connects billions of smart, identifiable devices.
- Transforms data → information → knowledge.
- Wide applications: home, cities, industry, health, etc.
- Key traits: dynamic, self-adapting, self-configuring, interoperable, integrated.

# Physical Design of IoT (Section 1.2)

Detailed Explanation of Link Layer, Network Layer, Transport Layer, and Application Layer Protocols

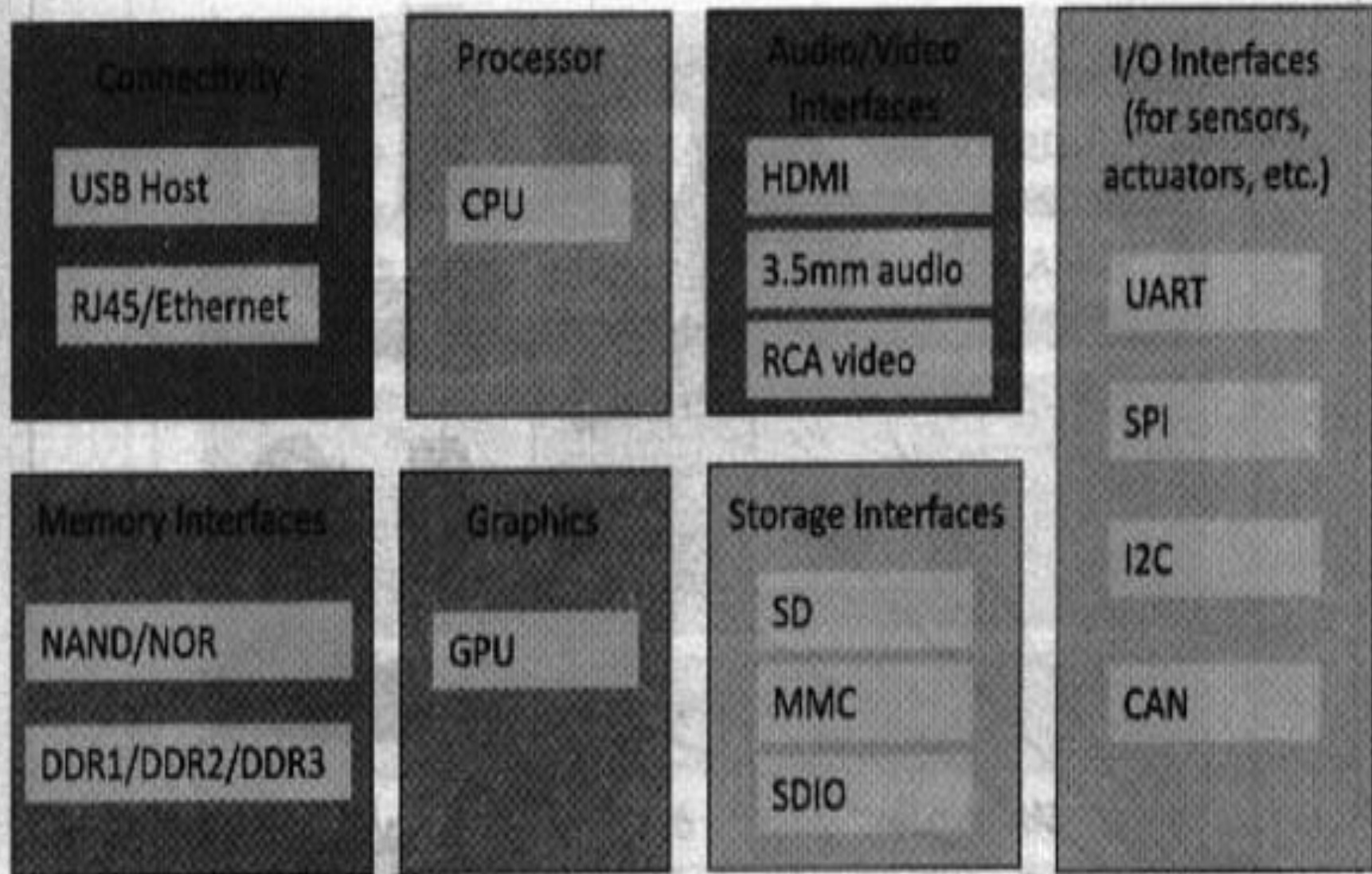


Figure 1.3: Generic block diagram of an IoT Device

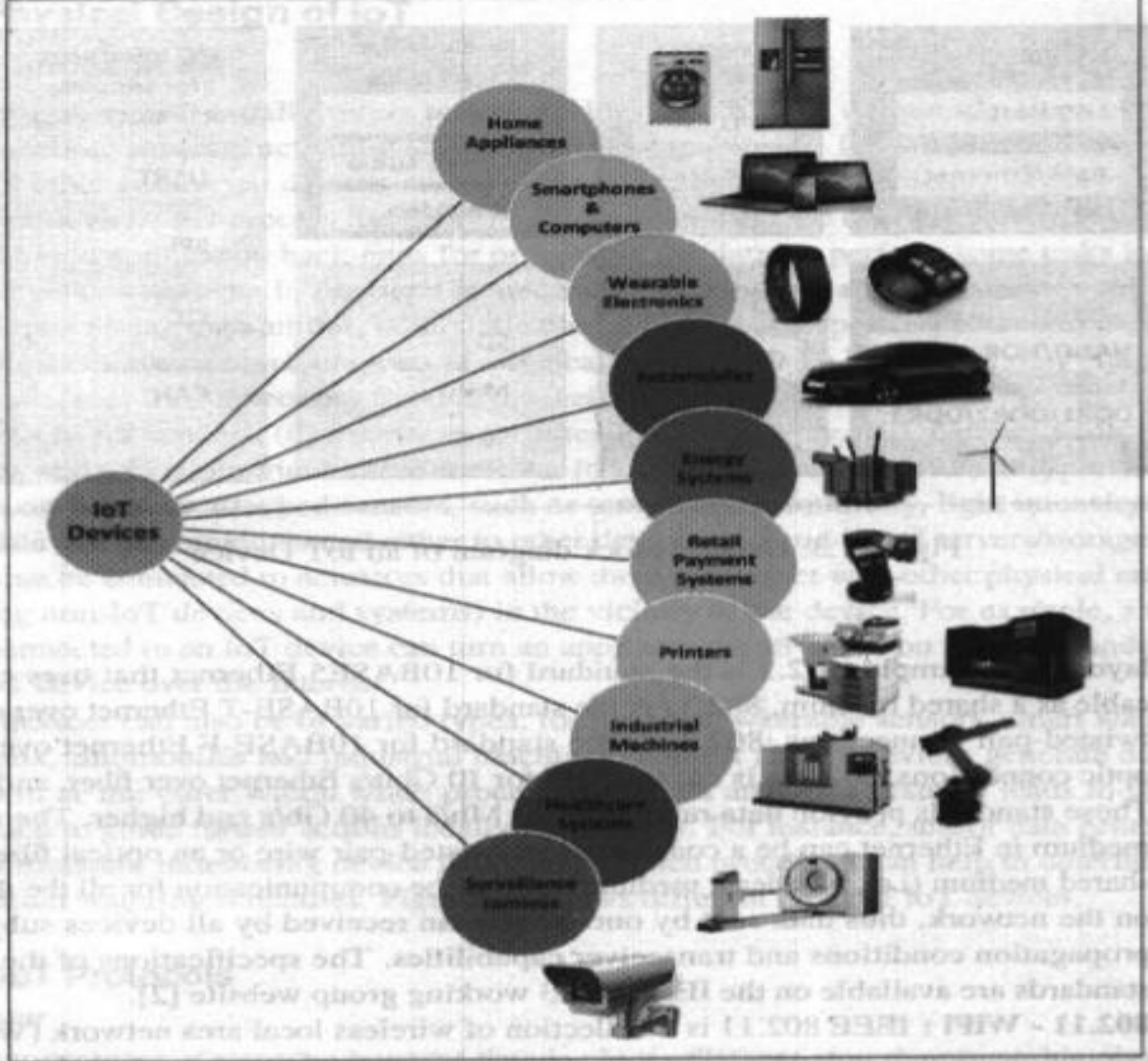


Figure 1.4: IoT Devices

# Introduction

- Physical Design of IoT describes the hardware and protocols that enable IoT communication.
- It uses a layered model: Link Layer, Network Layer, Transport Layer, Application Layer.
- Each keyword in these layers defines specific technologies that make IoT work.

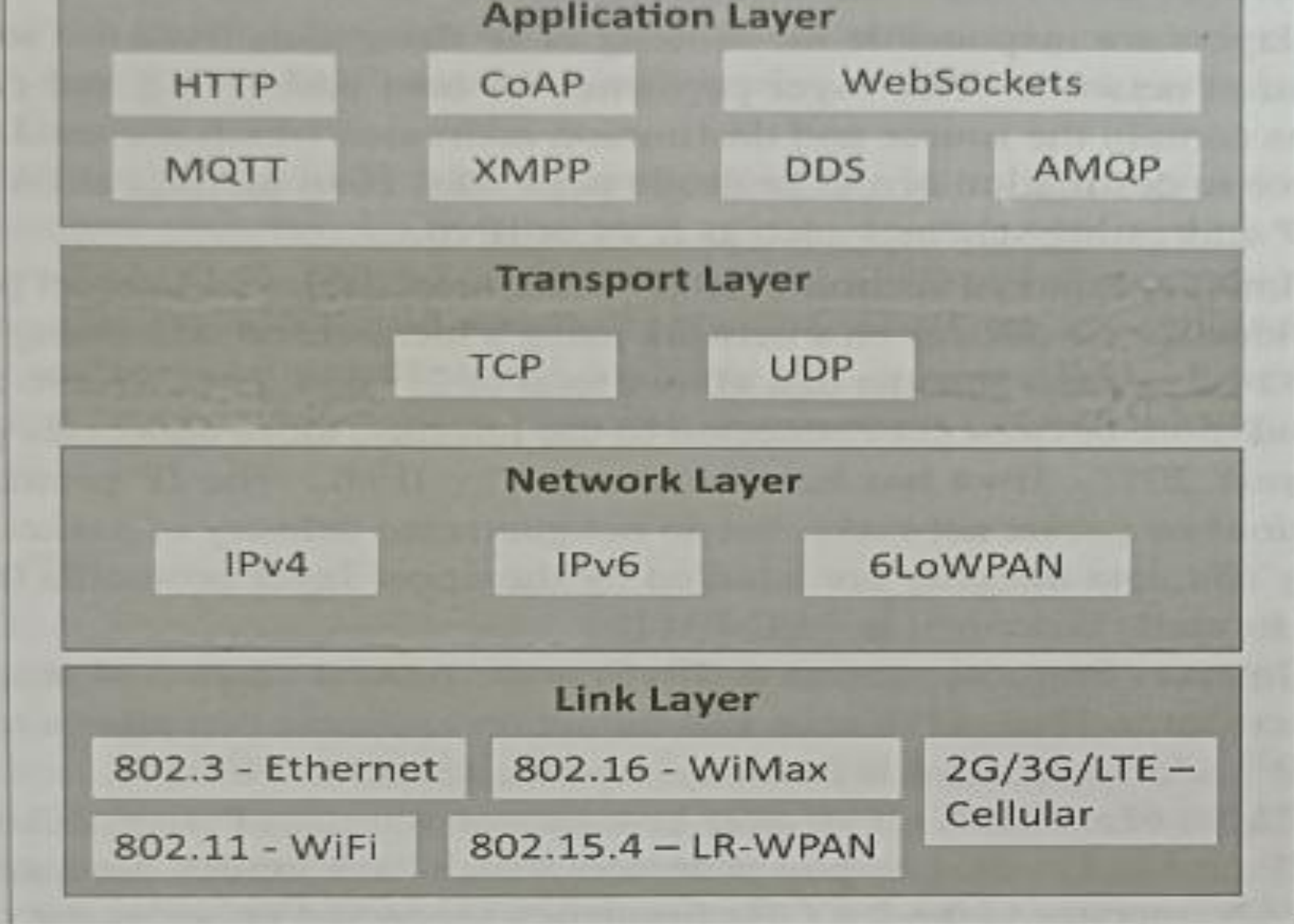


Figure 1.5: IoT Protocols

# IoT Protocol Stack (Figure 1.5 Explained)

Application, Transport, Network, and Link Layers

# Introduction

- IoT protocols are organized in layers
- Each layer has specific responsibilities
- This stack includes Application, Transport, Network, and Link layers
- Together they enable device-to-device and device-to-cloud communication

# Application Layer Protocols

- HTTP: Standard web protocol (e.g., Smart fridge REST APIs)
- CoAP(Constrained Application Protocol): Lightweight HTTP for IoT (e.g., Soil moisture sensors)
- WebSockets: Real-time bidirectional communication (e.g., Live CCTV feed)
- MQTT(Message Queuing Telemetry Transport) : Publish-subscribe model (e.g., Warehouse sensors)
- XMPP(Extensible Messaging and Presence Protocol): Messaging protocol (e.g., IoT chat updates)
- DDS(Data Distribution Service): Real-time data exchange (e.g., Industrial robots)
- AMQP: Reliable messaging (e.g., Banking IoT alerts)

# Transport Layer Protocols

- TCP: Reliable, ordered delivery
  - Example: ECG monitoring system
- UDP: Fast, lightweight, no guaranteed delivery
  - Example: Surveillance video streaming

# Network Layer Protocols

- IPv4: Widely used, but limited address space
- IPv6: Supports billions of IoT devices (unique addresses)
- 6LoWPAN: Runs IPv6 on IEEE 802.15.4 low-power devices
  - - Example: Smart streetlights with IPv6 addresses

# Link Layer Protocols

- 802.3 Ethernet: Wired, reliable (Factory IoT gateways)
- 802.11 Wi-Fi: High bandwidth, high power (Smart TVs, cameras)
- 802.16 WiMax: Long-range broadband (Rural IoT stations)
- 802.15.4 LR-WPAN: Low power, low data (ZigBee, Thread)
- 2G/3G/LTE Cellular: Wide coverage (GPS trackers, smart meters)

# Smart Agriculture Example

- Sensors connect via IEEE 802.15.4 LR-WPAN
- 6LoWPAN enables IPv6 addressing
- UDP chosen for efficiency
- CoAP application protocol used for lightweight communication
- Farmers access real-time data via HTTP on mobile app

# Summary

- IoT protocols form a layered architecture
- Link Layer: Physical connectivity (Ethernet, Wi-Fi, ZigBee, Cellular)
- Network Layer: Addressing and routing (IPv4, IPv6, 6LoWPAN)
- Transport Layer: Data delivery (TCP for reliability, UDP for speed)
- Application Layer: IoT services (MQTT, CoAP, HTTP, etc.)
- Each layer ensures efficient, scalable, and reliable IoT communication

# Understanding IEEE 802.15.4, LR- WPAN, and ZigBee

Explained in Simple Words

# IEEE 802.15.4 – The Road

- IEEE 802.15.4 is like the road. It only gives the basic path and rules for how devices can send wireless signals. By itself, it is just empty infrastructure – no houses, no people, just the road waiting to be used.

# LR-WPAN – The Neighborhood

- When devices such as smart bulbs, sensors, and switches actually start using the road (IEEE 802.15.4) to connect with each other, they form a Low-Rate Wireless Personal Area Network (LR-WPAN). This is like a neighborhood where all these devices live and can exchange messages.

# ZigBee and Others – The Vehicles

- On top of this neighborhood, protocols like ZigBee, 6LoWPAN, or Thread act like vehicles. Each vehicle carries different types of messages for different purposes – such as turning on lights, reporting temperature, or connecting devices to the Internet.

# The Full Analogy

- IEEE 802.15.4 = The road (basic wireless rules)
- LR-WPAN = The neighborhood (devices living on the road)
- ZigBee / 6LoWPAN / Thread = Vehicles (carry the actual messages)
- Together, they create a complete system where devices can live, talk, and perform smart tasks.

# IoT Protocols in a Smart City

A Story from Morning to Night

# Morning – Streetlights Turn Off

- As the sun rises, the smart streetlights in the city begin to turn off automatically. The command starts from the control center and travels through Ethernet cables (802.3) to a local gateway. From there, it reaches each streetlight through IEEE 802.15.4 (LR-WPAN), which is a low-power wireless technology ideal for small devices. Since these lights need to be connected to the Internet, they use IPv6 addresses, but because IPv6 packets are large, 6LoWPAN compresses and breaks them down to fit the tiny 802.15.4 frames. To make sure no command is lost, the system uses TCP for reliable delivery. Each streetlight then replies using CoAP, a lightweight messaging language, saying: 'I am OFF.'

# Morning Rush Hour – Buses on the Move

- During office hours, buses start moving across the city. Each bus has a GPS tracker that constantly sends its location. These trackers connect using LTE (cellular network), which allows communication even while moving. Every bus has a unique IPv6 address so that it can be identified easily. Since updates are sent every few seconds, speed is more important than 100% accuracy, so the data travels over UDP instead of TCP. The GPS coordinates are wrapped in CoAP, which keeps the messages short. When citizens check their mobile apps for bus arrival times, the app uses HTTP to fetch this information from the server and display it in a user-friendly way.

# ☐ Midday – Pollution Rises

- As traffic gets heavier, air pollution starts to increase. Tiny air quality sensors on lamp posts measure pollution levels like PM2.5. These sensors use IEEE 802.15.4 radios because they are battery-operated and need to save energy. Since IPv6 packets are too large for these radios, 6LoWPAN compresses the headers so that IPv6 can run smoothly. The pollution data is sent quickly using UDP, and at the application layer, it uses MQTT. In MQTT, sensors publish messages like 'PM2.5 = 160  $\mu\text{g}/\text{m}^3$ ' to a central broker. The control room dashboard and citizens' apps subscribe to this broker, so everyone gets instant updates when pollution rises.

# 🚦 Afternoon – Cameras and Traffic Lights

- At busy intersections, traffic cameras stream live video to the control room. These cameras use Wi-Fi (802.11) since it provides high bandwidth. Each camera has its own IPv6 address, and the video streams use UDP to keep them smooth, even if some frames are lost. Meanwhile, the older traffic lights still rely on IPv4 and Ethernet (802.3). When the control center sends commands like 'Turn Green', they use TCP, ensuring the instruction reaches safely without any errors. In this way, both modern cameras and older lights work together to manage traffic.

## Evening – Ambulance Emergency

- In the evening, an ambulance carrying a patient rushes to the hospital. The ambulance's system connects through LTE and uses its IPv6 address to stay connected to the traffic system. To clear its path, it sends an alert using XMPP at the application layer. The message is something like: 'Emergency vehicle approaching – clear route.' This alert reaches the traffic management system, which immediately turns all upcoming traffic lights green, creating a smooth corridor for the ambulance to pass quickly and save lives.



# Night – Self-Driving Cars and Toll Booths

- At night, self-driving cars move across the city streets. These cars use DDS (Data Distribution Service) to share real-time information. For example, if one car detects a slippery road, it instantly tells nearby cars: 'The road ahead is slippery!' The other cars receive this alert and slow down immediately, preventing accidents. Later, when a car reaches a toll booth, the system uses Wi-Fi to connect to the Internet. It sends the payment confirmation through TCP for reliability, using AMQP at the application layer. A secure message like 'Car ID 1234 – Payment successful' is sent to the bank to complete the transaction without errors.

# ✓ Summary of the Smart City Story

- From morning to night, the city runs smoothly because different IoT protocols work together. The Link Layer provides connectivity through Ethernet, Wi-Fi, ZigBee (802.15.4), LTE, and WiMax. The Network Layer makes sure every device has an address using IPv4, IPv6, and 6LoWPAN for compressed IPv6. The Transport Layer decides how data is carried, with TCP ensuring reliability and UDP ensuring speed. Finally, the Application Layer gives meaning to the data, with MQTT, CoAP, HTTP, WebSockets, XMPP, DDS, and AMQP handling specific roles. Together, these protocols create a smart city that saves energy, manages traffic, monitors pollution, guides ambulances, prevents accidents, and processes payments securely.

# Basics of LR-WPAN

- LR-WPAN – Low-Rate Wireless Personal Area Network
- It is IEEE 802.15.4 standard.
- Generally, It is operated at a 2.4 GHz ISM band. {868 MHz available in Europe and 915 MHz available in US}
- IEEE 802.15.4 is used for low-power wireless connectivity solutions like ZigBee, 6LOWPAN, and many more.
- It is operated at a low data rate with good performance of battery life.
- It is operated with lower distance communication {<100m}
- IEEE 802.15.4 defines the characteristics of the physical layer and MAC.



# Protocol Stack of IEEE 802.15.4

Application Layer	ZigBee, 6LOWPAN
Network Layer (Routing/ Network)	ZigBee, 6LOWPAN
Data Link Layer (MAC – CSMA/CA)	IEEE 802.15.4
Physical Layer (2.4GHz, 250kbps)	IEEE 802.15.4

- Media Access Control (MAC) is done by CSMA/CA (Carrier Sense Multiple Access Collision Avoidance).
- MAC defines medium access and flow control mechanisms.
- The Physical Layer defines operational frequency, transmission power, and modulation schemes.
- IEEE 802.15.4 utilizes a Direct Sequence Spread Spectrum (DSSS) coding scheme to transmit information.

# Understanding IEEE 802.15.4 with a Live Example

Smart Farming Case Study

# What is IEEE 802.15.4?

- A standard for Low-Rate Wireless Personal Area Networks (LR-WPAN)
- Foundation for ZigBee, 6LoWPAN, WirelessHART, Thread
- Provides low power, low cost, and low data rate communication
- Ideal for IoT devices like sensors and controllers

# Live Example: Smart Farming

- Soil moisture sensors placed across a farm
- Sensors send readings to a central controller
- Controller decides when to turn irrigation pump ON/OFF
- Communication happens via IEEE 802.15.4

# Devices Used

- Full Function Device (FFD):  
Controller/Gateway
  - - Acts as PAN coordinator
  - - Collects data and connects to Internet
- Reduced Function Device (RFD): Sensors
  - - Simple, battery-operated devices
  - - Send soil moisture readings

# Communication & Operation

- Frequency: 2.4 GHz (most common)
- Data rate: 40–250 Kb/s
- Sensors wake up, send data, then sleep to save energy
- Controller processes data → activates irrigation pump if soil is dry
- Uses CSMA/CA to avoid data collision

# Why IEEE 802.15.4 for IoT?

- Very Low Power – Long battery life for sensors
- Low Cost – Cheaper than Wi-Fi or Cellular
- Mesh Networking – Extended range via multiple nodes
- Perfect for Smart Homes, Agriculture, Industry, Healthcare

# Classroom Analogy

- Teacher = Controller (FFD)
- Students = Sensors (RFDs)
- Students speak only when they have something important
- They raise hands one by one (CSMA/CA)
- Teacher listens and takes action (pump ON/OFF)

# Summary

- IEEE 802.15.4 is the backbone for low-power IoT
- Enables efficient communication between small devices
- Ideal for scenarios like smart farming, smart homes, and healthcare
- Think of it as a low-power walkie-talkie for IoT devices

# IEEE 802.15.4 (LR-WPAN)

- Low-Rate Wireless Personal Area Network standard.
- Operates in 2.4 GHz frequency band with 40-250 Kbps data rate.
- Foundation for higher protocols like ZigBee.
- Designed for low-cost, low-power IoT devices.
- Max 100 meter

# Difference Between IEEE 802.15.4 and LR-WPAN

Explained with Smart Home Example

# Introduction

- IEEE 802.15.4: A standard defining PHY and MAC layers for low-power communication
- LR-WPAN: Low-Rate Wireless Personal Area Network built using IEEE 802.15.4
- Commonly used as the foundation for ZigBee, Thread, and 6LoWPAN networks

# What is IEEE 802.15.4?

- Defines PHY and MAC layers for LR-WPAN
- Specifies frequency bands (868 MHz, 915 MHz, 2.4 GHz)
- Data rates: 20 Kb/s to 250 Kb/s
- Uses CSMA/CA for channel access
- Responsible for reliable transmission and acknowledgment

# What is LR-WPAN?

- A wireless network built using IEEE 802.15.4 radios
- Includes devices: Full Function Devices (FFD) and Reduced Function Devices (RFD)
- Supports star, peer-to-peer, and mesh topologies
- Forms the basis for IoT applications like smart homes, healthcare, and agriculture

# Smart Home Example

- Smart bulbs = Reduced Function Devices (RFDs)
- Central hub = Full Function Device (FFD)
- Hub acts as PAN coordinator, controlling the network
- Bulbs send 'status ON/OFF' messages using IEEE 802.15.4 rules
- Together, hub + bulbs form LR-WPAN

# Key Difference

- IEEE 802.15.4 = The rules and technical standard (PHY + MAC)
- LR-WPAN = The actual network created using IEEE 802.15.4
- Example:
  - - IEEE 802.15.4 = English grammar rules
  - - LR-WPAN = A classroom conversation in English

# Summary

- IEEE 802.15.4 and LR-WPAN are related but not identical
- IEEE 802.15.4 defines how devices talk (PHY/MAC)
- LR-WPAN is the network where devices actually communicate
- Smart home lighting is a perfect example of LR-WPAN in action

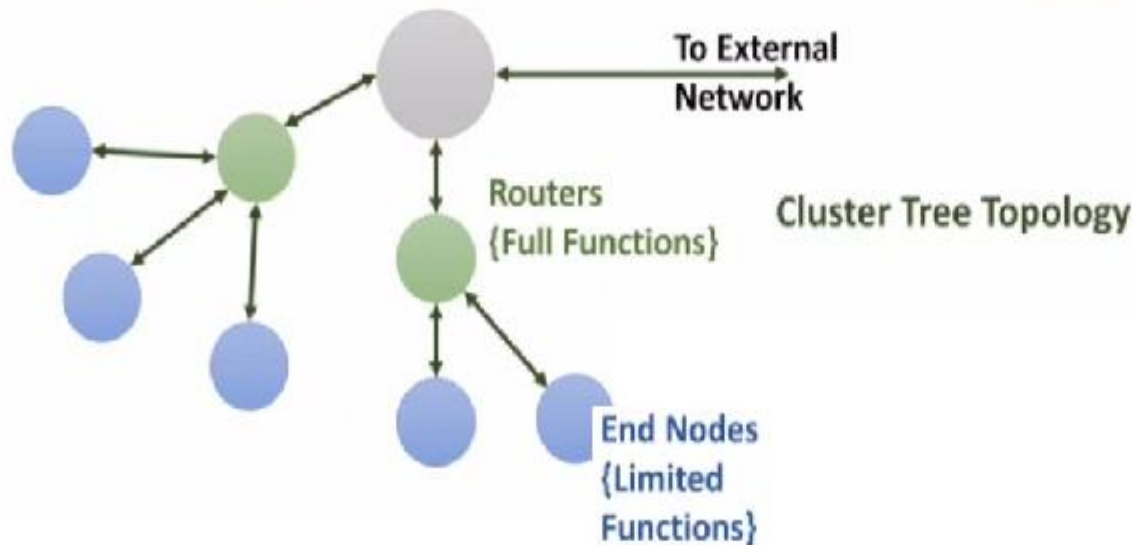
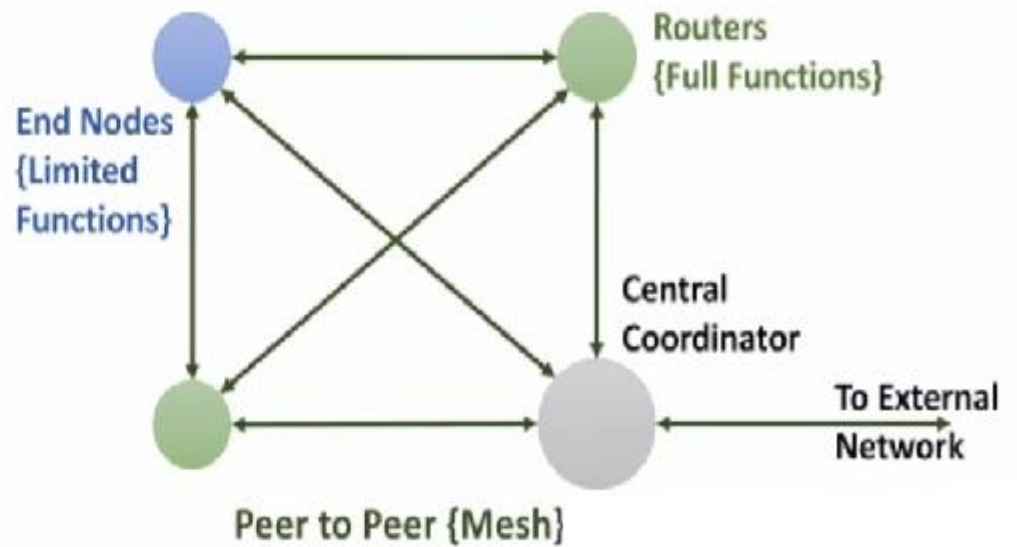
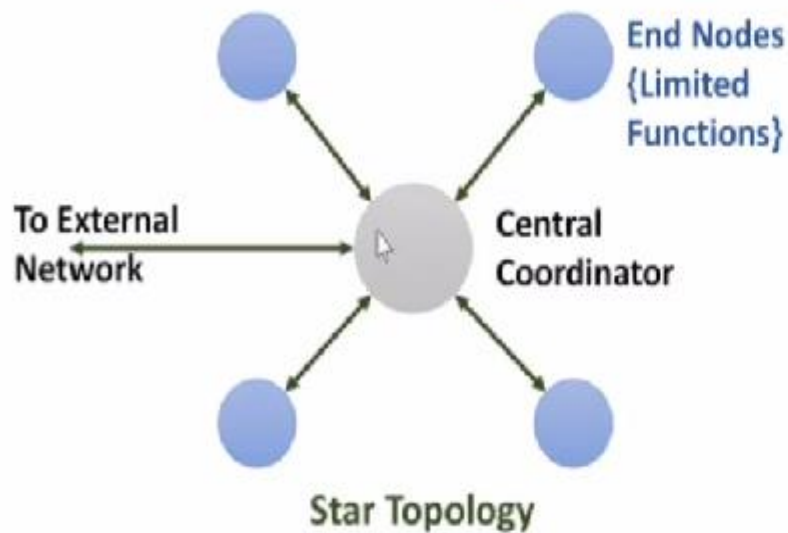
# Basics of ZigBee

- ZigBee is developed by ZigBee Alliance, ZigBee is a competitor of 6LOWPAN.
- ZigBee uses IEEE 802.15.4 at MAC and Physical Layer.
- ZigBee is designed for low-cost and low-power wireless IoT Networks.
- ZigBee is used in low data rate applications that requires long battery life and secure networking.
- ZigBee is simpler and less expensive than other WPANs such as Bluetooth and Wi-Fi.
- ZigBee operates at short range around 10m to 20m and using mesh networking range can be extended up to 500m.

# ZigBee

- **Built on IEEE 802.15.4 standard.**
- **Mesh networking, scalable and reliable for IoT.**
- **Used in home automation and industrial monitoring.**
- **Low data rate but very energy efficient.**
- **Uses ISM Band = Industrial, Scientific, and Medical band**
  - These are **radio frequency ranges** that are reserved internationally for **non-commercial use**, primarily for **industrial, scientific, and medical equipment**.
  - Later, they were also allowed for **short-range wireless communication** (like Wi-Fi, Bluetooth, ZigBee).
  - Devices can use these bands **without a license**, but they must follow power limits and technical regulations.

# Topologies used in ZigBee



# Understanding ZigBee with IEEE 802.15.4

Smart Home Example

# What is ZigBee?

- ZigBee is a wireless communication protocol built on IEEE 802.15.4
- Designed for low-power, low-data rate, and short-range applications
- Provides network and application layers above IEEE 802.15.4 PHY and MAC
- Supports star, tree, and mesh topologies
- Widely used in smart homes, industrial automation, and healthcare

# Why ZigBee?

- Extends IEEE 802.15.4 by adding routing and network formation
- Provides secure, reliable communication for IoT devices
- Operates in 2.4 GHz ISM band (global availability)
- Enables battery-powered devices to run for months or years
- Ideal for applications requiring many devices in a network

# Live Example: Smart Home Lighting

- Smart bulbs, switches, and sensors form a ZigBee network
- Devices communicate using IEEE 802.15.4 at the PHY/MAC level
- ZigBee provides network layer (routing, addressing) and application profiles
- Central hub acts as ZigBee coordinator
- Allows remote control of lights via smartphone app

# ZigBee Architecture

- Based on IEEE 802.15.4 PHY and MAC layers
- Adds Network Layer: handles routing, addressing, device discovery
- Adds Application Layer: defines profiles (Home Automation, Smart Energy)
- Device roles:
  - - Coordinator: Forms and manages the network
  - - Router: Forwards messages, extends range
  - - End Device: Low-power, communicates through router/coordinator

# How ZigBee Works

- Smart bulb sends ON/OFF status via IEEE 802.15.4 radio
- ZigBee network layer handles routing in mesh topology
- Coordinator receives status and forwards to hub/cloud
- Smartphone app communicates with coordinator through Internet
- Ensures reliable, low-power control of all devices

# Connection with IEEE 802.15.4

- IEEE 802.15.4 provides PHY + MAC (low-level communication)
- ZigBee adds Network + Application layers
- Together, they form a complete IoT stack for smart homes
- IEEE 802.15.4 = foundation, ZigBee = full system

# Analogy

- IEEE 802.15.4 = Local road (basic connectivity)
- ZigBee = Full city infrastructure (roads + traffic rules + buildings)
- Devices (cars) use the road but also need the city's structure to function
- ZigBee turns simple communication into a structured, functional network

# Summary

- ZigBee is built on top of IEEE 802.15.4
- Adds network and application layers for IoT use
- Example: Smart home lighting system
- Provides secure, reliable, and low-power communication
- IEEE 802.15.4 = base, ZigBee = complete IoT solution

# ZigBee Advantages and Disadvantages

A Comparison Overview

# Advantages of ZigBee

- ✓ Easy to install and implement
- ✓ Low cost, low power, and long battery life
- ✓ Supports many nodes (around 6500)
- ✓ More reliable and self-healing

# Disadvantages of ZigBee

- **X** Low data rate (250 kbps MAX)
- **X** Not as secure as Wi-Fi and Bluetooth
- **X** Requires additional devices (ZCs and ZRs), increasing cost
- **X** Lacks Internet Protocol support
- **X** Incompatible with other networks
- **X** Cannot communicate with Bluetooth or Wi-Fi

# Comparison: ZigBee Advantages vs Disadvantages

Advantages	Disadvantages
✓ Easy to install and implement	✗ Low data rate (250 kbps MAX)
✓ Low cost, low power, and long battery life	✗ Not as secure as Wi-Fi and Bluetooth
✓ Supports many nodes (around 6500)	✗ Requires additional devices (ZCs and ZRs), increasing cost
✓ More reliable and self-healing	✗ Lacks Internet Protocol support
	✗ Incompatible with other networks
	✗ Cannot communicate with Bluetooth or Wi-Fi

# Cellular Networks (2G, 3G, 4G, LTE)

- 2G: GSM, CDMA – 9.6 Kbps, basic IoT messaging.
- 3G: UMTS, CDMA2000 – improved speed for IoT.
- 4G/LTE: High speed up to 100 Mbps for video-enabled IoT.
- LTE-M and NB-IoT designed for IoT with low power wide area connectivity.

# WiFi, WiMax, Ethernet

- WiFi (802.11): High-speed wireless, used in smart homes, offices.
- WiMax (802.16): Wireless broadband access for IoT networks.
- Ethernet (802.3): Wired high-reliability connections in IoT systems.

# IPv4

- Internet Protocol version 4, most widely used until 2011.
- 32-bit addressing, total 4.3 billion addresses.
- Address exhaustion occurred due to rapid IoT and internet growth.
- Defined in RFC 791.

# IPv6

- Successor to IPv4 with 128-bit addressing.
- Supports  $3.4 \times 10^{38}$  unique addresses.
- Enables auto-configuration and improved security for IoT.
- Defined in RFC 2460.

# 6LoWPAN

- IPv6 over Low Power Wireless Personal Area Networks.
- Works with IEEE 802.15.4 link layer protocol.
- Uses header compression to fit IPv6 packets in small frames.
- Enables constrained IoT devices to use full IPv6 networking.

# Understanding 6LoWPAN with IEEE 802.15.4

Smart Streetlight Example

# What is 6LoWPAN?

- 6LoWPAN = IPv6 over Low-Power Wireless Personal Area Networks
- Adaptation layer that enables IPv6 to run on IEEE 802.15.4 networks
- Compresses IPv6 headers and fragments packets to fit 127-byte frames
- Allows IoT devices to connect directly to the Internet using IPv6

# Why 6LoWPAN is Needed

- IPv6 minimum packet size: 1280 bytes
- IEEE 802.15.4 frame size: only 127 bytes
- 6LoWPAN solves this mismatch by:
  - Compressing IPv6 headers (40 bytes → 2–3 bytes)
  - Fragmenting and reassembling large packets
  - Enabling billions of IoT devices to use IPv6

# Live Example: Smart Streetlights

- Streetlight controllers with sensors (light, motion)
- Each node uses IEEE 802.15.4 radios for local communication
- They form a LR-WPAN mesh network
- Central gateway collects data from nodes
- Problem: City wants IPv6 access for global monitoring
- Solution: 6LoWPAN compresses and adapts IPv6 for IEEE 802.15.4

# How 6LoWPAN Works

- Streetlight sensor sends IPv6 packet
- 6LoWPAN compresses and fragments the packet
- IEEE 802.15.4 transmits small frames over the air
- Gateway reassembles packets and forwards them as IPv6
- Each light has a unique IPv6 address → Accessible over Internet

# Connection with IEEE 802.15.4

- IEEE 802.15.4 provides PHY + MAC (radio and channel access)
- 6LoWPAN sits above it as an adaptation layer
- Together, they enable IPv6 on constrained IoT devices
- Foundation for higher protocols like RPL and CoAP

# Analogy

- IEEE 802.15.4 = Small rural road (narrow, low capacity)
- IPv6 = Big truck (large packet)
- 6LoWPAN = Logistic system that splits truck into smaller loads(Think of a bridge of certain capacity)
- Loads travel on small road with a bridge and get reassembled at destination

# Summary

- 6LoWPAN enables IPv6 over IEEE 802.15.4 networks
- Provides header compression and packet fragmentation
- Example: Smart streetlights sending data to city servers
- Connection: IEEE 802.15.4 (PHY/MAC) + 6LoWPAN (adaptation)
- Key enabler for large-scale IoT and Smart Cities

# TCP (Transmission Control Protocol)

- Connection-oriented, reliable transport protocol.
- Provides error detection, retransmission of lost packets.
- Ensures ordered delivery and congestion control.
- Used in email (SMTP), web (HTTP/HTTPS), file transfer (FTP).

# UDP (User Datagram Protocol)

- Connectionless, lightweight protocol.
- No guarantee of delivery, order, or duplicate elimination.
- Ideal for IoT applications needing speed and low overhead.
- Examples: sensor networks, video streaming.

# TCP vs UDP

- TCP: Reliable, ordered, but slower – best for critical data.
- UDP: Fast, low overhead, but unreliable – best for real-time IoT.
- Choice depends on IoT application requirements.

# HTTP (HyperText Transfer Protocol)

- Standard web protocol based on client-server model.
- Widely used but heavy for constrained IoT devices.
- RESTful APIs in IoT often use HTTP.
- Secure version is HTTPS.

# CoAP (Constrained Application Protocol)

- Specially designed for IoT constrained devices.
- Works like HTTP but based on UDP, lightweight.
- Supports RESTful communication.
- Example: Smart meters sending usage data.

# WebSockets

- Protocol for full-duplex, real-time communication.
- Maintains open TCP connection for instant data flow.
- Used in IoT dashboards, chat apps, stock tickers.
- Defined in RFC 6455.

# MQTT (Message Queue Telemetry Transport) - I

- Lightweight publish-subscribe messaging protocol.
- Clients connect to a broker and publish messages to topics.
- Other clients subscribe to topics to receive messages.
- Optimized for constrained devices and low bandwidth.

# MQTT (Message Queue Telemetry Transport) - II

- Broker manages message delivery between clients.
- Supports Quality of Service (QoS) levels for reliability.
- Ideal for unreliable networks with minimal overhead.
- Common in IoT telemetry and sensor networks.

# XMPP (Extensible Messaging and Presence Protocol)

- XML-based protocol for real-time communication.
- Supports messaging, presence detection, and data streaming.
- Originally for chat apps, now extended to IoT devices.
- Useful in device-to-device communication.

# DDS (Data Distribution Service)

- Data-centric publish-subscribe middleware standard.
- Supports scalable, high-performance real-time systems.
- Used in industrial IoT and mission-critical environments.
- Designed for low-latency data distribution.

# AMQP (Advanced Message Queuing Protocol)

- Open standard for message-oriented middleware.
- Ensures reliable message delivery and queuing.
- Used in finance, banking, and enterprise IoT integration.
- Supports message routing, queuing, and security.

# IoT Protocol Stack

- Link Layer: IEEE 802.15.4, WiFi, LTE, Ethernet.
- Network Layer: IPv4, IPv6, 6LoWPAN.
- Transport Layer: TCP, UDP.
- Application Layer: HTTP, CoAP, WebSockets, MQTT, XMPP, DDS, AMQP.
- Each layer builds on the lower one to enable IoT communication.

# Case Study: Smart Home Device Communication

- Smart sensor connects using ZigBee at Link Layer.
- IPv6 addressing provided via 6LoWPAN in Network Layer.
- Data sent using UDP for low overhead at Transport Layer.
- Application Layer uses MQTT broker to forward data to cloud.
- User views data in real-time on smartphone app.

# Summary

- Physical design of IoT explained through layered protocols.
- Link Layer: Connectivity standards for IoT devices.
- Network Layer: Addressing and routing (IPv4, IPv6, 6LoWPAN).
- Transport Layer: Reliable TCP vs fast UDP.
- Application Layer: Multiple protocols for IoT use cases.