

Chapter 4: IoT Reference Model

Purpose of the IoT Reference Model

IoT introduces both opportunities and challenges, especially in terms of:

- Interaction between “things” (devices),
- Levels of functionality,
- Security and interoperability.
- To handle this complexity:
 - A **Reference Model** is created to build a **common understanding** across the domain.
 - A **Reference Architecture** helps explain **core building blocks** needed to manage functionality, performance, deployment, and security.

A Reference Model defines **functional elements** and the **data flow** between them.

ITU-T (International Telecommunication Union – Telecommunication Standardization Sector) Reference Model

ITU's model includes:

- **4 main layers.**
- **Management and Security capabilities,** associated with all the layers.

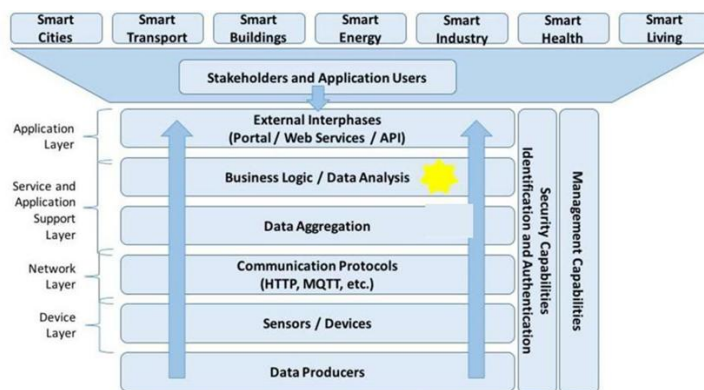
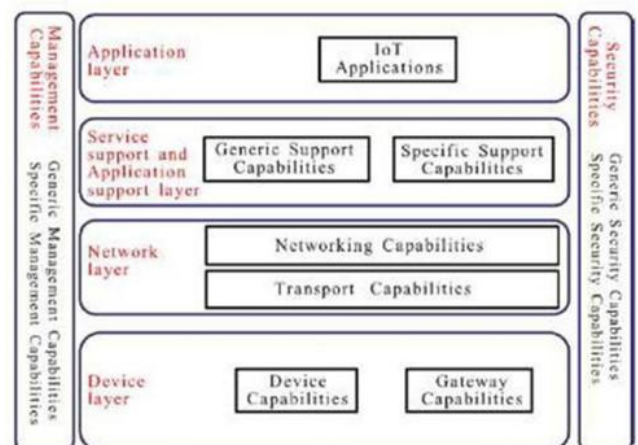


Figure 1. IoT Layered Architecture. Adapted from the ITU-T Reference Model [7]



The 4 Layers of the IoT Reference Model

1. Application Layer: This layer contains the **IoT applications** that serve the **end users**.

It **does not strictly define** what an application is — it's meant to be flexible and open-ended. It focuses on the **delivery of services** to users.

2. Service Support and Application Support Layer: This intermediate layer provides **common functionalities** needed to support IoT applications.

Capability Types:

- 1. Generic Support Capabilities:**
 - Common across different IoT apps.
 - Examples: data processing, data storage.
 - Can be used by or help build **specific capabilities**.

2. Specific Support Capabilities:

- Tailored to specific application requirements.
- Often divided into further **detailed groups** to serve different app needs (e.g., smart health vs smart farming).

3. Network Layer: Handles connectivity and data transfer.

Two Capability Types:

1. Networking Capabilities:

- Provide control functions for **network connectivity**.
- Includes: **access, authentication, authorization**.

2. Transport Capabilities: focus on providing connectivity for the transport of IOT service and application specific data information, as well as the transport of IoT-related control.

- Ensure data is transmitted reliably.
- Handles: -Transport of **IoT service/application-specific data**,
-Transport of **IoT-related control data**.
- Uses protocols like **HTTP, MQTT**, etc.

4. Device Layer: Responsible for data generation and basic communication.

Two Capability Categories:

a. Device Capabilities

- **Direct interaction:** Devices can communicate directly with the network (e.g., send/receive data). Devices are able to gather and upload information directly (without using gateway capabilities) to the communication network and can directly receive information (e.g., commands) from the communication network.
- **Indirect interaction:** Devices communicate **through a gateway**. Devices are able to gather and upload information to the communication network indirectly through gateway capabilities. On the other side, devices can indirectly receive information (e.g., commands) from the communication network.
- **Ad-hoc networking:** Devices form networks dynamically, useful for scalability. Devices may be able to construct networks in an ad-hoc manner in some scenarios which need increased scalability and quick deployment.
- **Sleeping/Waking-up:** Devices may enter low-power modes to save energy and wake up as needed.

b. Gateway Capabilities: Help bridge **devices** and **networks** with incompatible technologies.

Functions:

- **Multiple interfaces support:** Support wired (e.g., CAN bus) and wireless (e.g., ZigBee, Wi-Fi) communication.
- **Protocol conversion:**

- For different **device-level protocols** (e.g., ZigBee vs Bluetooth).
- For **device-to-network** protocol mismatches (e.g., ZigBee to LTE).

Management Capabilities: Used to **manage devices, networks, and applications**.

Two Types:

1. **Essential Generic Management Capabilities:**

- Remote device activation, diagnostics, software updates.
- Device working status management.
- Network topology management.
- **Traffic and congestion control:** Detect network overflow and reserve resources for critical data flows (e.g., healthcare).

2. **Specific Management Capabilities:**

- Linked to particular application requirements.
- Example: **Smart grid** needs constant powerline monitoring.

Security Capabilities: Security is layered and involves both generic and specific protections.

Types of Security Capabilities:

1. **Generic Security Capabilities** (application-independent):

- **Application Layer:** Authorization, authentication, data confidentiality/integrity, privacy, audits, antivirus.
- **Network Layer:** Authorization, authentication, signaling/data integrity, confidentiality.
- **Device Layer:** Device authentication, access control, data protection, integrity validation.

2. **Specific Security Capabilities:** Designed for particular threats or app scenarios.

Chapter 5: Communication Theory

Motivation

- IoT is **not just sensors** — it's about **transporting sensor data** from remote locations to the cloud.
- Wireless transmission is vital, and understanding **radio frequency (RF)** fundamentals is key to implementing reliable systems.
- Understanding **signal behaviors, interference, range, and protocols** is essential for IoT communication success.

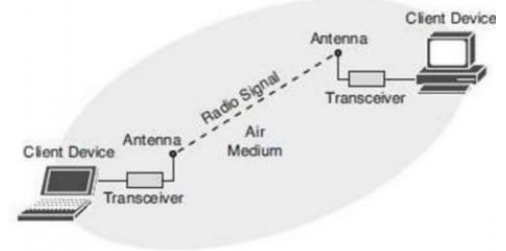
I. Radio Frequency (RF)

What is RF?

RF = oscillations in the range of **20 kHz to 300 GHz**.

Data is **modulated** onto a carrier signal for transmission and **demodulated** at the receiver.

Transmission occurs between **transmitter antenna** and **receiver antenna**.



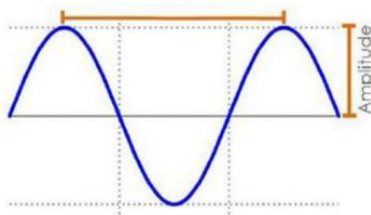
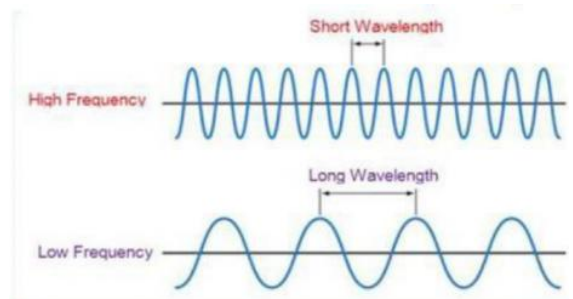
Key RF Characteristics:

1. **Frequency** – measured in Hertz (Hz); determines how often a signal cycle occurs.

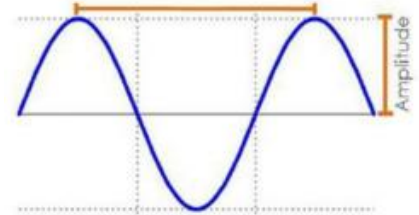
- 1 MHz = 1 million cycles/sec; 1 GHz = 1 billion cycles/sec.
- Example: Wi-Fi uses 2.4 GHz and 5.8 GHz.

2. **Wavelength (λ)** – distance between the start of one cycle and the next.

- $\lambda = \text{speed of light (300,000,000 m/s)} \div \text{frequency}$.
- Higher frequency $\Rightarrow$ shorter wavelength.
- E.g., at 900 MHz, $\lambda \approx 33.3$ cm.



Calculating Wavelength for 900MHz
 $\text{Lambda (wavelength)} = \text{Velocity} / \text{Frequency}$
 $= 300,000,000 \text{ (m/s)} / 900,000,000/\text{sec}$
 $= .33 \text{ m (33.3 cm) or approximately 13 inches}$

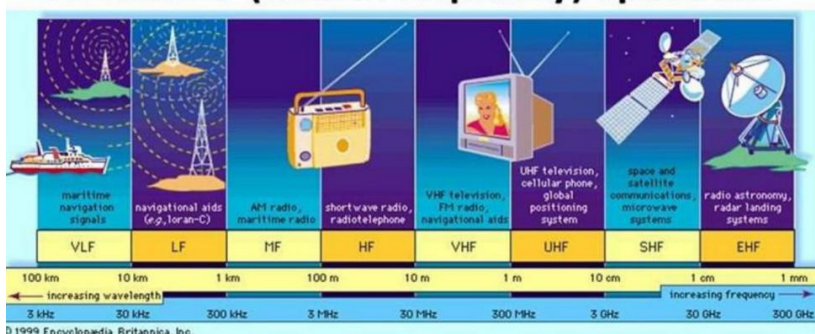


3. **Amplitude** – peak of the wave; related to **signal power**.

Real-World RF Considerations:

- Ideal RF path: **unobstructed line-of-sight**.
- Real world: **obstructions, signal reflections, noise, and interference**.
- RF regulations vary by country.
 - E.g., US uses ISM bands at 900 MHz, 2.4 GHz, 5.8 GHz.

General RF (Radio Frequency) Spectrum



0.003 MHz	Very Low Frequency (VLF)
0.03 MHz	Low Frequency (LF)
0.3 MHz	Medium Frequency (MF)
3 MHz	High Frequency (HF)
30 MHz	Very High Frequency (VHF)
300 MHz	Ultra High Frequency (UHF)
3 000 MHz	Super High Frequency (SHF)
30 000 MHz	Extra High Frequency (EHF)
300 000 MHz	

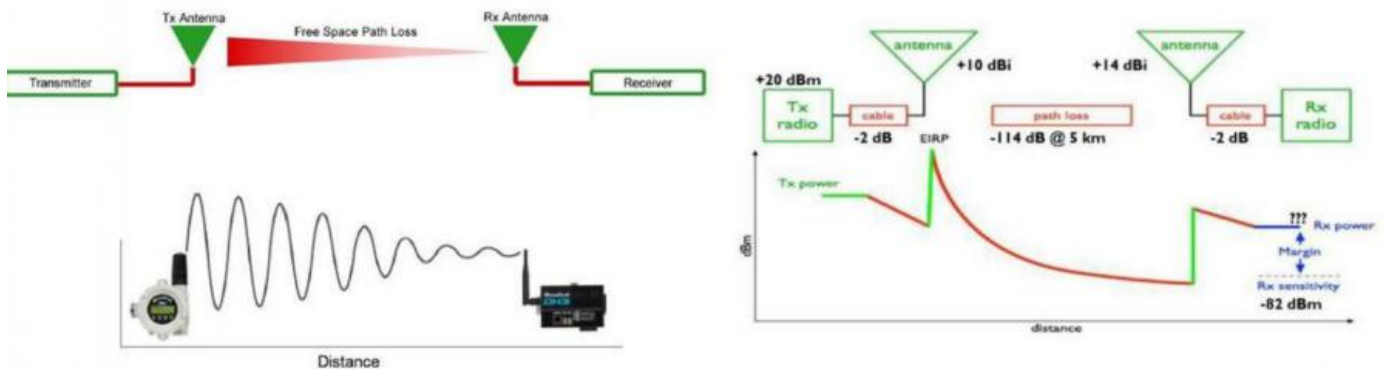
II. Link Budget

Purpose:

- Determines if a wireless system **will function correctly**.
- Calculates **all gains and losses** in the path from transmitter to receiver.

Link Budget Formula:

Received Power (dBm) = Transmitted Power (dBm) + Gains (dB) – Losses (dB)



Components:

1. **Transmitter Output Power:** Varies by device & regulations (e.g., 10 dBm for battery devices, 30 dBm in licensed systems).
2. **Transmitter Loss:** From cables, connectors, etc. (e.g., 4.3 dB loss).
3. **Antenna Gain**
 - Expressed in **dBi**, relative to an isotropic antenna.
 - Omni-directional vs directional antennas (e.g., 3 dBi gain).
4. **Free Space Path Loss (FSPL)**
 - Signal loss over distance due to geometric spreading:

$$\text{FSPL (dB)} = 92.45 + 20 \cdot \log(d \text{ in km}) + 20 \cdot \log(f \text{ in GHz})$$

or

$$\text{FSPL} = 36.56 + 20 \cdot \log(f \text{ in MHz}) + 20 \cdot \log(d \text{ in miles})$$

5. **Receiver Antenna Gain:** Also measured in dBi (e.g., +3 dBi).
6. **Receiver Loss:** Again due to cables/connectors (e.g., -4.3 dB).
7. **Received Signal Strength:** Computed from above values (e.g., -82.6 dBm).
8. **Receiver Sensitivity**
 - Minimum power level detectable by receiver (e.g., -110 dBm).
 - The **lower (more negative)**, the better.

9. Fade Margin

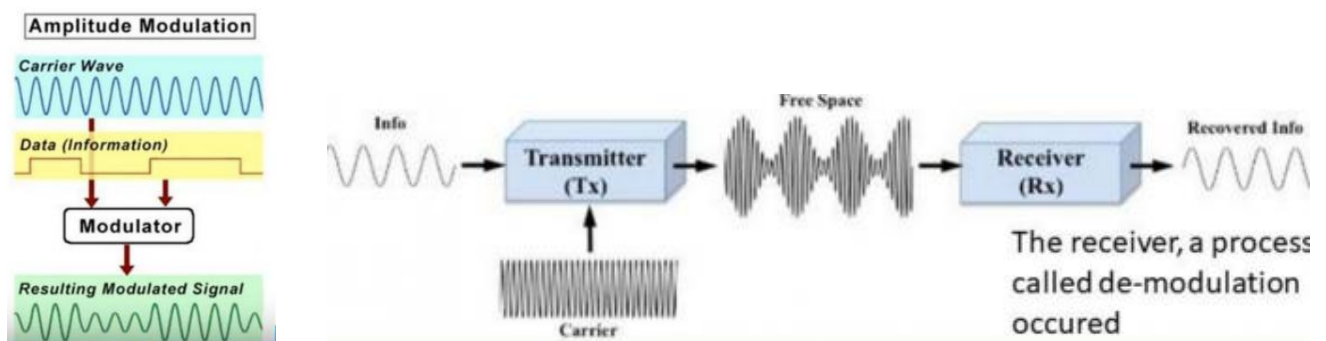
- Extra buffer (e.g., 20 dB) for **rain, terrain, or interference**.
- Helps ensure **reliable communication**.

III. Transmitter Basics

- A **transmitter (TX)** converts electronic signals into **modulated RF signals**.
- The **carrier signal** is modulated with the information signal (e.g., voice, data).
- Types of modulation:
 - **Amplitude Modulation (AM)** – varies wave height.
 - **Frequency Modulation (FM)** – varies wave frequency.

IV. Modulation / Demodulation

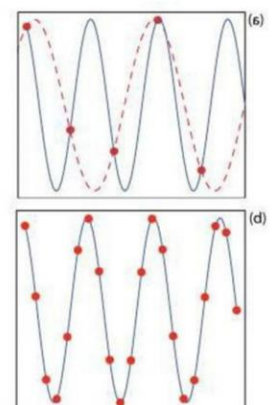
- **Modulation:** Combines the information signal with a high-frequency **carrier wave**.



- **Demodulation:** Extracts original info at the receiver.
- Purpose:
 - Efficient **long-distance transmission**.
 - Allows **multiplexing** (multiple signals in same bandwidth).

V. Sampling

- Instead of sending a continuous analog signal, only **samples** are taken and transmitted.
- These samples **reconstruct the original signal** at the receiver.



VI. Nyquist Theorem: A signal must be sampled at **more than twice** its **highest frequency component**.

Example: Human hearing: up to 20,000 Hz, Therefore, CD audio is sampled at **44.1 kHz**.

VII. Bit Error Rate (BER)

- **BER** = (# of incorrect bits received) ÷ (total bits transmitted).
- Affected by: **Noise, fading, interference, signal loss**.
- Example: Sent: 1010110100 Rec'd: 0010101010 → BER = 5 errors / 10 bits = 50%

Improving BER:

1. **Increase transmission power**
2. **Improve receiver sensitivity**
3. **Forward Error Correction (FEC):** Adds redundancy so receiver can fix errors. Example: triple redundancy + majority vote.

Summary Chart

Concept	Key Points
RF	Signals modulated over frequency; range 20 kHz–300 GHz
Link Budget	Calculates signal strength through all components
Modulation	Combines data with a carrier wave
Sampling	Digital approximation of analog signal
Nyquist Theorem	Sample rate > 2× highest signal frequency
BER	Measures transmission errors; improved by FEC

Chapter 6: Protocols

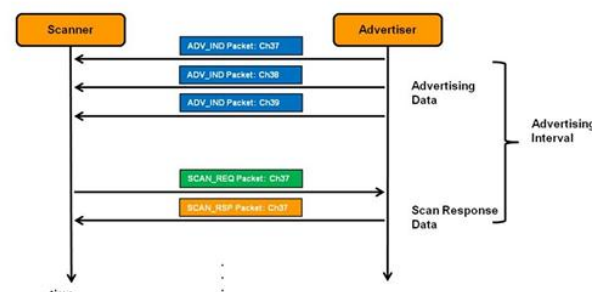
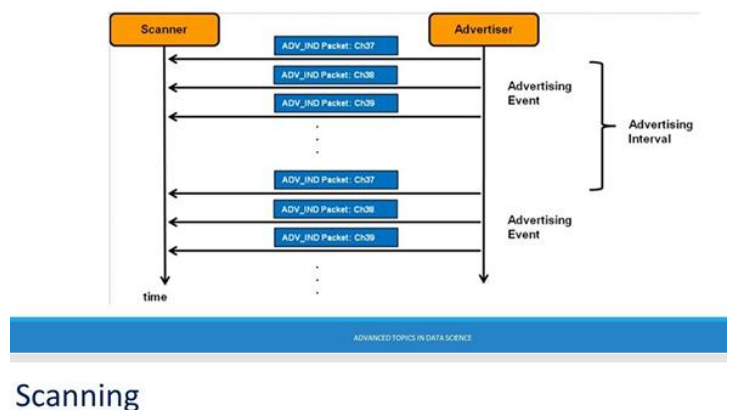
◆ Non-IP Based Wireless Protocols (WPAN)

WPAN = **Wireless Personal Area Networks** – short-range communication (a few meters), low power. Examples include Bluetooth, Zigbee, and Z-Wave.

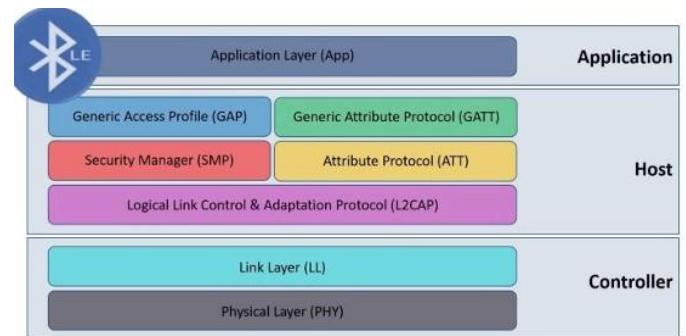
Advertising

1. Bluetooth 5.0

- **Key improvements:**
 - 4× range (~200m)
 - 2× speed (up to 2 Mbps)
 - 8× broadcasting capacity
 - Low Energy (BLE) mode for power efficiency (battery life up to 4–5 years)
- **Modes:**
 - **Advertising:** Sends packets for others to receive
 - **Scanning:** Listens for those packets
 - **Initiating:** Scanning + connecting
 - **Connected:** Master/slave communication



- **Standby:** No communication
- **Architecture:**
 - **PHY layer** (modulation in 2.4 GHz band, 40 channels) Controller
 - **Link Layer** (handles roles like advertiser, scanner, master/slave, CRC checks)



- **Discovery Process:** Involves repeated advertisement on 3 channels (Ch37, Ch38, Ch39). Scanners pick up these packets to connect.
- **Interference Handling:** Uses **frequency hopping** at 1600 hops/sec to avoid Wi-Fi and other Bluetooth interference.

2. Zigbee

- **Purpose:** Short-range, low-data-rate, **low-power** protocol for **control and sensor networks**.
- **Frequencies:** 2.4 GHz, 900 MHz, 868 MHz
- **Applications:** Home automation, medical data collection, industrial control
- **Network Components:**
 - **ZC (Coordinator):** Forms network, assigns channel, authenticates devices
 - **ZR (Router):** Forwards data; always on (not good for battery-powered devices)
 - **ZED (End Device):** Simple devices (e.g., light switch); only sends/receives via router
- **Channel Access:**
 - **Contention-free (GTS):** Time slot assigned
 - **Contention-based:** Uses **CSMA** to avoid collision
- **Topologies:**
 - **Star:** Simple, no routers
 - **Mesh:** Reliable, self-healing (data hops node to node)
 - **Tree:** Hierarchical, limited routing
- **Key Features:**
 - Up to 100m indoor, 300m LoS
 - 250 kbps speed
 - AES encryption
 - Fast join time (~30ms)
 - Supports 65,000 devices theoretically

3. Z-Wave

- Alternative to Zigbee; also mesh-based
- **Closed protocol** (ensures full device compatibility)
- **Greater range** (~100m), but **supports fewer devices** (~200+)
- **Frequencies vary by region**, limiting global portability
- Ideal for **home automation**, sensors, and control
- Data speed: **up to 100 kbps**

IP-Based Protocols

Why use IP?

- Compatibility with the internet
- No need for gateways when linking with other IP systems

4. 6LoWPAN

- **IPv6 over Low Power Wireless Personal Area Networks**
- Designed for small, low-power devices using **IEEE 802.15.4**
- Enables **direct Internet connectivity** using **compressed IPv6**
- **Edge Router** functions:
 - Compresses IPv6 headers (from 40 bytes down to 2–20 bytes)
 - Starts the network
 - Communicates with other devices and internet

5. Thread

- Built on **6LoWPAN** and **IEEE 802.15.4**
- Targeted at **home automation**
- Uses **mesh topology**
- Supports **250 devices**
- **AES encryption** built-in
- IP addressable — more scalable, secure
- Doesn't require keeping application state — saves power

6. Wi-Fi (IEEE 802.11)

- High-speed, high-bandwidth WLAN standard
- **Topologies:**

- **Infrastructure (BSS):** With central Access Point
- **Ad-hoc (IBSS):** Peer-to-peer, no AP
- **Distribution System (DS):** Multiple APs linked
- Common in homes and offices for general internet connectivity

Long-Range Protocols

7. 5G

- The latest mobile network technology
- **Speed:** Much faster than 4G
- **Latency:** Extremely low (1 ms vs 30 ms in 4G)
- **Connection types:**
 - **Macro Cells:** Wide area
 - **Small Cells:** For buildings, streets
- **Frequency bands:**
 - **Below 6 GHz** for broad coverage
 - **mmWave (26–28 GHz)** for high speed and capacity
- **Massive MIMO:**
 - 100+ antennas per tower for simultaneous high-speed connections
- Powers IoT, smart cities, autonomous vehicles

MQTT (Message Queuing Telemetry Transport)

- **Lightweight, publish-subscribe protocol**
 - Ideal for **IoT**, where devices have **limited power/bandwidth**
 - **How it works:**
 - Devices (clients) **publish** or **subscribe** to topics
 - **Broker** filters, routes messages to interested clients
 - **Benefits:**
 - Efficient bandwidth usage
 - Low update latency
 - Great for sensor communication
 - Scalable and reliable
-

Final Takeaways

- **Bluetooth, Zigbee, and Z-Wave** are optimized for short-range, low-power IoT uses.
- **6LoWPAN and Thread** bridge IoT with the internet via IPv6.
- **Wi-Fi and 5G** support higher speeds and longer distances, suitable for bandwidth-heavy applications.
- **MQTT** enables efficient and scalable communication among IoT devices.