VTU 21 Scheme

Internet of Things (21CS3657)

Module-4

IoT Connectivity Technologies: Introduction, IEEE 802.15.4, Zigbee, Thread, ISA100.11A, WirelessHART, RFID, NFC, DASH7, Z-Wave, Weightless, Sigfox, LoRa, NB-IoT, Wi-Fi, Bluetooth

Module 4 Handwritten

IoT Connectivity Technologies

- IOT Connectivity Technologies are communication protocols & standards that enable devices within IOT ecosystem to communicate, exchange data, and collaborate effectively.
- These technologies act as bridges allowing sensors, actuators & processing units to connect, share info & take coordinated actions.
- Commonly connectivity technologies include Wifi, Bluetooth, Zigbee, LoRa, NB-IoT & many others, each offering different features to meet specific needs in terms of range, power consumption, data rate & network size.

- Why are IOT Connectivity Technologies important ?
  1) seamless communication.
  2) Adaptability & Scalability
  3) Efficient Data Processing
  4) Power Management
  5) Device Compatability & Interoperability.

IEEE 802.15.4 -

- The IEEE 802.15.4 standard is widely adopted framework for low data rate wireless PAN, primarily used in IOT applns requiring lower power & moderate data transmission needs.
- Developed to support monitoring & control applns, it enables energy efficient communications. (low power)
- This standard uses only two first layers - Physical & datalink for operation along with two new layers
  - Logical link control (LLC) -
  - Service specific convergence sublayer (SSCS).

- IEE 802.15.4 standard supports 2 primary topologies,
  - Star Topology where devices connect to a central coordinator.
  - Mesh Topology which allows decentralized communication across nodes which is ideal for more extensive networks.

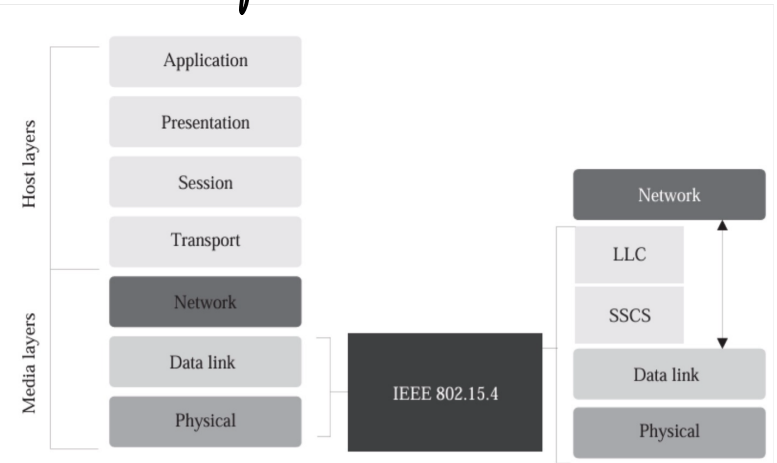


Fig: The operational part of IEEE 802.15.4s protocol stack in comparison to the OSI stack

- Comparing to the OSI Model, we have 2 extra layers which facilitate communication with higher layers.
- The direct sequence spread spectrum (DSSS) modulation technique is used in IEEE 802.15.4 for communication purposes, enabling a wider bandwidth of operation with enhanced security by modulating pseudo-random noise signal.
- This standard exhibits high tolerance to noise & interference and offers better measures for improving link reliability.
- Frequency Band - operates in ISM band (Industrial, Scientific & Medical) ensuring global applicability.
- Modulation Techniques for low speed is BPSK (Binary Phase Shift Keying) and for high speed is Offset Quadrature Phase shift keying (OQPSK) for encoding the msg which needs to be communicated.
- CSMA-CA is the channel access method used for maintaining the sequence of transmitted signals & prevent deadlocks.

- It utilizes infrequently occuring & very short packet transmission with a low duty cycle (typically < 1%) to minimise the power consumption.
  - Typical transmission power - 3 dBm (0.05mW)
  - Transmission Range - 10-75m (indoor), 1000m (outdoor).
- There are 7 variants identified with IEEE 802.15.4 -
  - Variant A / B = Base versions
  - Variant C = china assigned.
  - Variant D = Japan assigned
  - Variant E, F, G = Industrial Applications.

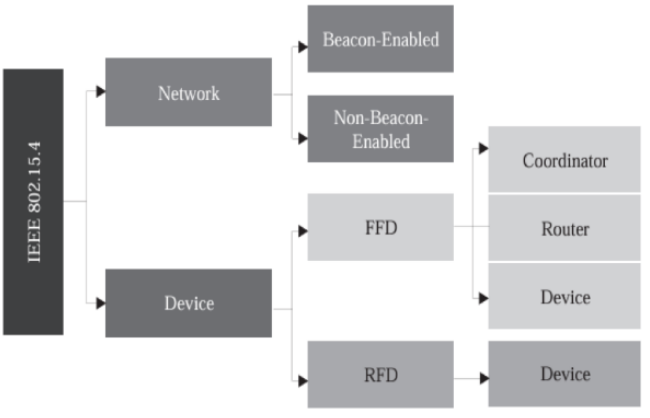


Fig: The various device and network types supported in the IEEE 802.15.4 standard

- Network types supported in IEEE 802.15.4 standard are,

i) Beacon Enabled Network
  - uses a PAN coordinator to manage synchronisation & timing.
  - frames sent using slotted CSMA/CA within a superframe structure.

ii) Non Beacon Enabled Network
  - uses unslotted CSMA/CS for contention based communication.
  - requires IDs of source & destination nodes.

- The IEEE 802.15.4 standard supports two types of devices,

i) Full Functional Devices (FFD) - FFDs can talk to all types of devices & support full protocol stack. These devices are costly & energy consuming due to increased requirements for support of full stacks.

ii) Reduced Function Device (RFD) - RFDs can only talk to an FFD & have lower power consumption requirements due to minimal CPU/RAM requirements.

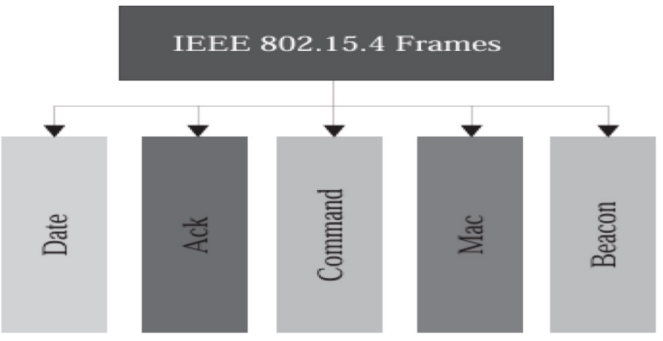


Fig: Various frame types supported in the IEEE 802.15.4 standard

- Frame Types in IEEE 802.15.4 -

i) Beacon frames - used for signalling & synchronization in beacon enabled networks.

ii) Data Frames - carry user data from source to destination nodes.

iii) Acknowledgement (Ack) Frames - confirm the successful reciept of a frame.

iv) MAC Frames - handle low layer tasks like addressing & channel access.

v) Command Frames - facilitate network management tasks, including association, disassociation & coordinator realignment.

Zigbee :-

- Zigbee is a wireless communication protocol designed for lower power, low data rate WPANs, using the IEEE 802.15.4 standard for its PHY and MAC layers.
- Lower Power & cost - Designed for energy efficient operation & cost effectiveness. Typically range is 10-100 meters with mesh configuration extending the network.
- It operates primarily at 250 kbps for data transfer.
  Frequencies - 2.4 GHz - 16 channels at 250 kbps.
  - 868.3 MHz - 1 channel at 20 kbps.
  - 902-928 MHz - 10 channels at 40 kbps.

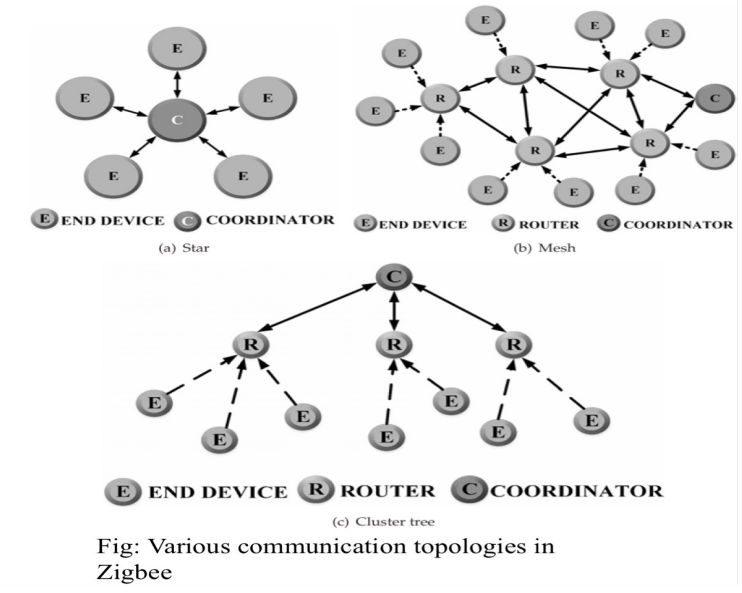


Fig: Various communication topologies in Zigbee

- Zigbee supports various network configurations such as Master to Master communication or Master to Slave communication. Several network topologies are supported in Zigbee, namely Star, Mesh & Cluster Tree.
- In Star topology, a coordinator initiates & manages the other devices in Zigbee network. The other devices which communicate with coordinator are called End Devices. As the star topology is easy to maintain & deploy.

- The Zigbee Mesh & Tree topologies by using multiple routers where the root of the topology is the coordinator. These configurations allow any Zigbee device or node to communicate with any other adjacent node.
- In a Zigbee Cluster Tree network, a coordinator is placed in the leaf node position of the cluster, which is intun, connected to a parent coordinator who initiates the entire network.

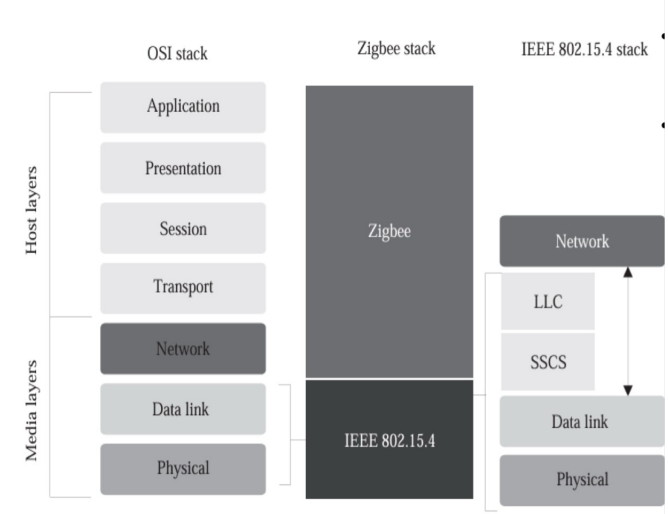


Fig: The Zigbee protocol stack in comparison to the OSI stack

ZigBee Protocol Stack VS OSI Stack

i) Physical Layer
- performs signal transmission / reception & modulation & demodulation.
- supports multiple frequency bands & channels for flexibility.

ii) MAC layer
- ensures reliable commn using CSMA-CA to avoid channel interference.
- manages syncheonisation via beacon frames.

iii) Network layer — handles network setup, device manag & routing. manages device connectn & commtn pathways.

iv) Application Support Sub layer — acts as bridge b/w network & appln layers. enables service matching, data management & Zigbee device operation.

v) Application Framework — key value pairs, generic messages.

Thread

- Thread is built upon the IEEE 802.15.4 radio standard, it is used for extremely low power consumption & low latency deployements.
- Thread removes the need for a mobile phone or proprietary gateway to be in range of devices for accessing the Internet.
- It is specially designed for IOT with the need for interoperability, security, power & architecture addressed in a single radio platform.
- IP Based Connectivity - Uses IPV6 for universal internet support, allowing devices to connect directly to internet or cloud without proprietary gateways. It simplifies device commtn, making it scalable for IOT ecosystems.
- Reliability & Self Healing - Mesh architecture supports self healing & configuration during device additions or removals, reducing single points of failure.
- Ideals for Smart Homes, Smart Buildings, Industrial IOT.

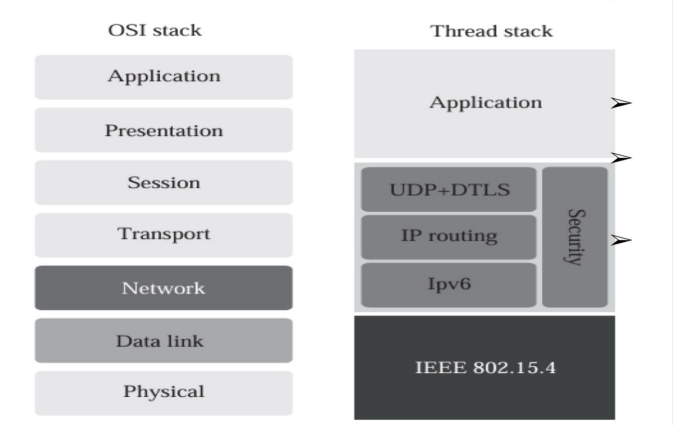


Figure The functional protocol stack of Thread in comparison to the OSI stack

· Thread Protocol Stack vs OSI stack -

- Application layer - Direct commⁿ b/w devices & applications.
- Transport layer - Uses UDP with DTLS for lightweight & secure data transport.
- Network layer - Implements IPV6 for universal internet connectivity, supporting IP routing.
- Data link & Physical layers - Built on IEEE 802.15.4 for low power, low latency communication.

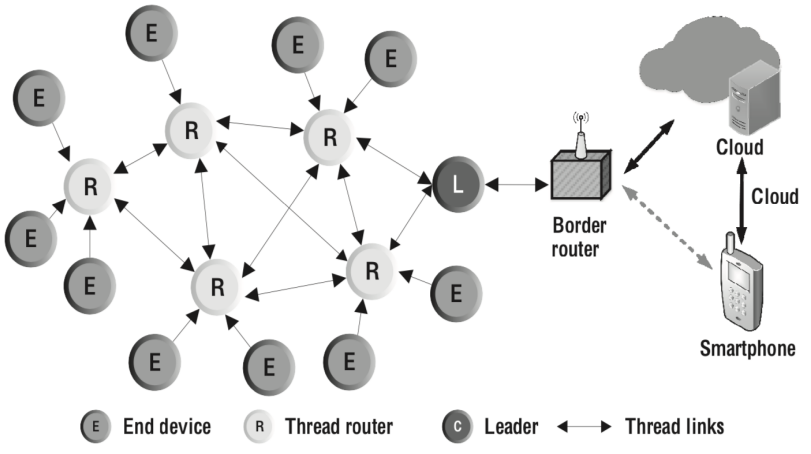


Figure 7.7 Outline of the Thread network architecture (from end devices to the cloud)

· Thread Network Architecture

i) Device Types

· End Device (E) - low power devices that communicate only with their parent router.

- Thread Router (R) - Routes msgs b/w devices & maintains connectivity.
- Leader (L) - Manages network operations, selects routers, & assigns addresses.
- Border Router - Connects Thread networks to external networks like Internet or cloud.
- Devices connect using Thread links, forming a mesh network.
- Cloud Integration - Supports direct comm^{n} with smartphones & cloud over IP networks.
- Devices can interact with smartphones, computers & other IP based systems without additional configuration, provided they share the same IP network.

ISA100.11A

- The ISA100.11A is a very low power communication standard & has been developed & managed by ISA (International Society of Automation).
- The standard was mainly proposed for Industrial plant Automation systems.
- The ISA100.11A is characterized by an IOT compliant protocol stack, which can also be integrated with wired networks using Ethernet, support for open access protocols & device level interoperability.
- Features
  - low power & high Security
  - IPV6 and UDP Support.
  - Flexible Topologies
  - Industrial Use Cases.

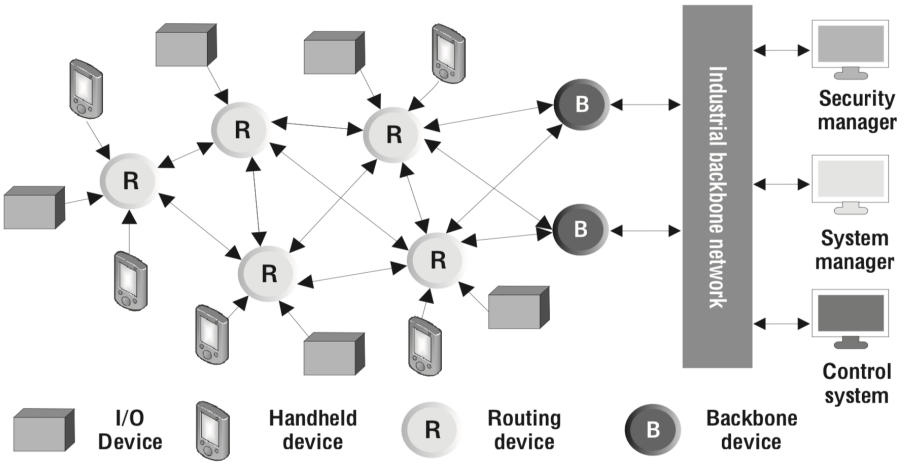


Figure 7.8 A typical ISA100.11A network architecture

ISA 100.11A Network Architecture -

i) Components include Field Devices include non-routing I/O devices, handheld devices & routing devices. It supports fixed & mobile deployements for flexibility in industrial plants.

- Backbone devices comprise routers, gateways, system managers & security managers. The fixed infaustructure connects the wireless network to industrial backbone.

ii) Downlink (DL) subnet refers to connected devices in the ISA100.11A network.

iii) Integration has WISN gateways bridge the ISA100.11A wireless network with the plant network.

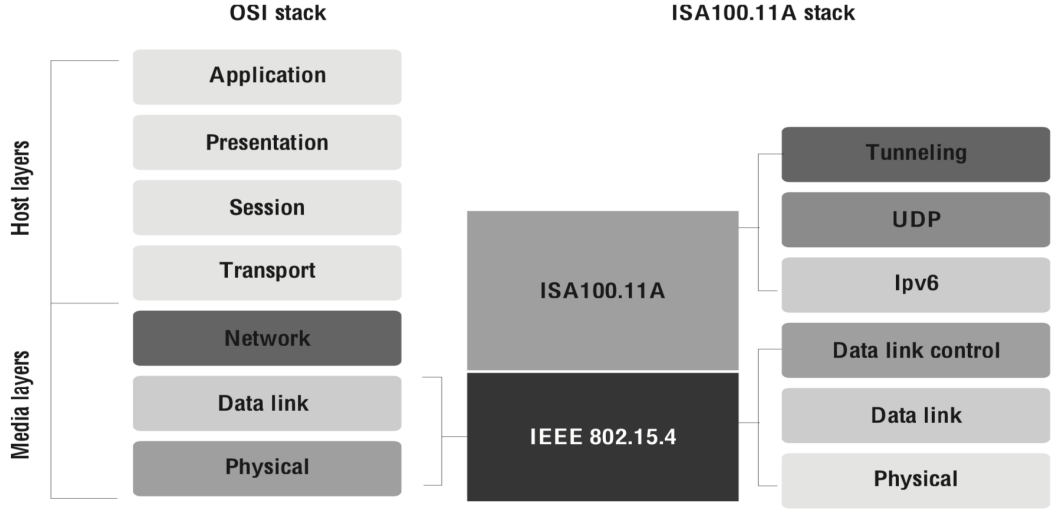


Figure 7.9 The ISA100.11A protocol stack in comparison to the OSI stack

i) Physical layer
- Based on IEEE 802.15.4 operates on 2.4 GHz frequency band. It uses DSSS modulation for reliable communication.

ii) Data link layer
- ensures packet creation, maintainence & forwarding.
- support adaptive channel hopping, error detection, and clock synchronization.
- includes data link control (DLC) for graph based routing.

iii) Network layer
- compliant with 6LOWPAN, enables IPV6 to 6LOWPAN protocol conversion.
- manages end to end routing using IPV6.

iv) Transport layer
- implements UDP for connectionless communication.

v) Application layer
- focuses on system management applications for industrial operations.

Wireless HART -

- Wireless HART can be considered as the wireless evolution of the highway addressable remote transducer protocol.
- It is a license free protocol, which was developed for networking smart field devices in industrial env.
- Key Features -
  - Wireless Adaptation
  - Reliability & Security
  - Mesh Network
  - Time Synchronized communication.

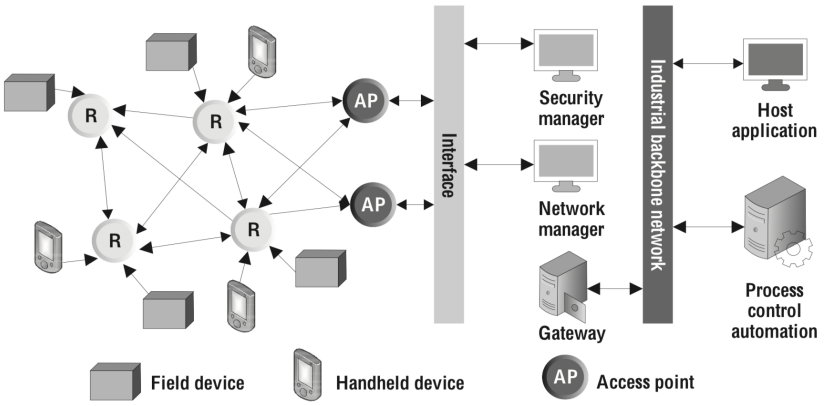


Figure 7.10 The WirelessHART network architecture

- Wireless HART Network Architecture -

i) Core Components :

- Field Devices - Measure & transmit process data.
- Gateways - Acts as a bridge to control system & backbone.
- Access Points - enhance network connectivity.
- Network Manager - centralizes control, scheduling & security.
- Security Manager - enforces secure communication.

ii) Topologies :

- primarily mesh based for high reliability.

iii) Interference Management :

- channel switching ensures minimal collisions & co-channel interfaces.

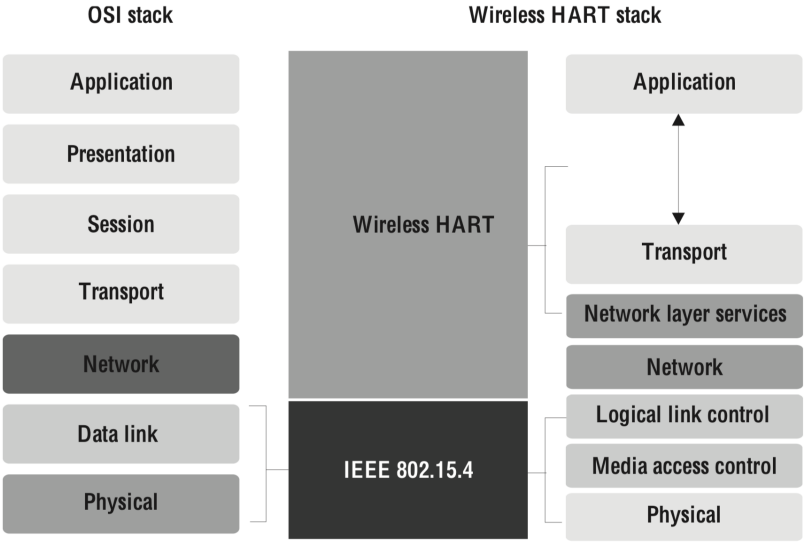


Figure 7.11 The WirelessHART protocol stack in comparison to the OSI stack

- Wireless HART Protocol Stack vs OSI Stack -

i) Physical layer - operates on 2.4 GHz frequency band with 15 channels for reliability. It incorporates channel hopping & channel backlisting to avoid interference.

ii) Data link layer - It implements TDMA for deterministic comm^n.
- Uses superframes grouped into time slots to synchronize transmissions.

iii) Network & Transport layers - handles routing, traffic manag, security & session control. It maintains a network graph for routing paths.
- supports mesh based open with all nodes capable of forwarding data.

iv) Application layer - provides seamless interfacing with legacy HART devices.
- Manages comm^n via command & response msgs b/w devices & gateways.

- Wireless HART's integration of reliability, security & compatibility with existing systems makes it ideal for industrial process control & automation.
- It is particularly suited for environments where traditional wired solutions are impractical.

RFID - (Radio Frequency Identification Device) -

- RFID enables wireless data capture & object categorization using RFID tags & readers. Unlike barcodes, RFID does not require a line of sight, making it more versatile in various applications.
- RFID Tags contains an integrated circuit & antenna enclosed in protected casing.
  - Passive Tags are powered by RFID reader, cost effective.
  - Active Tags are equipped with their own power source for extended range & functionality.
- RFID Reader (Interrogator) - It reads the data from tags via radio waves & transmits it to host system.
- Antenna facilitate communication b/w tags & reader.

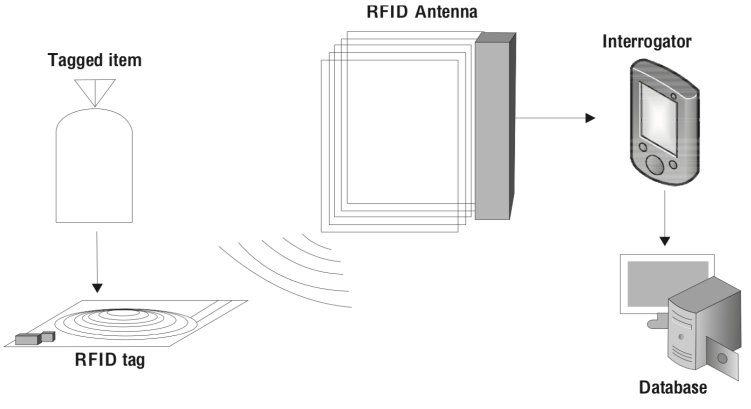


Figure 7.12 An outline of the RFID operation and communication

- How RFID works ?
  - RFID reader emits radio waves to detect & power tags.
  - Tags respond by transmitting their encoded data back to the reader.
  - Reader converts radio signals into digital data for processing.
  - Data is sent to a host system (via Wifi, Ethernet etc) & updated in a database.

- Applications -

i) Inventory management.
ii) Asset Tracking.
iii) Personnel Tracking.
iv) Supply Chain Management.

NFC (Near Field Communication) -

- NFC was jointly developed by Phillips & Sony as short range wireless connectivity standard, enabling peer to peer (P2P) data exchange network.
- Communication b/w NFC devices is achieved by the principle of magnetic induction, whenever the devices are brought close to one another.
- NFC can be used with other wireless technologies such as WiFi after establishing & configuring P2P networks.
- The typical NFC operating frequency for data is 13.56 MHz which supports data rates of 106, 212 or 426 Kbps.
- A small electric current is emitted by NFC Reader, which creates a magnetic field that acts as bridge in the physical space b/w 2 NFC devices.
- The generated EM field is converted back into electric impulses through another coil on client's device.
- Data such as identifiers, messages, currency, status & others can be transmitted using NFCs.
- Some of the most commonly used NFC platforms are smart phones, public transport card readers & commercial touch payment terminals.

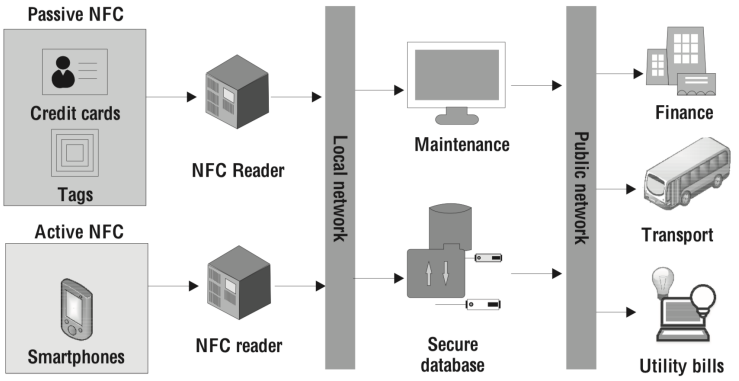


Figure 7.13 An outline of the NFC operation and communication

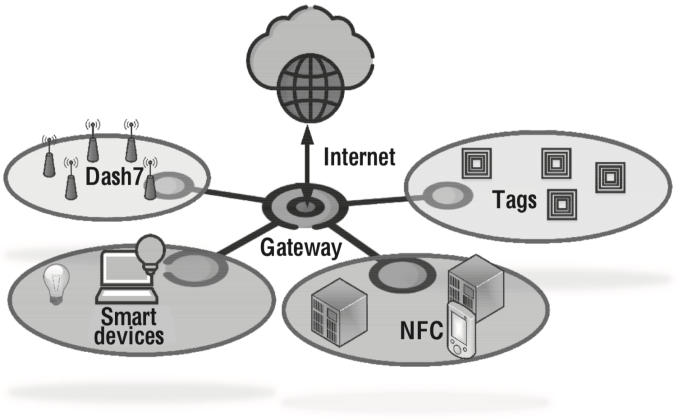
- NFC devices can be grouped into 2 types ← Passive NFC, Active NFC
  - Passive NFC Devices cannot process information, they simply store information, which is read by an NFC reader.
  - Active NFC Devices can communicate with active as well as passive NFC devices.
- Active devices are capable of reading as well as writing data to other NFC terminals or devices.

- NFC currently supports three information exchange modes -
  - Peer to Peer : It is most commonly used in NFC modes. It enables two NFC devices to exchange info. In P2P mode of information exchange, The transmitting device goes active while the recieving device becomes passive.
  - Read / Write Mode : This mode of info exchange allows only one way data transmission. An active NFC device connects to a passive devices to read info from it.
  - Card Emulation Mode : It enables an NFC device (generally smart phones) to act as a contactless credit card & make payments using just a simple tap on an NFC reader.

DASH7

- DASH7 is a wireless communication protocol derived from active RFID standards. It operates on 433 MHz frequency band and is widely adopted in diverse applications including agriculture, vehicles, consumer electronics & mobile devices.
- DASH7 is unique for its support for NFC compatibility and its adaptability to IOT communication systems.
- Key Features :-

- It operates at 433.92 MHz using Frequency Shift Keying (FSK) modulation for reliable msg transmission.
- DASH7 has a fully defined OSI compliant protocol stack, enhancing compatability with technologies like SigFox and LoRa. It integrates a file system, making it suitable for low-cost processing systems.
- It supports low power, low memory & tag to tag communicatn enabling dense network deployements.
- Effective communication Range - 1 to 10 km.
- Querying latency - 1 to 10 seconds.



- Smart Devices
- Tags
- NFC Devices
- Gateways
- Internet

Figure 7.14 The DASH7 communication architecture

· Applications of DASH7
- Agriculture
- Consumer Electronics
- Vehicles
- IOT Systems.

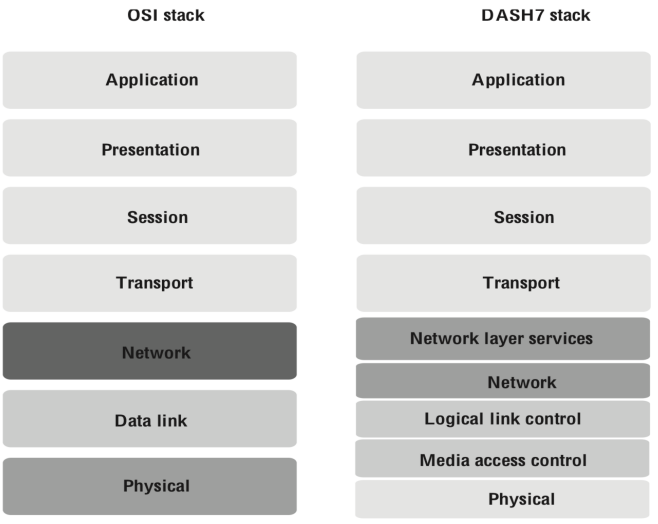


Figure 7.15 The DASH7 protocol stack in comparison to the OSI stack

· DASH7 Protocol vs OSI Stack -

i) Application Layer - manages user applns & services like device querying and data processing.

ii) Presentation & Session Layer - enables data formatting & session management for secure & reliable commtn.

iii) Transport Layer - handles end to end delivery of data, ensuring error correction & flow control.

iv) Network Layer Services - manages routing, device addressing & protocol adaptation to technologies like SigFox & LoRa.

v) Data link Layer - provides LLC & MAC ensuring collision free data transmission.

vi) Physical layer - utilizes 433MHz FSK modulation for data transmission over wireless channels.

Z- Wave -

- ZWave is a wireless commⁿ protocol designed for home automation offering a simpler & more economical alternative to Zigbee. It consumes less power than Wi-fi, has a greater range than Bluetooth, and supports a variety of devices, including sensors, locks, appliances & power distribution system.

- Key Features -

- It operates in 800-900 MHz frequency range, avoiding interference from WiFi and 2.4 GHz devices.
- It uses Gaussian Frequency Shift Keying (GFSK) modulation with pulse shaping, which limits the bandwidth & reduces signal interferences.
- It implements Manchester Encoding.
- It employs a source routed mesh network topology. Healing msgs enable the network to bypass radio dead spots.
- Each Z wave network has one central controller or hub that manages the devices.
- ZWave supports older devices, ensuring compatibility with earlier versions of protocols.
- A single Z Wave hub can manage up to 232 devices, all identified by unique Node IDs.

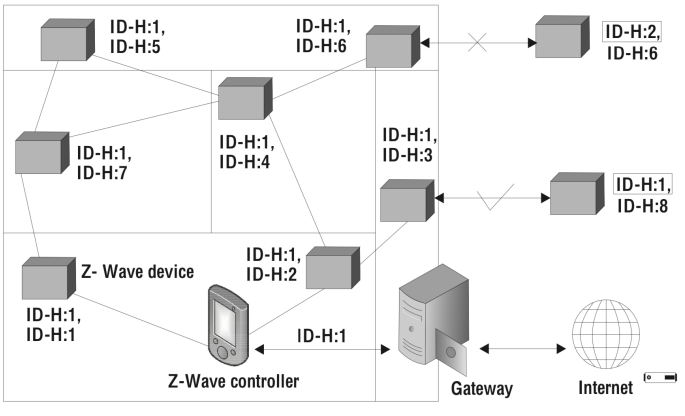


Figure 7.16 A typical Z-Wave deployment and communication architecture

· Zwave Deployement & Communication Architecture -

i) Zwave Controller - Acts as central hub & manages commtn with all Zwave devices in home network. It is connected to Internet to allow remote access & control.

ii) Zwave Devices - Sensors, Smart Locks & Thermostats
  - each device has unique node ID.

iii) Mesh Network - Msgs from devices outside the hub's range are routed through intermediary nodes.
  - Eg: A device in Room A communicates with hub via another device in Room B.

iv) Network IDs and Isolation - each logical Zwave network has unique Home ID. The devices with different Home IDs cannot communicate, ensuring privacy & isolation.

· Applications of Zwave:
- Home Automation
- Security systems.
- Energy efficiency.
- Elder Care.

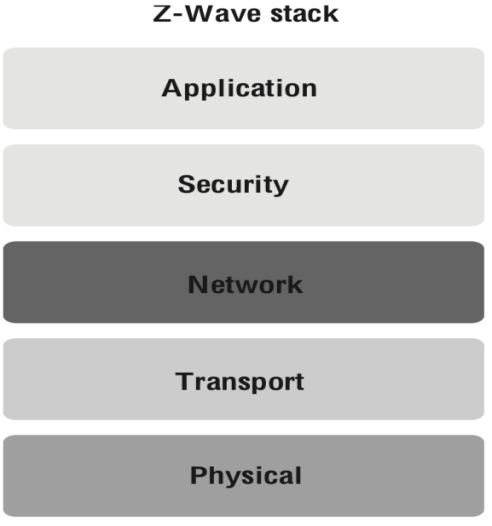


Figure 7.17 The Z-Wave protocol stack

· Zwave Protocol Stack -

- Appln layer: handles smart home functions like light control.
- Security layer: manages encryption & secure commtn.
- Network layer: supports source routing.
- Transport layer: ensures data reliability with ack & retransmission
- Physical layer: implements GFSK modulation & Manchester encoding.

Weightless -

- Weightless is a low power wide area network (LPWAN) standard designed for IOT applications that priortize low power consumption, low data throughput & moderate to high latency tolerance. It operates in sub GHz frequency bands (138 MHz to 923 MHz) & supports both licensed and unlicensed ISM bands, enabling long range, cost effective communication.
- Key Features -
- Standards
  - Weightless P
  - Weightless N
  - Weightless W.
- Network Design
  - Star Topology
  - Base Station Network (BSN).
- Message Transaction - bi-directional communication.
- Low Power & low complexity.
- Payload Size - designed for small payloads of less than 48 bytes, ideal for IOT use cases like sensors & actuators.

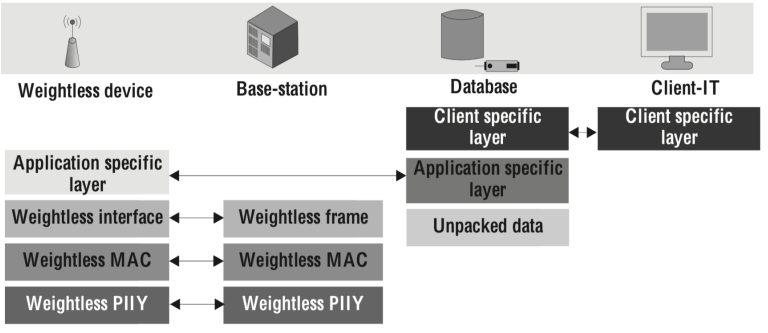


Figure 7.18 Typical components of the Weightless standard and its protocols

- End Devices
- Base Stations
- Base Station Network
- Protocol Layers
- Data Transmission Flow -

- Applications of Weightless -

i) Industrial IOT
ii) Smart Agriculture
iii) Asset Tracking
iv) Utility Monitoring
v) Environmental Monitoring.

Sigfox -

- Sigfox is a low power, wide area network (LPWAN) protocol designed for applications requiring minimal power & infrequent, small burts of data transmission.
- It is widely used in sectors like building automation, smart metering, agriculture & security.
- The technology leverages ultra-narrowband (UNB) transmission for improved resilience & effeciency.
- Ultra-Narrowband Technology
  - utilizes 192 KHz bandwidth for commtn
  - each msg occupies only 100 Hz of spectrum, reducing noise & interference effects.
  - robust against jamming & high noise environments.
- Frequency bands — 902 - 928 MHz.
- Data Rate - achieves transmission rates b/w 100-600 bits per sec.
- Msg Encoding - employs Binary Phase Shift Keying (BPSK) for encoding data.
- Security - implements AES encryption for authentication
- Commtn - Asynchronous & bi directional commtn with higher uplink budget than downlink.

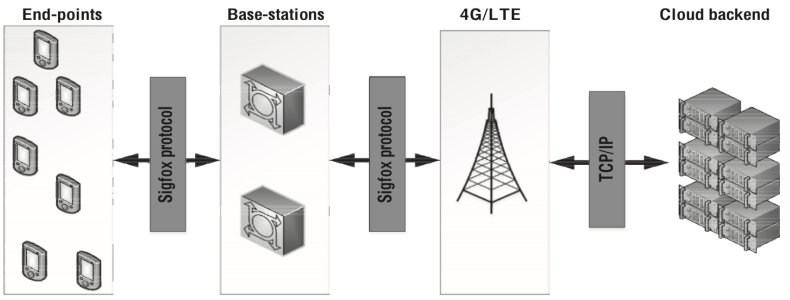


Figure 7.19 The Sigfox communication architecture

- Sigfox communication architecture -
- End Points
- Based Stations
- Cloud Backend
- Random Access Principle -

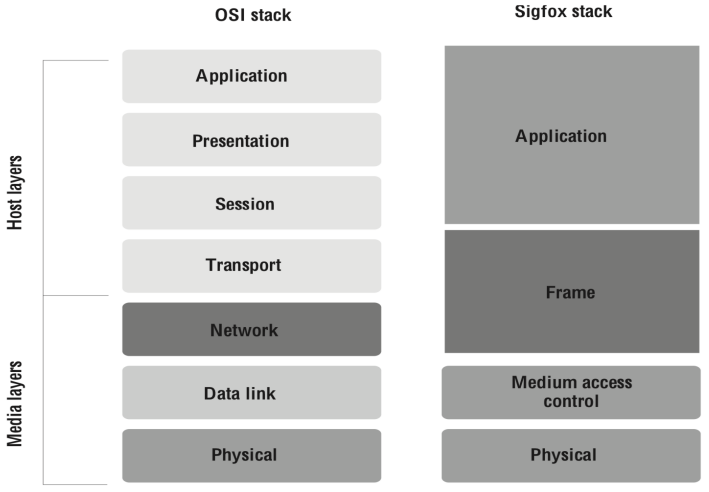


Figure 7.20 The Sigfox protocol stack in comparison to the OSI stack

- Sigfox Protocol Stack vs ISO-OSI Stack -

- Application layer - similar to OSI, handles appln specific logic.
- Frame layer - combines OSI presentation, session & transport layers.
- Medium Access Control (MAC) - manages access to ultra narrow band spectrum, similar to OSI data link layer.
- Physical layer - handles encoding & transmission through the UNB medium.

- Applications
  - Smart Metering
  - Agriculture
  - Security
  - Environmental Monitoring & Asset Tracking.

LoRa (Long Range) -

- LoRa is a patented wireless technology developed by Cycleo.
- It is widely used for low power, low range communications in IOT and Machine to Machine (M2M) applications.
- LoRa operates in the sub-GHz frequency bands (169 MHz, 433 MHz, 868 MHz, 915 MHz), enabling communication over distances ranging from 15-20 km with low data rates (27-50 Kbps). Its standout feature is spread spectrum modulation with chirp coding, allowing high reciever sensitivity & robust communication.
- Battery life - Optimized for long battery life, significantly outlasting alternatives like NB-IOT.
- It supports millions of devices in a single network deployement.
- It is ideal for asset tracking & management due to its excellent supports for mobile devices.
- It features multiple layers of security -
  - Network layer
  - Application layer
  - Device specific key.

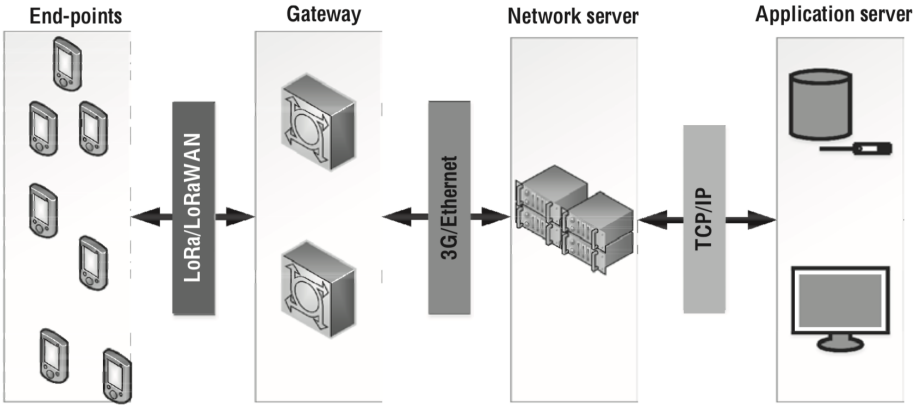


Figure 7.21 A typical LoRa deployment and communication architecture

- LoRa Deployement & Communication Architecture -

i) End Points / Nodes.
ii) Gateways
iii) Network Server
iv) Application Server
v) Connectivity

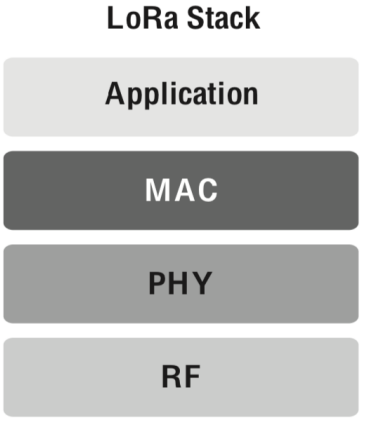


Figure 7.22 The LoRa protocol stack

- LoRa Protocol Stack -

- Application layer - defines the appln logic & protocols specific to IOT services.
- MAC layer - handles medium access control, including scheduling, acknowledgment & retransmissions.
- PHY layer - implements the chirp spread spectrum modulation, ensuring robust tranmission.
- RF layer - responsible for actual radio frequency transmission & reception.

- Applications
  - Smart Cities
  - Agriculture
  - Utilities
  - Logistics.

- Advantages
  - Secure
  - Scalable
  - Low Power
  - Long Range.

NBIOT (NarrowBand IOT) -

- NBIOT is a cellular based IOT technology developed by 3rd Gen Partnership Project (3GPP) aiming to deliver a highly reliable & energy efficient solution for IOT applications.
- It operates within existing cellular networks, typically over 2G, 3G or 4G & provides a low power wide area network (LPWAN) solution. NBIOT is particularly suited for applications that require small amounts of data transmission with long battery life.
- NBIOT offers better spectrum efficiency & system capacity than other LPWAN technologies, ensuring stable commtn even in dense urban areas / indoor environments.
- NBIOT can support battery life upto 10 years.
- It uses OFDM Modulation – Orthogonal Frequency Division multiplexing to improve system capacity & spectrum efficiency.
- NBIOT supports confidentiality, authentication & integrity features ensuring secure communication.
- It is well suited for static IOT applications – env sensors etc.
- doesnot support mobility.

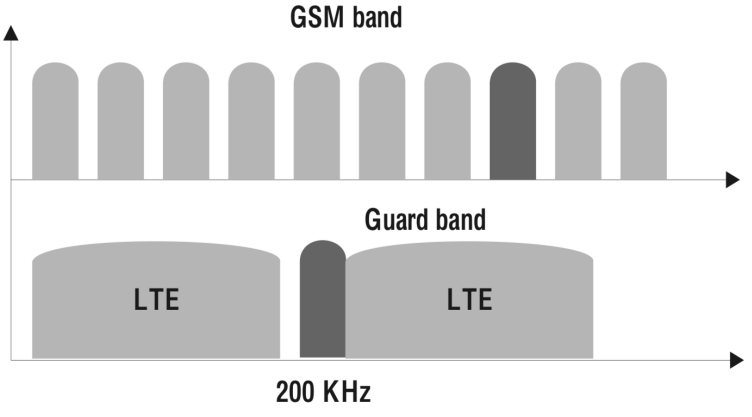


Figure 7.23 A location of NB-IoT band within the LTE spectrum

- The fig tells allocation of NBIOT within LTE spectrum-
- GSM Band: (around 200 kHz) for communicatn which allows it to make use of existing cellular infrastructure & avoid requiring dedicated spectrum.
- Gaurd Bands: Gaurd bands are unused parts of LTE spectrum that are typically left b/w channels to avoid interference. NBIOT can utilize these gaurd bands, which ensures minimal infrastructure with existing LTE systems.
- LTE Spectrum - NBIOT operates in a narrow 200KHz channel, which is much smaller than the channels used in standard LTE standards. This narrow channel is a key reason why NBIOT can support many more devices with lower energy consumptions.

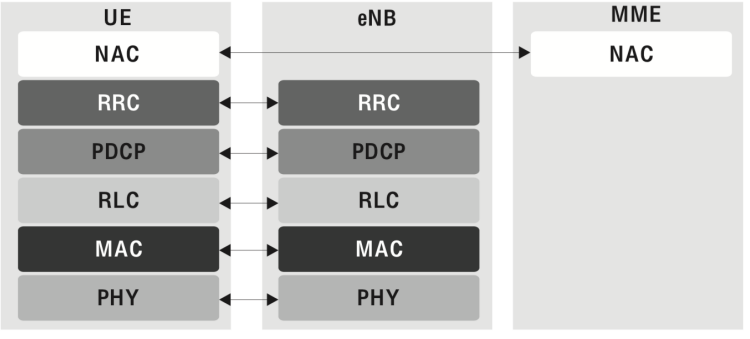


Figure 7.24 The NB-IoT protocol stack with respect to its entities

- The fig illustrates the protocol stack of NBIOT, showing layers & components involved in commstn from the user equipment (UE) to the network.

i) UE (User Equipment) – IOT devices

ii) NAC (Network Access Controller) - controls access b/w user equip & the evolved Node B (eNB) which is the base station in LTE.

iii) RRC (Radio Resource Control) - responsible for controlling the radio connection b/w UE and network.

iv) PCDP (Packet Data Convergence Protocol) - Handles data compression & encryption at higher layers of protocol.

v) RLC (Radio Link Control) - ensure the reliable transmission of data packets b/w UE & eNB performing error correctn and retransmission of lost packets if necessary.

vi) MAC (Medium Access Control) - coordinates access to physical channel. It determines when & how each device communicates over the shared air interface.

vii) eNB (evolved NodeB) - This is the base station in the LTE network responsible for managing commtn b/w UAE & the core network. It performs functions like scheduling & resource allocation.

viii) MME (Mobility Management Entity) - Manages mobility & session setup for the devices. In context of NBIOT, the MME supports device connectn & ensures that data can be routed efficiently.

ix) PHY (Physical layer) - The actual physical transmission medium. This layer is responsible for modulation & transmission of data over the air interface.

- Use Cases for NBIOT :-
  - Smart Metering.
  - Environmental Monitoring.
  - Agricultural IOT.
  - Smart Cities.

- Advantages :-
  - Battery life
  - lower power consumption
  - coexistence with existing cellular networks.
  - Security.

WiFi -

- Wifi is widely used wireless networking technology that enables local area networking (LAN) for devices. It operates under IEEE 802.11 standards, offering connectivity within a defined range, such as homes, Offices & public spaces.
- It operates in 2.4 GHz & 5 GHz ISM bands. These bands are divided into multiple channels, enabling multiple devices to share the same frequency spectrum without interference.
- wifi uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to manage channel access.
- TDMA is used to allow multiple devices to share the same channel by assigning each device specific time slots for communication.
- WiFi Versions -
  - 802.11a - Operates at 5 GHz & provides upto 54 Mbps using OFDM.
  - 802.11b - Operates at 2.4 GHz & supports upto 10 Mbps.
  - 802.11g - also operates at 2.4 GHz but achieves 54 Mbps using OFDM.
  - 802.11n - works on both 2.4 GHz & 5 GHz bands, offering speeds upto 140 Mbps using advanced MIMO techniques.
- Data Transfer & Range -
  - WiFi supports high data rates suitable for multimedia & Internet based appln. The range depends on factors like frequency band & obstacles:
    - 2.4 GHz - offers a long range but lower speeds.
    - 5 GHz - provides higher speeds but a shorter range.

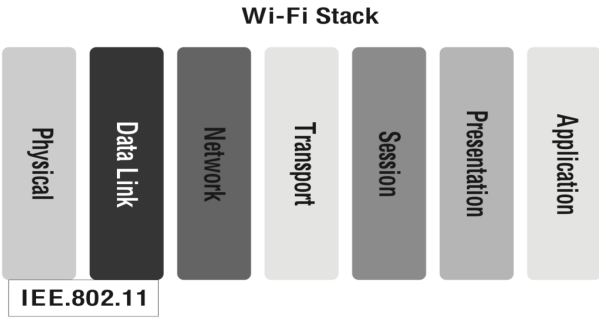


Figure 7.25 The IEEE 802.11 Wi-Fi stack

- Physical layer
- Datalink layer
- Network layer
- Transport layer
- Session, Presentation, Application layer

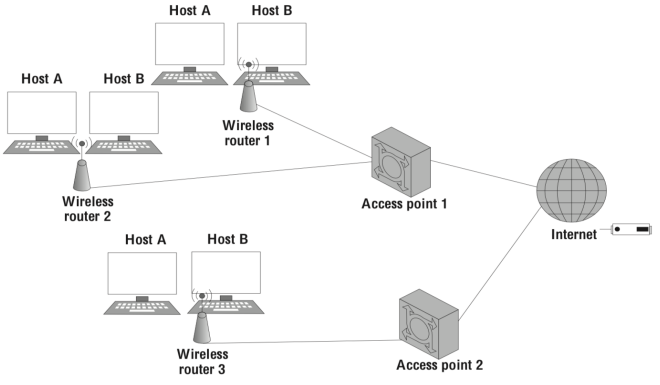


Figure 7.26 The Wi-Fi deployment architecture

- Access Points (APs) - These are hardware devices (routers) that provide wireless access to devices within their range.
- Wireless Routers - These routers connect the WLAN to broader internet, forwarding data b/w the devices & the internet.
- Hosts (Devices) - WiFi enabled devices like laptops, smartphones, & IOT devices connect to the access points for communication.

- Applications Of WiFi -
- Home Networking.
- Business Networks.
- Public WiFi
- IOT Integration.

- Advantages -
- High Speeds
- Flexibity
- Compatibility
- Scalability

- Limitations -
- Range
- Interference
- Power Consumption
- Security.

Bluetooth :-

- Bluetooth, defined by IEEE 802.15.1 standard, is a short range wireless commn technology deligned for low power commun^n b/w 2 or more devices. Intially developed as a cable replacement technology, it supports both data & voice transmission.
- It opeates in 2.4GHz ISM Band, utilizing frequency hopping spread spectrum (FHSS) to minimize interference.
- Adaptive Frequency Hopping (AFH) performs 800 hops per sec across 79 channels, each 1MHz wide.
- Range - 10 meters. Basic Rate Mode uses Gaussian Frequency Shift Keying (GFSK) modulation. It supports data rates of upto 1Mbps.
- Advanced modulation schemes involve [4 DQPSK (2Mbps)
  8 DPSK (3Mbps)

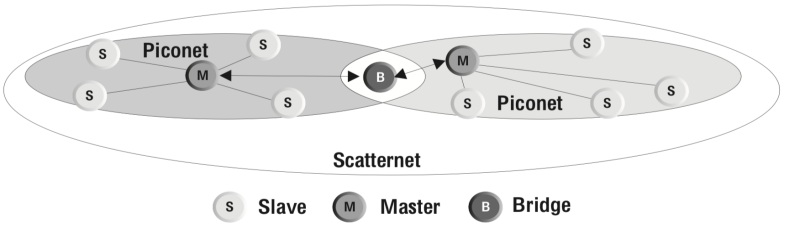


Figure 7.27 The Bluetooth device network architecture

- Bluetooth Network Architecture -
- A single master device can connect to upto seven slave devices simultaneously to form a piconet.
  - Piconet - A small, localized network with one master & upto seven slaves. A slave can only be part of one piconet at a time.
- Multiple piconets can interconnect via a bridge device to form a scatternet.
  - Scatternet is formed by interconnecting two or more piconets.
  - A bridge device can link two piconets, serving as a slave in one & a master in the other.

- Applications of Bluetooth -
- PAN (SmartPhones, Laptops, Headphones).
- IOT Integration (Smart home devices, wearable techs)
- Data transfer (File Sharing & Device Synchronization)
- Audio & Telephony (Wireless audio devices & hands-free communication).

Advantages -
- low power consumption.
- Interference Resistance.
- Cost Effectiveness.
- Security.

Disadvantages -
- Short range.
- lower data rates.
- Scalability
- interference in crowded env.

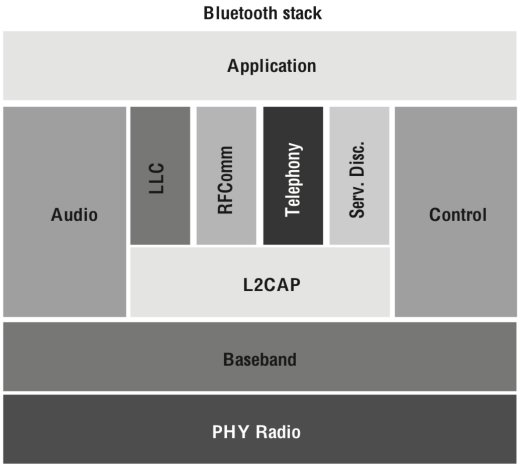


Figure 7.28 The Bluetooth protocol stack

i) Physical layer - handles transmission of radio signals.

ii) Baseband layer - manages the physical links b/w devices.

iii) L2CAP (Logical Link Control & Adaptation Protocol) -
- multiplexes logical connectn & ensures data segmentatn, flow control & data integrity.

iv) Link Manager Protocol (LMP) - performs authentication, connection setup & data transfer.

v) Host Controller Interface (HCI) - provides access to hardware controls & facilitates device discovery.

vi) RFCOMM (Radio Frequency Communication) - Acts as a cable replacement protocol, enabling serial data streaming.

vii) Service Discovery Protocol (SDP) - discovers services provided by the others.

viii) Application layer - supports user facing functionalities such as audio & telephony devices.