MODULE 3

Principles of Connected Devices and Protocols in IoT

Syllabus

RFID and NFC (Near-Field Communication), Bluetooth Low Energy (BLE) roles, LiFi , WPAN std : 802.15 standards: Bluetooth, IEEE 802.15.4, Zigbee, Z-wave, Narrow Band IoT, Internet Protocol and Transmission Control Protocol, 6LoWPAN, WLAN and WAN , IEEE 802.11, Long-range Communication Systems and Protocols: Cellular Connectivity-LTE, LTE-A, LoRa and LoRaWAN

3.1 Radio Frequency Identification (RFID) 3-3

3.1.1 Architecture of RFID 3-3

3.1.2 Different Types of RFID System 3-4

3.1.3 RFID Applications and Use cases 3-4

3.2 Near Field Communication (NFC) 3-4

3.2.1 History of Near Field Communication 3-4

3.2.2 Modes of Operation 3-5

3.2.3 Applications of Near Field Communication 3-5

3.3 Bluetooth Low Energy (BLE) 3-6

3.3.1 Difference Between Bluetooth Low Energy and Bluetooth Classic is shown below 3-6

3.3.2 Bluetooth Low Energy Architecture 3-7

3.4 Li-Fi (Light Fidelity) 3-8

3.4.1 Applications of Li-Fi 3-9

3.4.2 Advantages of Li-Fi Over Wi-Fi 3-9

3.5 WPAN (Wireless Personal Area Network) 3-10

3.6 802.15 Standard Bluetooth: 3-10

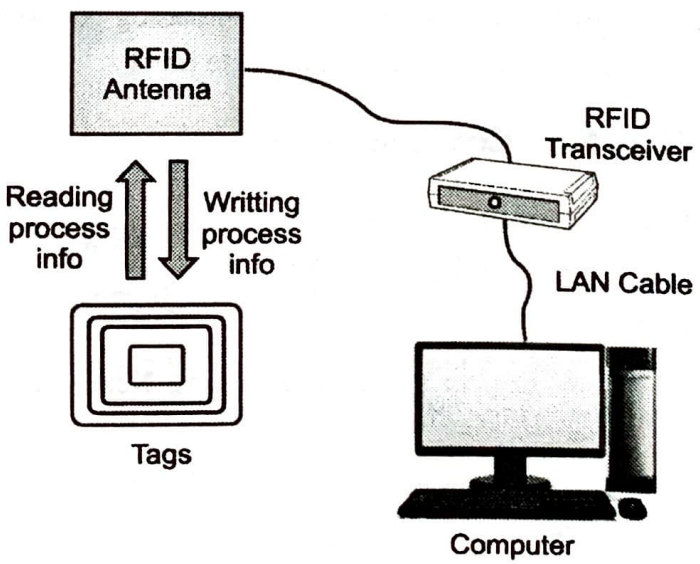
3.6.1 Bluetooth Applications 3-11
3.6.2 Bluetooth Protocol Stack 3-12
3.6.3 Functions of the Core Protocols 3-12
3.7 IEEE 802.15.4 3-12
3.7.1 IEEE 802.15. Protocol Stacks include: 3-13
3.8 Zigbee 3-15
3.9 Z-Wave 3-15
3.9.1 Z-Wave Network 3-16
3.10 Narrow Band IoT 3-16
3.11 Internet Protocol (IP) 3-19
3.11.1 Transmission Control Protocol 3-21
3.12 6LoWPAN 3-21
3.12.1 Advantages of 6LoWPAN 3-22
3.12.2 6LoWPAN Application Areas 3-22
3.13 WLAN and WAN 3-23
3.13.1 Types of WLANS 3-23
3.13.2 Frame Format of IEEE 802.11 3-24
3.13.3 Advantages of WLANs 3-24
3.13.4 Disadvantages of WLANs 3-24
3.13.5 Wide Area Network 3-25
3.14 Long Range Communication System and Protocol:Cellular Connectivity LTE, LTE-A, LoRa and LoRaWAN 3-25
3.14.1 Long Term Evolution 3-26
3.14.2 LTE-A 3-27
3.14.3 LoRa 3-28
3.14.4 LoRaWAN 3-29
3.15 Multiple Choice Questions 3-30
• **Chapter End...**

3.1 RADIO FREQUENCY IDENTIFICATION (RFID)

- Tags and readers are the two separate entities of smart transmission known as Radio Frequency Identification (RFID). One or multiple antenna's are there for receiver that emits radio waves and receive signal back from transmitter i.e. Tags. Tags can be active or passive which uses radio waves to communicate their presence and supporting information to nearby readers.
- Passive RFID Tags are operating by support of readers and do not have battery in their architecture. Passive tags are used in application like tracking inventory, access control and in wholesale and retail sector.
- Active tags are having inbuilt battery support to perform actions. RFID tags can contain a variety of data, ranging from a single serial number to many pages of information. Readers are mobile in nature so that they can carry from one location to another location very easily and they can be easily mounted on anywhere. The active tages are used to track real time location and high speed environments like toll. Reader systems may also be included into the design of a cabinet, chamber, or building.

3.1.1 Architecture of RFID

- The architecture mainly consists of Transceiver which is connected with antenna and set of tags where the data is stored. The antenna creates communication between transmitter and receiver. The server is responsible for storing and matching the data, if data is matched then valid entry is found and data is validated or if data is not matched then data it shows error.
- Static readers and mobile readers are the two different categories of RFID readers.The RFID reader is a network-connected gadget that can be carried about or fixed to a surface. It sends signals that turn on the tag using radio waves. After being turned on, the tag returns a wave to the antenna, where it is converted into information.



(1C1)**Fig. 3.1.1 : Architecture of RFID System**

3.1.2 Different Types of RFID System

1. **Low Frequency RFID System :** This system has very low transmission range generally from few inches to 5 feet's. Its frequency range is from 30 KHz to 500 KHz.
2. **High-frequency RFID system :** Its operating frequency is from 3MHz to 30MHz. The standard range is anywhere from a few inches to several feet.
3. **UHF RFID systems :** Its frequency ranges from 300 MHz to 960 MHz and can generally be read from 25+ feet away.
4. **Microwave RFID systems :** These run at 2.45 Ghz and can be read from 30+ feet away.

3.1.3 RFID Applications and Use Cases

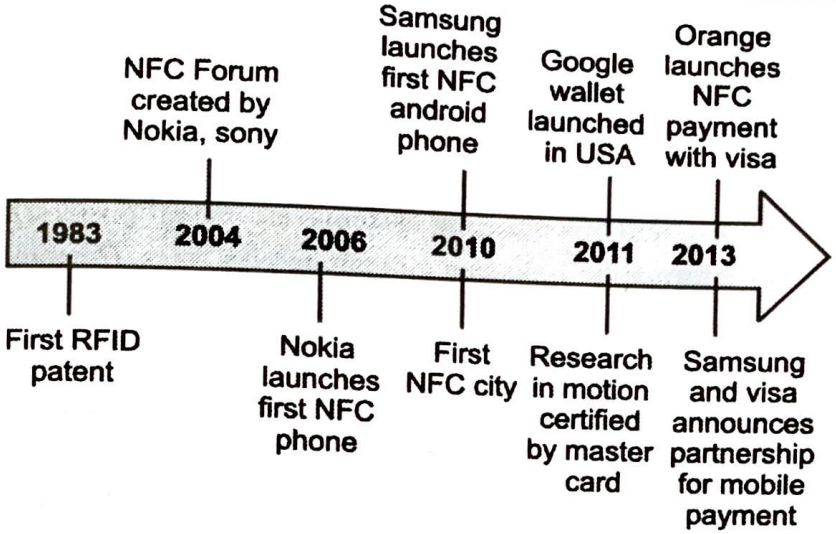
1. Retail Sector
2. Transport
3. Inventory Control
4. Vehicle Tracking
5. Customer service and loss control.
6. Shipping
7. Healthcare
8. Animal Tracking

3.2 NEAR FIELD COMMUNICATION (NFC)

- A set of protocols known as near-field communication (NFC) allows two electronic devices to communicate at a 4 cm distance.NFC relies on the inductive coupling of two antennae on NFC-enabled devices, such as a smartphone and a printer, which can communicate in either or both ways. NFC is working in short range with high frequency.
- Your smartphone, tablet, wearables, payment cards, and other devices become increasingly smarter thanks to near-field communication (NFC), a short-range wireless technology.
- Whether paying bills, exchanging business cards, or downloading coupons, NFC allows for quick, simple information transfer across devices with just a single touch.

3.2.1 History of Near Field Communication

- The first patent of RFID was granted to Charles Walton.
- In 2004 Forum was created by Nokia and Sony for NFC.
- Nokia 3161 was the NFC phone launched.
- In 2009 NFC forum release peer to peer standard. Samsung Nexus was the first android phone launched in 2010.
- Google launched NFC to share contacts, Video and Audio. Apple introduced apple pay using NFC in iPhone 6, 6s and advanced version.

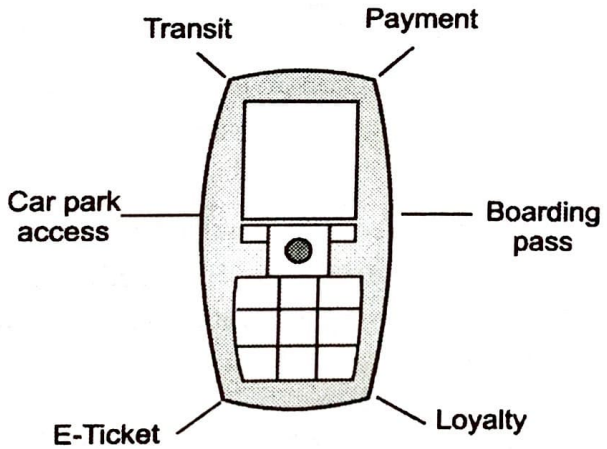


(1C2)**Fig. 3.2.1 : Timeline of Near Field Communication**

3.2.2 Modes of Operation

- Near field communication is working in two modes of Operation: Active mode and passive mode
- In Active mode, electromagnetic field and exchange of data is generated by NFC chip in both devices. Example of active mode is Bluetooth, xender and share it.
- There is only one active devices and other uses field to share information in Passive mode.

3.2.3 Applications of Near Field Communication



(1C3)**Fig. 3.2.2 : Applications of RFID**

1. **Smart Cards :** Smart cards with NFC integration make it simpler to pay than the traditional, multi-step payment process. Customers can purchase NFC-embedded smart cards from reputable payment processors like Visa and MasterCard. Smart cards with NFC integration can be used to quickly pay for groceries, pay parking fines, accrue shopping points, and redeem coupons with just a single tap. Smart cards with NFC chips are offered by all the major banks worldwide.
2. **E-wallet :** Beginning this decade, mobile-based cashless payment systems gained popularity, and more businesses are now accepting them for the convenience of their customers. Payments can be

done using smart phone applications by just tapping or waving the card in close range. Using an implanted NFC tag, service providers can incorporate a payment option into smartphones. The most widely used mobile payment apps are Apple Pay, Google Wallet.

3. **Smart Ticketing :** Smart tickets that incorporate integrated smart chips can take the place of conventional airline, railroad, and bus ticketing systems, etc. Smart posters, movie tickets, concert tickets, ads, leaflets, and information links can all contain NFC tags. Customers will be able to tap NFC tags placed at designated locations to enter a reserved area or activate tickets. All it takes is a quick scan of the smart tag to get further details.

4. **Medicine and Healthcare :** The FC integrated system is applicable to medical and healthcare tasks. By adding NFC tags to patient documents, NFC makes it easier to check in, make payments, check a patient's status, and trace records. It also improves the accuracy and simplicity of providing medications. Devices with NFC integration can be quickly paired and set up. Access to medical equipment and gadgets is simple for medical practitioners.

3.3 BLUETOOTH LOW ENERGY (BLE)

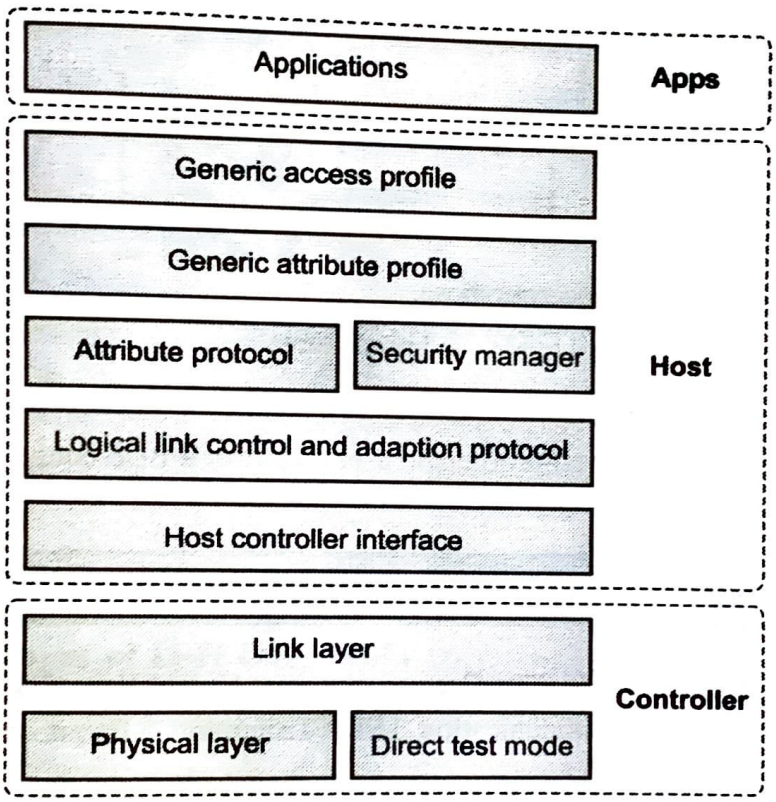
- The Bluetooth Low Energy (LE) communication is built to operate at extremely low power levels.
- The Bluetooth LE radio offers manufacturers a significant amount of flexibility to create products that match the specific connection requirements of their market by transmitting data over 40 lines in the 2.4GHz ISM frequency spectrum.
- BLE supports a variety of communication topologies, ranging from point-to-point to broadcast and, most recently, mesh, making it possible to build dependable, extensive device networks using Bluetooth technology.
- One device can now use BLE features to determine the location, size, and direction of another device.
- Bluetooth Low Energy is designed to offer significantly lower power and cost while keeping a similar communication range as compared to Classic Bluetooth.Native support for Bluetooth Low Energy is provided by the mobile operating systems iOS, Android, Windows Phone, BlackBerry, Linux, macOS, Windows 8, Windows 10, and Windows 11.

3.3.1 Difference Between Bluetooth Low Energy and Bluetooth Classic is shown below

Parameter	Bluetooth Low Energy	Bluetooth Classic
Channels	40 channels with 2 MHz spacing	79 channels with 1 MHz spacing
Data Transports	• Asynchronous Connection-oriented • Isochronous Connection-oriented	• Asynchronous Connection-oriented • Synchronous Connection-oriented

	• Asynchronous Connectionless • Synchronous Connectionless • Isochronous Connectionless	
Communication Topologies	• Point-to-Point (including piconet) • Broadcast Mesh	Point-to-Point (including piconet)
Channel Usage	Frequency-Hopping Spread Spectrum (FHSS)	GFSK, $\pi/4$ DQPSK, 8DPSK
Power	0.01–0.50 W	1 W

3.3.2 Bluetooth Low Energy Architecture



(1C4)**Fig. 3.3.1 : Bluetooth Low Energy Architecture**

The Detail Architecture is explained as follows

Physical Layer and Link Layer

The analogue communications circuitry is actually present in the physical layer. The radio divides the 2.4 GHz ISM (Industrial, Scientific, and Medical) band into 40 channels. The component that has a direct interface with the physical layer is the link layer

Host Controller Interface (HCI)

In order for the controller and host to communicate with one another, HCI defines a set of instructions and events.

L2CAP

- In this layer, there are two functionalities. In the beginning, it performs the function of a protocol multiplexer, taking several protocols from the top levels and encapsulating them in the typical BLE packet structure.
- The Attribute Protocol (ATT) and the Security Manager Protocol are the two primary protocols for Bluetooth Low Energy that the L2CAP layer is responsible for routing (SMP)
- A straightforward client/server stateless protocol based on attributes provided by a device is known as the Attribute Protocol (ATT). Whether a device is a master or a slave in BLE, it can be a client, a server, or both. Data is sent to clients by servers in response to requests from clients for data. Each server houses data arranged as attributes, each of which is given a specific value.
- A protocol and a set of security algorithms make up the Security Manager (SM).

Generic Access Profile (GAP)

GAP establishes different sets of rules and concepts to regulate and standardize the low level operation of devices:

1. Roles and interaction between them.
2. Operational modes and transitions across those.
3. Security aspects, including security modes and procedures.

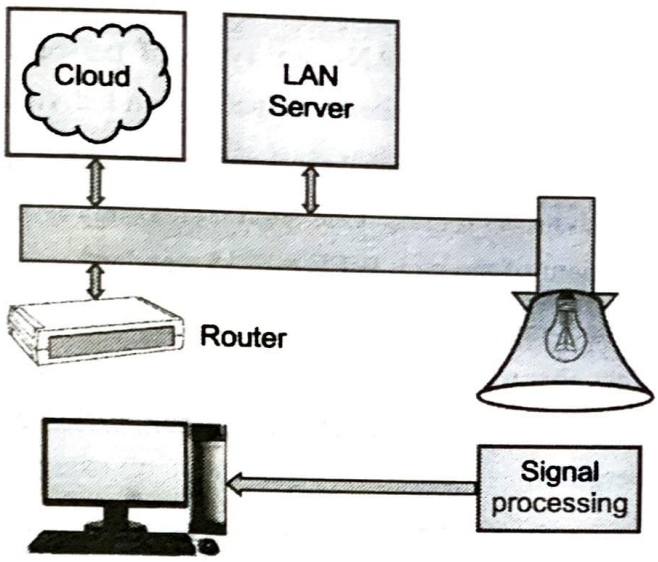
The Generic Attribute Profile

The specifics of how to exchange all profile and user data over a BLE connection are established in the Generic Attribute Profile (GATT).

3.4 LI-FI (LIGHT FIDELITY)

- Light Fidelity is referred to as Li-Fi. The German physicist Harald Haas first presented the concept in 2011 at the Visible Light Communication TED (Technology, Entertainment, Design) Global Talk (VLC).
- Light emitting diodes (LEDs) are used in the wireless optical networking technology known as Li-Fi to transmit data. The term "Li-Fi" refers to visible light communication (VLC) technology that complies with the IEEE standard IEEE 802.15.7 and employs light as a medium to deliver high-speed communication in a manner similar to Wi-Fi. Similar to Wi-IEEE Fi's 802.11 standard, the IEEE 802.15.7 is a high-speed, bidirectional, and fully networked wireless communication technology standard. The following Fig. 3.5 shows the concept of Li-Fi
- At the downlink transmitter, a light bulb is used to implement it. Since it only uses light, the light bulb typically glows at a constant current supply. However, quick and subtle variations in current can be made to produce optical outputs, making it easily applicable in places like airplanes, hospitals, and other places where radio frequency communication is frequently problematic.

- Simple operation involves transmitting a digital 1 when the LED is on and a digital 0 when it is off. Since the LED can be swiftly turned on and off, good opportunities for data transmission result. Therefore, all that is needed is a controller that encodes data into some LEDs so that they flicker in accordance with the data we wish to transmit. Your lamp can process more data the more LEDs there are in it.



(1C5)**Fig. 3.4.1 : Li-Fi Working**

3.4.1 Applications of Li-Fi

1. Health technologies
2. Airlines
3. Power Plant
4. Under sea working
5. GPS usage

3.4.2 Advantages of Li-Fi Over Wi-Fi

1. High speed connectivity of the rate of 500mbps.
2. Li- Fi uses light rather than radio frequency signals so are intolerant to disturbances.
3. VLC could be used safely in aircraft without affecting airlines signals.
4. Integrated into medical devices and in hospitals as this technology doesn't deal with radio waves, so it can easily be used in all such places where Bluetooth, infrared, Wi-Fi and internet are broadly in use.
5. Under water in sea Wi-Fi does not work at all but light can be used and hence undersea explorations are good to go now with much ease.
6. There are billions of bulbs worldwide which just need to be replaced with LED's to transmit data.
7. Security is a side benefit of using light for data transfer as it does not penetrate through walls.
8. On highways for traffic control applications like where Cars can have LED based headlights, LED based backlights, and they can communicate with each other and prevent accidents.

9. Using this Technology worldwide every street lamp would be a free data access point.
10. The issues of the shortage of radio frequency bandwidth may be sorted out by Li-Fi.

3.5 WPAN (WIRELESS PERSONAL AREA NETWORK)

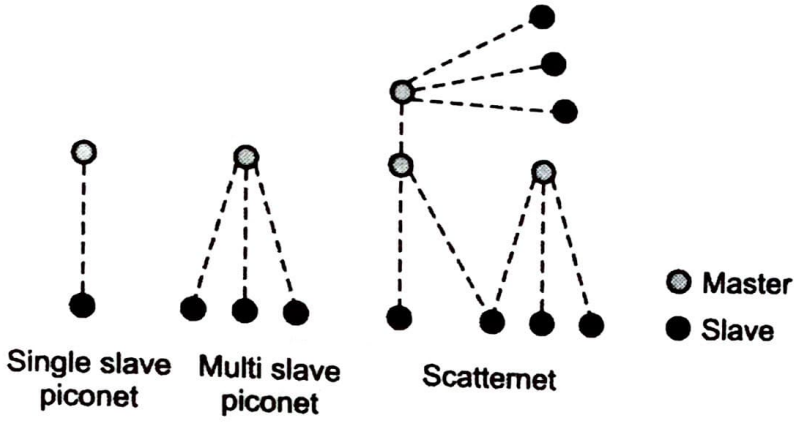
- Wireless personal area networks, or WPANs, are types of personal area networks that connect devices to one another and are centred on the workspace of an individual.
- A wireless personal area network often employs a technology that allows communication over a relatively limited range of about 10 metres. One such technology is Bluetooth, which served as the foundation for the development of the new IEEE 802.15 standard.
- A WPAN could be used for a variety of purposes, including connecting all the common computing and communication devices that many people have on their desks or carry around with them today, or it could have a more niche use, such as enabling communication between the surgical team and the surgeon during an operation.
- Connecting is a crucial idea in WPAN technology. The ideal situation would be for any two WPAN-equipped devices to be able to communicate as if they were physically connected by a cable when they are in close proximity to one another (within a few metres) or when they are a short distance from a central server.
- The capability of each device to selectively lock out other devices, limiting superfluous interference or unwanted access to information, is another crucial aspect.
- The goal is to enable smooth operation across systems and appliances in the home or workplace. If two devices are physically close to one another, they can connect to each other and other devices in the same WPAN.
- Additionally, WPANs will be connected globally. So, for instance, an archaeologist working on location in Greece may use a PDA to immediately access databases at the University of Minnesota in Minneapolis and send research to those databases.

3.6 802.15 STANDARD BLUETOOTH:

- One of the most popular short-range wireless communication standard.
- Known as IEEE 802.15.1, now maintained by SIG (Special Interest Group)

Due to its numerous uses in audio devices like headsets, mobile phones, home stereos, MP3 players, laptops, desktop computers, tablets, and more, Bluetooth has now become a part of our daily life. If two devices are Bluetooth compliant, one can send data (meeting schedules, phone numbers), audio, graphic pictures, and video between them. The detailed Bluetooth standards are described in the IEEE 802.15.1 standard.

Bluetooth Network classified as follows



(1C8)**Fig. 3.6.1 : Bluetooth Architectures**

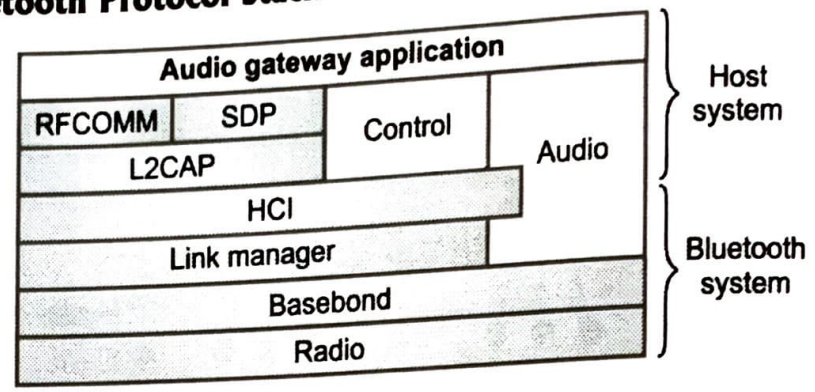
- Numerous bluetooth users make up the Bluetooth network. Piconet and scatternet are the two different types of network topologies used in Bluetooth. One master and one slave, as well as one master and several slaves, make up a piconet.
- The piconet can only have a maximum of 7 active slaves. A piconet, or small network, will therefore have a maximum of 8 devices talking with one another. Slaves can only transmit when the master Bluetooth device requests it. In parking state, there will be roughly 255 slaves.
- The master polls the active slaves to send data. Every station will receive an 8-bit parking address. In one piconet, 255 parked slaves are possible. In just 2 milliseconds, the parked station can connect.
- In just 2 milliseconds, the parked station can connect. The remaining stations have additional time to join. Within the range of the bluetooth radio, there are about 10 such piconets.
- Scatternet is a collection of many piconets. A device may take part in several piconets. It will timeshare and require synchronisation with the current piconet's master.
- Data rates based on various versions, ranging from 720 kbps to around 24 Mbps, are supported. Depending on the Bluetooth power class that is available, it will have a range of coverage of between 1 and 100 metres.

3.6.1 Bluetooth Applications

Following are few of the many Bluetooth applications :

1. One can receive and make call using Bluetooth compliant wireless headset.
2. Operate computer using mouse/keyboard and take print outs wirelessly eliminating cables.
3. Home automation

3.6.2 Bluetooth Protocol Stack



(1C7)Fig. 3.6.2 : Bluetooth Protocol Stack

3.6.3 Functions of the Core Protocols

- **Radio :** This is a physical layer equivalent protocol that lays down the physical structure and specifications for transmission of radio waves. It defines air interface, frequency bands, frequency hopping specifications and modulation techniques.
- **Baseband :** This protocol takes the services of radio protocol. It defines the addressing scheme, packet frame format, timing, and power control algorithms.
- **Link Manager Protocol (LMP) :** LMP establishes logical links between Bluetooth devices and maintains the links for enabling communications. The other main functions of LMP are device authentication, message encryption, and negotiation of packet sizes.
- **Logical Link Control and Adaptation Protocol (L2CAP) :** L2CAP provides adaption between upper layer frame and baseband layer frame format. L2CAP provides support for both connection-oriented as well as connectionless services.
- **Service Discovery Protocol (SDP) :** SDP takes care of service-related queries like device information so as to establish a connection between contending Bluetooth devices.

3.7 IEEE 802.15.4

A low-cost, low-data-rate wireless access technology for powered or battery-operated devices is IEEE 802.15.4. This explains the operation of low-rate wireless personal area networks (LR-WPANs).

3.7.1 IEEE 802.15. Protocol Stacks include:

1. **Standardization and alliances : It specifies low-data-rate PHY and MAC layer requirements for wireless personal area networks (WPAN).**

   (i) **ZigBee:** ZigBee is a low-rate task group 4 in the Personal Area Network task group. It is a form of home networking technology. A technological standard called ZigBee was developed for managing and sensing the network. Since ZigBee is the Personal Area Network of Task Group 4, it was developed by the Zigbee Alliance and is based on IEEE 802.15.4.

(ii) **6LoWPAN** : A number of applications, including wireless sensor networks, employ the 6LoWPAN standard. The term IPv6 over Low power Wireless Personal Area Networks is derived from the fact that this type of wireless sensor network distributes data as packets and utilises IPv6.

(iii) **Wireless HART :** A time-synchronized and self-organizing architecture is used in this wireless sensor network technology.

(iv) **Thread :** Thread is an IPv6-based networking protocol for low-power Internet of Things devices in IEEE 802.15. 4-2006 wireless mesh network. Thread is independent.

2. **Physical Layer**

- A wide variety of PHY possibilities in ISM bands, from 2.4 GHz to sub-GHz frequencies, are made possible by this standard. 20 kilobits per second, 40 kilobits per second, 100 kilobits per second, and 250 kilobits per second are among the data transmission speeds supported by IEEE 802.15.4.
- The main design presupposes a 10-meter range and a 250 kilobits per second data rate. Even lower data rates are feasible to further decrease power consumption.

3. **MAC layer**

By deciding which devices in the same area will share the given frequencies, the MAC layer establishes links to the PHY channel. At this layer, data packet scheduling and routing are also managed.

4. **Topology**

IEEE 802.15.4-based networks can be designed with a star, peer-to-peer, or mesh topology. Mesh networks link a lot of nodes together. This makes it possible for nodes that are out of communication range to communicate with one another and relay information using intermediary nodes.

5. **Security**

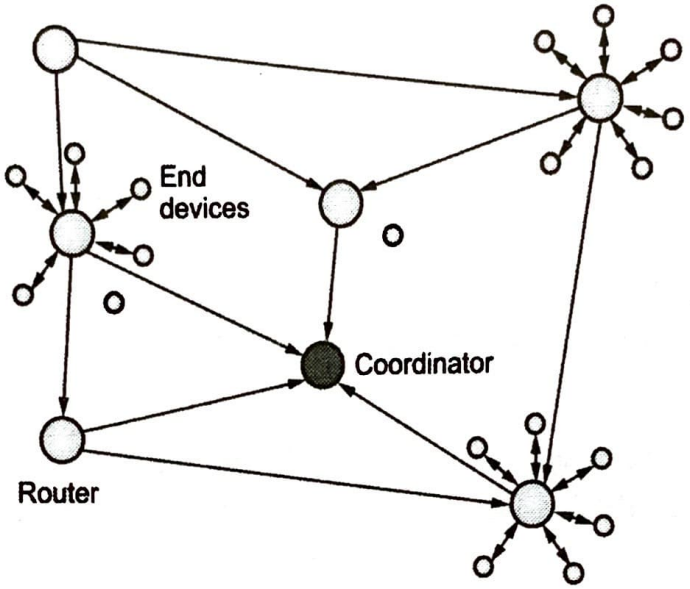
The Advanced Encryption Standard (AES) with a 128-bit key length is the primary encryption method used by the IEEE 802.15.4 standard to protect data.

3.8 ZIGBEE

- Zigbee is now very well-liked for wireless applications requiring modest data rates. Zigbee technology is utilised in a variety of applications, including smart energy, healthcare, and home automation.
- Zigbee devices are used in smart energy applications to monitor and regulate energy and water use, which benefits consumers by enabling them to conserve both resources and money. It can connect an infinite number of health monitoring devices in the medical area, among many others. Switches,

dimmers, occupancy sensors, and load controllers are all used in home automation to regulate domestic lights.

- It operates on two frequencies: 868/915 MHz and 2450 MHz. Data speeds in the 868/915 frequency range from 20 to 40 kbps, whereas those in the 2450 MHz spectrum are around 250 kbps. Additionally, because zigbee end devices include a security layer, they can enter a sleep state to conserve battery life and protect information security.
- Zigbee network is comprised of coordinator(C), router(R) and end devices (E). Zigbee supports mesh-routing.



(1C8)**Fig. 3.8.1 : Zig-bee Network**

Coordinator

- Always first coordinator need to be installed for establishing zigbee network service, it starts a new PAN (Personal Area Network), once started other zigbee components viz. router(R) and End devices(E) can join the network(PAN).
- It is responsible for selecting the channel and PAN ID.
- It can assist in routing the data through the mesh network and allows join request from R and E.
- It is mains powered (AC) and support child devices.
- It will not go to sleep mode.

Router

First router needs to join the network then it can allow other R & E to join the PAN. It is mains powered (AC) and support child devices.It will not go to sleep mode.

End Devices

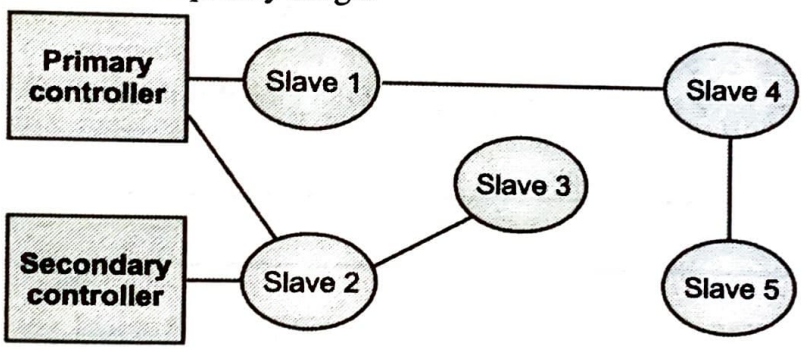
It cannot allow other devices to join the PAN nor can it assist in routing the data through the network. It is battery powered and do not support any child devices. This may sleep hence battery consumption can be minimized to great extent.

3.9 Z-WAVE

- An important use for the wireless communications system Z-Wave is the automation of homes and businesses. It is a mesh network that communicates from device to device using low-energy radio waves, enabling wireless control of smart home appliances like smart lights, security systems, thermostats, sensors, smart door locks, and garage door openers.
- A Z-Wave system can be controlled remotely from a smart phone, tablet, or computer, as well as locally through a smart speaker, wireless keyboard, or wall-mounted panel, with a Z-Wave gateway or central control device acting as both the hub and controller, similar to other protocols and systems aimed at the residential, commercial, MDU, and building markets. Through its collaboration, Z-Wave enables application layer interoperability across home control systems made by various manufacturers.

3.9.1 Z-Wave Network

- Slaves and controllers make up the Z-wave network. There is one primary controller and multiple subordinate controllers. The nodes in a Z-wave network that send out control commands are known as controller devices.
- Additionally, it broadcasts the commands to other nodes. The slave devices are the nodes that respond to commands based on them and also carry them out. The directives are also forwarded to other network nodes by slave nodes. As a result, the controller can establish connection with nodes that are outside of the radio frequency range.



(1C9)**Fig. 3.9.1 : Z Network**

- **Controllers :** A controller device will have full routing table for this mesh network and it will host it. Hence controller can communicate with all the nodes of z-wave network.
- **Slaves :** The slave devices/nodes in z-wave network receive the commands and performs action based on the commands. These slave nodes are unable to transmit information directly to the other slave nodes or controllers unless they are instructed to do so in the commands. The slave nodes do not compute routing tables. They can store routing tables. They will act as a repeater.
- **Home ID :** The z-wave protocol uses Home ID field to separate the networks from each other. It is 32 bit unique identifier which will be pre-programmed in all the controller devices. At the start, all

the slave nodes will have Home ID value as zero. All the slave devices need Home ID value in order to communicate in the z-wave network. This will be communicated to all by the controller. Controllers exchange Home ID which makes it possible for more than one controller to control slave nodes.

- **Node ID :** This node ID is 8 bit value. Similar to Home ID, they are also assigned to slave nodes by controller. Node ID's are used in order to address individual nodes in a z-wave network. These Node ID's are unique within a network defined by a unique Home ID.

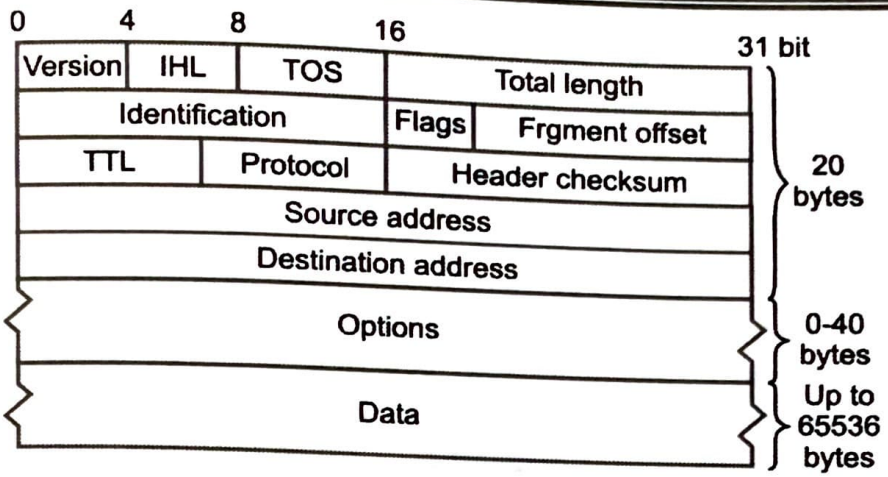
3.10 NARROW BAND IOT

- A large variety of new IoT devices and services are made possible by the standards-based low power wide area (LPWA) technology known as narrowband-Internet of things (NB-IoT). In deep coverage, NB-IoT dramatically increases spectrum efficiency, system capacity, and user device power consumption. A variety of use cases can accommodate battery life of more than 10 years.
- The challenging requirements of expanded coverage - rural and deep interiors - and ultra-low device complexity are met by new physical layer signals and channels. The NB-IoT modules' initial cost is anticipated to be similar to that of GSM/GPRS. Although the underlying technology is considerably simpler than GSM/GPRS today, its cost is anticipated to drop significantly as demand rises.
- All significant manufacturers of mobile devices, chipsets, and modules support NB-IoT, which can coexist alongside 2G, 3G, and 4G mobile networks. The security and privacy aspects of mobile networks, such as support for user identity secrecy, entity authentication, confidentiality, data integrity, and mobile equipment identification, are also advantageous to it. The initial NB-IoT commercial launches have been accomplished, and the global rollout is anticipated to begin in 2017 or 2018.

3.11 INTERNET PROTOCOL (IP)

The fourth version of the Internet Protocol is called Internet Protocol version 4 (IPv4) (IP). The Internet and other packet-switched networks use it as one of its primary core protocols for internetworking. The first production-ready release of IPv4 was made available on the SATNET in 1982 and the ARPANET in January 1983.

- Internet Protocol is connectionless and unreliable protocol. It ensures no guarantee of successfully transmission of data.
- In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.
- Internet protocol transmits the data in form of a datagram as shown in the following diagram:



(1C10)**Fig. 3.11.1 : IP Header Format**

- **Version :** The first header field in an IP packet is the four-bit version field. For IPv4, this is always equal to 4.
- **Internet Header Length (IHL) :** The IPv4 header is variable in size due to the optional 14th field (options). The IHL field contains the size of the IPv4 header; it has 4 bits that specify the number of 32-bit words in the header. The minimum value for this field is 5which indicates a length of 5 × 32 bits = 160 bits = 20 bytes. As a 4-bit field, the maximum value is 15; this means that the maximum size of the IPv4 header is 15 × 32 bits = 480 bits = 60 bytes.
- **Differentiated Services Code Point (DSCP) :** Originally defined as the type of service (ToS), this field specifies differentiated services (DiffServ) per RFC 2474.Real-time data streaming makes use of the DSCP field. An example is Voice over IP (VoIP), which is used for interactive voice services.
- **Explicit Congestion Notification (ECN) :** This field is defined in RFC 3168 and allows end-to-end notification of network congestion without dropping packets. ECN is an optional feature available when both endpoints support it and effective when also supported by the underlying network.
- **Total Length :** This 16-bit field defines the entire packet size in bytes, including header and data. The minimum size is 20 bytes (header without data) and the maximum is 65,535 bytes. All hosts are required to be able to reassemble datagrams of size up to 576 bytes, but most modern hosts handle much larger packets. Links may impose further restrictions on the packet size, in which case datagrams must be fragmented. Fragmentation in IPv4 is performed in either the sending host or in routers. Reassembly is performed at the receiving host.
- **Identification :** This field is an identification field and is primarily used for uniquely identifying the group of fragments of a single IP datagram. Some experimental work has suggested using the ID field for other purposes, such as for adding packet-tracing information to help trace datagrams with spoofed source addresses, but RFC 6864 now prohibits any such use.

- **Flags :** A three-bit field follows and is used to control or identify fragments. They are (in order, from most significant to least significant):
  - bit 0: Reserved; must be zero.
  - bit 1: Don't Fragment (DF)
  - bit 2: More Fragments (MF)

  If the DF flag is set, and fragmentation is required to route the packet, then the packet is dropped. This can be used when sending packets to a host that does not have resources to perform reassembly of fragments. It can also be used for path MTU discovery, either automatically by the host IP software, or manually using diagnostic tools such as ping or traceroute.

  For unfragmented packets, the MF flag is cleared. For fragmented packets, all fragments except the last have the MF flag set. The last fragment has a non-zero Fragment Offset field, differentiating it from an unfragmented packet.
- **Fragment offset :** This field specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram in units of eight-byte blocks. The first fragment has an offset of zero. The 13 bit field allows a maximum offset of $(213 - 1) \times 8 = 65{,}528$ bytes, which, with the header length included ($65{,}528 + 20 = 65{,}548$ bytes), supports fragmentation of packets exceeding the maximum IP length of 65,535 bytes.
- **Time to live (TTL) :** An eight-bit time to live field limits a datagram's lifetime to prevent network failure in the event of a routing loop. It is specified in seconds, but time intervals less than 1 second are rounded up to 1. In practice, the field is used as a hop count—when the datagram arrives at a router, the router decrements the TTL field by one. When the TTL field hits zero, the router discards the packet and typically sends an ICMP time exceeded message to the sender.

  The program traceroute sends messages with adjusted TTL values and uses these ICMP time exceeded messages to identify the routers traversed by packets from the source to the destination.
- **Protocol :** This field defines the protocol used in the data portion of the IP datagram. IANA maintains a list of IP protocol numbers as directed by RFC 790.
- **Header checksum :** The 16-bit IPv4 header checksum field is used for error-checking of the header. When a packet arrives at a router, the router calculates the checksum of the header and compares it to the checksum field. If the values do not match, the router discards the packet. Errors in the data field must be handled by the encapsulated protocol. Both UDP and TCP have separate checksums that apply to their data.

  When a packet arrives at a router, the router decreases the TTL field in the header. Consequently, the router must calculate a new header checksum.
- **Source address :** This field is the IPv4 address of the sender of the packet. Note that this address may be changed in transit by a network address translation device.
- **Destination address :** This field is the IPv4 address of the receiver of the packet. As with the source address, this may be changed in transit by a network address translation device.

3.11.1 Transmission Control Protocol

TCP delivers end-to-end packet transmission and is a connection-oriented protocol. It serves as the foundation for relationship. It exhibits the following key features:

- Transmission Control Protocol (TCP) corresponds to the Transport Layer of OSI Model.
- TCP is a reliable and connection oriented protocol.
- TCP offers:
  - Stream Data Transfer.
  - Reliability.
  - Efficient Flow Control
  - Full-duplex operation.
  - Multiplexing.
- TCP offers connection oriented end-to-end packet delivery.
- TCP ensures reliability by sequencing bytes with a forwarding acknowledgement number that indicates to the destination the next byte the source expect to receive.
- It retransmits the bytes not acknowledged with in specified time period.

TCP Services

TCP offers following services to the processes at the application layer:

1. Stream Delivery Service	2. Sending and Receiving Buffers
3. Bytes and Segments	4. Full Duplex Service
5. Connection Oriented Service	6. Reliable Service

1. **Stream Deliver Service :** TCP protocol is stream oriented because it allows the sending process to send data as stream of bytes and the receiving process to obtain data as stream of bytes.
2. **Sending and Receiving Buffers :** It may not be possible for sending and receiving process to produce and obtain data at same speed, therefore, TCP needs buffers for storage at sending and receiving ends.
3. **Bytes and Segments :** The Transmission Control Protocol (TCP), at transport layer groups the bytes into a packet. This packet is called segment. Before transmission of these packets, these segments are encapsulated into an IP datagram.
4. **Full Duplex Service :** Transmitting the data in duplex mode means flow of data in both the directions at the same time.
5. **Connection Oriented Service :** TCP offers connection oriented service in the following manner:

   (i) TCP of process-1 informs TCP of process – 2 and gets its approval.

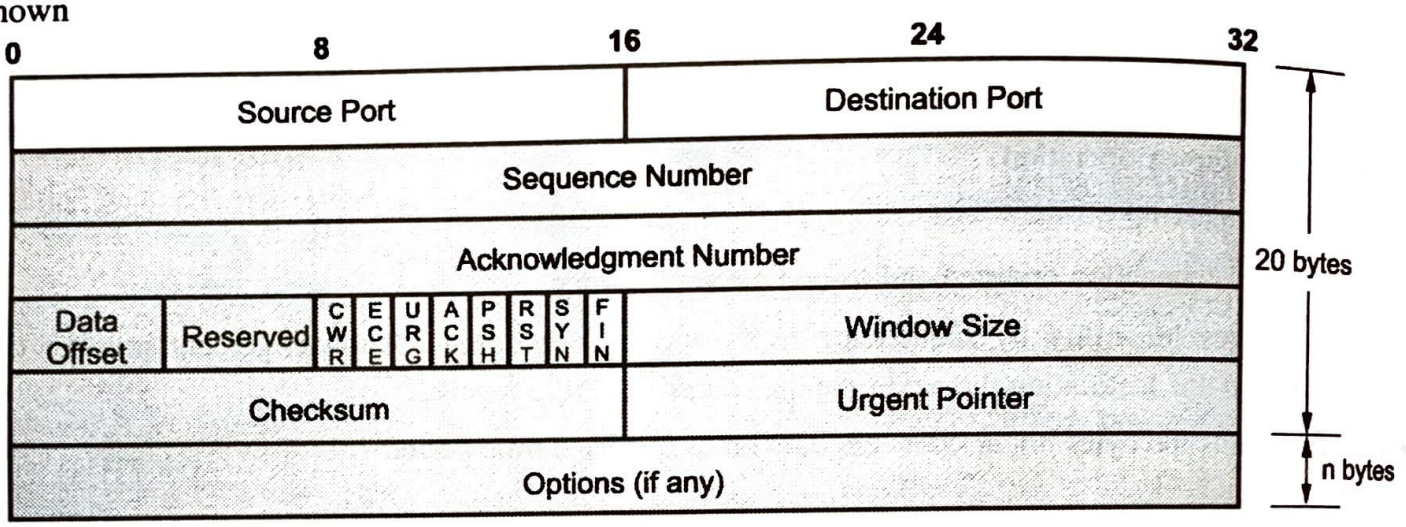
(ii) TCP of process – 1 and TCP of process – 2 and exchange data in both the two directions.

(iii) After completing the data exchange, when buffers on both sides are empty, the two TCP's destroy their buffers.

▶ **6. Reliable Service :** For sake of reliability, TCP uses acknowledgement mechanism.

☞ TCP Header Format

A TCP header consists of data bytes to be sent and a header that is added to the data by TCP as shown



(1C10)**Fig. 3.11.2 : TCP Header Format**

The header of a TCP segment can range from 20-60 bytes. 40 bytes are for options. If there are no options, a header is 20 bytes else it can be of upmost 60 bytes.

Header fields

- **Source Port Address –** A 16-bit field that holds the port address of the application that is sending the data segment.
- **Destination Port Address –** A 16-bit field that holds the port address of the application in the host that is receiving the data segment.
- **Sequence Number –** A 32-bit field that holds the sequence number, i.e, the byte number of the first byte that is sent in that particular segment. It is used to reassemble the message at the receiving end of the segments that are received out of order.
- **Acknowledgement Number –** A 32-bit field that holds the acknowledgement number, i.e, the byte number that the receiver expects to receive next. It is an acknowledgement for the previous bytes being received successfully.
- **Header Length (HLEN) –** This is a 4-bit field that indicates the length of the TCP header by a number of 4-byte words in the header, i.e if the header is 20 bytes(min length of TCP header), then this field will hold 5 (because 5 x 4 = 20) and the maximum length: 60 bytes, then it'll hold the value 15(because 15 x 4 = 60). Hence, the value of this field is always between 5 and 15.

- **Control flags** – These are 6 1-bit control bits that control connection establishment, connection termination, connection abortion, flow control, mode of transfer etc. Their function is:

  URG: Urgent pointer is valid

  ACK: Acknowledgement number is valid (used in case of cumulative acknowledgement)

  PSH: Request for push

  RST: Reset the connection

  SYN: Synchronize sequence numbers

  FIN: Terminate the connection

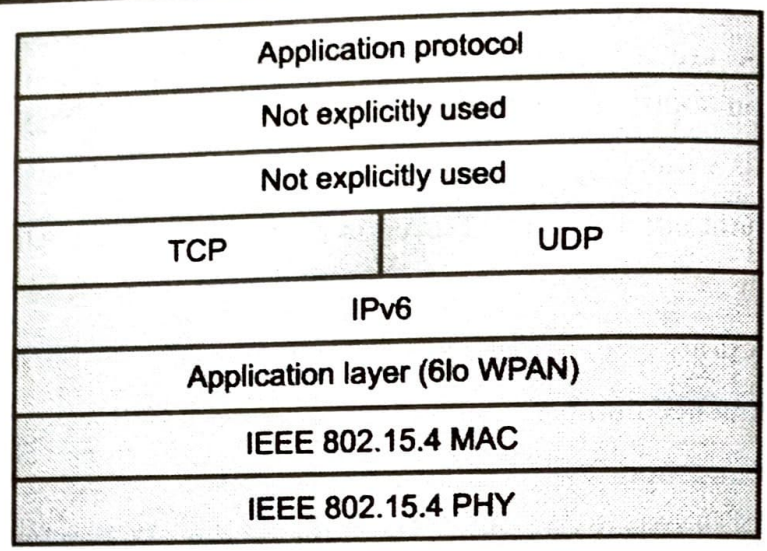
- **Window size** – This field tells the window size of the sending TCP in bytes.
- **Checksum** – This field holds the checksum for error control. It is mandatory in TCP as opposed to UDP.
- **Urgent pointer** – This field (valid only if the URG control flag is set) is used to point to data that is urgently required that needs to reach the receiving process at the earliest. The value of this field is added to the sequence number to get the byte number of the last urgent byte.

3.12 6LOWPAN

- Every node in the low power wireless mesh network known as 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) has a unique IPv6 address. This enables the node to establish a direct connection utilizing open standards with the Internet.
- The concept behind 6LoWPAN is that low-power, low-processing-power devices should be able to participate in the Internet of Things and that the Internet Protocol can and should be applied to even the smallest devices.

3.12.1 Advantages of 6LoWPAN

1. It works great with open IP standard including TCP, UDP, HTTP, COAP, MATT and web-sockets.
2. It offers end-to-end IP addressable nodes. There's no need for a gateway, only a router which can connect the 6LoWPAN network to IP.
3. It supports self-healing, robust and scalable mesh routing.
4. Offers one-to-many & many-to-one routing.
5. The 6LoWPAN mesh routers can route data to others nodes in the network.
6. In a 6LowPAN network, leaf nodes can sleep for a long duration of time.
7. It also offers thorough support for the PHY layer which gives freedom of frequency band & physical layer, which can be used across multiple communication platforms like Ethernet, WI-Fi, 802.15.4 or Sub-1GHz ISM with interoperability at the IP level.



(1C11)**Fig. 3.12 1 : LoWPAN Protocol Stack**

3.12.2 6LoWPAN Application Areas

- **Automation :** There are enormous opportunities for 6LoWPAN to be used in many different areas of automation.
- **Industrial monitoring :** 6LoWPAN has a lot of potential in automated industries and industrial plants. Automating routine tasks can result in significant savings. Furthermore, 6LoWPAN can link to the cloud, opening up a wide range of possibilities for data monitoring and analysis.
- **Smart Grid :** Smart grids enable smart meters and other devices to build a micro mesh network. They are able to send data back to the grid operator's monitoring and billing system using the IPv6.
- **Smart Home:** By connecting your home IoT devices using IPv6, it is possible to gain distinct advantages over other IoT systems.

3.13 WLAN AND WAN

The term "wireless LANs" refers to wireless computer networks that connect devices inside a constrained area without the usage of wires (Local Area Network). The restricted region includes places like homes, schools, campuses, office buildings, train platforms, etc. where users linked by wireless LANs can move about.

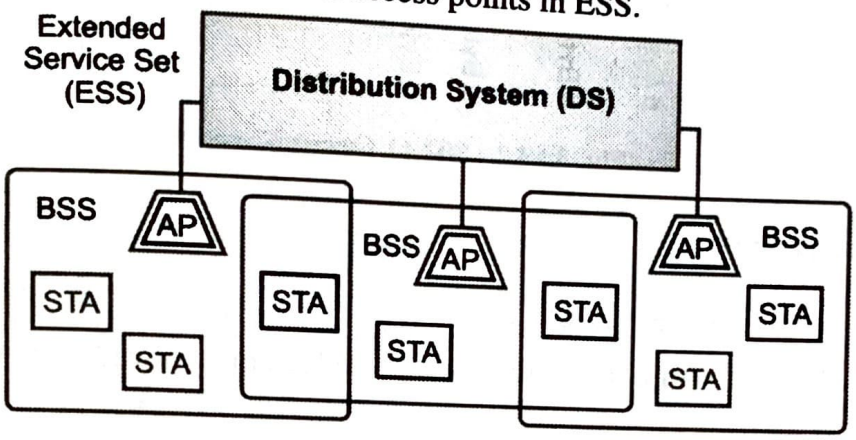
Most WLANs are based upon the standard IEEE 802.11 standard or WiFi.

Components of WLANs

The components of WLAN architecture as laid down in IEEE 802.11 are

- **Stations (STA)** – Stations comprises of all devices and equipment that are connected to the wireless LAN. Each station has a wireless network interface controller. A station can be of two types –
  - Wireless Access Point (WAP or AP)
  - Client

- **Basic Service Set (BSS)** – A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories :
  - Infrastructure BSS
  - Independent BSS
- **Extended Service Set (ESS)** – It is a set of all connected BSS.
- **Distribution System (DS)** – It connects access points in ESS.



(1C12)**Fig. 3.13.1 : Architectures of WLAN**

3.13.1 Types of WLANS

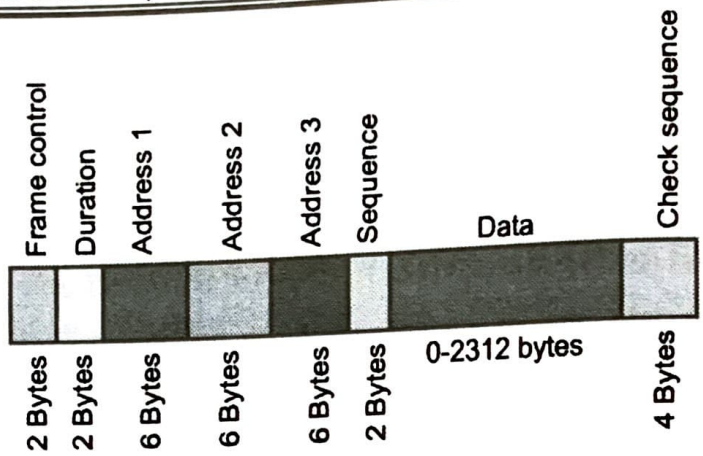
WLANs, as standardized by IEEE 802.11, operates in two basic modes, infrastructure, and ad hoc mode.

- **Infrastructure Mode :** Mobile devices or clients connect to an access point (AP) that in turn connects via a bridge to the LAN or Internet. The client transmits frames to other clients via the AP.
- **Ad Hoc Mode** : Clients transmit frames directly to each other in a peer-to-peer fashion.

3.13.2 Frame Format of IEEE 802.11

The main fields of a frame of wireless LANs as laid down by IEEE 802.11 are :

- **Frame Control :** It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.
- **Duration :** It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel.
- **Address fields :** There are three 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.
- **Sequence :** It a 2 bytes field that stores the frame numbers.
- **Data** : This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.
- **Check Sequence :** It is a 4-byte field containing error detection information.



(1C13)Fig. 3.13.2 : 802.11 Frame Format

3.13.3 Advantages of WLANs

(1) They provide clutter-free homes, offices and other networked places.

(2) The LANs are scalable in nature, i.e. devices may be added or removed from the network at greater ease than wired LANs.

(3) The system is portable within the network coverage. Access to the network is not bounded by the length of the cables.

(4) Installation and setup are much easier than wired counterparts.

(5) The equipment and setup costs are reduced.

3.13.4 Disadvantages of WLANs

(1) Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.

(2) Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.

(3) WLANs are slower than wired LANs.

3.13.5 Wide Area Network

- A computer network known as a wide area network (WAN) is one that spans a substantial geographic area, such as an entire country, continent, or even the entire world. The technologies used by WAN allow data, picture, audio, and video to be transmitted over vast distances and between various LANs and MANs.
- **The distinguishing features of WAN are :**
  - WANs have a large capacity, connecting a large number of computers over a large area, and are inherently scalable.
  - They facilitate the sharing of regional resources.
  - They provide uplinks for connecting LANs and MANs to the Internet.

- Communication links are provided by public carriers like telephone networks, network providers, cable systems, satellites etc.
- Typically, they have low data transfer rate and high propagation delay, i.e. they have low communication speed.
- They generally have a higher bit error rate.

- **Example of WAN**
  - The Internet
  - 4G Mobile Broadband Systems
  - A network of bank cash dispensers.

3.14 LONG RANGE COMMUNICATION SYSTEM AND PROTOCOL:CELLULAR CONNECTIVITY LTE, LTE-A, LORA AND LORAWAN

3.14.1 Long Term Evolution

- The project name for the creation of a high performance air interface for cellular mobile communication systems is LTE (Long Term Evolution). It is the final phase of the transition to the fourth generation (4G) of radio technology intended to boost the speed and capacity of mobile phone networks. LTE is marketed as 4G while the earlier generations of mobile telecommunication networks are referred to as 2G or 3G.
- LTE (Long-Term Evolution) is a fourth-generation (4G) wireless standard that provides increased network capacity and speed for cellphones and other cellular devices compared with third-generation (3G) technology.
- LTE offers higher peak data transfer rates than 3G, initially up to 100 Mbps downstream and 30 Mbps upstream. It provides reduced latency, scalable bandwidth capacity and backward-compatibility with the existing Global System for Mobile communication (GSM) and Universal Mobile Telecommunications Service (UMTS) technology. The subsequent development of LTE-Advanced (LTE-A) yielded peak throughput on the order of 300 Mbps.
- LTE has a direct role in the development of the current 5G standard, called 5G New Radio. Early 5G networks, referred to as non-standalone 5G (NSA 5G), require a 4G LTE control plane to manage 5G data sessions. NSA 5G networks can be deployed and supported by the existing 4G network framework, lowering capital and operating expenses for operators rolling out 5G.

Why is LTE called 'Long-Term Evolution'?

- The 3rd Generation Partnership Project (3GPP) developed LTE. The standard was described as the next step in the progression of mobile telecommunications and follows the 2G GSM and 3G UMTS specifications. LTE is commonly marketed as 4G LTE.LTE did not originally qualify as true 4G.

- The International Telecommunication Union (ITU) initially defined 4G as a cellular standard that would deliver data rates of 1 Gbps to a stationary user and 100 Mbps to a user on the move. In December 2010, the ITU softened its stance, applying 4G to LTE, as well as several other wireless standards.

3.14.2 LTE-A

- LTE-A stands for LTE-Advanced. It is a standard for mobile communication that is one generation beyond LTE (Long Term Evolution). Whereas LTE was a 3G communication standard, LTE-A is a 4G or fourth generation communication standard.
- The benefits of a fourth generation communication network are many. Perhaps most simply, LTE-A offers faster speeds than 3G. As defined by the International Mobile Telecommunications-Advanced Standard, 4G must offer a nominal data rate of 100 Mbit/s when a user is physically moving at high speeds relative to a data station, and 1 Gbit/s when the user and station are fixed relative to one another. Additionally, LTE-A allows for global roaming, smooth handover between networks, and interoperability with existing wireless standards.
- For wireless communication, LTE-A or 4G LTE is the current state-of-the-art.

LTE-A features

- As one would expect, a 4G network offers several advantages over a 3G network. In order to be classified as 4G, a network must meet certain criteria, as governed by the International Telecommunications Union.
- Requirements for a 4G communication standard include:
  - All-Internet Protocol (IP) packet switched network (for increased network efficiency)
  - Interoperability with existing wireless standards
  - Specific nominal data rates for mobile and stationary users
  - Network resources are dynamically shared in order to support more simultaneous users per cell
  - Scalable channel bandwidth up to 40 MHz
  - Peak link spectral efficiency of 15 bit/s/Hz for downlink, and 6.75 bit/s/Hz for uplinks
  - Seamless connectivity with smooth handovers across networks
  - Global roaming with universal connectivity
  - Service sufficient for multimedia support
- Though 4G data speeds are greater than 3G data speeds, it is worth noting that Megabits (Mbit) are different than Megabytes (MB) – the two are commonly mistaken for one another.
- A Megabyte refers to the size of a digital file; Megabit refers to upload and download speeds of digital files. A Megabit is 1/8th as large as a Megabyte. To download a 1MB file in 1 second, your network connection must be 8Mbps (or Mbit/s).

3.14.3 LoRa

- LoRa is a radio modulation technique that is essentially a way of manipulating radio waves to encode information using a chirped (chirp spread spectrum technology), multi-symbol format. LoRa as a term can also refer to the systems that support this modulation technique or the communication network that IoT applications use.
- The main advantages of LoRa are its long-range capability and its affordability. A typical use case for LoRa is in smart cities, where low-powered and inexpensive internet of things devices (typically sensors or monitors) spread across a large area send small packets of data sporadically to a central administrator.
- LoRa (short for long range) is a spread spectrum modulation technique derived from chirp spread spectrum (CSS) technology. Semtech's LoRa is a long range, low power wireless platform that has become the de facto wireless platform of Internet of Things (IoT). LoRa devices and networks such as the LoRaWAN® enable smart IoT applications that solve some of the biggest challenges facing our planet: energy management, natural resource reduction, pollution control, infrastructure efficiency, and disaster prevention.
- LoRa devices have amassed several hundred known uses cases for smart cities, homes and buildings, communities, metering, supply chain and logistics, agriculture, and more. With hundreds of millions of devices connected to networks in more than 100 countries and growing, LoRa is creating a smarter planet.

Key Features of LoRa

- **Long Range**

  Connects devices up to 30 miles apart in rural areas and penetrates dense urban or deep indoor environments

- **Low Power**

  Requires minimal energy, with prolonged battery lifetime of up to 10 years, minimizing battery replacement costs

- **Secure**

  Features end-to-end AES128 encryption, mutual authentication, integrity protection, and confidentiality

- **Geolocation**

  Enables GPS-free tracking applications, offering unique low power benefits untouched by other technologies

- **High Capacity**

  Supports millions of messages per base station, meeting the needs of public network operators serving large markets

- **Low Cost**

  Reduces infrastructure investment, battery replacement expense, and ultimately operating expenses

3.14.4 LoRaWAN

- LoRaWAN is a low-power, wide area networking protocol built on top of the LoRa radio modulation technique. It wirelessly connects devices to the internet and manages communication between end-node devices and network gateways.
- Usage of LoRaWAN in industrial spaces and smart cities is growing because it is an affordable long-range, bi-directional communication protocol with very low power consumption devices can run for ten years on a small battery. It uses the unlicensed ISM (Industrial, Scientific, Medical) radio bands for network deployments.
- An end device can connect to a network with LoRaWAN in two ways:
  - **Over-the-air Activation (OTAA) :** A device has to establish a network key and an application session key to connect with the network.
  - **Activation by Personalization (ABP) :** A device is hardcoded with keys needed to communicate with the network, making for a less secure but easier connection.

LoRaWAN has three different classes of end-point devices to address the different needs reflected in the wide range of applications:

Class A – Lowest power, bi-directional end-devices

- The default class which must be supported by all LoRaWAN end-devices, class A communication is always initiated by the end-device and is fully asynchronous. Each uplink transmission can be sent at any time and is followed by two short downlink windows, giving the opportunity for bi-directional communication, or network control commands if needed. This is an ALOHA type of protocol.
- The end-device is able to enter low-power sleep mode for as long as defined by its own application: there is no network requirement for periodic wake-ups. This makes class A the lowest power operating mode, while still allowing uplink communication at any time.
- Because downlink communication must always follow an uplink transmission with a schedule defined by the end-device application, downlink communication must be buffered at the network server until the next uplink event.

Class B – Bi-directional end-devices with deterministic downlink latency

- In addition to the class A initiated receive windows, class B devices are synchronized to the network using periodic beacons, and open downlink 'ping slots' at scheduled times. This provides the network the ability to send downlink communications with a deterministic latency, but at the expense of some additional power consumption in the end-device. The latency is programmable up to 128 seconds to suit different applications, and the additional power consumption is low enough to still be valid for battery powered applications.

Class C – Lowest latency, bi-directional end-devices:

- In addition to the class A structure of uplink followed by two downlink windows, class C further reduces latency on the downlink by keeping the receiver of the end-device open at all times that the device is not transmitting (half duplex). Based on this, the network server can initiate a downlink transmission at any time on the assumption that the end-device receiver is open, so no latency. The compromise is the power drain of the receiver (up to ~50mW) and so class C is suitable for applications where continuous power is available.

For battery powered devices, temporary mode switching between classes A & C is possible, and is useful for intermittent tasks such as firmware over-the-air updates.

3.15 MULTIPLE CHOICE QUESTIONS

Q. 3.1 An interconnected collection of piconet is called _____

(a) Scatternet (b) Micronet
(c) Mininet (d) Multinet

✓**Ans. : (a)**

Q. 3.2 Coordinator ZigBee devices act as the bridge between _____.

(a) Different networks (b) Different edge devices
(c) Different fog devices (d) All of the above

✓**Ans. : (a)**

Q. 3.3 Which of the following IEEE standards is followed by the physical and MAC layer protocols in ZigBee?

(a) IEEE 801.15.4 (b) IEEE 802.15.4
(c) IEEE 803.15.4 (d) IEEE 804.15.4

✓**Ans. : (b)**

Q. 3.4 IEEE 802.11g, has a data rate of _____ Mbps.

(a) 1 (b) 2 (c) 11 (d) 22

✓**Ans. : (d)**

Q. 3.5 Which bluetooth version enables low energy?

(a) Bluetooth 3.0 (b) Bluetooth 4.0
(c) Bluetooth 2.0 (d) Bluetooth 1.0

✓**Ans. : (c)**

Q. 3.6 What is the Access technique used by an LTE or LTE-A network?

(a) WCDMA (b) FDMA
(c) PDMA (d) OFDMA

✓**Ans. : (d)**

Q. 3.7 IEEE has defined the specifications for a wireless LAN called _____, which covers the physical and data link layers.

(a) ieee 802.3 (b) ieee 802.5
(c) ieee 802.11 (d) ieee 802.2

✓**Ans. : (c)**

Q. 3.8 What is header of datagram in IPv4_____

(a) 20 to 60 bytes (b) 20 to 80 bytes
(c) 20 to 40 bytes (d) 0 to 20 bytes

✓**Ans. : (a)**