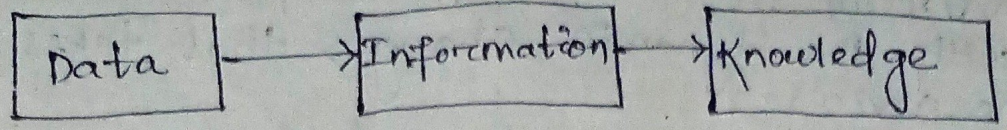



Def' of IOT :-
A dynamic global network infrastructure with self configuring capabilities based on standard and inter-operable communication protocols where physical and virtual things have identifiers, physical attributes and virtual personalities and use intelligent interfaces and are seamlessly integrated into the information network, often communicate data associated with users and their environment.

L-8 Application of IOT :—

Characteristics of IOT :-

i) connectivity :-
→ Connectivity is an important requirement of the IOT infrastructure.
→ Things of IOT should be connected to the IOT infrastructure.
→ Anytime, Anywhere, anyone can be connected to the IOT infrastructure and connectivity should be guaranteed at all the times.

ii) Intelligence and Identity :-
→ The extraction of knowledge from the generated data is very important.
→ For example :- A sensor generates data but that data will only be useful if it is interpreted properly.
→ Each IOT device has an unique identity and this identification is helpful in tracking the equipment and sometimes querying its status.

iii) Enormious Scalability :-
→ The number of elements that needs to be managed and that communicate with each other will be much larger than the devices connected to the current internet.
→ The management of data generated from these devices and there interpretation for application purposes becomes more critical.

iv) Dynamic and self adapting :-

→ The primary activity of internet of things is to collect data from its environment and this is achieved with the dynamic changes that takes place around the devices.
→ This state of these devices changed dynamically.
→ In addition to the state of device the number of devices also changes dynamically with a person, place and time.

v) Architecture :-

→ IOT architecture can not be homogeneous in nature.
→ It should be hybrid, supporting different manufactured product to function in the IOT network.
→ IOT is not being owned by any of the engineering branch.
→ IOT is a reality when multiple domains come together.

vi) Safety :-

→ There is a danger of the sensitive personal details of the users getting compromized when all of his or her devices are connected to the internet.
→ This can caused a loss to the user, hence data security is the major challenge.
→ As the equipment involved is fuse, IOT network may also be at risk and equipment safety is also be critical.

Dt - 18.01.24

vii) Sensing :-

→ IOT would not be possible without sensors which will detect or measure any changes in the environment to generate data that can report on their status or even interact with the environment.
→ This sensing information is simply the analog input from the physical world but it can provide the reach understanding of our complex world.

viii) Heterogeneity :-

→ Heterogeneity in IOT is one of the key characteristic.
→ Devices in IOT are based on different hardware platforms and networks that can interact with other devices or service platforms through different networks.

→ IoT architecture should support direct network connectivity between heterogeneous networks.

→ The key design requirements for heterogeneous things and their environments in IoT are scalabilities, modularity, extensibility and interoperability.

ix) Security :-

→ IoT devices are naturally vulnerable to security threads.

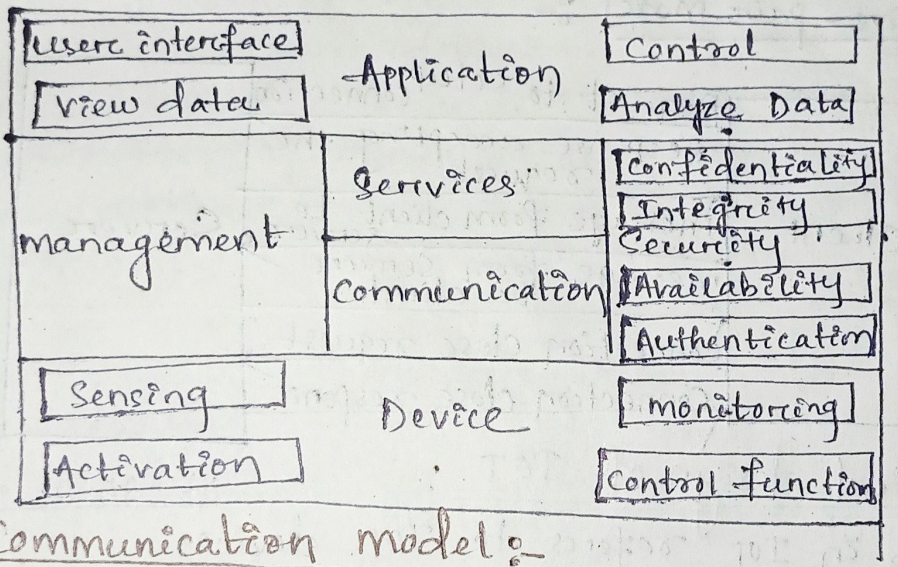
→ As we gain efficiencies, novel experiences and other benifits from the IoT, it would be a mistake to forget about Security Concerns associated with it.

→ There is a high level of transparency and privacy issues with IoT.

→ It is a important to secure the end points, the networks and the data in transfered across all of it means creating a security paradism.

## Logical Design of IoT :-

Dt - 20.01.24

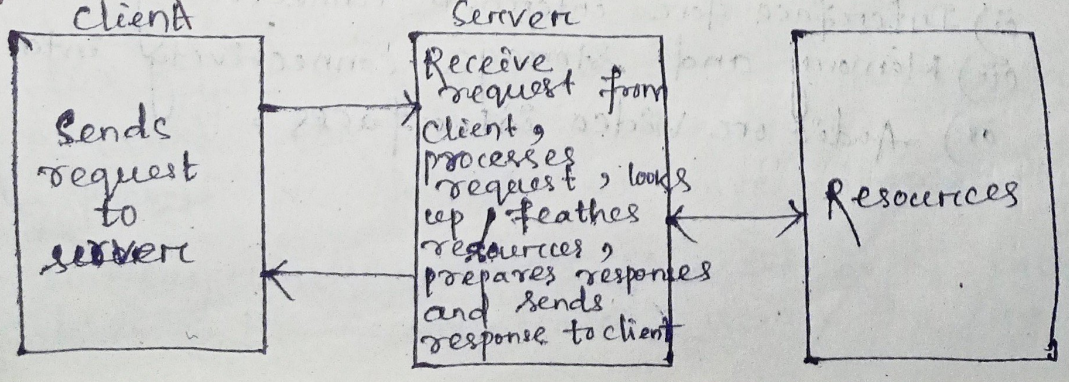



## IoT Communication model :-

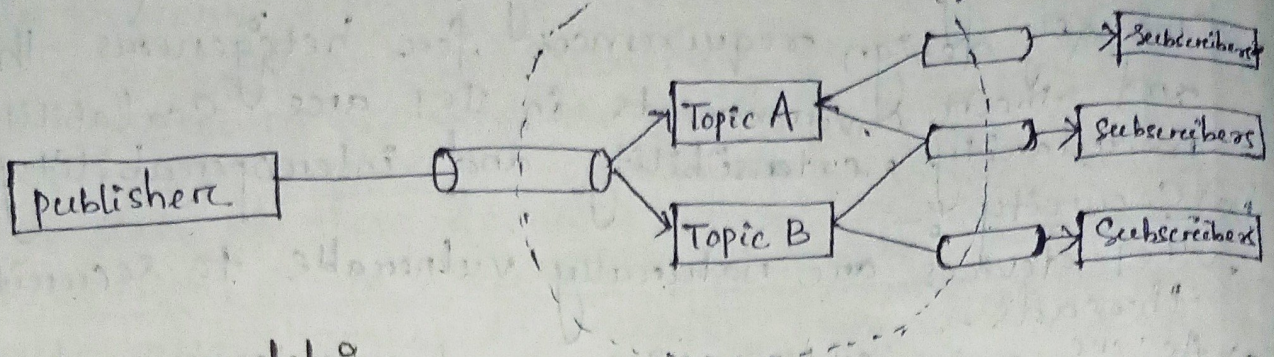
→ Four types of communication model :-

i) Request - Response model.
ii) Publish - Subscribe model
iii) Push - pull model
iv) Exclusive - pair model.

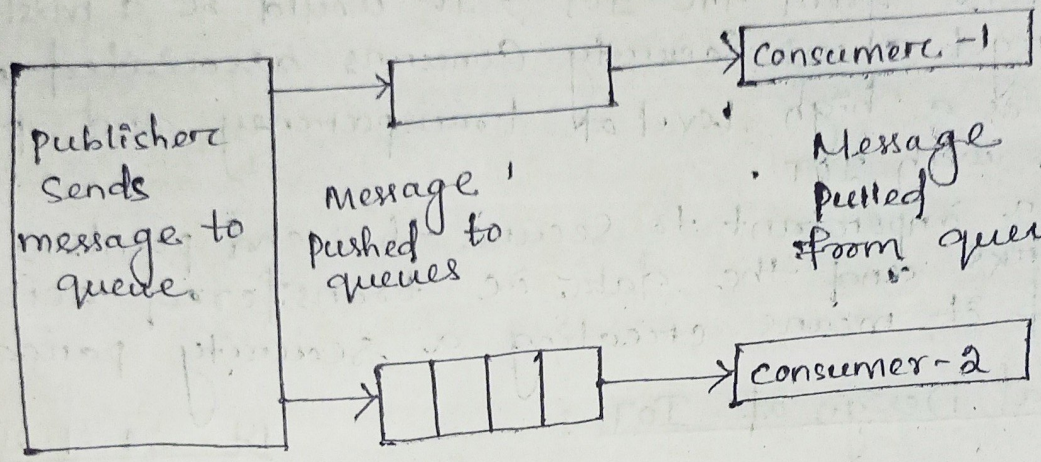
### i) Request - Response model :-



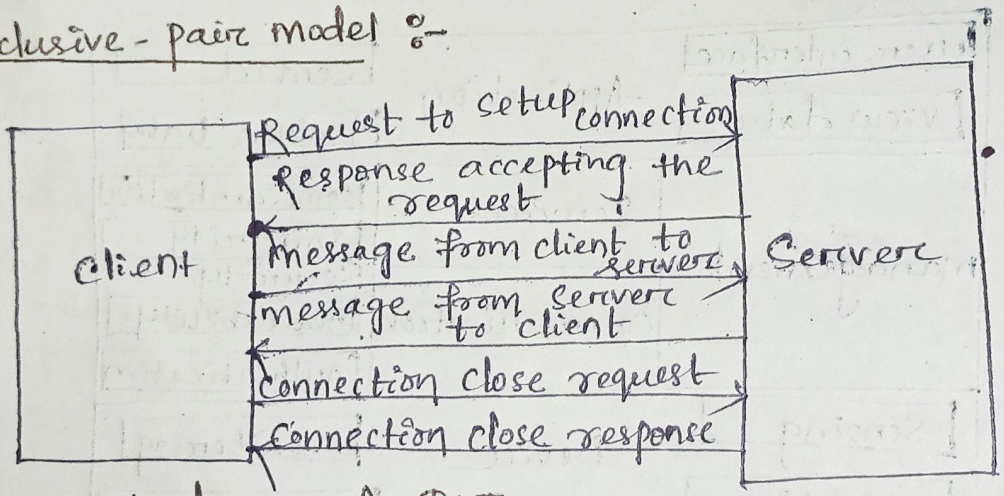
ii) Publish - Subscribe model :-




iii) Push-pull model :-

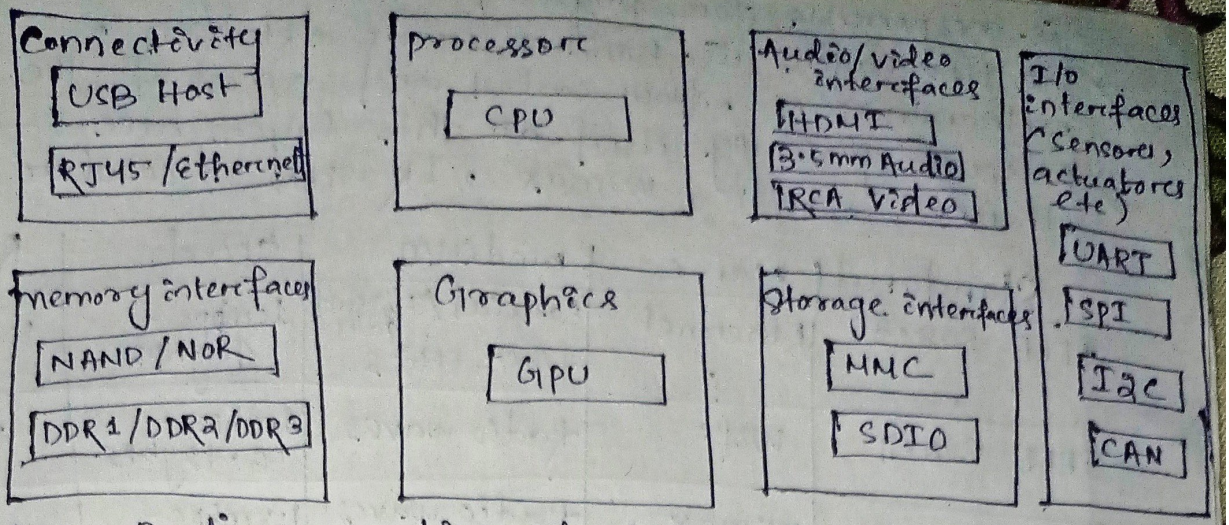



iv) Exclusive - pair model :-




Physical design of IoT :- Dt - 25.01.24

→ Things in IoT refers to IoT devices
→ Things can exchange data with other connected devices and applications, collect data from other devices and process the data either locally or send it to centralized servers or cloud.
→ IoT devices can have several interfaces like :-
  i) I/O interface for Sensors.
  ii) Interface for internet connectivity.
  iii) Memory and Storage connectivity interfaces.
  iv) Audio or video interfaces.

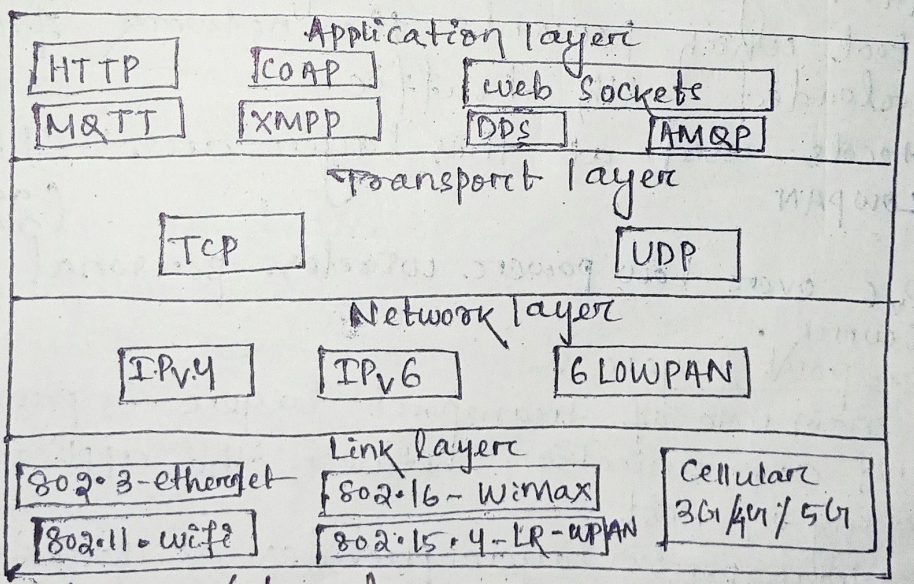



RCA - Radio corporation of America
UART - Universal asynchronous receiver or transmitter
CAN - control area network
I2C - Inter integrated circuit.
SPI - Serial peripheral interface.

Def?:- physical design of IOT follows a protocol that contains a set of rules to govern the communication between two or more devices.

→ A protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods.

## Physical Design of IOT (protocols) :- Dt - 29.01.24




### i) Datalink layer / link layer :-

→ The link layer is responsible for establishing and terminating links between the node.
→ The packets or datagrams travel through these links.
→ The link layer also defines the format of packet that is to be communicated across the link and

is responsible for physical addressing.

→ The link layer also handles error detection, retransmission, flow control and access of the link.

→ protocols generally used at this layer are, ethernet, wifi, wimax, LR-WPAN, cellular etc.

| Standard | Name | medium | Speed | Range |
|---|---|---|---|---|
| IEEE 802.3 | Ethernet | coaxial / Twisted pair fiber optics | 10mbps - 40gbps | 100m |
| IEEE 802.11 | Wifi | Radio waves | 1mbps - 6.75gbps | 30m |
| IEEE 802.16 | Wimax | Radio waves | 1.5mbps - 1gbps | 50km |
| IEEE 802.15.4 | LR-WPAN | Bluetooth | 40kbps - 250kbps | 10m |
| 2G/3G/4G/5G | cellular | Radio waves | 9.6kbps - 100mbps | 16km |

Network layer :-

→ The main role of network layer is to transfer the packets from sender to receiving post.

→ The network layer also handles routing which involves selecting the next node and forwarding the next packets across the communication path.

→ The network layer is also responsible for logical addressing i.e. IP addressing and for congestion control which prevents the network from being overloaded with traffic.

→ protocols used at this layer are :- IPv4 (add. size-32), IPv6 (add. size-64), 6LOWPAN

IPv6 over low power wireless personal area network.

Transport layer :-

→ The main role of transport layer is providing end to end communication between the applications running on host.

→ The transport layer provides a logical communication channel through the end applications can communicate with each other.

→ The transport layer is implemented on the end host.

→ It is not present in the routers.

→ The transport layer is also responsible for reliable delivery of the message across the end nodes, flow-control and multiplexing and demultiplexing of the

channel at end node.
→ Protocols used at this layer are :- TCP, UDP.

Dt- 30.01.24

Application layer :-
→ The application layer is where users of an IOT applications interact with the IOT system.
→ The application layer allows the users to interact with the sensors and access other services provided by the communication network.
→ The application layer provides services like authentication, naming, message formating, E-mail etc to the users.
→ Protocols used at this layer are:- HTTP, COAP, MQTT, DDS, web sockets, AMQP

HTTP :- (Hypertext transfer protocol)
→ It uses TCP, stateless, Request-Response model.

COAP :- (constraint application model)
→ It uses UDP, Request-Response model.

MQTT :- (message queue telemetry transport)
→ It follows publish-subscribe model.
→ No security.
→ Used with low power devices.

XMPP :- (extensible messaging and presence protocol)
→ Real time communication for sending XML data.

AMQP :- (Advanced message queuing protocol)
→ Support both point to point and publisher-subscribe model.
→ High performance and secure protocol.
→ It uses Tcp.

web socket :-
→ Full duplex connection over a single socket connection.
→ Uses Tcp.

DDS :- (Data distribution Service)
→ middleware standard reliable than MQTT
→ follows publish-subscribe model.
→ It uses UDP.

Design challenges in IOT :-

1) Interoperability :-
→ Interoperability refers to the ability of different systems, devices or components to work together seamlessly and exchange data efficiently.
→ In the context of IOT interoperability is a critical challenge as a large number of diverse devices are being connected to the internet.

→ The lack of Standardization in the IOT can lead to difficulties in communication and data exchange between the devices ~~with~~ which resulting in an fragmented and inefficient system.

→ To overcome this challenge organization and industry groups are working to establish standard and protocol to ensure intercopercability between the IOT devices.

ii) Security :- Dt - 1.02.24

→ Security is a critical concern in the IOT as it involves the protection of sensitive data and systems from @ unauthorised access, theft or damaged.

→ IOT devices are less vulnearable to cyber attacks due to their increased exposer to the internet and they are limited computing resources.

→ four types of security :-

a) Device security
b) network security.
c) Data security.
d) privacy.

a) Device security :-
ensuring that IOT devices are protected from malware and unauthericised access.

b) Network security :-
protecting the communication between IOT devices, IOT infrastructure and the network from cyber attacks.

c) Data security :-
Security the data collected and transmitted by IOT devices from unauthericised access or tampering.

d) Privacy :-
protecting the privacy of individuals whose personal information is collected and transmitted by IOT devices.

iii) Scalability :-

→ Scalability refers to the ability of a system to handle increasing workloads or numbers of users without a significant decline in performance.

→ Scalability is a major challenge as the number of collected devices is rapidly growing and leading to an increased volume of data and communications.

→ factors are :-

a) Data management :
effectively managing and storing the large amount of data generated by IOT device

b) Network capacity:-
Ensuring that networks have sufficient capacity to handle the increased volume of data and communications.

c) Device management:-
Efficiently managing the growing number of IOT devices and ensuring that they can be easily configured and maintained.

Dt - 3.02.24

iv) Reliability :-
→ Reliability refers to the ability of a system to perform its intended functions consistently and without failure over time.
→ In the context of IOT reliability is a critical concern as the failure of even a single IOT device can have significant consequences.

a) Device failure :-
Ensuring that IOT devices are designed and built to be reliable and function correctly even in haresh environment.

b) network connectivity :-
Maintaining stable and reliable connections between IOT devices and network even in the face of hardware or software failures.

c) Data accuracy :-
Ensuring that data collected and transmitted by IOT devices is accurate and reliable.

v) Power consumption :-
→ Power consumption refers to the amount of energy that a system or a device can use.
→ In the context of the IOT power consumption is a critical challenge as many IOT devices are designed to be small, low power and operate using batteries.

a) Battery life :-
Ensuring that IOT devices have sufficient battery life to operate without frequent recharging or replacement.

b) energy efficiency :-
Making sure that IOT devices are designed to use energy efficient and reduce the overall power consumption of the system.

c) power management :-
Implementing effective power management techniques

Such as sleep modes to reduce the consumption of IOT devices when they are not in use.

Deployment challenge with IOT :- 01-5.02.24

1) Connectivity :-
→ It is the foremost concern while connecting devices, applications and cloud platforms.
→ Connected devices that provide useful front and information are extreamely valuable.
→ But poor connectivity becomes a challenge where IOT sensors are required to monitor processed data and supply informations.

2) Cross platform capability :-
→ IOT applications must be developed, keeping in mind the technological changes of the future.
→ It's development requires a balance of hardware and software functions.

3) Data collection and processing :-
→ In IOT development data plays an important role and it is critical to process and use the stored data.
→ Along with security and privacy development teams needs to ensure that they plan well for the way data is collected, stored and processed within an environment.

4) Lack of skill set :-
All the development challenges can only be handled if there is a proper skill resource working on the IOT application development.

5) Integration :-
Ensuring that IOT devices and systems integrate seamlessly with existing technology and infrastructure.

6) Network Infrastructure :-
Building and maintaining the network infrastructure needed to support the large number of connected IOT devices.

7) Device management :-
Efficiently managing and maintaining the large number of IOT devices in a deployment.

8) Data management :-
Managing and analyzing the larege amount of data generated by IOT devices and Integrating with existing data system.

9) Securcity :-
Ensurcing that the IOT deployment is secure from threads such as eyber attacks, data breach and Unauthercised access.

10) Cost :-
Balancing the cost of deploying and maintaining an IOT system with the benifits it delivers.

Unit-2 Dt- 6.02.24

# Components of IOT

Identification, Sensing, Communication, Computation, Services, Semantics

**Identification :-**

- The identification component deals with naming and addressing.
- Some of the naming schemes for naming the IOT devices are electronic product code (EPC) and uCode
- These schemes can be used to provide unique names to the IOT devices.
- The technologies that are used for addressing, the IOT devices are IPv4, IPv6 etc.
- Using these technologies we can assign IP addresses to IoT devices which are unique across a network.

**Sensing :-**

- The sensing components includes sensors, actuators, and ~~wearable~~ wearable devices.
- Sensors are tiny devices which can sense physical phenomena and represent them in a human readable format.
- The actuator is a device which receive instructions and performs an operation on another device.
- Sensors are generally act as input and actuators are act as output.
- Wearable items are portable smart devices which can send and perform operations and sent notifications.

**Communication :-**

- The communication component plays a key role in an IOT system.
- This component helps in sensing the data from sensors to a server and again backed from servers to computing devices to which sensors are attached.
- This component contains different networking devices like switches, routers etc. and different protocols like RFid, Bluetooth, IEEE 802.15.4 → wifi etc.

Dt - 8.01.24

**Computation :-**

- The computation components involves hardware and software.
- The hardware contain devices like Sensors, actuators computing devices etc.
- Examples of computing devices are Node MCU, Arduino, Raspberry pi etc.
- These computing devices are used for performing computation on the data gathered by the Sensores and

run programs.

→ The software typically runs on a computing device may be a middleware software or APIs on the cloud.

→ Examples of such software are Contiki OS, Tiny OS, AWS, Azure, google cloud platform.

Services :-

→ Different types of services can be provided in an IOT system.

→ They might be provided as middleware services.

→ Examples of services are identity related services, information aggregation services, collaborative awareness services, ubiquitous services.

Semantics :-

→ The semantic component deals with the interoperability.

→ ~~Different devices~~ It allows different devices to communicate with each other seamlessly.

→ Some of the technologies are languages that provides semantic interoperability and resource, description framework (RDF)

→ Web Ontology language (OWL) and efficient XML Interchange (EXI).

| | | |
|---|---|---|
| Identification | Naming | Epc, ucode |
| | Addressing | IPv4, IPv6 |
| Sensing | | Sensors, Actuators wearable |
| Communication | | RFID, NFC, UWB, Bluetooth, BLE, IEEE 802.15.4, z-wave, wi-fi |
| Computation | Hardware | Arduino, Raspberry Pi |
| | Software | contiki OS, Tiny OS, AWS, Azure, google cloud |
| Semantics | | RDF, OWL, EXI |
| Services | | Identity related, information aggregation, Collaboration awareness. |

Dt - 10.02.24

## Control units :-

→ The internet of things is rarely discussed without processing the collected data from real world and the processed data for any conclusion.

→ Sensors are the source of IoT data.

→ Driven by new innovations in materials and nano-technology, sensor technologies are developing at a rapid speed and with a result of increased accuracy, decreased size and cost.

→ This results in to provide ability to measure or detect things that were not previously possible.

i) Transducer :-

→ A better term for a sensor is transducer.

→ Physical device that converts one form of energy into another form is called transducer.

→ The transducer converts some physical phenomenon into an electrical impulse that can then be interpreted to determine a reading.

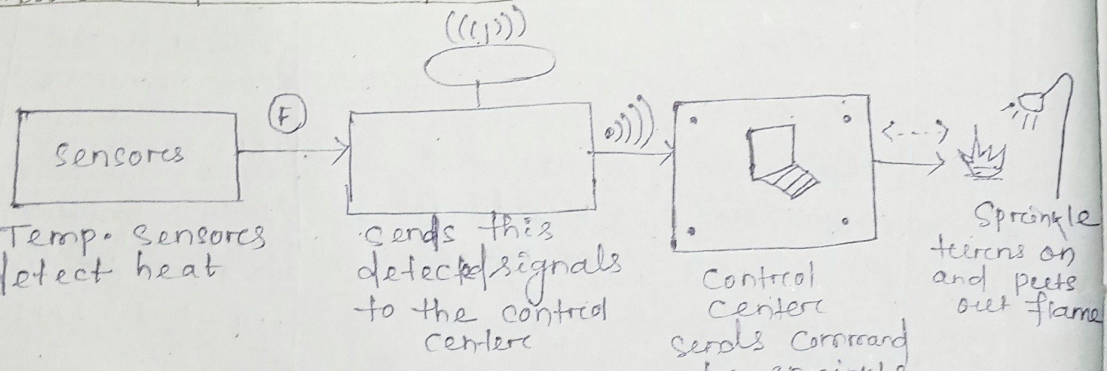
ii) Actuator :-

→ Another type of transducer which opercates in the reverse direction of a sensor.

→ It takes an electrical input and turns it into physical actions.

→ For example : An electric motor, A hydraulic system

Sensor to Actuator flow :-




Different types of Sensor :-

i) pressure sensor.
ii) Proximity sensor.
iii) optical sensor.
iv) accelercation sesor.
v) Load sensor.
vi) Humidity sensor.
vii) tilt / level sensor. etc.

Type of Acturatores :-

i) LED
ii) Relay

iii) motores
iv) Lasers
v) Speakers
vi) LCD display. etc.

Dt- 12.02.24

## Bluetooth :-

→ It was invented by Ericsson in the years of 1994.
→ Bluetooth has been used as a wireless channel for connecting devices.
→ Since then bluetooth has become the standard for wireless communication in wearable gadget and other devices.
→ Bluetooth is now available in automobiles, speakers, medical equipments, wireless ~~head~~ earphone etc.
→ Bluetooth is a short range wireless technology means for transmitting data over a short distance between two electronic devices.

## Bluetooth with IOT :-

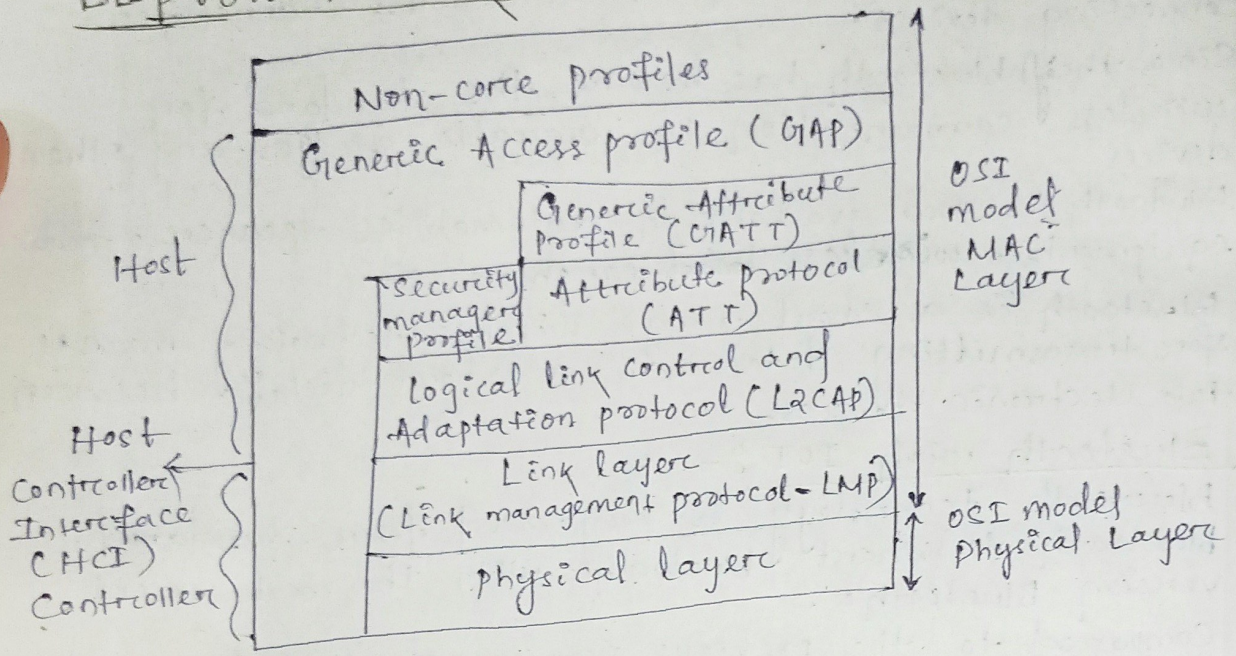
→ Bluetooth technology is progressed from standard bluetooth to smart bluetooth with the most recent version Bluetooth 5.
→ Compared to the previous version Bluetooth 5 provides five times the range, quadruple the data speed and 800% greater data transmitting frequency.
→ Furthere more bluetooth low energy (BLE) is a form of bluetooth optimized for low powerd devices and can assist IOT devices in conserving energy by keeping them in sleep mode until they are connected.
→ BLE is perfect for IOT applications since it can pair and reconnect with devices in 10 seconds instead of 10 seconds with traditional bluetooth.
→ This not only improve operating efficiency but also increases device availability.
→ The hardware Communication, software system and application layers make off a typical IOT design with bluetooth serving as the communication layer.
→ The communication layer which is consist of a multi-layer stack that includes data connection, network or transport and session protocol is a vital link between the layers.
→ Bluetooth which is often known as BLE is a data communication layer that links sensores to sensores or sensores to getways.

→ On the other hand the network layer is incharge of routing or transporting package across the network using the best pathways possible.

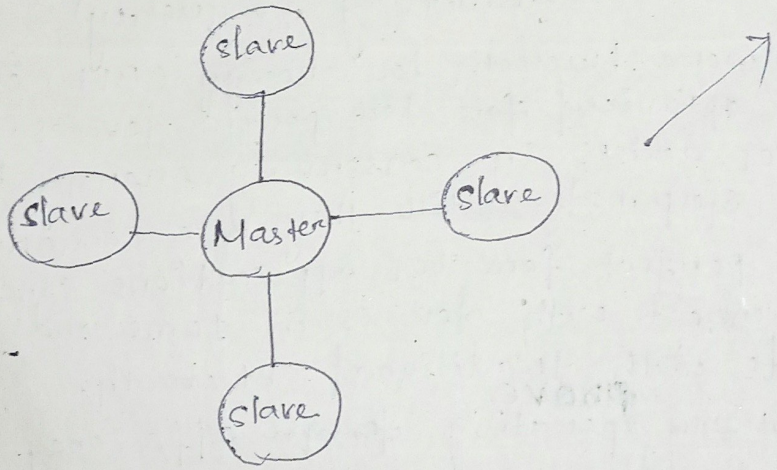
→ The session layer protocols allows communication between different aspects of the IOT communication Subsystem

Dt- 13.02.24

## BLE Protocol stack :-




## Stare topology :-




### piconet

i) Device can function either a master or slave.

ii) Servers have smaller coverage area.

iii) Supports maximum 8 nodes.

iv) Less efficient in terms of uses of bandwidth.

### scatternet

i) Device can function as master or slave or master plus slave.

ii) Servers have large coverage area.

iii) It supports more than 8 nodes.

iv) It is more efficient in terms of uses of bandwidth.

→ BLE belongs to IEEE standard of 802.15.4.1

Star topology:-

→ Star is the only topology accepted by BLE
→ Any data exchange between two slave devices shall pass through the unique master.
→ A slave device may not be connected to two master units at a time.
→ Using a similare protocol stack as classic bluetooth, the differences between them stack above the L2CAP layer.

BLE protocol stack :- Dt - 16.02.24

i) Physical Layer :-

→ The transmitter uses GFSK (Gussian frequency shift keying) modulation and operates at unlicensed 2.4 GHz frequency band.
→ Using this physical layer BLE offfers data rates of 1mbps for bluetooth version 4.2 and 2mbps for bluetooth version 5.0
→ It uses frequency hopping transceiver.
→ Two physical layer variance are specified as encoded and coded.
→ A TDD (Time division duplex) topology is employed in both of the physical modes.

ii) Link layere :-

→ It is responsible for advertising, scanning, creating or maintaining connections.
→ The role of BLE devices is changed in peer-peer that will be unicast or broadcast mode.

iii) HCI :-

→ It provides commenications between controllers and host through standard interface types.
→ This HCI layer can be implemented either using API or by interfaces such as UART (universal asynchronous receiver and transmitters) / SPI / USB.

iv) L2CAP :-

→ This layer offers data encapsulation services to upper layer.
→ This allows logical end to end data communications.

v) SMP :- (security manager protocol)

→ This layer provides methods for device pairing and key distribution.
→ It offfers services to other protocol stack layers in order to securely connect and exchange data between BLE

devices.

Dt - 26.02.24

## Zigbee :-

→ Zigbee is one of the wireless personal area network specification.
→ It is design to meet low power and low datarate applications is developed under IEEE 802.15.4 standard.
→ Typically zigbee is used in establishing a smart home for devices from different manufactures to communicate with each other to enable automation.
→ If we want a network for short range communication for streaming audio we go for bluetooth. where as streaming video and large files we use wifi.
→ But we need a network using which we can connect a large number of battery power devices
→ For this purpose we can not go for wifi because of its high energy requirement. and we can not go for bluetooth as only a small number of devices can be connected to using bluetooth.
→ Finally we need a network that can connect many battery powered devices and to consume low power, zigbee technology was developed.
→ Zigbee revolves around control and sensore network.
→ Hence it is one of the most common standard and applications for the internet of thing.

## Mesh topology :-

→ Zigbee network use mesh topology which gives a separate link for every device pair in the network
→ Even if one link fails, the network can utilize another alternate path or link for communication.
→ Hence it is reliable.

## Physical devices of zigbee :-

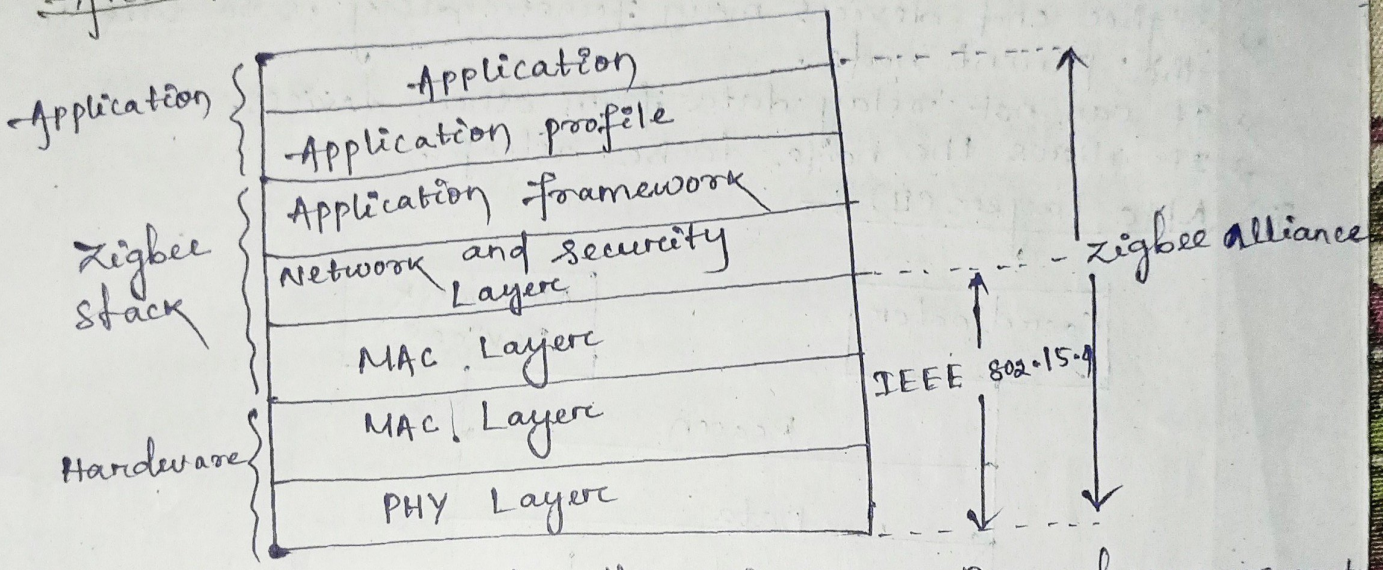
1) Coordinator
2) Router
3) End devices.

→ The radio designs used by zigbee are optimized for low cost in large scale production.
→ It has few analog stages and use digital circuits where ever possible.
→ The protocols are designed to communicate data through hostile RF environment.

→ The current protocols supports becon and non-becon enable networcks.
→ In Non-becon enable network an unslotted CSMA-CA channel access mechanism is used.
→ In this type of network the routers typically have their receivers continuously active, requiring a more roberst power supply.
→ Zigbee devices are basically of three types :-
i) coordinator
ii) Routers
iii) End devices.

Dt- 27.02.24

Architecture :-




→ Zigbee alliance contains the software, Brand management network, security and application layers.
→ IEEE 802.15.4 describes hardware, physical and MAC layer.

i) Physical layer :-
→ It activates and deactivates the radio transceiver.
→ Energy detection is within the current channel.
→ Link quality indication (LQI) service is provided for received datapackets.
→ Clear channel assesment for CSMA-CA.
→ Channel frequency selection.
→ Data transmission and reception.

ii) MAC Layer :-
a) Device class :-
→ There are two type of devices based upon their functionality.
→ Full function device (FFD) is a device which can talk to any device.

→ Reduced function device (RFD) is a device which can not talk to all devices.

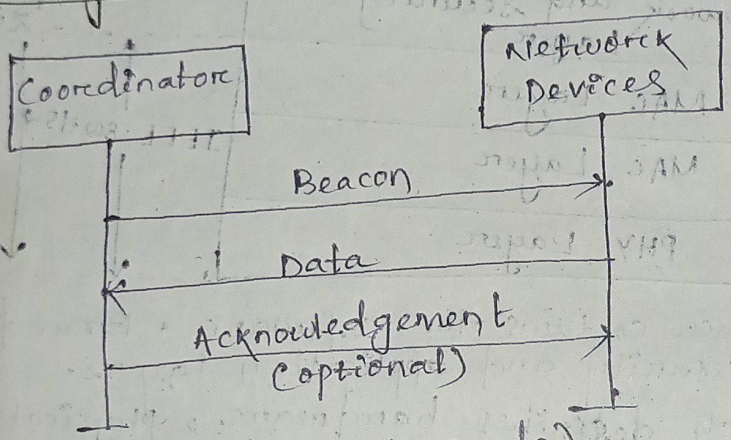
b) Address :-
→ All devices must have 64 bit IEEE addresses.
→ A short address of 16 bit can be allocated to reduce data packet.

c) Device :-
i) coordinator :-
→ It is the root of the network tree.
→ It act as a bridge to other networks.

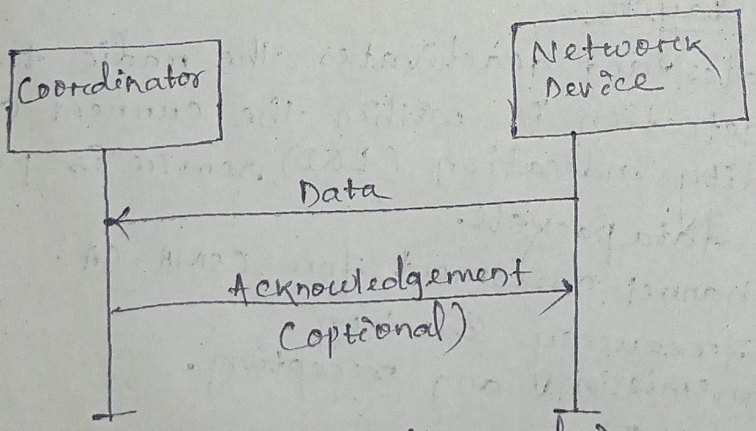
ii) Routers :-
→ Zigbee routers is act as an intermediate routers.

iii) End devices :-
→ Zigbee end devices main functionality is to talk to the parent node.
→ It can not relay data from other devices.
→ It allows the node to be asleep.

iii) MAC layers (II) :-




(Beacon Enable Mode)




(Non-Beacon enable mode)

Transmission mode :-
→ In Becon enable mode data are transmitted periodically and repeatative low latency of data is available.
→ In Non-Beacon enable mode network devices are not receiving any kinds of message from

coordinator and data intermittend is there.

Dt- 29.02.30

## Zigbee Network properties :-

→ Zigbee built on physical layer and media access control defined in IEEE standard 802.15.4 for low rate wireless personal area network.
→ WPAN low rate is the newest technology and provides specifications for devices that have low data rate, consume less power and are thus characterised by long battery life.
→ It operates in the ISM band of 2.4 giga Hz in world wide except 784 MHz in China and 868 MHz in Europe. and 915 MHz in USA and Australlia.
→ It is also more economical than wifi and bluetooth which make it simpler.
→ The devices can run for years on inexpensive batteries for a host of monitoring and controlling applications.

## Applications :-

→ Zigbee is intended for embedded applications with low power consumption and low datarates.
→ As Mobility is a constraint, hence it is not suitable with radio equipment.
→ Typical application areas includes :-
i) Automation system.
ii) wireless sensor Networks
iii) Industrial control.
iv) Medical data collection
v) smoke alarm etc.

## Advantages :-

→ zigbee is the best network for battery powered devices as it allows them to turn off when they are not used.
→ Though battery powered, zigbee devices can have a good life span due to the networks power saving capabilities.
→ zigbee is an open standard, as a result there are a large variety of devices available from different manufacturers.
→ zigbee devices are available at low cost.
→ The network stage reliable due to its mesh topology.
→ Extending a wifi network is more time consuming and costly than extending a zigbee network.

Disadvantages :-

→ If the one coordinator fails, the whole network goes down.
→ when the coordinator is replaced, all the zigbee devices are not automatically connected through the new coordinator.
→ Every connected has to be manually established again.
→ The open standared of zigbee brought compatibility issues which means not every zigbee device is compartible with every zigbee network.
→ zigbee 3.0 forces the manufacturers to follow a specific standard to be certified.
→ Due to its low bandwidth zigbee does not support audio and video applications.

telemetry - 2.03.24

MQTT :- (Message queuing transport).

→ MQTT is a light weight, publish - subscribe base, messaging protocol designed for resource constraint devices and low bandwidth, high latency or unreliable networks.
→ It is widely used in IOT applications providing efficient communication between sensors, actuators and other devices.

Different features of MQTT protocol :-

1. Light weight :-

→ IOT devices often constraints in terms of processing powers, memory and energy consumption.
→ MQTT's minimal overhead and small packet size make it ideal for these devices as it consumes fewer resources, enabling efficient communication even with limited capabilities.

2. Reliable :-

→ IOT networks can experience high latency or unstable connection.
→ MQTT supports for different quality of service (QOS) levels, session awareness and persistent connection to ensure reliable message delivery even in challenging conditions.

3. Secure communications :- TLS (transport layer security) / SSL (

→ Security is crucial in IOT network as they often transmit sensitive data

→ MQTT supports TLS (transport layer security) and Secure socket layer (SSL) encryption to ensure data confidentiality during transmission.
→ Authentication and Authorization mechanism can be achieved by username or password credentials or client certificates.
→ to safeguarding → the access to the network, and its resources.

4. Bi-directionality :-
→ MQTT's publish-subscribe model allows for seamless bidirectional communication between devices.
→ Client can both publish messages to topics and subscribe to receive messages on specific topics which enables effective data exchange in diverse IOT ecosystem without direct coupling between devices.
→ This model also simplifies the integration of new devices to ensure easy scalability.

5. Continuous and stateful sessions :-
→ MQTT allows clients to maintain stateful sessions with the brokers which enable the system to remember subscription and undelivered messages even after disconnection.
→ clients can also specify a keep alive interval during the connection which prompts the brokers to periodically check the connection status.
→ If the connection disconnect, the brokers stores undelivered messages and attempts to deliver them when the client reconnects.
→ This feature ensures reliable communications and reduces the risk of data loss.

6. Large Scale IOT device support :- Dt- 4.03.24
→ IOT systems often involve a large number of devices which require a protocol that can handle massive scale deployment.
→ MQTT is light weight in nature, low bandwidth consumption and efficient use of resources make it well suited for large scale IOT applications.

7. Language support :-
→ IOT systems often includes devices and applications developed using various programming languages.

→ MQTT's broad language support enables easy integration with multiple platforms and technology and fostering seamless communication and interoperability in diverse IOT application.

How MQTT works :-

→ To understand how MQTT protocol operates, we need to learn the concept of MQTT client, MQTT broker, publish-subscribe model, topic.

Components :-

MQTT client :-

→ Any applications or devices running the MQTT client library is an MQTT client.

→ for example an instant messaging app that uses MQTT as a client., various sensors that use MQTT to report data are a client and various MQTT testing tools are also a client.

MQTT broker :-

→ MQTT broker handles client connection, disconnection, subscription, unsubscription request and routing messages.

→ A powerful MQTT broker can support massive connection and minimum level message throughput, helping IOT service provider to focus on business and quickly create a reliable MQTT application.

Publish-subscribe model :-

→ The publish subscribe pattern is different from client server pattern in which it separate the client and send messages from the client that receives messages.

Subscribe model :-

→ Publishers and subscribers do not need to establish a direct connection that the MQTT broker is responsible for routing and distributing of all messages.

Topic :-

→ The MQTT protocol routes the messages based on topic where the topic distinguishes the hierarchy.

QOS :-

→ MQTT provides three kind of QOS and guarantee

Messaging reliability in different network Environment

i) QoS 0 :-
→ The message is delivered atmost once.
→ If the client is not available currently, it will loose the messages.

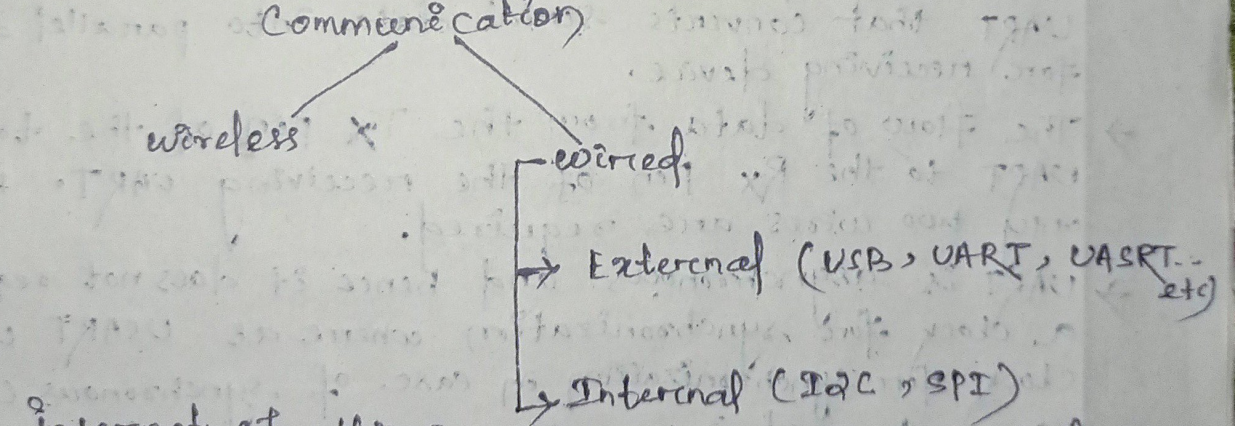
ii) QoS 1 :-
→ The message is delivered atleast once.

iii) QoS 2 :-
In this the message is delivered only once.

Work flow :-
Step-1 : client initiate a connection to the broker using TCP/IP with optional TLS or SSL encryption for secure communications.
Step-2 : client either publish messages to specific topics or subscribe to topics to receive messages.
Step-3 : The broker recives published message and forward them to all client and subscribe to the relevant topics.

ii) It ensures reliable message delivery according to the specified QoS level, and manage message storage for disconnected clients based on session type.

Wired communication & protocols :- Dt - 5.03.24




→ The internet of things refers to a network of devices which communicate with each other through the internet by wired or wireless medium.
→ when connected a laptop or smartphone to an IoT infrastructure, it can automate and form a network of all the connected devices.
→ The type of network choosen depends on the network range, network bandwidth, power uses and security etc.

## External communication protocols :-

(1) USB :- (Universal serial Bus)

→ USB stands for Universal serial Bus. Hence it is a serial communication protocol for connecting devices with USB ports.

→ It also provides a fast Master-slave interface supporting up to 127 devices.

→ A PC is generally the master or host and each of the other components or devices link to it are called slaves.

→ USB 1.X, USB 2.X, USB 3.X uses 4 lines Vcc, GND, D+, D-.

→ Data is though transferred in the form of packets which is compost of 8 bits with least significant bit (LSB) is transmitted fast.

Pros :-

→ It is simple and fast.

→ It is almost acceptable in everywhere.

Cons :-

→ It requires powerful master slave devices.

→ particular drivers are required.

(2) USART / UART :- (Universal asynchronous receiver transmitter)

→ USART stands for Universal synchronous asynchronous receiver transmitter.

→ UART converts data into serial data.

→ Though UART communicate directly by converting data into serial form and transmit it into the receiving UART that converts serial data into parallel data for receiving device.

→ The flow of data from the Tx pin of the transmitting UART to the Rx pin of the receiving UART. Hence only two wires are required.

→ UART is asynchronous and hence it does not required a clock for synchronization where as USART uses a clock for synchronization in case of synchronous communication.

→ It can be used in asynbronous communication also. Hence USART is a dual type of serial communication.