IOT Module 2

PAGE No. DATE / /

* Communications Criteria :- describes the characteristics and attributes of access technologies.

- Generally, for smart object connectivity, wireless communication is prevalent
  - as it eases deployment
  - allow smart objects to move without loosing connectivity.

Criteria / Attributes of communication :-

01] Range :-

- Short Range :- tens of meters of max dist betn 2 devices alternative to serial cable.
  Eg: Bluetooth (IEEE 802.15.1), Visible light communications (VLC)

- Medium Range :- tens to hundreds of meters betn 2 devices.
  In wireless → Examples are IEEE 802.11 WiFi, Low Rate WPAN, SUN (Smart Utility N/w), LORA, etc.
  In wired :- 802.3 Ethernet, Narrowband Power line Communications (PLC)

- Long Range : greater than 1 mile (1.6 Km) betn 2 devices.
  Wireless → 2G, 3G, 4G, Outdoor Wifi, Low Power wide area commu. (LPWA).
  Wired → Ethernet over optical fiber, Broadband PLC.

* (NB-IOT) Narrow band - IoT is a technology designed for connecting many small, low-power devices to internet. It is part of grp of technologies known as Low Power wide area (LPWA) networks. which are built to handle lots of devices with minimal ~~use~~ energy use.

DATE / /

NB-IoT is especially good at reaching devices in areas with poor signal. It helps devices to use less battery power, so that they may last more than 10 years, which is ideal for long-term appln like env monitoring, etc.

02] Frequency Bands :-
Radio spectrum is regulated by countries/or organizations (Eg: International Telecom. Union (ITU))

- freq bands leveraged by wireless communications are split between licensed and unlicensed bands.

- Licensed :- applicable to long-range access technologies. users must subscribe to services.
Common licensed spectrum for ~~cellular~~ IOT :-
Cellular (900 - 2100 MHz), NB-IoT (700 - 900 MHz)

- Unlicensed :- (ISM) → industrial, scientific & medical portions of radio bands. It has no guarantee & interference protections offered
ISM bands for IoT → 2.4 GHz, 5 GHz, 915 MHz for wifi.

ISM Bands in India :-
1) 900 MHz : more robust, less prone to interference less attenuation. low bandwidth hence, small data transfer speed.
2) 2.4 GHz :- higher b/w. allows more data transfer speed. Components are smaller, ~~&~~ cheaper.
Congested due to abundance of wifi, Bluetooth. Attenuation much more quickly. will not pass thr metal.

India also allow 865-867 MHz ISM band.

3] 5GHz: Higher b/w. allows large data transfer speed. less congested, few RF devices in this band low transmit power limitations. High attenuation in cables, requires very high gain antennas.

5] Power Consumption :-

- Powered Nodes :- node has a direct connection to a power source. ease of deployment is limited by the availability of a power source.
  - makes mobility more complex.

- Battery powered nodes :- bring more flexibility to IoT devices. batteries are small, can be charger or recharged. IOT wireless access tech. must take care of need of low power consumption, & connectivity for battery-powered nodes.

2)

6] Topology :- 3 main topologies are: star, mesh & peer to peer.
for long range & short range → star topology
for medium range: Star, peer to peer, or mesh.
IEEE 802.15.4, wired PLC are generally deployed as a mesh technology. Indoor Wifi deployments are generally star topologies.
(full function device)

* FFD :- A powerful device in the network that can handle all kinds of tasks, including coordinating other devices, sending / receiving data & routing messages. An FFD could be like a central smart home hub that connects to all your smart lights, etc.

DATE / / /

* RFD (Reduced function device) :- A simpler, more specialized device that performs specific tasks and communicates with FFDs, typically to save power & reduce complexity.
(A device that can implement a subset of protocol functions to perform specialized part)
Eg: In same smart home, RFD can be a temperature sensor sends info to FFD.

5] Constrained Devices :-
Constrained nodes have limited resources that impact their networking feature set and capabilities.
There are 3 classes for constrained nodes.

Class 0, 1, 2	RAM	
Class 0	<10KB	(Push buttons)
Class 1	>10KB	(Sensors)
Class 2	>50KB.	(Smart meter)

6] Constrained-Node Networks :-
They are also known as low-power & lossy networks (LLNs).
When evaluating protocols used in this networks, there are few imp things to look at :-

1) Data Rate & Throughput
Data rate is how fast data can be send over NW.
Throughput is how much data actually gets sent.
It is less than data rate due to congestion or interference.

2) Latency & ~~determination~~ determinism :-
In networks, where timely ~~delay~~ delivery is crucial, special techniques like Time Slotted Channel Hopping (TSCH) are used,

Determinism refers to how predictable network's performance is.

3) Overhead & Payload:
Extra data needed to manage & control the network (headers)
payload :- actual data you want to send (data).

If you want to send more data than limit, it needs to be broken down into small chunks. This process is called fragmentation.

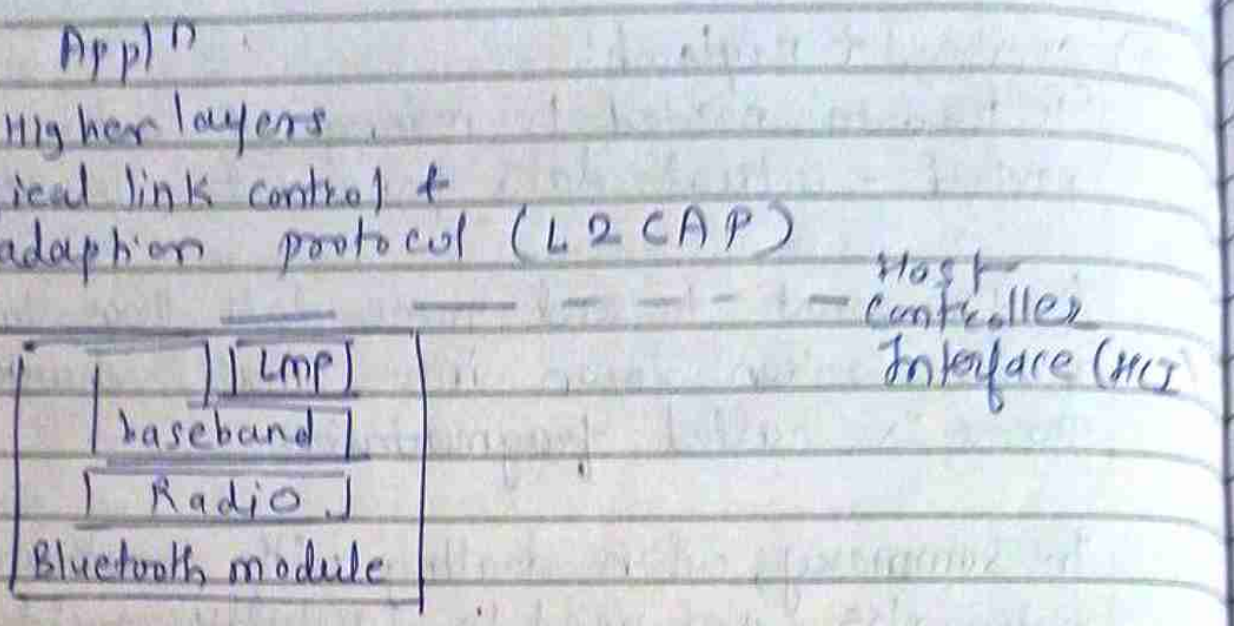
In summary, when dealing with constrained-node networks, you need to carefully consider how fast data can be sent, how quickly it can be processed, how much extra data is needed for network management, & how to handle large data by ~~breaking~~ fragmentation.

* IoT Access Technologies :-

It refers to various methods and standards used to connect IoT devices to a network.

1* Bluetooth :- It is widely used wireless technology designed for short range communication between devices. operates in 2.4 GHz ISM band & is designed for low power, low cost wireless communication.
Key features :-
Short Range
low power consumption
low data rate
frequency hopping : Uses freq hopping spread spectrum to reduce interference.

Architecture:-



- Bluetooth module :- Physical h/w component
- Radio :- this layer deals with physical aspects of radio wave transmission including freq hopping, modulation, etc
- Baseband :- handles digital aspects of data transmission (addressing, packet formatting, timing & power control)
- Link Manager Protocol (LMP): manages links betn devices (authentication)
- HCI :- It handles communication betn Bluetooth module & Host device.
- L2CAP :- provides connection-oriented & connectionless service for data transfer betn upper & lower layers.
- Higher layers :- represent appln that use Bluetooth tech like file transfer, audio streaming, etc

PAGE No.
DATE / /

Q* IEEE 802.15.4 phy & mac :—

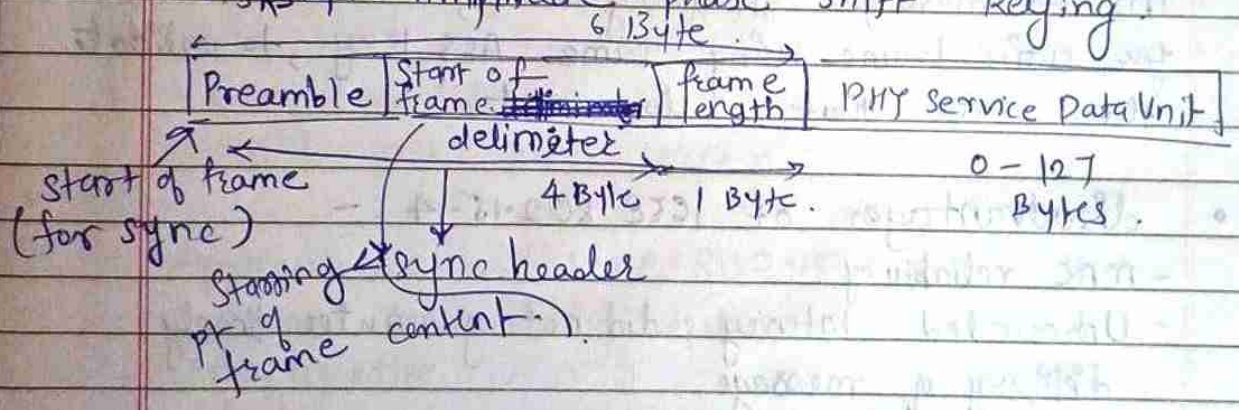
It is a standard developed for low data rate wireless personal area networks (WPANs). It defines physical & MAC layers for communicn in this networks.

Purpose :— • Low-Data-Rate communication • Low Power • Cost effective.

- Physical layer :— handles actual transmission & reception of radio signals over air.

freq bands :— 2.4 GHz (16 channels, with 250 Kbps)
915 MHz (10 channels, 250 Kbps)
868 MHz (3 channel, 100 Kbps).

Modulation :— OQPSK : offset quadrature phase-shift keying (PHY)
BPSK PHY : binary phase shift keying
ASK PHY :— Amplitude phase shift keying.



- Media Access Control (MAC) Layer :— controls how data is accessed & transmitted over physical medium.
  - defines how devices in same area will share freq allocated. (Use CSMA/CA)

main tasks :—
- PAN (Personal area N/w) association & disassocn by a device
- Reliable link communications betn 2 peer mac entities.
- Device security.

PAGE No.
DATE / /

MAC frame :—

frame control	seq no.	Destn PAN id	Destn address	Source PAN id	Source add	frame payload	frame check seq
← Header →						← Payload →	← footer →

- Topology used by IEEE 802.15.4 → Star, p2p, mesh
IEEE 802.15.4 does not define a path selection for a mesh ~~technology~~ topology.
  - mesh-under : Path sel^n can be done at layer 2
  - mesh-over : Path sel^n can occur at layer 3 in routing

- Security :— It uses Advanced Encryption Standard (AES) with 128 bit key length as base encryption algorithm.
MIC → message integrity code, which is calculated for entire frame using same AES key, to validate the data that is sent.

- disadvantages of IEEE 802.15.4 :—
  - MAC reliability.
  - Unbounded latency : did not guarantee timely delivery of message.
  - multipath fading → common issue in wireless communication where signals take multiple paths to reach receiver, causing interferance & signal degradation.

∴ To improve 802.15.4, it has 2 amendments :—

1) IEEE 802.15.4e :-
was introduce to expand mac layer feature set
- modifications to frame format was made to support more efficient & reliable communication.
- added more security features.
- new mechanisms to provide determinism.
- freq hopping → to reduce impact of interference by frequently changing commu channel.
- more suitable for applicn. in factory & process automation, smart grids, etc.

2) IEEE 802.15.4g :- focuses on expanding physical layer to better support large-scale outdoor wireless mesh n/w, specifically for (FANs) Field Area N/w or (SUN) Smart Utility N/w commun.
- new phy layer definations to support diff modulation schemes & freq bands
- MAC modifications → to ensure compatibility with new PHY layer.

Applications of IEEE 802.15.4 :-
- Home & building automation
- Automotive N/w
- Industrial sensors wireless N/ws.
- Interactive toy & remote controls.

PAGE No.
DATE / /

- Well known protocol stacks which uses 802.15.4
  - ZigBee
  - ZigBee IP
  - 6LoWPAN → IPV6 low power wireless PAN.

* ZigBee :—

ZigBee is wireless communicn standard. Used for PAN with simple, low cost, low energy consumption.
- Built on top of IEEE 802.15.4 which defines PHY & MAC layer of this protocol.

- Key features :—
  - low power
  - low data rate
  - Short-range communicn
  - mesh networking
  - Security
  - Low Cost

ZigBee Protocol Stack.

Appln / Profiles	ZigBee or vendor Specific
Appln Support	Platform Stack
N/w & Security layer	
MAC layer	IEEE 802.15.4
PHY Layer	

- ZigBee predefines many appln profiles for certain industries. Vendors can optionaly create their own custom ones
- Appln support layer deals with n/w of zigbee devices with higher layer appln
- N/w & security layer → provides mechanisms for n/w startup, configuration routing, & securing commun.

Utilizes AODV routing across mesh n/w. also utilizes 128 bit AES encryption for MAC security.

* ZigBee IP:—
Standard ZigBee didn't support interoperability with other IoT standards. ZigBee IP was created to ~~inte~~ incorporate open standards, enhancing compatibility & communication with other IoT devices
- It adopts protocols like IPv6, 6LoWPAN, ICMPv6, Neighbour Discovery (ND) & RPL for routing of packets.
- By supporting these open standards, ZigBee IP ensures compatibility with broader IoT ecosystems & aligns with current Internet Protocols at all layers below appln layer.

* Wi-SUN Phy layer:— is part of (Wi-SUN) wireless smart utility N/w standard.
It enhances IEEE 802.15.4 standard by increasing payload size, improving error detection, and supporting multiple modulation schemes.

- 802.15.4g & 15.4e made it harder for devices from diff manufacturers to work together. To solve this, Wi-SUN alliance was formed to ensure interoperability.
- Increased payload size up to 2047 bytes. IPv6 packets can be sent without needing to be fragmented at layer 2, which simplifies commu & reduces overhead.
- Improved error protection
- Supports multiple data rates channels.

Modulation scheme supported

- MR-FSK : multi rate multi regional freq Shift Key (good transmit freq)
- MR-OFDM :- multi rate, multi regional orthogonal freq div multi → good data rate
- MR-O-QPSK → multi rate M regional Offset quadrature Phase Shift keying (cost effective design).

3 * 802.11ah :— WiFi

IEEE 802.11ah also known as WiFi HaLow is a wireless networking standard that is part of wifi family, specifically designed for IoT appln that req low power consumption, extended range, suppert large no. of devices.

- Advantages :—
  1) Leverages WiFi's popularity :- most successful wireless endpoints.
  2) Supports High Data Rate devices such as those used in audio-vedio analytics
  3) Extended Range & Penetration → operates in sub-1 GHz freq band (Range upto 1 Km)
  4) Low Power Consumption.

- Appln :- 1) Smart Grid : Connecting sensors & meters over wide area for utilities monitoring 2) Industrial Appln 3) Extended Range wifi.

→ provides wifi connectivity over larger distances, suitable for rural areas or large industrial sites.

- Disadv of traditional wifi.
  - It was having limited signal penetration as compared to wifi HaLow
  - Unsuitable for battery powered nodes.
  - Scalability issues.

- 802.11ah Topology:—
  Uses star topology, where all devices connect to a central access point.
  To further extend range of wifi HaLow, simple relay hops can be used:—
  - Max of 2 hops.
  - Client-Handled Relay Operation → flexible way to cover large areas.

4* LoRaWAN → low Range Wide Area N/W.
a type of low-Power Wide Area N/W that enables wireless communication over long distances while using very low power. Particularly suited for IoT appln.

- LPWA tech:- LPWA tech are designed for appln requiring long-range comm, low power consumption & support large no. of connected devices.
  - Unlicensed-band LPWA tech:- LoRaWAN operates in unlicensed freq bands such as 868 MHz & 915 MHz.
  - Licensed-band LPWA:- tech like NB-IoT & other LTE variations operate in licensed freq bands.

DATE / /

- LoRa (long Range) : initially LoRa was a PHY layer modulation scheme. It uses modulation techniq called chirp spread spectrum, which allows robust commun even below noise floor, making it resistant to interference.

- LoRaWAN architecture :-

1. PHY layer :- Chirp Spread Spectrum modulation (allows devices to communicate even in env with significant noise).
freq bands :- unlicensed freq bands
433 MHz, 779 - 787 MHz, 863 - 870 MHz (used in India)
902 - 928 MHz.

2. MAC layer & Device Classes :-
Class A :- Default class for battery powered devices bidirectional commun.
Class B :- for devices that req more freq downlink commn.
Class C :- for devices that are continuously powered (eg mains powered) & can afford to keep their receiving windows always open for near - instantaneous downlink communication.

- LoRaWAN Gateway :-

Gateways act as central hubs in star n/w topology. They can handle multiple channels & demodulate several signals

PAGE No.
DATE / /

- **Security in LoRaWAN:-**

2 layeres of security:-

1. N/w security: Handled at MAC layer. Each device uses networks session key to ensure data integrity and authentication. This key helps compute (MIC) for every message, preventing unauthorized access.
2. App^n security: Involves appln session key used for encrypting & decrypting appln level data betn end device & appln server.

- Use cases for LoRaWAN:-

- Smart Grid:-
- Industrial Appln
- Smart Cities

IoT Stack

TCP/IP model	IoT	Device management
Data format	Binary, JSON, CBOR	
Appln layer	COAP, MQTT, XMPP	
Transport	UDP, DTLS	
Internet lay	IPv6/IP Routing, 6LOWPAN	
N/w or link layer	IEEE 802.15.4 mac, IEEE 802.15.4 Phy	

- IoT 2.0 interoperability:-
  - Easy to deploy new things and appln using data models.
  - Write once, run anywhere software.
  - N/w effect enabled
  - Any app to any thing via M2M (machine to machine)

* Internet Layer:-

A] • IPv6 :-

Problems with IPv4 : Shortage of address space
Lack of quality of service guarantee

- New features of IPv6:-
  - Enlarge address space
  - fixed header format helps speed processing/forwarding.
  - Better support for quality of service.
  - Neighbor discovery & Auto-configuration.
  - Header format simplification.

- hierarchical address architecture.
- new 'anycast' address (route to 'best' of several replicated servers)

IPv6 header fields:-
- Source add (16 octets)
- Destn address (")
- Version: 6
- Traffic class:- identify class of service. Eg DSCP, etc.
- Flow label: identify datagrams in same 'flow'
- next header: identify upper layer protocol for data
- hop limit, payload length.
- Checksum is removed to reduce processing at routers
- fragmentation not allowed at intermediate routers.

8). 6LoWPAN:- IPv6 over low power Wireless Personal Area Network.

Key technology designed to enable IPv6 comm° in low power consumption networks.
Historically, proprietary protocols & link only solutions were used, as IP was considered too demanding in terms of memory & b/w for these constrained devices.

Key Elements of 6LoWPAN:-

1) ~~Adaption~~ Adaptation layer:- 6LoWPAN introduces adaptation layer bet^n link layer & N/W layer. This facilitates efficient transmission of IPv6 datagrams over 802.15.4 links, addressing specific constraints of low-power devices.

2] Header Compression: Reduces overhead of IPv6 headers. (less data)
3] Fragmentation: Allows large IPv6 datagrams to be broken into smaller fragments that can be transmitted over N/w.
4] Layer-Two forwarding: Supports the delivery of IPv6 datagrams over multiple radio hops.

- Advantages of 6LoWPAN:—
  - IP enabled link
  - Interoperability: Provides standard-based commun^{n} betn low power devices & ensures they can interoperate with other devices using IP. Also integration with existing IP devices
  - Standardization & further development. Promotes the dev of standardized communic^{n}. functions among low-power IEEE 802.15.4 devices

c] Routing: RPL → Routing Protocol for low-power and lossy networks.
- RPL specifies routing protocol specially adapted for the needs of IPv6 communication over 'low power lossy networks" (LLNs) supporting
  - peer to peer traffic (point to point)(P2P)
  - point to multipoint communication (P2MP) from a central server to multiple nodes on LLN
  - multipoint to point (MP2P) communication

The base RPL specification is optimized only for MP2P traffic or P2MP, and P2P is optimized only through use of additional mechanisms.

- Topology :- RPL organizes a topology as a directed Acyclic Graph (DAG) that is partitioned into one or more Destination Oriented DAGs (DODAGs). A RPL Instance is a set of (DODAGs) identified by a RPL Instance ID.

Procedure — When a node A sends a packet to a node B within RPL domain, packet first follows the graph up to the root where routing info is stored. At this point, root inspects the destn, consults its routing table that contain path to destination. The root routes packet to its destn using a specific routing header for IPv6.

RPL message control :- RPL uses ICMPv6 control message to manage network

1. DAG Information Obj (DIO): Helps node discover & join an RPL instance by enabling nodes to analyse and choose their DODAG parents.
2. DAG Info Solicitation (DIS): Allows a node to request DIO messages from its neighbours. Multicasted by nodes seeking to obtain DIO info.
3. DAO-ACK (Destn advertisement Obj Ack) provides ack that DAO message is successfully received.

DODAG formation :- Built incrementally from root to leaf nodes. Joining nodes may request DIOs from neighbours by multicasting DIS. DSTN (Destn Advertisement trigger Seq. number) used to request updated destn info. from child nodes.

* Transport Layer :-

TCP Header :-
- Source Port
- Destination Port
- Sequence Number
- Ack number
- offset, Reserved, TCP flags.
- Window
- Checksum
- Urgent Pointer
- TCP options (optional)

- In IPv6, UDP checksum is mandatory to ensure data integrity accross networks.

RFC 6282 exception :-
RFC 6282 allows an endpoint to skip the UDP checksum if authorized by upper layer.

Conditions for skipping Checksum :-
- Tunneling :- tunneled PDU (Protocol Data Unit) has its own addressing, security & integrity checks.
- Message Integrity Check : When using additional security measures like IPsec Authentication Header, which provides integrity verification.

* In summary, while UDP checksum is req in IPv6, RFC 6282 permits its omission under certain conditions where other layers / protocols provide sufficient integrity & security checks.

* Application Layer Protocols :—

• A] CoAP – Constrained Application Protocol (CoAP) :–
CoAP is a specialized protocol for interacting with resources on constrained devices & networks.
– CoAP follows REST principles, similar to HTTP, allowing clients to interact with resources using standard methods like GET, POST, PUT & DELETE.
– Supports both synchronous & asynchronous.
– for constrained devices and networks
– Specialized for M2M applications (machine to machine).
– Easy to Proxy to/from HTTP.

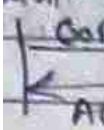
– CoAP is not intended to replace HTTP but to complement it in constrained env. where HTTP may be too heavy.
– not a general HTTP compression.
– CoAP operates in IoT space & is designed to work alongside web technologies, not to function independently from them.
– along with constrained n/w, CoAP protocol also operate over traditional IP networks.
– This includes applications to monitor simple sensors (Eg temp, light sensors), to control actuators & to manage devices.

Appln.
CoAP Req/Response
CoAP messages
UDP

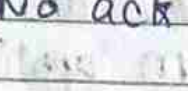
TCP & HTTP are too heavy for 6LoWPAN devices such as sensors. CoAP is thus based on UDP and a compressed simplified message exchange

- messaging model :—

1) Reliable message transmission :—
Reliability is provided by marking a message as confirmable (CON). It is retransmitted using default timeout & exponential backoff until recipient sends an ack msg



2) Unreliable message transmission :—
msg that does not req reliable transmission can be sent as Non-confirmable msg (NON). No ack.



★ For req examples → see ppt (pg 48, 49, 50)

- B] MQTT :— message queuing telemetry transport
It is lightweight messaging protocol designed for efficient communication in constrained environments, like in IoT.
- It is a publish/subscribe model. Devices can receive messages they are interested in. Publishers & subscribers are decoupled, they don't need to know each other.
- Content-Agnostic messaging :— Protocol does not enforce any constraints on content of messages, allowing it to be used for various appln where diff types of data need to be transmitted
- Quality of Service (QoS) levels :—
MQTT offers 3 levels to ensure diff guarantees
i) QoS 0 - 'At most once' :— message loss can occur. Suitable for scenarios where occasional loss of message is acceptable.

Eg: Sensor data reporting where freq updates are provided

ii] At least once (QoS 1) :- msg are guaranteed to be delivered, but duplicates may occur.

iii] QoS 2 : (Exactly once) :- messages are assured to arrive without duplication or loss.

Appl^n → financial transactions / billing systems.

- A small transport overhead and protocol exchanges minimized to reduce network traffic. (fixed len header is just 2 Bytes)
- mqTT is designed to be open, simple, lightweight & easy to implement
- Supports always-connected & sometimes-connected models.
- Provides session awareness.
- 'Last will & testament' enable appl^{n}s to know when a client goes offline abnormally.

mqTT msg formal.

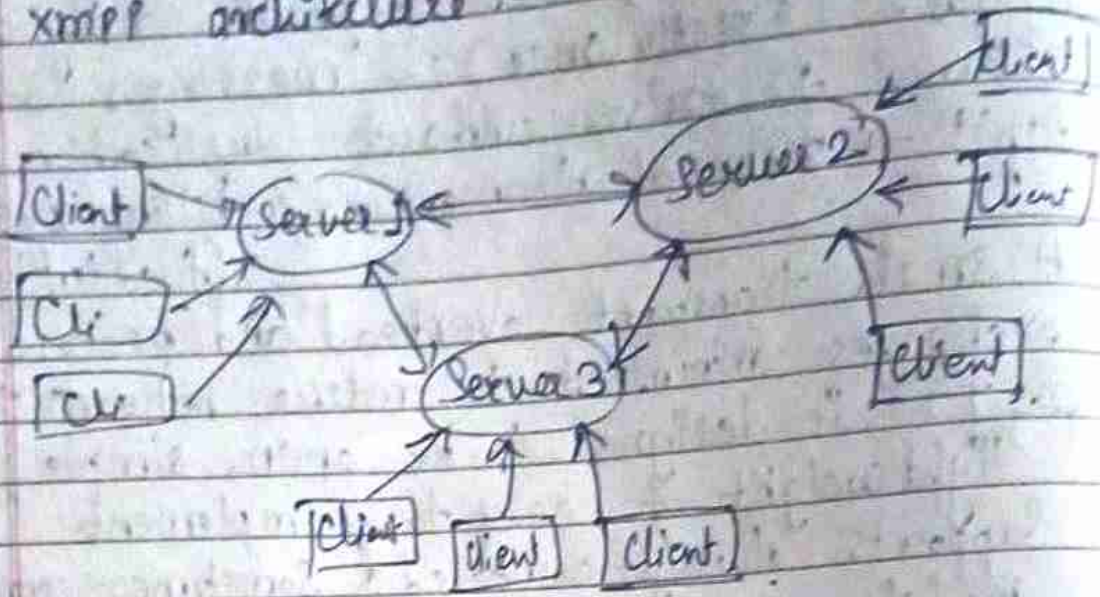
fixed header (present in all)
Variable header (present in some)
Payload (pres in some)

c] XMPP :- Extensible Messaging and Presence Protocol is a TCP communications protocol based on XML that enables near-real-time exchange of structured data between 2/more connected entities.

- features include presence information and contact list maintenance
- XMPP has been extended for use in publish-subscribe systems.

- Perfect for IoT applications

xmpp architecture :—



Server-Server Port: 5269

Client-Server Port: 5222

- Addressing scheme :- node@domain/resource
- xmpp uses a client-server model. Client connects to xmpp servers to exchange messages. Servers handles routing of messages, presence info, etc.

- Advantages :- 1) decentralized nature.
2) Works similar to email, operating across a distributed n/w of transfer agents rather than relying on single, central server or broker.
3) Its easy for anyone to run their own xmpp server allowing us to create & manage own n/w of devices.
4) If security is required, the server could be isolated on a company intranet behind secure authentication protocols using TLS encryp.
- Disadv :- 1) lack of end to end encryption.
2) lack of Quality of Service (QoS).