INDIRA GANDHI DELHI TECHNICAL UNIVERSITY FOR WOMEN

IoT & its applications in AI

ASSIGNMENT

Submitted To:

Dr. SRN Reddy

Dean (Examination)

Submitted By:

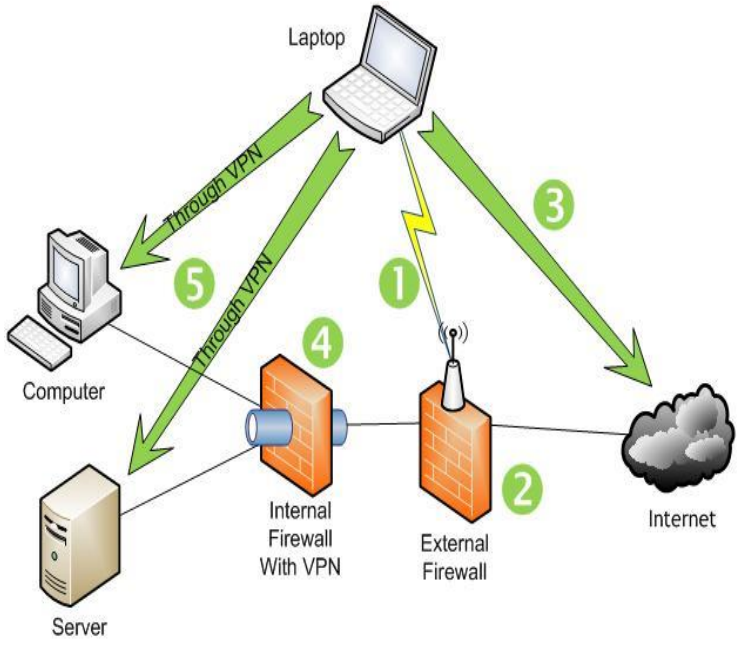
Name- Chhavi Sharma

Roll No.- 01902102019

M.Tech. CSE (2nd Semester)

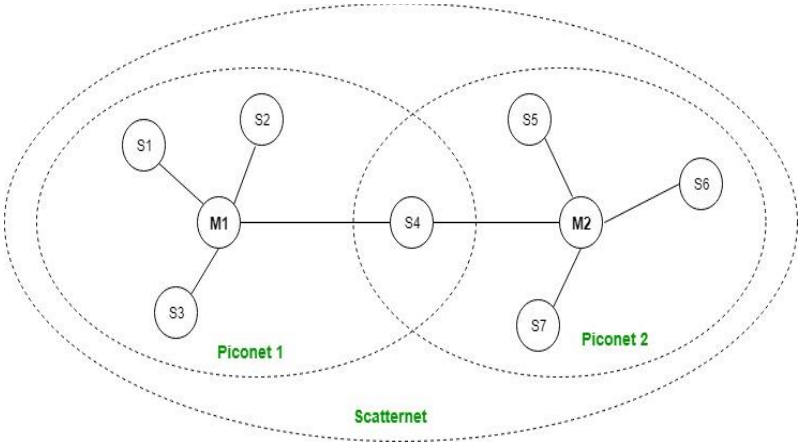
Ques1:-Explain and draw the architecture of Wi-Fi, Bluetooth and zigbee

Ans:- (a) **Wi-Fi -** Wi-Fi is a popular wireless networking technology. Wi-Fi stands for "wireless fidelity". The Wi-Fi was invented by NCR corporation/AT&T in Netherlands in 1991. By using this technology we can exchange the information between two or more devices. Wi-Fi has been developed for mobile computing devices, such has laptops, but it is now extensively using for mobile applications and consumer electronics like televisions, DVD players and digital cameras. There should be two possibilities in communicating with the Wi-Fi connection that may be through access point to the client connection or client to client connection. Wi-Fi is a one type of wireless technology. It is commonly called as wireless LAN (local area network). Wi-Fi allows local area networks to operate without cable and wiring. It is making popular choice for home and business networks. A computer's wireless adaptor transfers the data into a radio signal and transfers the data into antenna for users.



(b) Bluetooth:- It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz. Maximum devices that can be connected at the same time are 7. Bluetooth ranges upto 10 meters. It provides data rates upto 1 Mbps or 3 Mbps depending upon the version. The spreading technique which it uses is FHSS (Frequency hopping spread spectrum). A bluetooth network is called **piconet** and a collection of interconnected piconets is call **scatternet**.

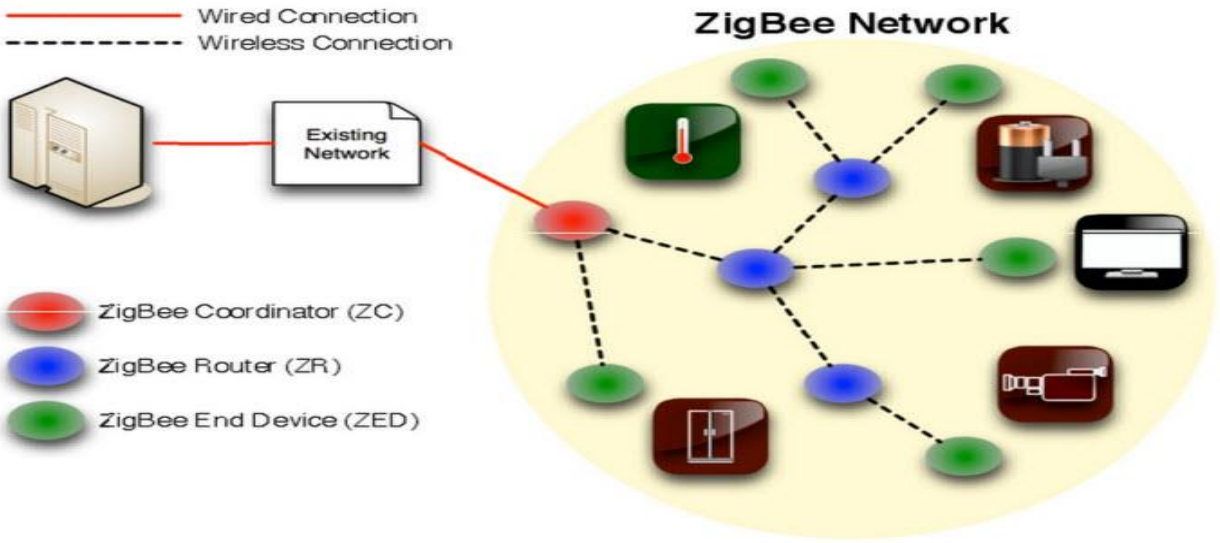
Its key features are robustness, low complexity, low power and low cost. The technology also offers wireless access to LANs, PSTN, the mobile phone network and the Internet for a host of home appliances and portable handheld interfaces.



Bluetooth Architecture

(c) Zigbee:- Zigbee communication is specially built for control and sensor networks on IEEE 802.15.4 standard for wireless personal area networks (WPANs), and it is the product from Zigbee alliance. This communication standard defines physical and Media Access Control (MAC) layers to handle many devices at low-data rates. These Zigbee's WPANs operate at 868 MHz, 902-928MHz and 2.4 GHz frequencies. The date rate of 250 kbps is best suited for periodic as well as intermediate two way transmission of data between sensors and controllers.

Zigbee is low-cost and low-powered mesh network widely deployed for controlling and monitoring applications where it covers 10-100 meters within the range. This communication system is less expensive and simpler than the other proprietary short-range wireless sensor networks as Bluetooth and Wi-Fi.



Ques2:- Differentiate between Wi-Fi, Bluetooth and zigbee.

Ans:- The mention wireless technologies are the standards defined by IEEE,

ZigBee:- IEEE 802.15.4-2003 (Low Rate WPAN) deals with low data rate but very long battery life (months or even years) and very low complexity. The standard defines both the physical (Layer 1) and data-link (Layer 2) layers of the OSI model. Basically used in RF TV remotes and has very very low data rates and range.

Bluetooth:- based on IEEE 802.15.1, defines physical layer (PHY) and Media Access Control (MAC) specification for wireless connectivity with fixed, portable and moving devices within or entering personal operating space. Range is limited and data rates can go from 1.2 Mbps for commercial (mobile Bluetooth) to 10 Mbps industrial/military purpose.

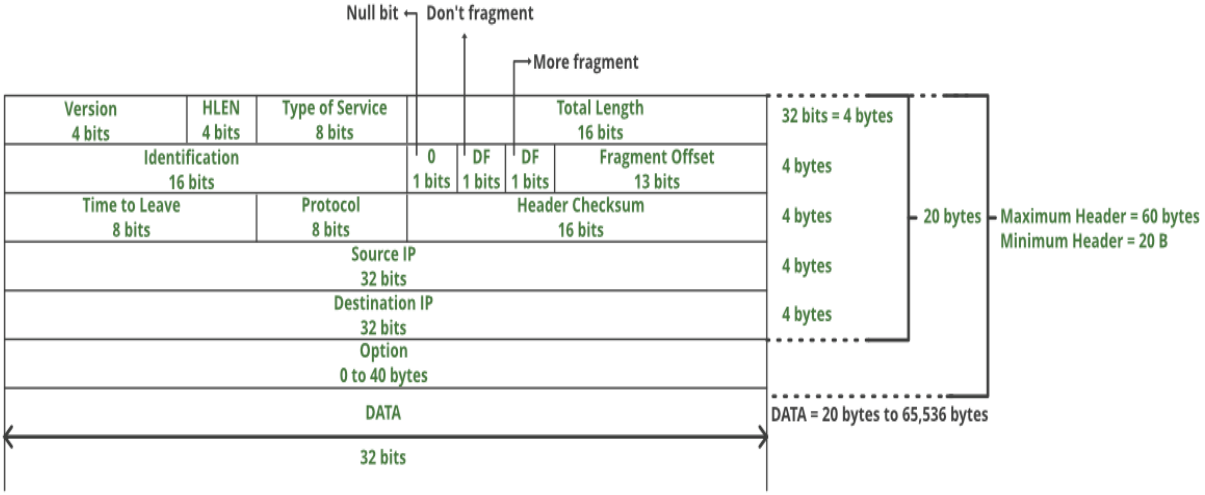
Wi-Fi:- IEEE 802.11, basically is a wireless LAN, its works similar to that of LAN but has wireless connectivity. The range is limited from few 100 meters to max 500 meters.

Parameter	Bluetooth® Low Energy (BLE)	Wi-Fi®	Zigbee®
Data Rate	1 – 3 Mbps	300 Mbps	20kb/s, 40 kb/s, 250kb/s
Frequency Band	2.4 GHz	2.4 GHz and 5 GHz	868/915 MHz, 2.4 GHz
Range	10m	190 m	100m
Security	E0 Stream cipher	WEP, WPA authentication, 128-bit Advanced Encryption Standard (AES), VPN, Firewall	128-bit AES
Risk of Data Collision	High		Medium
Maximum Number of Nodes	8	2,007	>65,000
Power Efficiency	Acceptable to Good	Varies	Excellent
Of Note	Once paired, connecting is automatic.	Connecting is automatic once it is set up.	Mesh capability creates greater signal reliability
Applications	To replace wiring in handheld devices.	The main connectivity resource for home, work, retail, and more.	Power-sipping applications; remote sensor and wireless controls
Benefits	Convenience, Cost, connect to Android, Blackberry, iOS, Tizen, and Windows.	Most widely used wireless connectivity solution. Connect to iOS and Android.	Reliable, Low Power, Cost effective, "Assemble and Forget"
Draw-backs:	Short range	Not always reliable. Higher power consumption	Not mainstream for connection to smartphones, etc.
IEEE	IEEE 802.15.1	IEEE 802.11n	IEEE 802.15.4
Markets	Mainly for portables. Widely adopted in consumer markets, retail	Ubiquitous; Widely adopted in nearly every market. Replaces cables in work areas or homes.	Better known in Industrial markets, smart homes, smart lighting.
Attractiveness as a hacking target:	Low to medium	High	Low
Find ready-to-connect modules at:	mouser.com, adafruit.com, sparkfun.com	mouser.com, adafruit.com, sparkfun.com	mouser.com, adafruit.com, sparkfun.com

Ques3:-Draw and explain the datagram header of IPv4 and IPv6. Differentiation between IPv4 and IPv6.

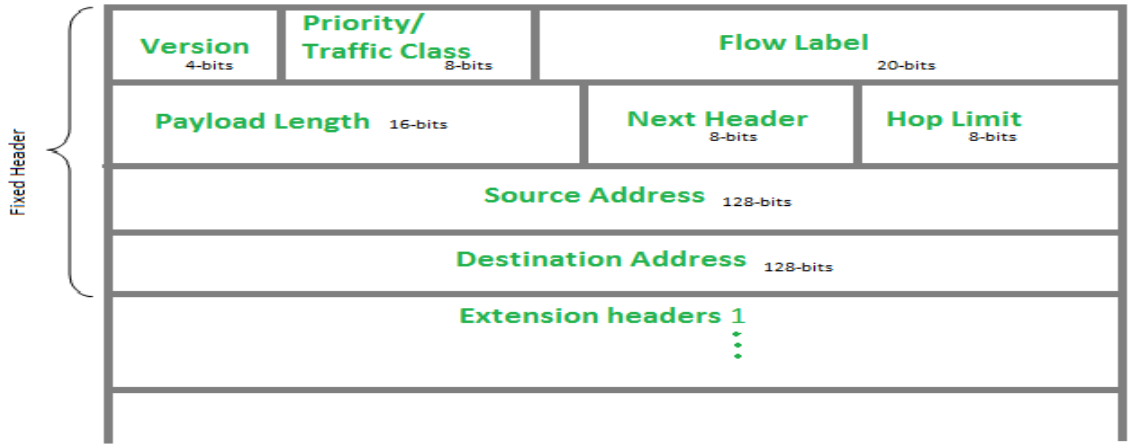
Ans:- IPv4 Datagram Header

Size of the header is 20 to 60 bytes.



- **VERSION:** Version of the IP protocol (4 bits), which is 4 for IPv4.
- **HLEN:** IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.
- **Type of service:** Low Delay, High Throughput, Reliability (8 bits)
- **Total Length:** Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.
- **Identification:** Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)
- **Flags:** 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)
- **Fragment Offset:** Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.
- **Time to live:** Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.
- **Protocol:** Name of the protocol to which the data is to be passed (8 bits)
- **Header Checksum:** 16 bits header checksum for checking errors in the datagram header
- **Source IP address:** 32 bits IP address of the sender
- **Destination IP address:** 32 bits IP address of the receiver
- **Option:** Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.

IPv4 Datagram Header:-



- **Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110.
- **Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
- **Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
- **Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
- **Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.
- **Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
- **Source Address** (128-bits): This field indicates the address of originator of the packet.
- **Destination Address** (128-bits): This field provides the address of intended recipient of the packet.
- **Extension Headers :** In order to rectify the limitations of *IPv4 Option Field*, Extension Headers are introduced in IP version 6. The extension header mechanism is very important part of the IPv6 architecture. Next Header field of IPv6 fixed header points to

the first Extension Header and this first extension header points to the second extension header and so on.

Difference Between IPv4 and IPv6:

IPV4	IPV6
IPv4 has 32-bit address length.	IPv6 has 128-bit address length.
It Supports Manual and DHCP address configuration.	It supports Auto and renumbering address configuration.
In IPv4 end to end connection integrity is Unachievable.	In IPv6 end to end connection integrity is Achievable.
It can generate 4.29×109 address space.	Address space of IPv6 is quite large it can produce 3.4×1038 address space.
Security feature is dependent on application.	IPSEC is inbuilt security feature in the IPv6 protocol.
Address representation of IPv4 in decimal.	Address Representation of IPv6 is in hexadecimal.
Fragmentation performed by Sender and forwarding routers.	In IPv6 fragmentation performed only by sender.
In IPv4 Packet flow identification is not available.	In IPv6 packet flow identification are Available and uses flow label field in the header.
In IPv4 checksum field is available.	In IPv6 checksum field is not available.
It has broadcast Message Transmission Scheme.	In IPv6 multicast and any cast message transmission scheme is available.
In IPv4 Encryption and Authentication facility not provided.	In IPv6 Encryption and Authentication are provided.
IPv4 has header of 20-60 bytes.	IPv6 has header of 40 bytes fixed.

Ques4:- Draw and Explain 6LoWPAN protocol.

Ans:- 6LoWPAN is a simple low cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements as it provides IPv6 networking over IEEE 802.15.4 networks. It is formed by devices that are compatible with the IEEE 802.15.4 standard and characterized by short range, low bit rate, low power, low memory usage and low cost, where its architecture is shown in Figure 1 . When a lower processing capability sensor node in a 6LoWPAN or so-called reduced function device (RFD) wants to send its data packet to an IP-enabled device outside the 6LoWPAN, it first sends the packet to the higher processing capability sensor node or so-called full function device (FFD) in the same PAN. The FFDs which react as a router in 6LoWPAN will forward the data packet hop by hop to the 6LoWPAN gateway. The 6LoWPAN gateway that connect to the 6LoWPAN with the IPv6 domain will then forward the packet to the destination IP-enabled device by using the IP address.

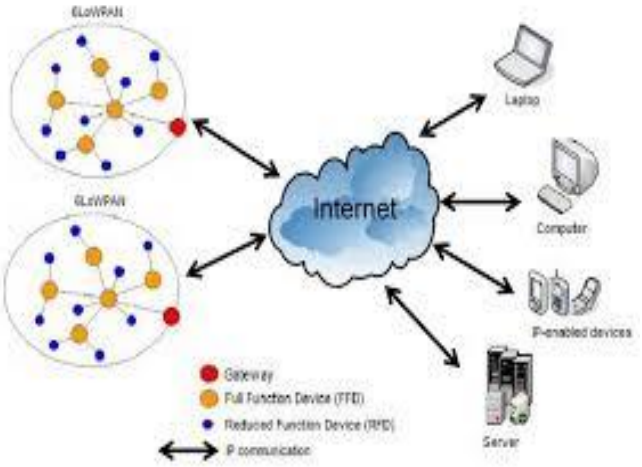


Figure1:- 6LoWPAN Architecture

Figure2 describes the reference model of 6LoWPAN protocol stack. It adopts IEEE 802.15.4 standard PHY and MAC layers which are specified in [2], [3] as its bottom layers while chooses IPv6 in its network layer. Basically, IEEE 802.15.4 standard specifies PHY and MAC layers for low-rate wireless personal area network (LR-WPAN). The PHY layer specification dictates how the IEEE 802.15.4 devices may communicate with each other over a wireless channel. There are total of 27 channels defined in the PHY layer. These channels are allocated into different frequency bands with varying data rates as showed in Table 1. At MAC layer, it specifies when the devices may access the channel for communication. The basic tasks provided by the MAC layer are beacon generation and synchronization, supporting PAN association and disassociation, managing channel access via Carriers Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism, and etc.

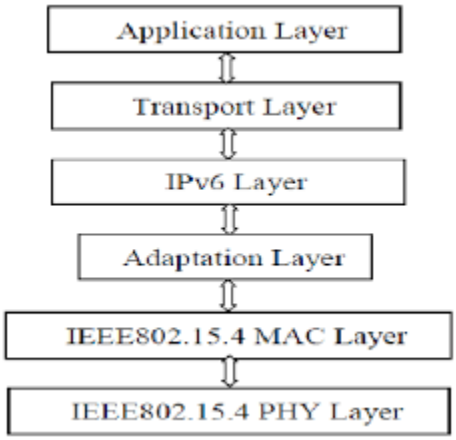


Figure:-2 The reference model of 6LoWPAN protocol stack.

Mechanisms in 6LoWPAN adaptation layer:- The minimum maximum transmission unit (MTU) for an IPv6 packet over IEEE 802.15.4 is 1280 octets. However, the maximum MAC frame size defined by IEEE 802.15.4 as showed in Figure 3 is 127 bytes where 25 bytes are reserves for frame overhead and left only 102 bytes for payload. The situation becomes worse if link-layer imposes further overhead for the security purpose by adding an Auxiliary Security Header in the MAC frame, which in the maximum case leaves only 81 bytes for IPv6 packet. Thus, a full IPv6 packet does not fit in an IEEE 802.15.4 frame. Furthermore, since the IPv6 header in an IPv6 packet is 40 bytes, there is only 41 bytes left for the upper layers. Reserving either 8-bytes User Datagram Protocol (UDP) header or the 20-bytes Transmission Control Protocol (TCP) header that added at the transport layer, the IPv6 packet impractically leaves only several bytes space for the application data use. Therefore, in order to implement the seamless connection of MAC layer and IPv6 network layer, 6LoWPAN working group suggested that adding an adaptation layer between MAC layer and the network layer to achieve the header compression, fragmentation and layer-two forwarding [5], [13] – [15]. In header compression, 6LoWPAN defined HC1 encoding as an optimized compression scheme for link-local IPv6 communication. Some IPv6 header fields such as IPv6 length fields and IPv6 addresses are eliminated from a packet as long as the adaptation layer can derive them from the headers in the link-layer frame or based on simple assumption of shared context. Furthermore, the header fields that come from adaptation, network, and transport layers usually carry the common value. Hence, in order to reduce transmission overhead, header compression mechanism is used to compress those header fields to a few bits while reserving an escape value for the less common ones appear. Table 2 compares the sizes of IPv6 header fields and the 6LoWPAN compressed header fields.

Header Field	IPv6 header length	6LoWPAN HC1 length	Explanation
Version	4 bits	------	Assuming communicating with IPv6.
Traffic class	8 bits	1 bit	0 = Not compressed. The field is in full size. 1 = Compressed. The traffic class and flow label are both zero.
Flow label	20 bits		
Payload length	16 bits	------	Can be derived from MAC frame length or adaptation layer datagram size (6LoWPAN fragmentation header).
Next header	8 bits	2 bits	Compressed whenever the packet uses UDP, TCP or Internet Control Message Protocol version 6 (ICMPv6).
Hop limit	8 bits	8 bits	The only field always not compressed.
Source address	128 bits	2 bits	If Both source and destination IPv6 addresses are in link local, their 64-bit network prefix are compressed into a single bit each with a value of one. Another single bit is set to one to indicate that 64-bit interface identifier are elided if the destination can derive them from the corresponding link-layer address in the link-layer frame or mesh addressing header when routing in a mesh.
Destination address	128 bits	2 bits	
HC2 encoding	------	1 bit	Another compression scheme follows a HC1 header.
Total	40 bytes	2 bytes	Fully compressed, the HC1 encoding reduces the IPv6 header to two bytes.

Table:- Comparison of IPv6 header and compressed 6LoWPAN header fields.

6LoWPAN APPLICATION AREAS:-

- **Automation:** There are enormous opportunities for 6LoWPAN to be used in many different areas of automation.
- **Industrial monitoring:** Industrial plants and automated factories provide a great opportunity for 6LoWPAN. Major savings can be made by using automation in every day practices. Additionally, 6LoWPAN can connect to the cloud which opens up many different areas 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.

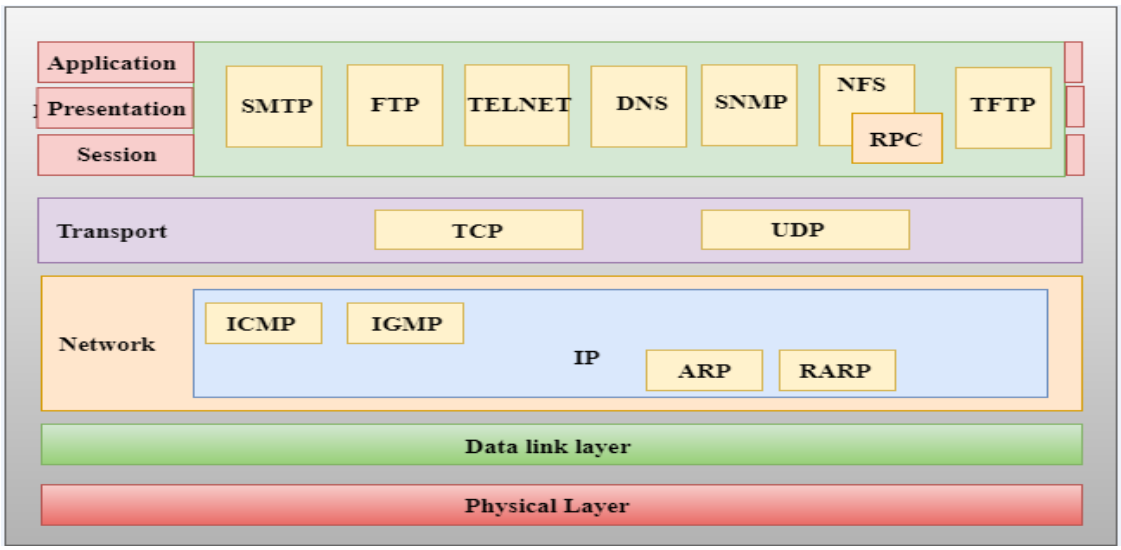
Ques5:- Explain and differentiate TCP and UDP.

Ans:- **(a)TCP/IP model:-** The TCP/IP model was developed prior to the OSI model.

- The TCP/IP model is not exactly similar to the OSI model.

- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.



- It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

1. **Network Access Layer** – This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data. We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer – This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:
   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host Layer – This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are.

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Application Layer – This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

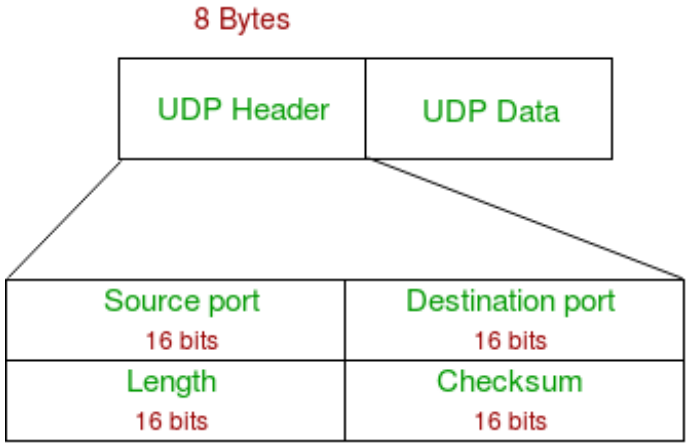
1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is

efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.

2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

(b) USER DATAGRAM PROTOTCOL(UDP):- User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is **unreliable and connectionless protocol.** So, there is no need to establish connection prior to data transfer.
Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of Internet services; provides assured delivery, reliability and much more but all these services cost us with additional overhead and latency. Here, UDP comes into picture. For the real time services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also save bandwidth.
User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

UDP Header – UDP header is **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. First 8 Bytes contains all necessary header information and remaining part consist of data. UDP port number fields are each 16 bits long, therefore range for port numbers defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or process.



1. **Source Port :** Source Port is 2 Byte long field used to identify port number of source.
2. **Destination Port :** It is 2 Byte long field, used to identify the port of destined packet.
3. **Length :** Length is the length of UDP including header and the data. It is 16-bits field.
4. **Checksum :** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

Notes – Unlike TCP, Checksum calculation is not mandatory in UDP. No Error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting.

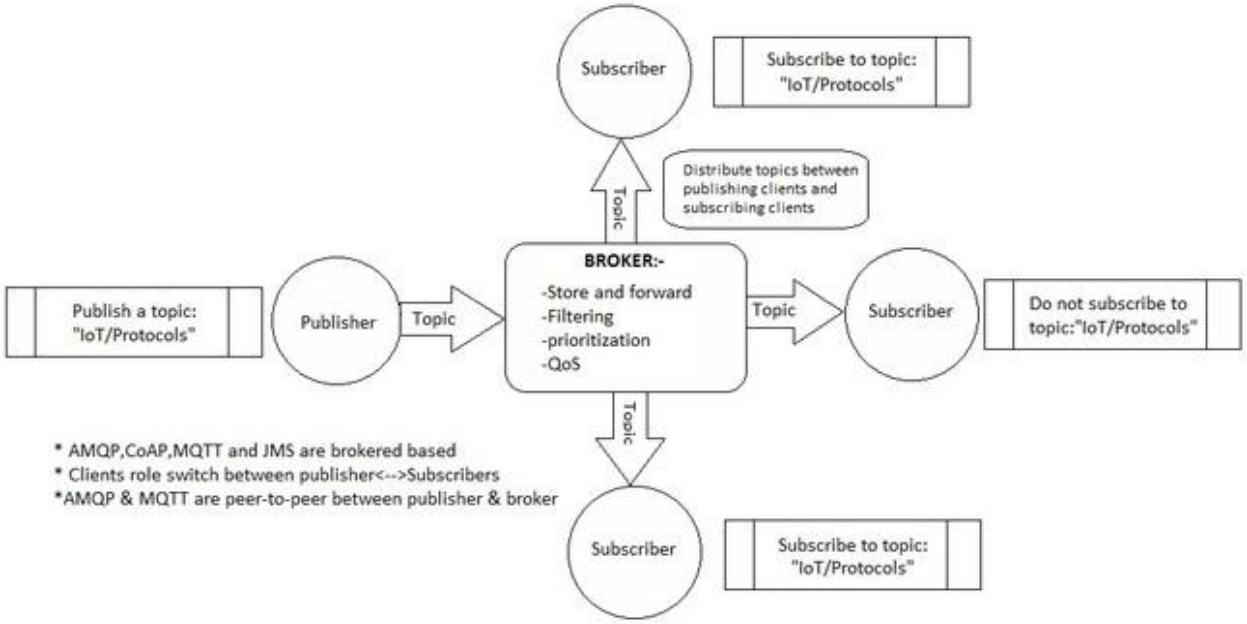
Differentiate between TCP and UDP

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).
TCP has a (20-80) bytes variable length header.	UDP has a 8 bytes fixed length header.

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
TCP is heavy-weight.	UDP is lightweight.
TCP doesn't supports Broadcasting.	UDP supports Broadcasting.

Ques6:- Explain MQTT protocol and its architecture.

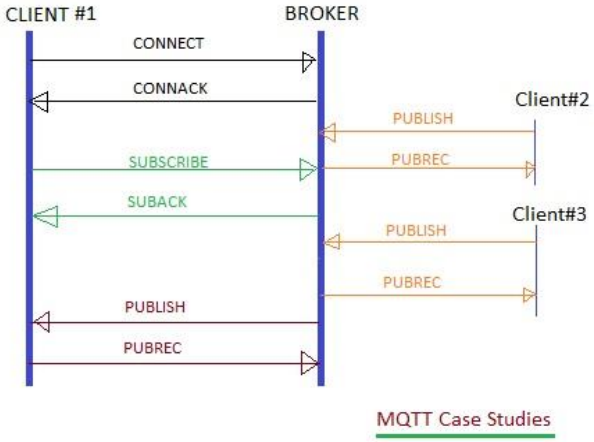
Ans:- MQTT is broker based protocol. In these end devices (i.e. Clients) communicate via a broker. The broker is a server which can be installed on any machine in the cloud. There are different types of brokers such as HiveMQ, Mosquitto etc. The single client and broker can also communicate with each other.



MQTT Architecture

As MQTT runs above TCP/IP layer, it is also connection oriented protocol. The client establishes connection with the broker (i.e. Server) before the communication. MQTT is a publish-subscribe protocol. Here both client and server publish about any information (i.e. A Parameter such as temperature, humidity, event (ON/OFF) etc.) to each other using "PUBLISH" message. Any number of clients or end devices can subscribe for an event with the broker. Due to this subscription, when there is a change in any event or parameter, the broker will intimate to the subscribed clients about the change in event or parameter (i.e. Temperature, humidity, etc.).

MQTT Protocol Architecture Working Operation



Let us understand the working operation of MQTT protocol architecture. The figure depicts MQTT message flow between client and broker. We will take two MQTT use cases to understand the working operation of MQTT architecture.

MQTT Use Case#1: Broker wants to switch ON or OFF the light connected with remote client#1

➡Initially connection is established by client#1 with a broker using CONNECT and CONNACK messages.

➡Next Broker communicates with Client#1 to switch ON or OFF the light interfaced with it. The messages such as PUBLISH and PUBREC are used for it.
This use case is used to switch ON/OFF the street lights in Zigbee or LoRaWAN network. The lights are usually connected with end nodes or end devices in these wireless networks. The single Zigbee or LoRaWAN gateway controls multiple end nodes. Multiple such gateways are needed to cover the entire city.

MQTT Use Case#2: Client#2 or client#3 wants to update temperature/humidity status to the broker based on sensors

➡Client#2 and Client#3 will intimate temperature or humidity update to the broker using PUBLISH message. This information is stored in the database and will be sent to all the subscribers who have subscribed to these topics (i.e. Temperature, humidity). This information is "pushed" to all the subscribed clients of the topics.

➡If client#1 has already subscribed for subscription to topics (i.e. Temperature, humidity), it will get the information from broker using PUSH operation.

This use case is used for obtaining different types of sensing information automatically whenever there are any updates. For this purpose, different types of sensors (such as humidity sensor, temperature sensor, etc.) are interfaced with end nodes. These end nodes publish information (of any event updates) to the broker. The broker intimates changes to all the subscribed clients. The communication between gateway

There are two dominant data exchange protocol architectures viz. broker based and bus based. In this MQTT tutorial we have studied broker based MQTT protocol architecture. Wireless IoT technologies such as zigbee, LoRaWAN uses MQTT for communication between clients and router. Protocols such as AMPQ, CoAP and JMS also use broker based architecture. Protocols such as DDS, REST and XMPP use bus based architecture.

Ques7:- Write a short note on HTTP, CoAP, XMPP, AMQP AND MQTT.

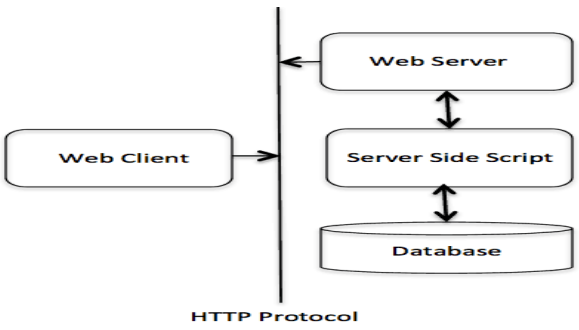
Ans:- (a) HTTP:- The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation for data communication for the World Wide Web (i.e. internet) since 1990. HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers.

Basically, HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web. The default port is TCP 80, but other ports can be used as well. It provides a standardized way for computers to communicate with each other. HTTP specification specifies how clients' request data will be constructed and sent to the server, and how the servers respond to these requests.

There are three basic features that make HTTP a simple but powerful protocol:

1. HTTP is connectionless
2. HTTP is media independent
3. HTTP is stateless

BASIC ARCHITECTURE



Client:- The HTTP client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a TCP/IP connection.

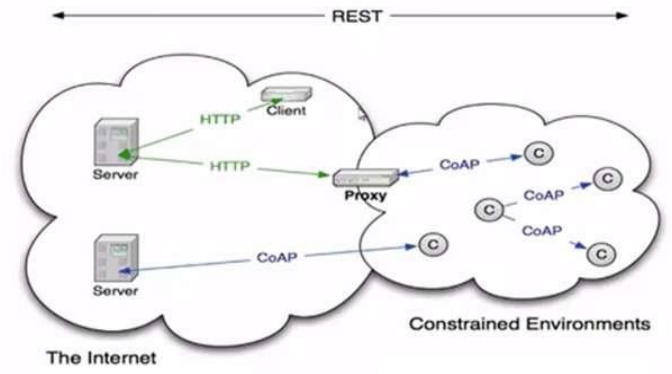
Server:-The HTTP server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity-body content.

(b) CONSTRAINT APPLOCATION PROTOCOL(CoAP):- Constrained Application Protocol (CoAP) is a protocol that specifies how low-power compute-constrained devices can operate in the internet of things (IOT). Designed by the Internet Engineering Task Force (ITEF), CoAP is specified in IETF RFC 7252.

CoAP is designed to enable simple, constrained devices to join the IOT even through constrained networks with low bandwidth and low availability. The protocol is generally used for machine-to-machine (M2M) communication.

CoAP functions as a sort of HTTP for constrained devices, enabling such component level equipment as sensors or actuators to communicate on the IOT, being controlled and passing along their data as part of a system. The protocol is designed for reliability in low bandwidth and high congestion through its low power draw and low network overhead. According to Jullian Vermillard, Sierra Wireless principle engineer of software, in a network with limited connectivity or a lot of congestion CoAP can continue to work where TCP-based protocols such as MQTT fail to complete a handshake.

The efficient and conservative traits of CoAP can enable devices operating in poor signal quality to send their data reliably or enable a satellite in orbit maintain to its distant communication successfully. Despite CoAp's ability to run on small devices, it supports networks with billions of nodes. For security, the DTLS parameters chosen for default are an equivalent to 3072 bit RSA keys.



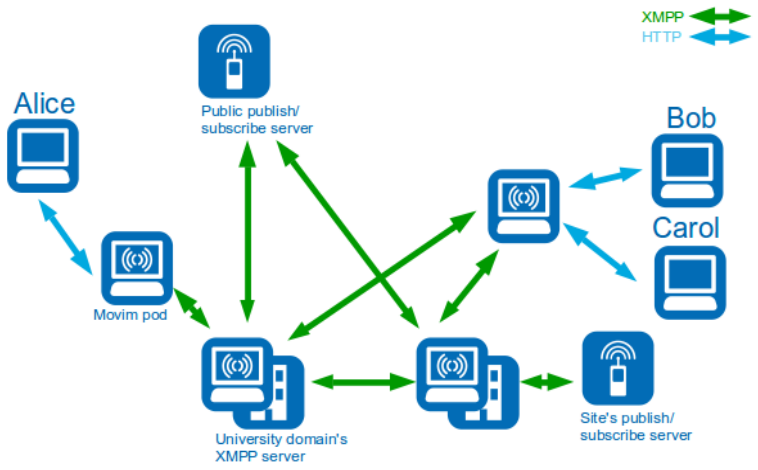
CoAP Architecture

(c) XMPP:- XMPP is a short form for Extensible Messaging Presence Protocol. It's protocol for streaming XML elements over a network in order to exchange messages and presence information in close to real time. This protocol is mostly used by instant messaging applications like WhatsApp.
Let's dive into each character of word **XMPP**:

- **X :** It means eXtensible. XMPP is a open source project which can be changed or extended according to the need.
- **M :** XMPP is designed for sending messages in real time. It has very efficient push mechanism compared to other protocols.
- **P :** It determines whether you are online/offline/busy. It indicates the state.
- **P :** XMPP is a protocol, that is, a set of standards that allow systems to communicate with each other.

These are the basic requirements of any Instant Messenger which are fulfilled by XMPP:

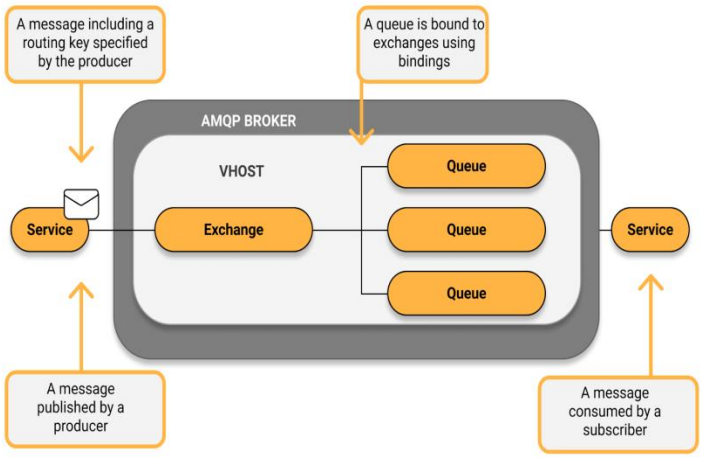
1. Send and receive messages with other users.
2. Check and share presence status
3. Manage subscriptions to and from other users.
4. Manage contact list
5. Block communications(receive message, sharing presence status, etc) to specific users.



(d) AMQP:- Advanced Message Queuing Protocol (AMQP) is an application layer protocol that focuses on process-to-process communication across IP networks. An encoding schema and a set of procedures allow for two different servers to communicate regardless of the technology used. Overall, the goal of AMQP is to enable message passing through broker services over TCP/IP connections. AMQP is considered a compact protocol, since it's a binary protocol, meaning that

everything sent over AMQP is binary data. A binary protocol avoids sending useless data over the wire.

The Advanced Message Queuing Model



Components of AMQP

Message Queue:-A queue acts as a buffer that stores messages that are consumed later. A queue can also be declared with a number of attributes during creation. For instance, it can be marked as durable, auto-delete and exclusive, where exclusive means that it can be used by only one connection and this queue will be deleted when that connection closes.

Exchanges and Exchange Types:-A channel routes messages to a queue depending on the exchange type and bindings between the exchange and the queue. For a queue to receive messages, it must be bound to at least one exchange.

Binding:-A binding is a relation between a queue and an exchange consisting of a set of rules that the exchange uses (among other things) to route messages to queues.

Message and Content:-A message is an entity sent from the publisher to the queue and finally subscribed to by the consumer. Each message contains a set of headers defining properties such as life duration, durability, and priority.

Connection:-A connection in AMQP 0.9.1 is a network connection between your application and the AMQP broker, e.g. a TCP/IP socket connection.

Channel:-A channel is a virtual connection inside a connection, between two AMQP peers. Message publishing or consuming to or from a queue is performed over a channel (AMQP). A channel is multiplexed, one single connection can have multiple channels.

Virtual Hosts:-Virtual hosts (vhost) provide a way to segregate applications in the broker. Different users can have different access privileges to different vhost. Queues and exchanges is created so they only exist in one vhost

Ques8:- Write down the differentiation between HTTP, CoAP, XMPP, AMPQ AMD MQTT protocol.

Ans:- Comparative Analysis of Messaging Protocols for IoT Systems: MQTT, CoAP, AMQP and HTTP

Criteria	MQTT	CoAP	AMQP	HTTP
1. Year	1999	2010	2003	1997
2. Architecture	Client/Broker	Client/Server or Client/Broker	Client/Broker or Client/Server	Client/Server
3. Abstraction	Publish/Subscribe	Request/Response or Publish/Subscribe	Publish/Subscribe or Request/Response	Request/Response
4. Header Size	2 Byte	4 Byte	8 Byte	Undefined
5. Message Size	Small and Undefined (up to 256 MB maximum size)	Small and Undefined (normally small to fit in single IP datagram)	Negotiable and Undefined	Large and Undefined (depends on the web server or the programming technology)
6. Semantics/ Methods	Connect, Disconnect, Publish, Subscribe, Unsubscribe, Close	Get, Post, Put, Delete	Consume, Deliver, Publish, Get, Select, Ack, Delete, Nack, Recover, Reject, Open, Close	Get, Post, Head, Put, Patch, Options, Connect, Delete
7. Cache and Proxy Support	Partial	Yes	Yes	Yes
8. Quality of Service (QoS)/ Reliability	QoS 0 - At most once (Fire-and-Forget), QoS 1 - At least once, QoS 2 - Exactly once	Confirmable Message (similar to At most once) or Non-confirmable Message (similar to At least once)	Settle Format (similar to At most once) or Unsettle Format (similar to At least once)	Limited (via Transport Protocol - TCP)
9. Standards	OASIS, Eclipse Foundations	IETF, Eclipse Foundation	OASIS, ISO/IEC	IETF and W3C
10. Transport Protocol	TCP (MQTT-SN can use UDP)	UDP, SCTP	TCP, SCTP	TCP
11. Security	TLS/SSL	DTLS, IPSec	TLS/SSL, IPSec, SASL	TLS/SSL
12. Default Port	1883/ 8883 (TLS/SSL)	5683 (UDP Port)/ 5684 (DLTS)	5671 (TLS/SSL), 5672	80/ 443 (TLS/SSL)
13. Encoding Format	Binary	Binary	Binary	Text
14. Licensing Model	Open Source	Open Source	Open Source	Free
15. Organisational Support	IBM, Facebook, Eurotech, Cisco, Red Hat, Software AG, Tibco, ITSO, M2Mi, Amazon Web Services (AWS), InduSoft, Fiorano	Large Web Community Support, Cisco, Contiki, Erika, IoTivity	Microsoft , JP Morgan, Bank of America, Barclays, Goldman Sachs, Credit Suisse	Global Web Protocol Standard

Extensible Messaging and Presence Protocol (XMPP):- XMPP is an open standard messaging protocol formalized by IETF [46], and was initially designed for instant messaging and the exchange of messages between applications. It is a text-based protocol, based on Extensible Markup Language (XML) that implements both client-server and publish-subscribe interaction [89], running over TCP. In IoT solutions it is designed to allow users to send messages in real time, in addition to managing the presence of the user. XMPP allows instant messaging applications to achieve all basic features, including authentication, end-to-end encryption and compatibility with other protocols. XMPP supports client-server interaction model, but there are new extensions that enable also for generic publish-subscribe model to be used. These extensions enable XMPP entities to create topics and publish information; an event notification is then broadcasted to all entities that have subscribed to a specific node.

One of the most important characteristics of this protocol are its security features, which makes it one of the more secure messaging protocols surveyed. Unlike the other protocols surveyed, for example MQTT and CoAP, where the TLS and DTLS encryptions are not built-in within the protocol specifications, XMPP specification already incorporates TLS mechanisms, which provides a reliable mechanism to ensure the confidentiality and data integrity. New additions to the XMPP specifications also include extensions related to security, authentication, privacy and access control. Beside TLS, XMPP implements SASL, which guarantees server validation through an XMPP-specific profile

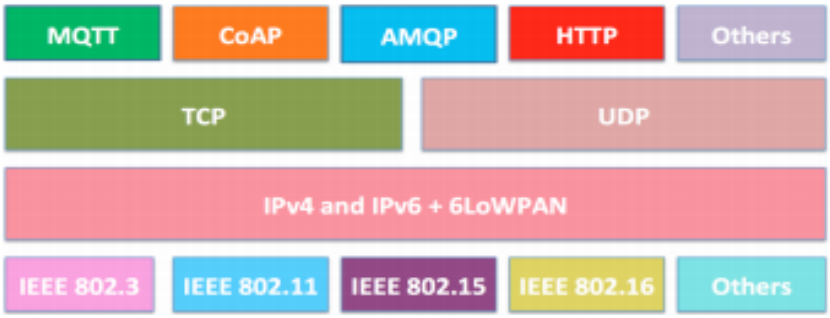


Fig. 1: Protocol Stack for IoT Systems

Ques9:- Write a detailed case study on any 4 areas.

Ans:- (a) Smart cities and Smart Homes:-

Introduction:-

In this case study we are going to talk about how IOT can help in building the smart cities and smart homes as you know that throughout the world and even in countries like India, there is a lot of focus on building smart cities. Of course, the scope of smart cities in each of these different countries is different and the scope again depends on the priority areas of each of these countries and their government. Now for instance in India, since the last few years, there have been a couple of cities that have been identified and phase wise these cities have been given funds to build or to transform them as smart cities.

So, when we talked about smart cities; what is it. So, in addition to the regular infrastructure that is there in any city for example, the urban infrastructure consisting of office buildings residential areas hospitals schools transportation police and so on you also need something in addition to make the cities smart. So, what is this in addition let us talk about. So, smart means what smart means that it is in terms of the services that are given to the respective stake holders of these cities. So, citizens are able to do things in a better manner in an improved manner then usual and how is that made possible that is made possible with the help of nothing, but the ICT technologies information and communication technologies which also includes electronics embedded electronics different other advanced topologies in electrical in a electrical sciences and so on. So, computers electronics put together can make these cities smart.

Example:- So, first of all let us consider any smart city. So, if we are talking about a smart city we need to have the basic components for example, transport there has to be a railways there has to be hospitals there has to be schools there has to be let us say traffic control traffic control waste management waste management banking then.

So, like this these are some of the different things in a smart city right and one thing I have missed which is very much essential is the police. So, as you can see that we have to transform all of these different components of any city to be smart. So, for which the technology is that we have studied. So, far in the previous lectures will have to be taken help of. So, definitely will have to take help of sensors sensor networks sensor networks then actuators then the different other communication technologies RFID, NFC, ZWAVE and so and so forth. So, many different things that we have covered in all these previous lectures of this course on IoT, so, all these will have to be used in order to make this transformation. So, these are the different ICT information and communication technologies that will have to be used right.

- **Analogy:-**

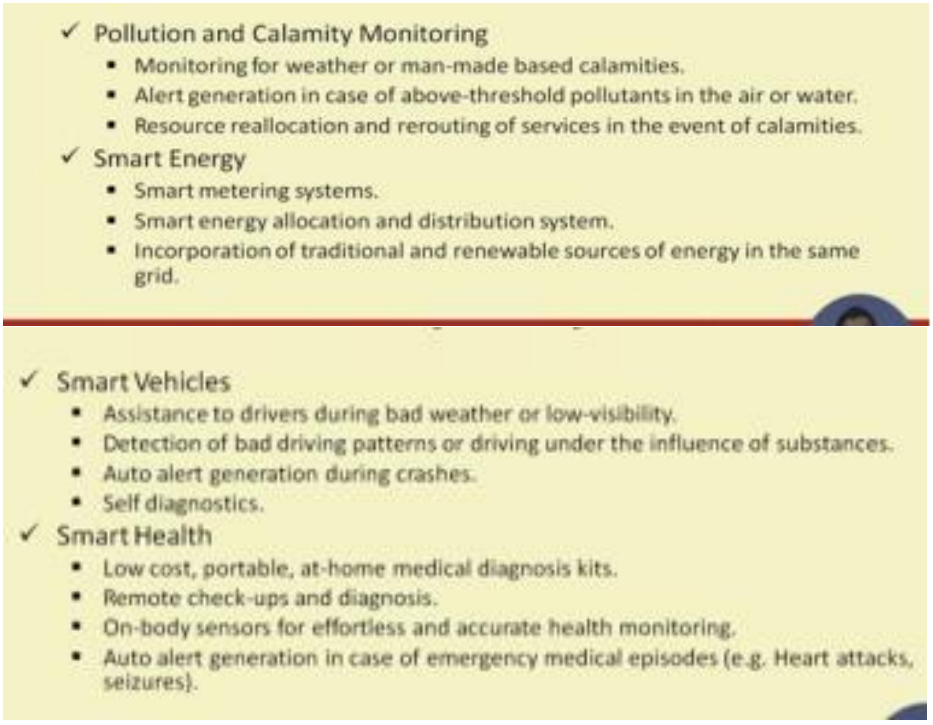
Humans	Smart Cities
Skeleton	Buildings, Industries, People
Skin	Transportation, Logistics
Organs	Hospital, Police, Banks, Schools
Brain	Ubiquitously embedded intelligence
Nerves	Digital telecommunication networks
Sensory Organs	Sensors, Tags
Cognition	Software

So, all these basically necessitate the building of smart cities using advanced ICT tools. So, let us draw some analogy when we talk about a human when we talk about a human humans have the skeleton the skin the organs different types of organs brains nerves sensory organs cognition and so on in the smart city as well in the same way has as a human has a skeleton skin and organs smart cities or rather any city rather any city has buildings industries people transportation logistics hospital police banks schools. So, these are there, but on top of that if there is a human with skeleton skin and organs, but no brains no nerves no sensory organs no cognition. So, you do not have you know life in that human you do not have any life in that human.

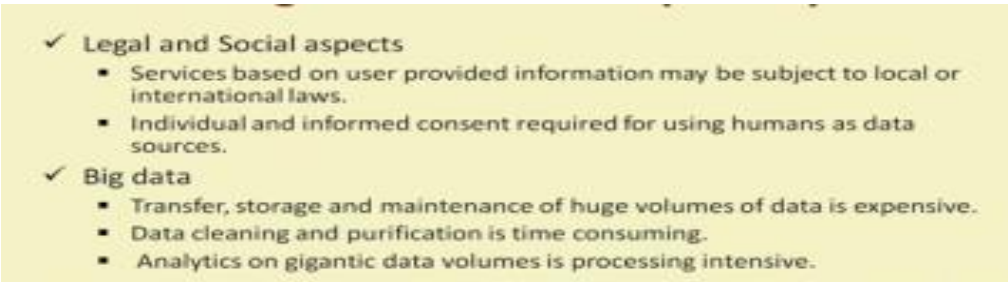
- **Focused Areas:-**
  1. **Application Focus Areas:-** These are some of the application focus areas we have smart economy. So, because of the ever increasing competitiveness you need to improve you need to improve your infrastructure the economy to make it smart. So, I will talk about that in more detail shortly now you need to also improve the citizen participation in any good governance in any good governance you need to improve you need to increase the citizen participation and how is that possible you need to take help of the ICT tools.

  2. **Current Focus Areas:-** Now, we have the different focus areas we have smart homes smart parking lots in a smart home situation we need to have I will talk about smart homes in more detail later on, but in a smart home situation we have the health monitoring done in a smart way at home this you know the medical data made available to the doctors whenever there is a health criticality the corresponding house physician would be informed the physician can

take requisite action based on the severity of severity or criticality of the of the health of the patient.



- **IOT Challenges in Smart Cities:-** There are different IOT challenges in smart cities security and privacies one. So, because you know all these different infrastructure are made available to all different types of citizens. So, you know you expose yourself to different types of attacks the government officers there are different files etcetera you know you make yourself vulnerable to different types of attacks privacy leaks and so on when you open up more and more



There are legal and social issues as well for example, services that are based on users user provided information may be subject to local or other national and international laws and that also has to be taken care of in a very smart way individual and informed consent is required for using humans as data sources big data issues are there you know huge volumes of data coming at high speeds and you know different types of vary various types of data media you know text data and so on.

Que10:-Comparison between HTTP, AMQP and MQTT.

Ans:

	HTTP	AMQP	MQTT
Get	Yes	Yes	No
Caching Read	Yes	No	Yes
Put	Yes	No	No
Post	Yes	Yes	No

Delete	Yes	No	No
Content filtering	No	Yes	No
Typed headers	No	Yes	No
Resumeable transfer	Yes	Yes	Yes
Transactions	No	Yes	No
SSL/TLS	Yes	Yes	Yes
Kerberos	Yes	Yes	No
SASL	No	Yes	Yes
Symmetric Protocol	No	Yes	No
Socket Multiplexing	No	Yes	Yes
Out-of-order messaging	No	Yes	Yes
Server initiated transfers	No	Yes	No
Single packet send	Yes	Yes	Yes
Store-and-forward	No	Yes	Yes
Publish-and-subscribe	No	Yes	Yes
Defined error recovery	No	Yes	No
Well defined addresses	Yes	Yes	Yes
Content-based routing	No	Yes	No
Credit-based flow control	No	Yes	No