217529- Internet of Things

Unit Number: 4

Unit Name: **IOT Systems, Network and Protocols**

Unit Outcomes: CO4

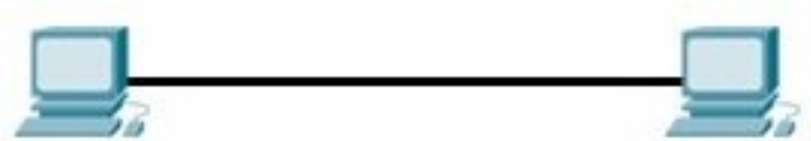
Analyze trade-offs in interconnected wireless embedded device networks.
Select Appropriate protocols for IoT Solutions.

Syllabus

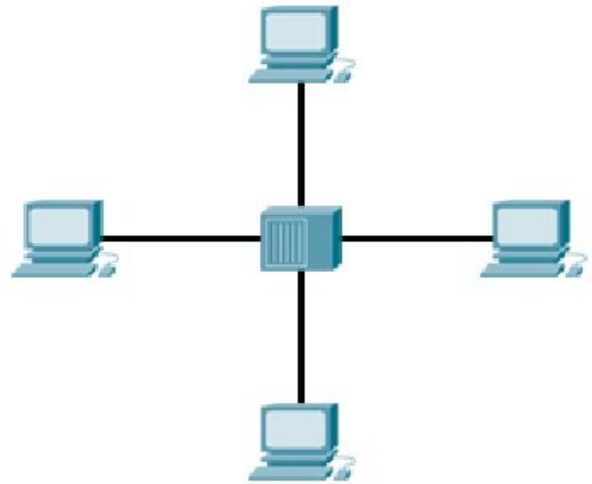
- Study of RF Wireless Sensors, Wireless networks;
- Wireless Sensor Networking (WSN),
- Cellular Machine-to- Machine (M2M) application networks,
- Computer Connected to Internet,
- Network Devices; Device configuration and management,
- Exchange information in real time without human intervention, IoT Protocols

What is Network

- A computer network can be described as a system of interconnected devices that can communicate using some common standards called the Internet protocol suite or TCP/IP. These devices communicate to exchange network resources, such as files and printers, and network services.
- Here is an example of a computer network consisting of two computers connected together:



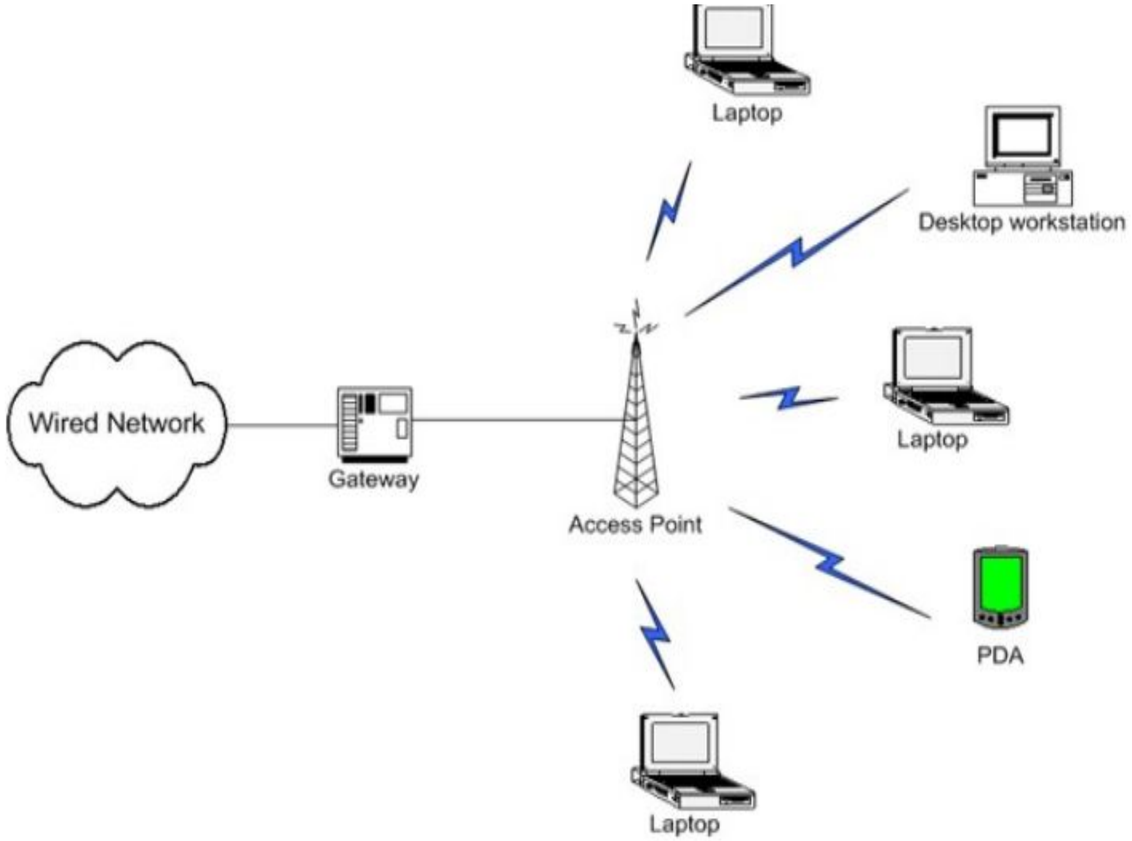
- The example above shows that the two computers are directly connected using a cable. This small network can exchange data between just these two computers.
- What if we want to expand our network? Then we can use network devices such as routers, switches, or hubs, to connect two or more computers together:



Types of Computer Networks

- Listed below are the most common types of computer networks:
  - Local Area Network (LAN) – LANs are commonly used in small to medium size companies, households, buildings, etc., with limited space.
  - Personal Area Network (PAN) – PAN covers a short distance of 10 meters. Bluetooth is an example of PAN.
  - Metropolitan Area Network (MAN) – MANs are used in a single geographic region, such as a city or town.
  - Wide Area Network (WAN) – WANs cover larger areas like different states and countries.
  - Wireless Local Area Network (WLAN) – Wireless LAN is used for wireless networks, connecting wired and wireless devices.

Wireless Networking..



- A wireless network is a computer network that uses wireless data connections between network nodes.
- Wireless networking is a method by which homes, telecommunications networks and business installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.
- Admin telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.
- Examples of wireless networks include cell phone networks, wireless local area networks (WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave networks.

Types of wireless networks

- **Wireless Local Area Networks (LAN):** A wireless local-area network (WLAN) is a **group of connected computers or other devices that form a network** based on radio transmissions rather than wired connections. A Wi-Fi network is a type of WLAN

- **Wireless Personal Area Networks (PAN):**WPAN is **PAN (Personal Area Network)** where the interconnected devices are centered around a **person's workspace and connected through wireless medium**. That's why it is also called as Person's centered short range wireless connectivity. Typically the range is within about 10 meters means very short range.

- **Wireless Metropolitan Area Networks (MAN):**WMAN is a wireless metropolitan area network that can **cover a whole city.** It is larger than WLAN (wireless local area network) and smaller than WWAN (wireless wide area network). WMAN is managed by any private organization or government agencies. Wireless MAN is accessed by only authorized users. It can cover a distance of 30 miles. WMAN can establish a network between different buildings or university campuses within the city.

- **Wireless Wide Area Networks (WAN):** A wide-area network, or WAN, is a telecommunications network that **connects various local area networks to each other and to headquarters, cloud servers, and elsewhere.** Enterprise WANs allow users to share access to applications, services, and other centrally located resources.

WLAN

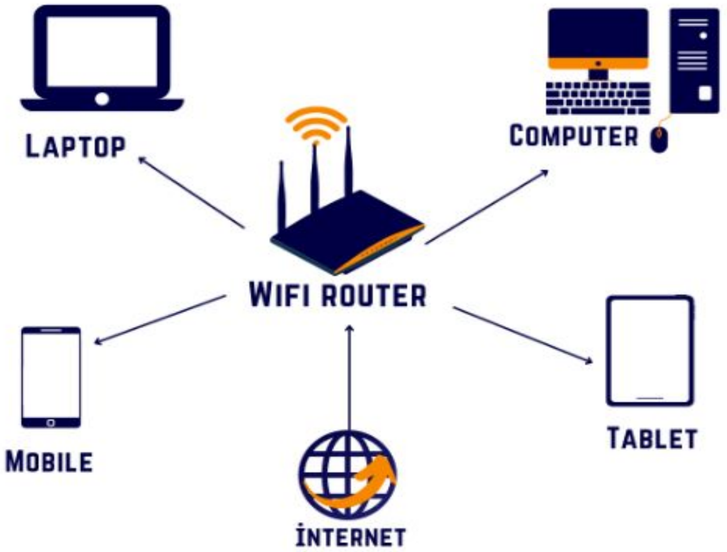
WLAN

WIRELESS LOCAL AREA NETWORK

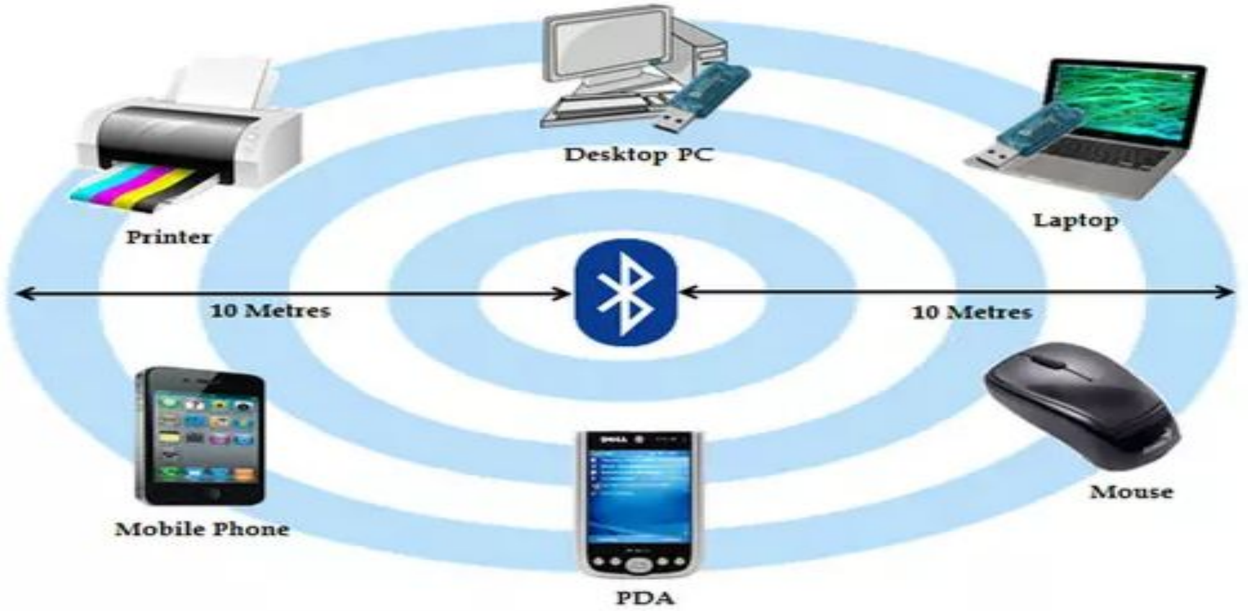
Wireless Local Area Network or WLAN is a wireless network that allows two or more devices to be wirelessly connected to form a local area network on a limited scale.

WLAN has a number of benefits

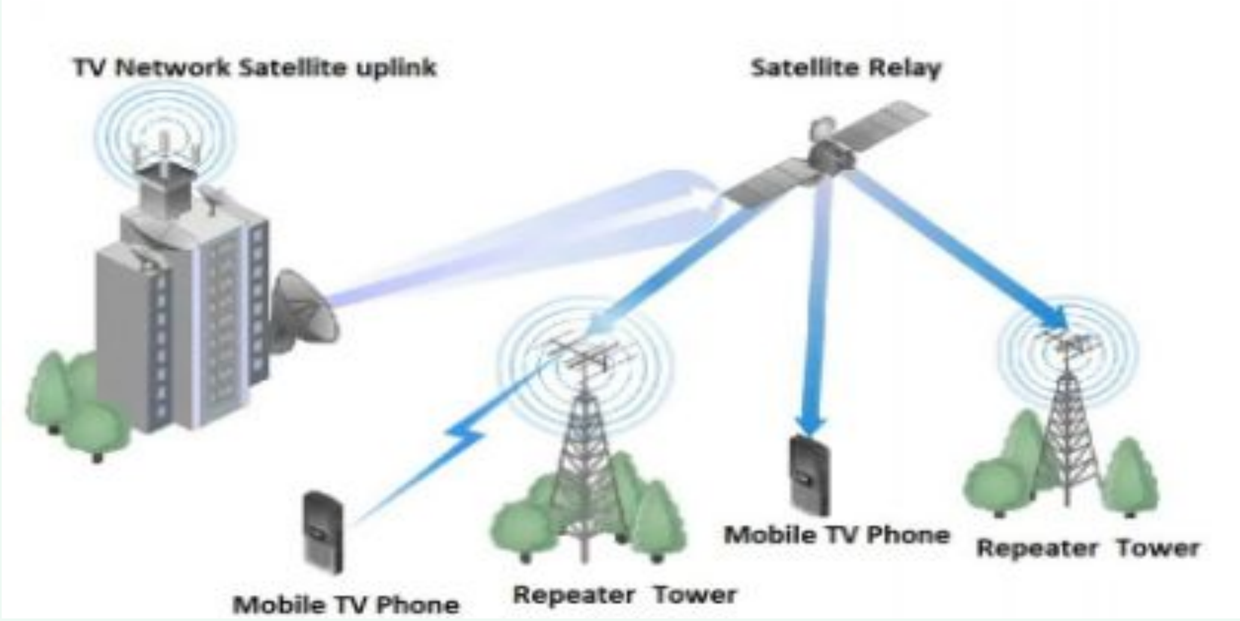
- Internet connectivity while on the move
- Cost effective
- Less hassle for IT and maintenance staff
- Flexibility for organizations



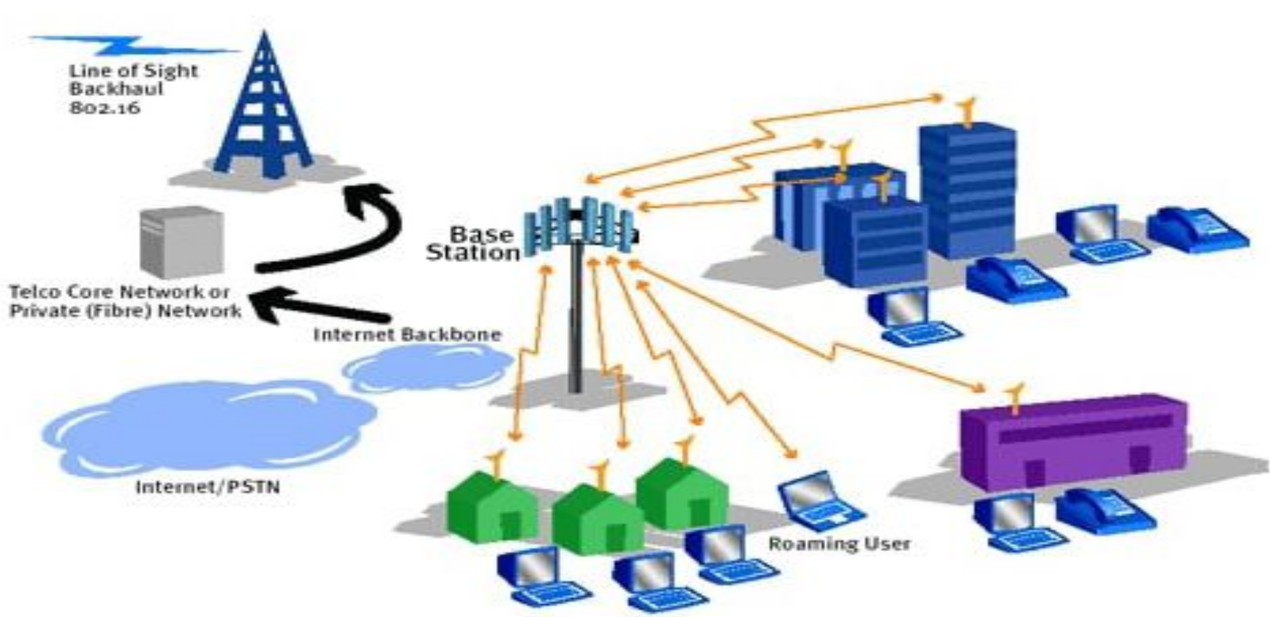
WPAN



WWAN



WMAN



wireless networks, along with their ranges and typical use:

Type	Geographic Range	Usage	Standards
Wireless Personal Area Network (WPAN)	Within reach of an individual	Alternative, or replacement, to cables for peripherals	Bluetooth, ZigBee, NFC
Wireless Local Area Network (WLAN)	Within a building or campus	Wireless extension of wired network	IEEE 802.11(Wi-Fi)
Wireless ad hoc network (Also referred to as a wireless mesh network or mobile ad hoc network, or MANET)	Typically 100m which can be extended by multihop communication of nodes	Variety of applications where central nodes can't be relied upon, i.e. field operations, surveillance network, home and street lighting networks	Not restricted to any one technology or protocol
Wireless Metropolitan Area Network (Wireless MAN)	Citywide	Allows several WLANs to interconnect to cover a metropolitan area and provide a connection to a WAN	IEEE 802.16 (WiMAX)
Wireless Wide Area Network (Wireless WAN or WWAN)	Regional, national, or global	Typically delivered to smartphones and other handheld devices	GSM/UMTS, CDMA One/CDMA2000 and WiMAX
Cellular network	Regional, national, or global	Voice and data cellular networks	Cellular(UMTS, LTE, 0G-5G, etc.)

Sensor

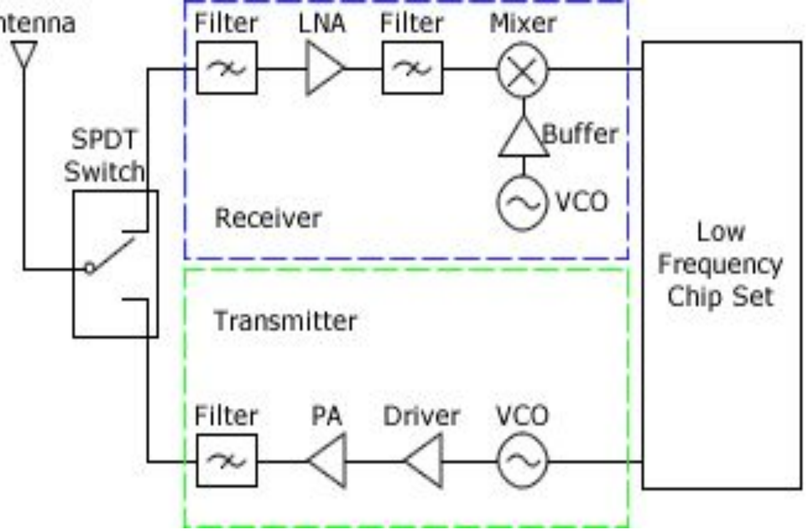
- A **SENSOR** is a device which measures a physical quantity and converts it into a signal which can be read by an observer or by an instrument.

- Technological progress allows more and more sensors to be manufactured on a microscopic scale as microsensors using MEMS (Micro-Electro-Mechanical Systems) technology.

What Is A Wireless Sensor?

- A wireless sensor is a device that can gather sensory information and detect changes in local environments.
- Wireless sensors are designed to measure specific parameters about their physical surroundings and produce outputs, often electrical signals, for further processing.
- A **wireless sensor network** is made up of sensor nodes. Sensor nodes comprise four basic **components** which are the **power unit**, the **sensing unit**, the **processing unit**, and the **transceiver unit**.
- The sensing unit is made up of data converters and sensors, once an analog variable; like sound, is sensed, analog to digital converters (like ADCs) convert the signal to digital format before it is passed into the processing unit. The processing unit is usually a microcontroller which computes the data fed into it and passes the processed data to a transceiver.
- The processing unit also manages the radio network protocols of the system. As for the power unit, it is made up of batteries that delivers power for the sensor node to operate. Additional components of a sensor node include USB connectors, embedded antennas, and oscillators.

RF Wireless Sensors..



- RF wireless sensors are devices that use **radio frequency (RF) signals** refer to a **wireless electromagnetic signal** to communicate wirelessly with a central hub or controller. Radio waves are a form of electromagnetic radiation with identified radio frequencies that range from 3 kHz to 300 GHz.
- Frequency refers to the rate of oscillation (of the radio waves.) **RF propagation occurs at the speed of light and does not need a medium like air in order to travel.** RF waves occur naturally from sun flares, lightning, and from stars in space that radiate RF waves as they age.
- RF communication is used in many industries including television broadcasting, radar systems, computer and mobile platform networks, remote control, remote metering/monitoring, and many more. While individual radio components such as mixers, filters, and power amplifiers can be classified according to operating frequency range, they cannot be strictly categorized by wireless standard (e.g. Wi-Fi, Bluetooth, etc.) because these devices only provide physical layer (PHY) support.
- In contrast, RF modules, transceivers, and SoCs often include data link layer support for one or more wireless communication protocols.

Advantages

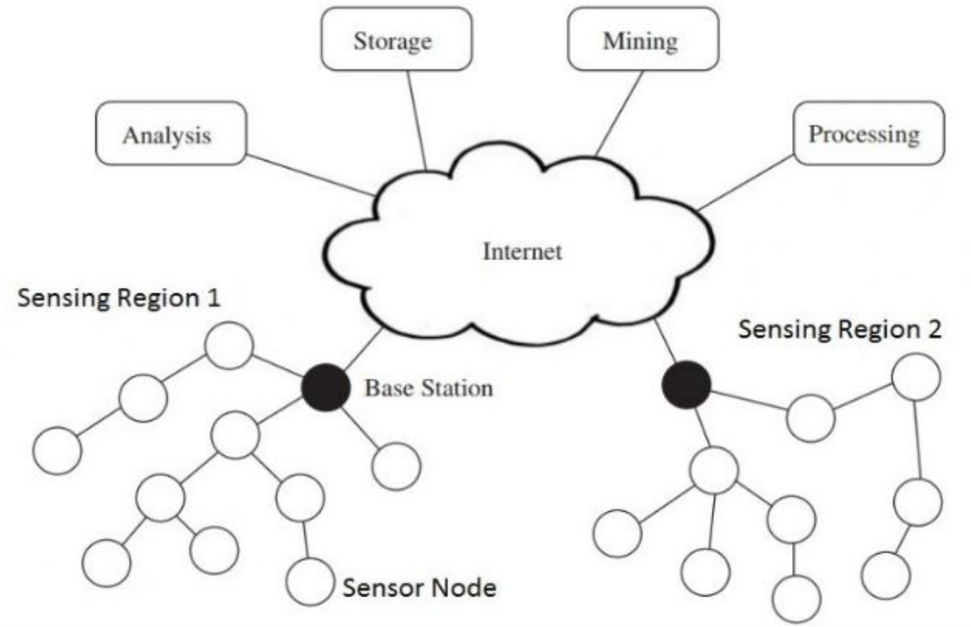
- **Flexibility:** RF wireless sensors are easy to install and can be placed in difficult to reach or hazardous locations without the need for cables or wiring. This flexibility allows for easy reconfiguration and scalability of the system.
- **Reduced installation costs:** Without the need for wiring and cabling, the installation costs of RF wireless sensors are significantly reduced, making them a more cost-effective option.
- **Increased reliability:** With fewer cables and wires to maintain, RF wireless sensors can provide a more reliable solution for monitoring and control systems.
- **Improved accessibility:** RF wireless sensors can be placed in locations that are difficult to access, such as underground or in hard-to-reach areas.
- **Lower maintenance costs:** RF wireless sensors require less maintenance than wired sensors, reducing ongoing maintenance costs.
- **Real-time monitoring:** RF wireless sensors can provide real-time data, allowing for immediate identification and response to changes in the monitored environment.
- **Reduced power consumption:** With the use of energy harvesting or low-power consumption technologies, RF wireless sensors can operate for extended periods on battery power, reducing the need for frequent battery replacement or recharging

Disadvantages

- **Limited range:** RF wireless sensors have a limited range, and obstacles like walls or other obstructions can reduce their effective range even further. This can limit the scope and scale of the sensor network.
- **Interference:** RF wireless sensors are vulnerable to interference from other wireless devices operating on the same frequency band. This can cause signal loss or corruption, reducing the accuracy and reliability of the sensor readings.
- **Security concerns:** Wireless sensor networks can be vulnerable to security breaches, as the signals can potentially be intercepted or hacked, allowing unauthorized access to the data.
- **Battery life:** RF wireless sensors are typically battery-powered, and battery life can be limited, depending on the frequency of transmission and the power requirements of the sensor. This can result in more frequent battery replacement or recharging, adding to the maintenance costs.
- **Cost:** While RF wireless sensors may offer reduced installation costs, the initial cost of the sensors and associated network infrastructure can be higher than wired solutions.
- **Data rate:** RF wireless sensors typically have lower data rates compared to wired solutions, which can limit the amount of data that can be transmitted and processed in real-time.

WSN

- Wireless Sensor Networks (WSNs) can be defined as a **self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location.**
- A typical sensor network consists of sensors, controller and a communication system. If the communication system in a Sensor Network is implemented using a Wireless protocol, then the networks are known as Wireless Sensor Networks or simply WSNs.

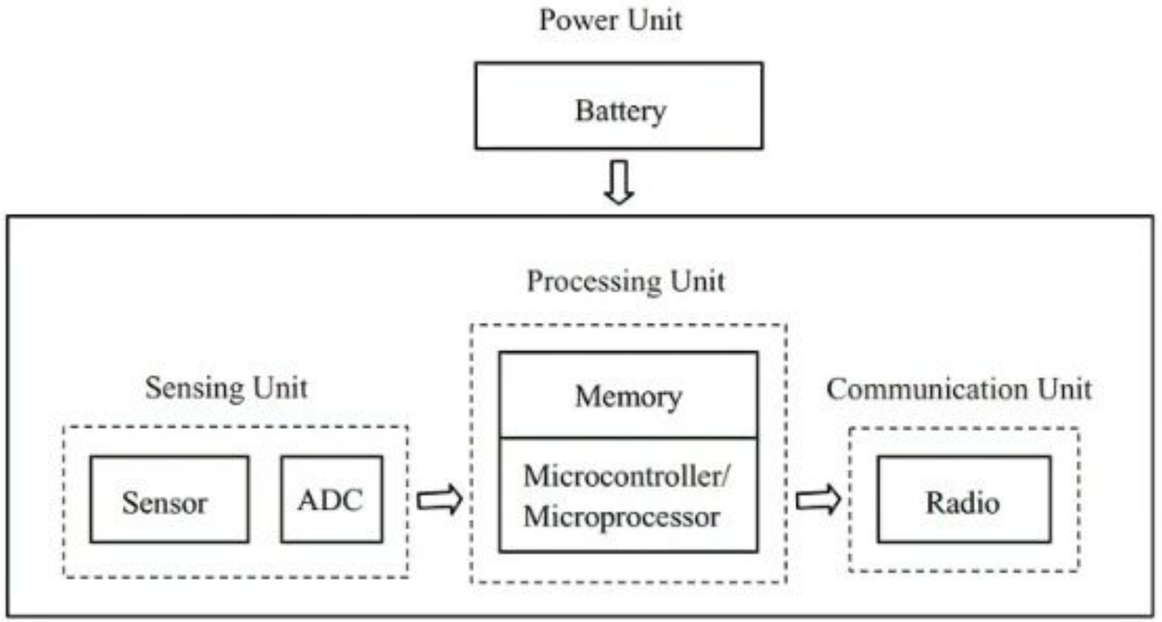


▪ A Wireless Sensor Network consists of Sensor Nodes (we will see about this later) that are deployed in high density and often in large quantities and support sensing, data processing, embedded computing and connectivity.

Elements of WSN

- A typical wireless sensor network can be divided into two elements. They are:
  - **Sensor Node**
  - **Network Architecture**

- A **Sensor Node** in a WSN consists of four basic components. They are:
  - Power Supply
  - Sensor
  - Processing Unit
  - Communication System



Cont..

- The **sensor collects the analog data** from the physical world and an **ADC converts this data to digital data**. The main processing unit, which is usually a microprocessor or a microcontroller, performs an intelligent **data processing and manipulation.**

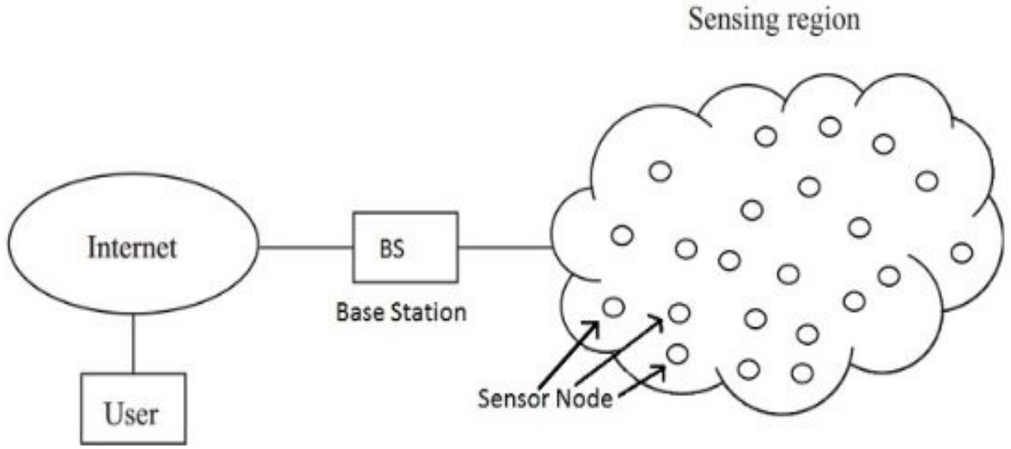
- Communication system consists of **radio system**, usually a short-range radio, for data transmission and reception. As all the components are low-power devices, a small battery like CR-2032, is used to power the entire system.

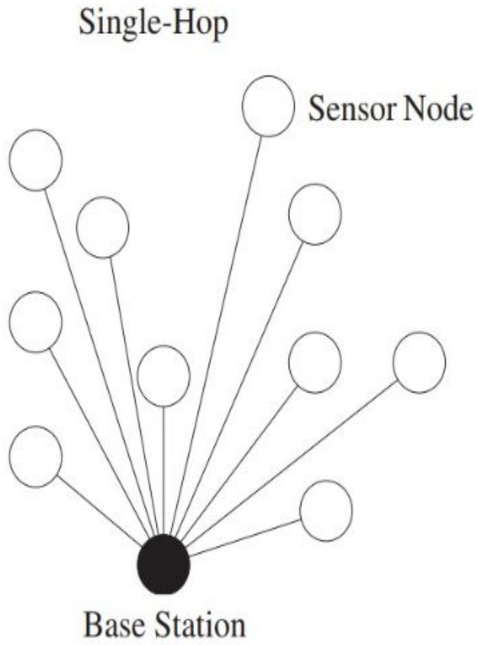
- Despite the name, a Sensor Node consists of not only the sensing component but also other important features like processing, communication and storage units.

- With all these features, components and enhancements, a Sensor Node is responsible for physical world data collection, network analysis, data correlation and fusion of data from other sensor with its own data.

Cont....

- **Network Architecture:** When a large number of sensor nodes are deployed in a large area to co-operatively monitor a physical environment, the networking of these sensor node is equally important. A sensor node in a WSN not only communicates with other sensor nodes but also with a Base Station (BS) using wireless communication.

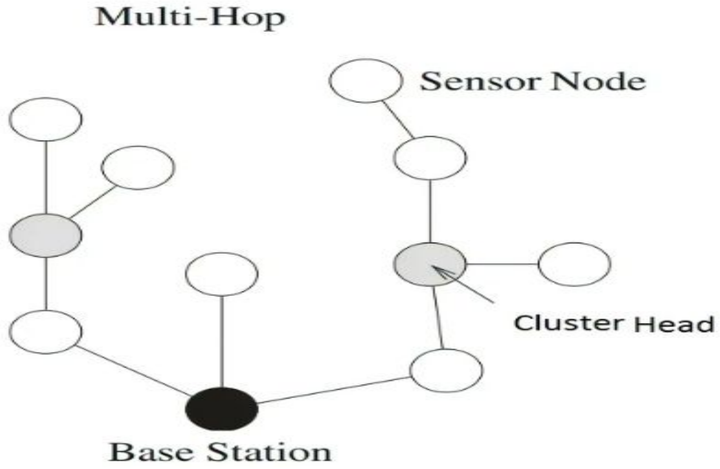




- The base station sends commands to the sensor nodes and the sensor node perform the task by collaborating with each other. After collecting the necessary data, the sensor nodes send the data back to the base station.
- A base station also acts as a gateway to other networks through the internet. After receiving the data from the sensor nodes, a base station performs simple data processing and sends the updated information to the user using internet.
- If each sensor node is connected to the base station, it is known as Single-hop network architecture. Although long distance transmission is possible, the energy consumption for communication will be significantly higher than data collection and computation.

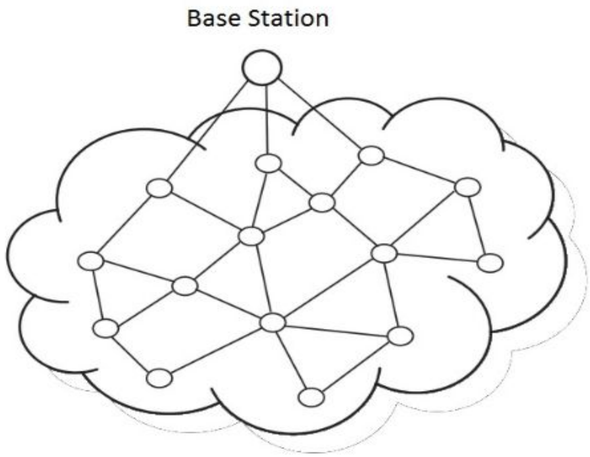
cont..

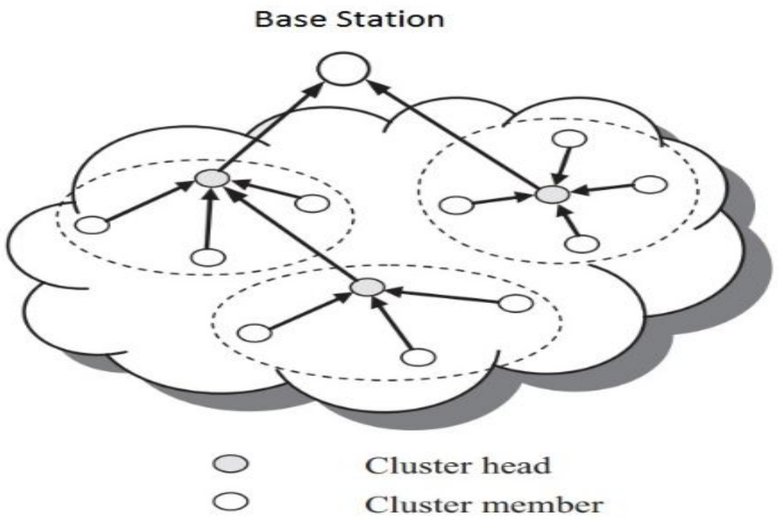
- Hence, Multi-hop network architecture is usually used. Instead of one single link between the sensor node and the base station, the data is transmitted through one or more intermediate node.



- This can be implemented in two ways.
  - Flat network architecture and Hierarchical network architecture.

- In flat architecture, the base station sends commands to all the sensor nodes but the sensor node with matching query will respond using its peer nodes via a multi-hop path.

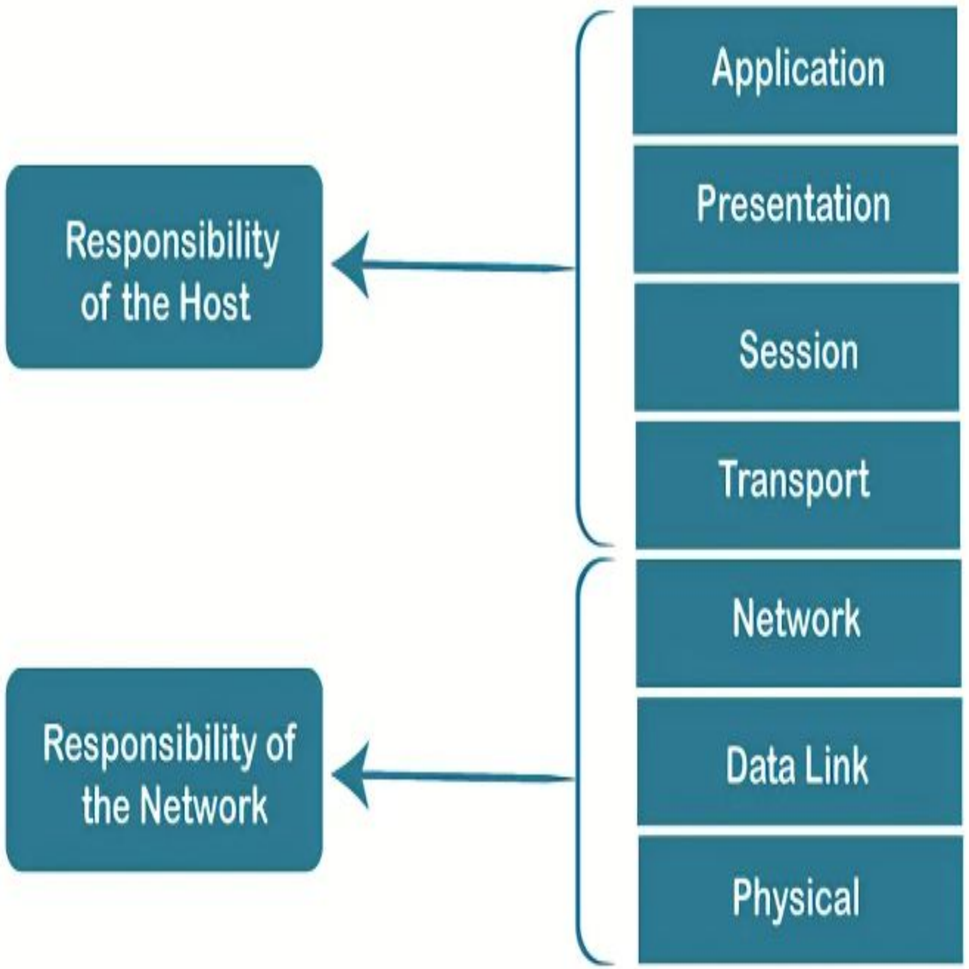




In hierarchical architecture, a group of sensor nodes are formed as a cluster and the sensor nodes ransmit data to corresponding cluster heads. The cluster heads can then relay the data to the base tation.

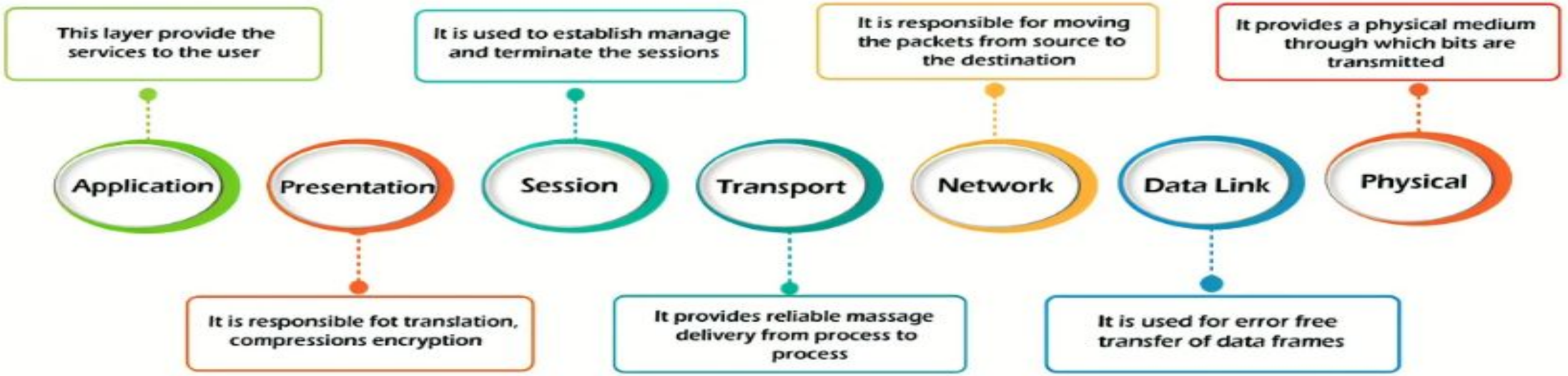
OSI Model Visualization

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a **software application in one computer moves through a physical medium to the software application in another computer.**
- OSI consists of **seven layers**, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

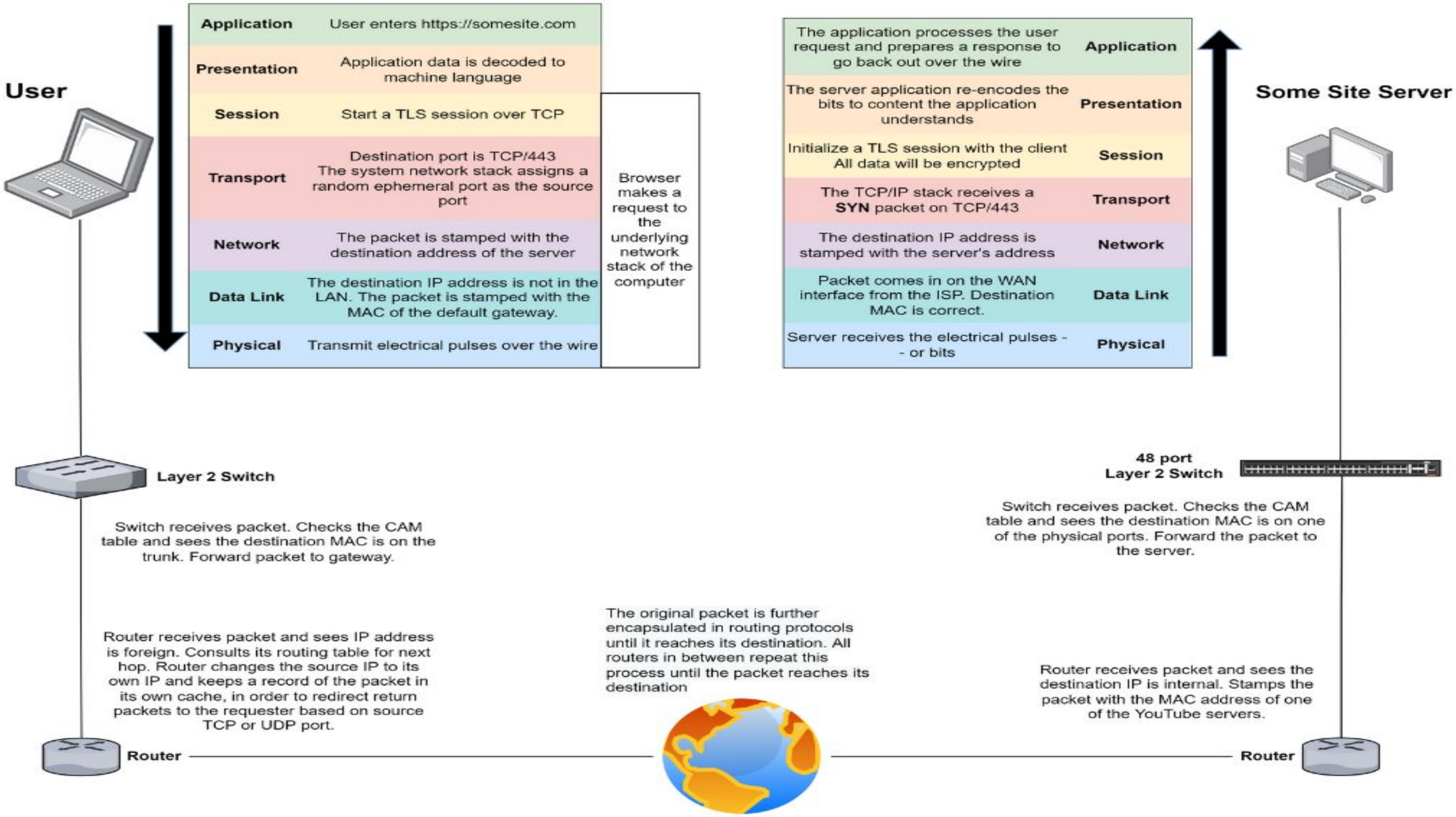


Cont..

- There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:



Cont..


User
Application
User enters https://somesite.com
Presentation
Application data is decoded to machine language
Session
Start a TLS session over TCP
Transport
Destination port is TCP/443
The system network stack assigns a random ephemeral port as the source port
Network
The packet is stamped with the destination address of the server
Data Link
The destination IP address is not in the LAN. The packet is stamped with the MAC of the default gateway.
Physical
Transmit electrical pulses over the wire
Browser makes a request to the underlying network stack of the computer
Layer 2 Switch
Switch receives packet. Checks the CAM table and sees the destination MAC is on the trunk. Forward packet to gateway.
Router receives packet and sees IP address is foreign. Consults its routing table for next hop. Router changes the source IP to its own IP and keeps a record of the packet in its own cache, in order to redirect return packets to the requester based on source TCP or UDP port.
Router
The original packet is further encapsulated in routing protocols until it reaches its destination. All routers in between repeat this process until the packet reaches its destination
Router receives packet and sees the destination IP is internal. Stamps the packet with the MAC address of one of the YouTube servers.
Router
48 port
Layer 2 Switch
Switch receives packet. Checks the CAM table and sees the destination MAC is on one of the physical ports. Forward the packet to the server.
Some Site Server
The application processes the user request and prepares a response to go back out over the wire
Application
The server application re-encodes the bits to content the application understands
Presentation
Initialize a TLS session with the client All data will be encrypted
Session
The TCP/IP stack receives a SYN packet on TCP/443
Transport
The destination IP address is stamped with the server's address
Network
Packet comes in on the WAN interface from the ISP. Destination MAC is correct.
Data Link
Server receives the electrical pulses -- or bits
Physical

Layer and Protocols

OSI LAYER	DEVICES	PROTOCOLS
APPLICATION layer 7		SNMP, SMTP, FTP, TELNET, HTTP, NCP, SMB, AppleTalk
PRESENTATION layer 6		NCP, AFP, TDI
SESSION layer 5		NetBIOS
TRANSPORT layer 4		NetBEUI, TCP, SPX, NWlink
NETWORK layer 3	Routers, layer 3 (or IP) switches.	IP, IPX, NWlink, NetBEUI
DATA LINK layer 2	Bridges and switches, Ethernet incorporates both this layer and the Physical layer.	-
PHYSICAL layer 1	Hubs, repeaters, network adapters, Parallel SCSI buses. Various physical-layer Ethernet incorporates both this layer and the data-link layer. Token ring, FDDI, and IEEE 802.11.	-

Piller 1: M2M: Machine to Machine

- **M2M stands for machine-to-machine, mobile-to-machine, and machine-to-mobile Communications.**

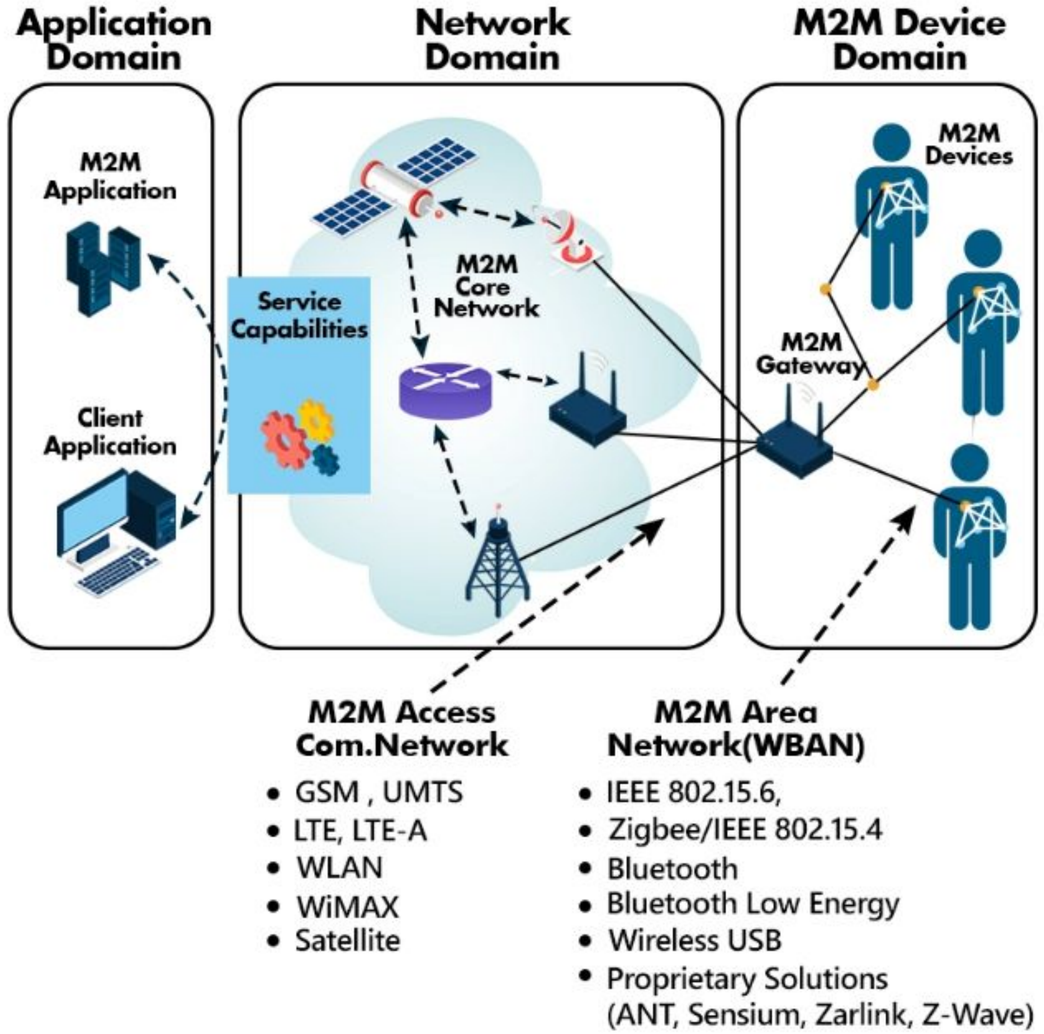
- The automatic communications between devices without any or with very little human intervention. It often refers to a system of remote sensors that is continuously transmitting data to a central system.

- To simplify, M2M is where **two or more machines directly communicate and exchange information to each other through either a wired or a wireless connection.**

- Machine to Machine (M2M) can be defined as a "**direct, point-to-point**" communication standard between devices usually of the same type. It's also meant for a specific on-premise application, which can be through wired or "non-Internet"-based wireless methods, such as Zigbee, RFID, Bluetooth, Wi-Fi, BLE, LoRaWAN, Sigfox, 6LoWPAN, and more.

Piller 1: M2M: Machine to Machine

- **M2M stands for machine-to-machine, mobile-to-machine, and machine-to-mobile Communications.**



- **The three main domains of M2M architecture are:**

1. **M2M application:** As the name suggests, the M2M application domain offers **applications to use M2M technology** conveniently. Examples include server and end-user applications.

2. **M2M network domain:** M2M network domain acts as a **bridge** between the M2M application domain and the M2M device domain. It is made of two parts called the M2M core and M2M service capabilities.

3. **M2M device domain:** M2M device domain contains a**ll the devices** that can connect to the M2M network easily. The device domain can also be called the M2M area network. The M2M device domain includes devices that can connect directly over a network, devices that cannot directly connect to a network and may perhaps require an M2M gateway and proprietary devices.

Working of M2M

- M2M devices send data across a network by sensing information.
- M2M stands for "machine-to-machine" communication. It refers to the **automated exchange of data and information between two or more machines or devices, without requiring human intervention.**
- M2M communication is often used in the context of the Internet of Things (IoT), where sensors and other devices are connected to a network and exchange information with each other in real-time. For example, a smart thermostat may communicate with a smart meter to adjust the temperature in a building based on the energy usage and weather conditions.
- M2M communication can be achieved using various technologies and protocols, including cellular networks, Wi-Fi, Bluetooth, Zigbee, and MQTT. The data exchanged between machines can be in various formats, such as text, numbers, images, or video.
- M2M communication enables automation and remote monitoring of various processes and systems, leading to increased efficiency, productivity, and cost savings. It has applications in various industries, including manufacturing, transportation, healthcare, and agriculture.

Difference between M2M and IoT

M2M	IoT
M2M means direct machine to machine communication	IoT means Internet of Things – a network of internet-connected devices able to sensor, collect and exchange information
Created for businesses to connect with machines	Evolved from M2M and created for both businesses and consumers
Hardware-based	Hardware and software-based
Usually wired connection	Wireless connection
Does not require internet connection	Requires internet connection
2+ machines communicating	Network with thousands of devices communicating
Supports point-to-point communication	Supports Cloud communication
Communicates through a proprietary cellular or wired network	Communicates on standards-based IP networks
Best for small-scale applications	Easy to large-scale applications
M2M applications include vending machines, ATMs, smart meters	IoT applications include smart cities, offices and homes, telehealth, connected cars and EV charging networks, wearables

Application.. Smart Water

Application.. Smart Water

- A smart water system is an integrated set of sensors and ICT systems that enable utilities to remotely and continuously monitor and diagnose problems, prioritize and manage maintenance issues and use data to optimize all aspects of the water distribution network helping to better manage their water assets. It includes two-way real time communications with field sensors, measurement and control devices; along with software and services

- Data collection is obtained in part from integrated wireless sensing multi-probes which are deployed within the water distribution network, enabling sampling and transmittance of relevant data such as hydraulics (pressure, flow), acoustics (hydrophone) and water quality (pH, ORP and conductivity) in real-time. However pipes are buried under streets and sidewalks and are difficult and expensive to access. Further there is no inherent power supply in pipes as there is with electric utilities.

- In the case of agriculture, with sensors and smart controllers, it allows to automatically **conserve water by watering only when it's needed** - take in many different weather variables (t**emperature, humidity, wind, and rainfall**) and the type of plants, sprinkler heads, and soil to calculate and adjust to the appropriate run time for that day

Application.. Smart Water

- Smart water metering technology will enable to track usage more accurately at the consumer end and implement intelligent water pricing plans which would encourage water conservation. Different types of sensors that are used in Smart water controllers include:
- 1. Flow sensors 2. Pressure sensors 3. Sensors for potable water monitoring,
- 4. Sensors for chemical leakage detection in rivers 5. Sensors for pollution. 6. Rain sensors
- 7. Moisture sensors

- Sensors placed throughout the water distribution network and smart meters at consumer place will help manage end-to-end distribution, from reservoirs to pumping stations to smart pipes to intelligent metering at the user site. The sensors could be remotely monitored to provide information about the state of the pipe and allow taking proactive action on problems detected on the distribution network and better control over assets. Actions can be taken remotely (e.g. Pressure regulation within a system, bypassing a section of pipe until maintenance carried out), or even self-healing triggered within a ‘smart pipeline system’ by the sensors themselves.

Purpose of Networking Devices

- When there are a large number of devices in a network, too many data packets get transmitted over the same network path. This can lead to congestion and degradation in performance.

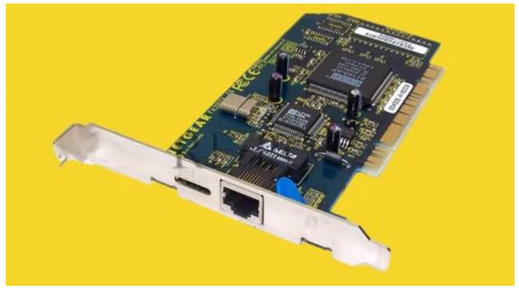
- The purpose of networking devices is to **enable smooth communication between different hardware connected to a network**. Addition of a network device helps in hassle free sharing of network resources between different systems.

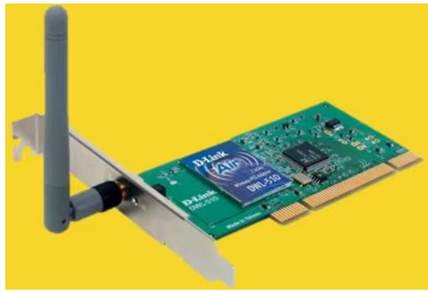
- While computer network devices like hubs send network data to all connected devices, intelligent network devices like routers not only have a fixed source and destination system but they also choose the most efficient route to transmit data.

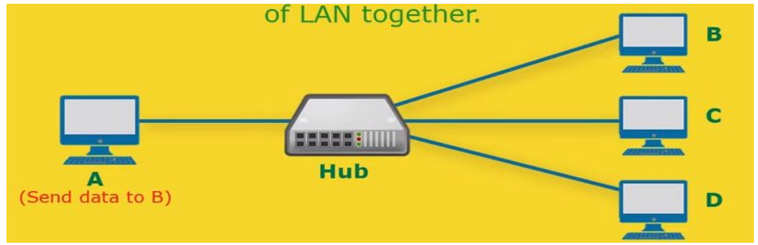
- **Network management** is a system that manages and operates multiple networks within a system. A combination of software and hardware is used in network management systems to gather and analyze data and push out configuration changes to improve performance, reliability, and security.

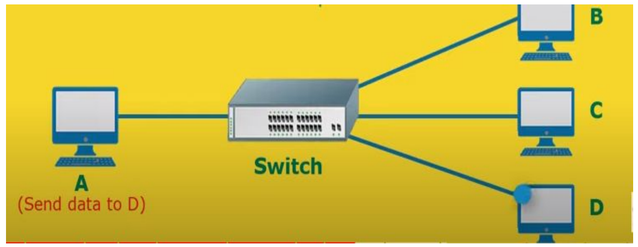
What are network devices?

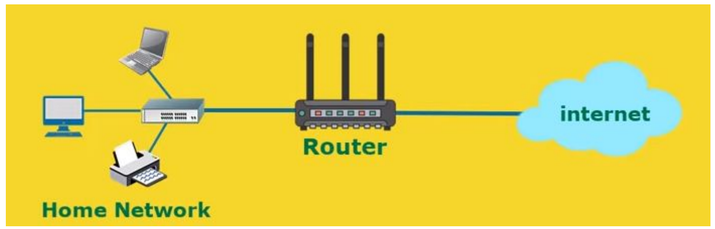
- Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network.
- Types of network devices Here is the common network device list:
  - NIC Card and Wi-Fi Card
  - Hub
  - Switch
  - Router
  - Bridge
  - Gateway
  - Modem
  - Repeater
  - Access Point
    - Link to See working

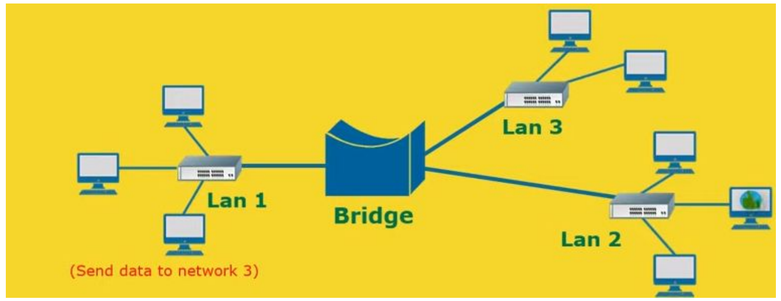


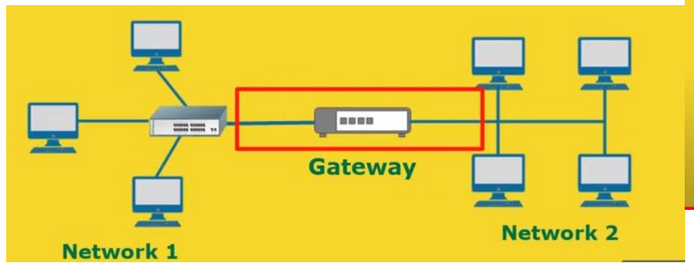


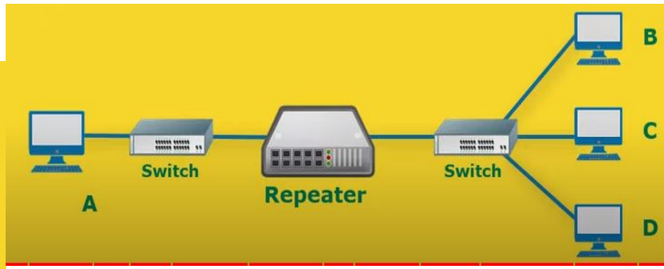












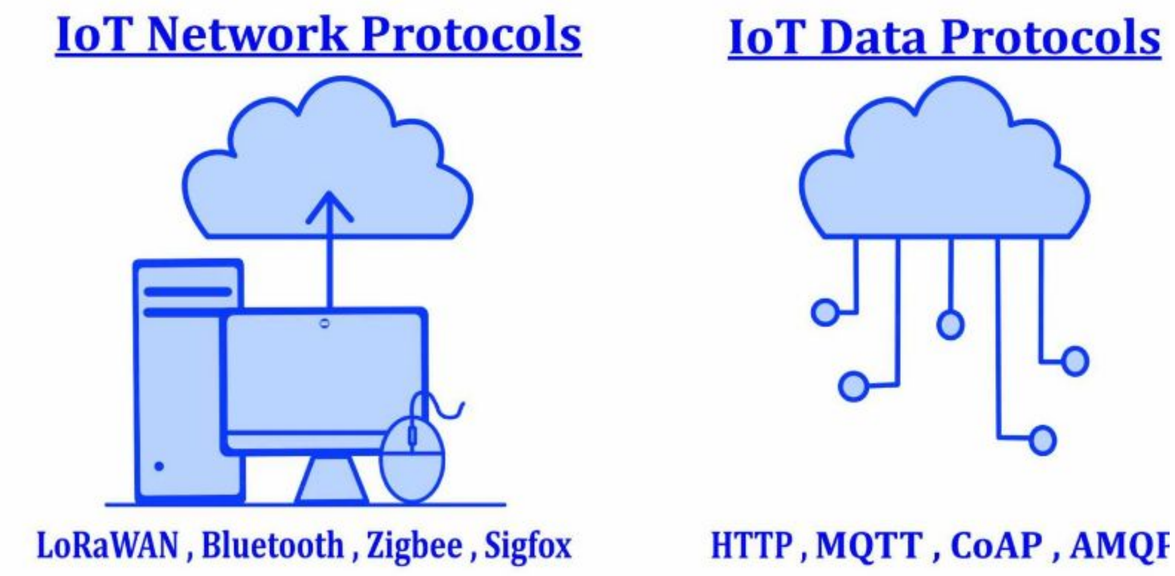
Component of computer network..

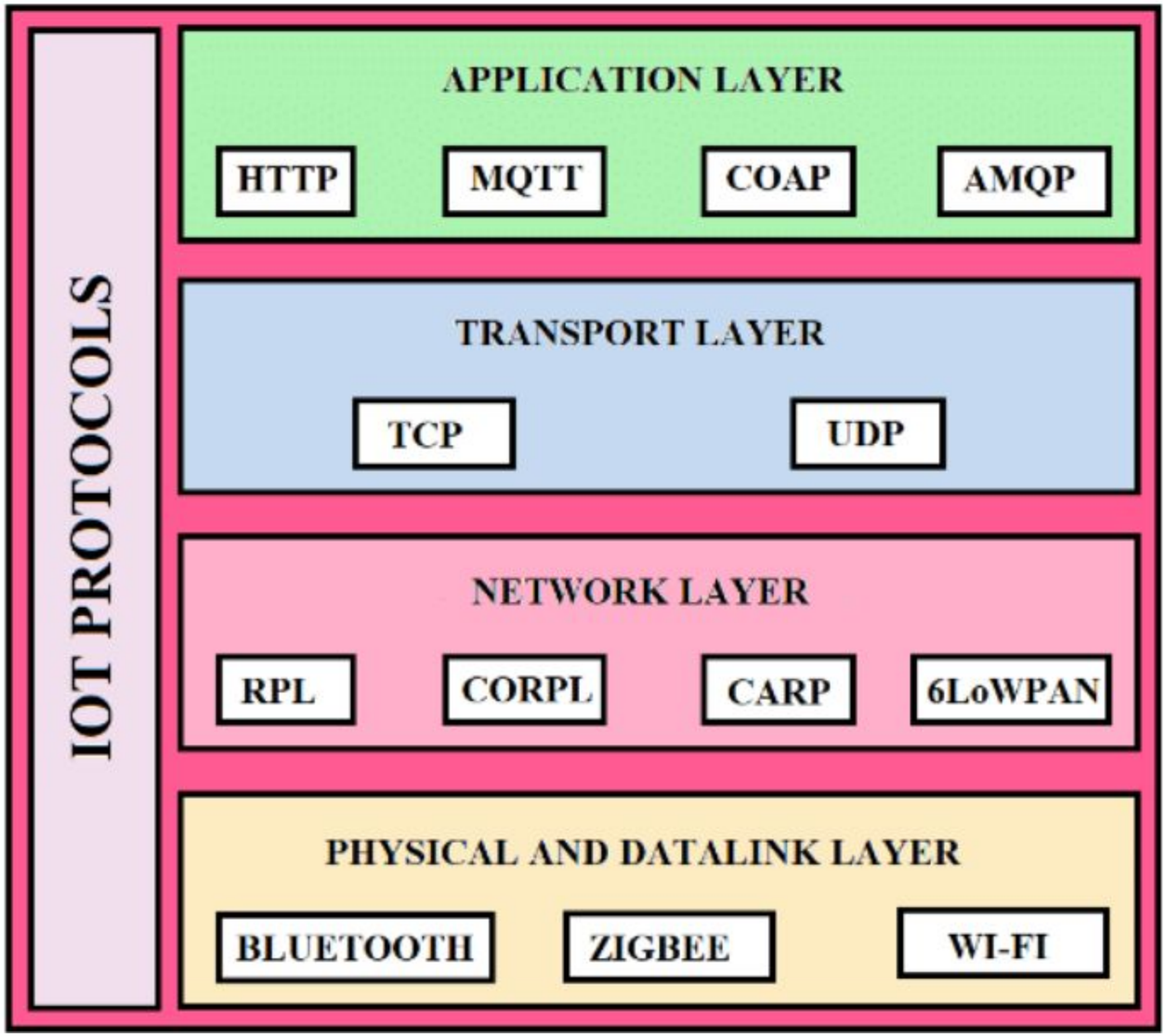
- The key parts that are required to install a network are included in the components of the Computer network. From simple to complex there are numerous types of networks in Computer networks.

- The components that we need to install for a network mainly depend upon the type of Network.
  - Node
  - Media or Link
  - Service
  - Communication protocols
- Link
- To connect to the Internet and other computers on a network, a computer must have a NIC (network interface card) installed. A network cable plugged into the NIC on one end and plugged into a cable modem, DSL modem, router, or switch can allow a computer to access the Internet and connect to other computers.

IOT Protocols..

- Internet of Things (IOT) is the technology that allows us to transmit data from and commands to smart devices in real-time.
- IoT is a network of devices connected via the Internet, with a hub that can analyze the aggregated data. The IoT endpoints can be a person, an animal, a home, a farm, a building, or a whole city.
- But in all cases these things “talk” to each other without any human intervention via an IoT protocol.



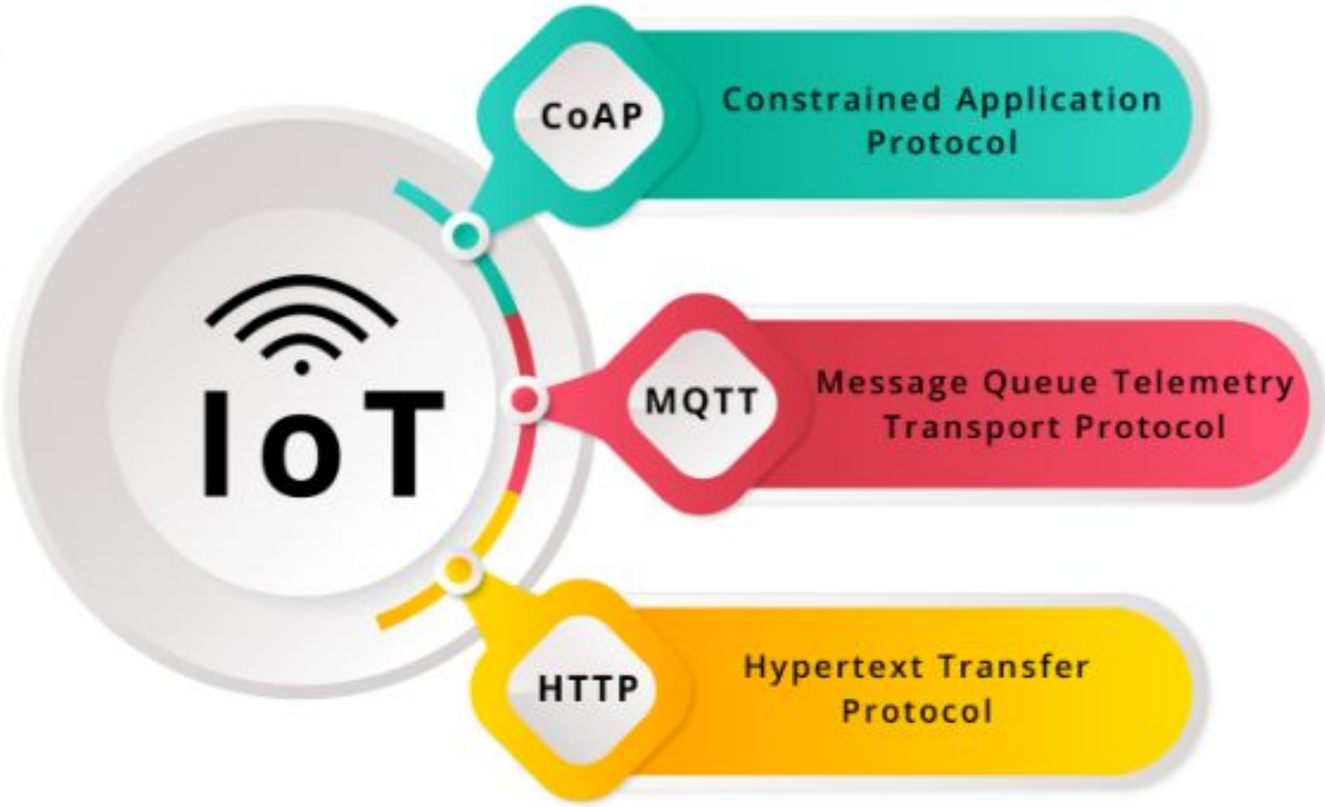


Introduction..

- CoAP is a simple protocol with low overhead specifically designed for constrained devices (such as microcontrollers) and constrained networks. This protocol is used in M2M data exchange

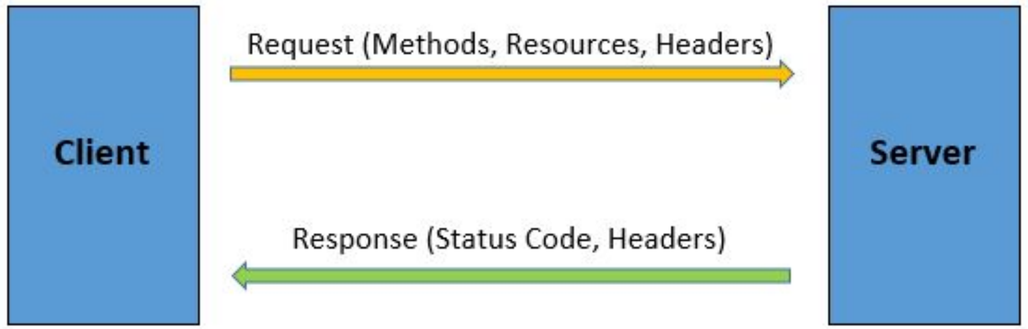
- MQTT (Message Queuing Telemetry Transport) is a machine to machine internet of things connectivity protocol. MQTT is based on subscriber, publisher and broker model. Within the model, the publisher's task is to collect the data and send information to subscribers via the mediation layer which is the broker.

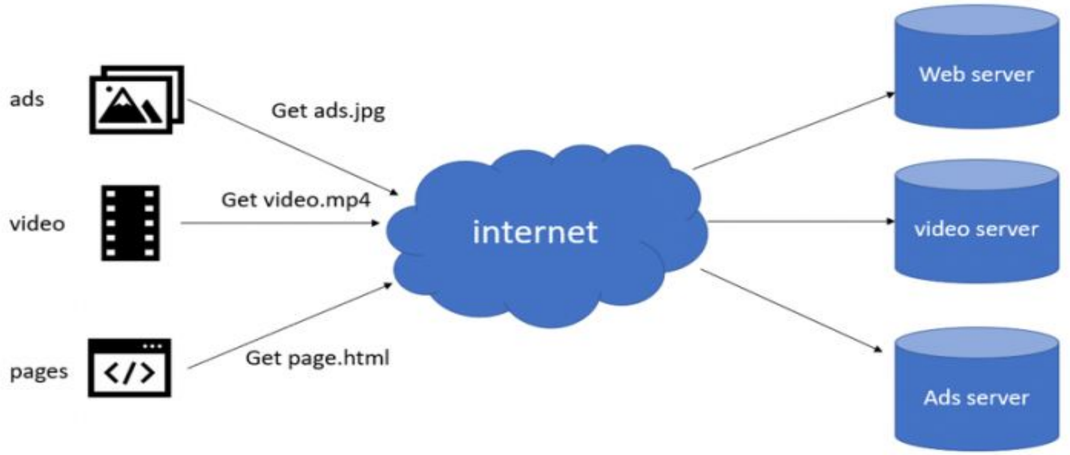
- HTTP stands for Hypertext Transfer Protocol, an application protocol for distributed, collaborative, hypermedia information systems that allows users to communicate data on the World Wide Web
  - Example: http://www……: URL beginning with HTTP scheme



HTTP..

- HTTP stands for Hypertext Transfer Protocol, an application protocol for **distributed, collaborative, hypermedia information systems that allows users to communicate data on the World Wide Web**
- Example: http://www……: URL beginning with HTTP scheme
- To be more specific, HTTP is a stateless request/response protocol where clients request information from a server and the server responds to these requests accordingly (each request is independent of the other). It allows the fetching of resources, such as HTML document

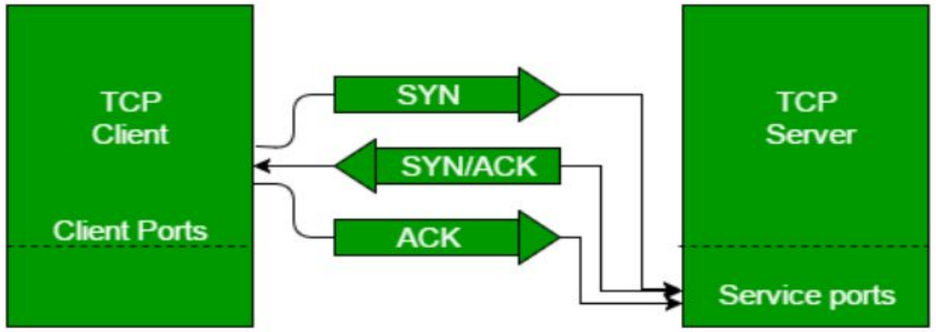


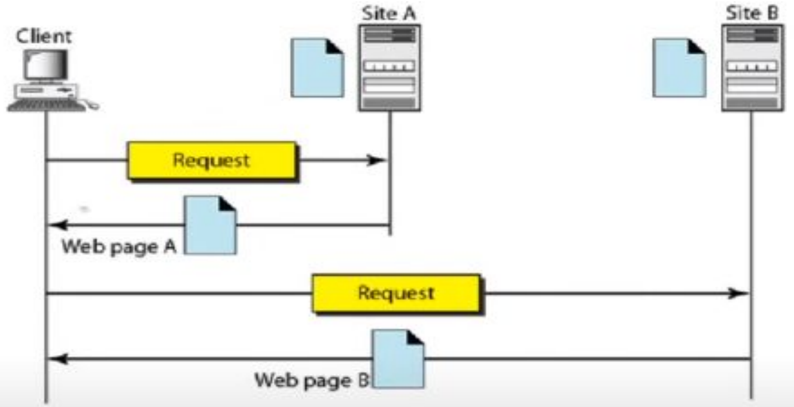


- HTTP was invented alongside HTML to create the first interactive, text-based web browser: the original World Wide Web. Today, the protocol remains one of the primary means of using the Internet.

HTTP Working..

- HTTP data rides above the **TCP protocol,** which guarantees **reliability of delivery**, and breaks down large data requests and responses into network-manageable chunks.
- This is how it works: at first, clients send a SYN packet to the server and then the web server will respond with SYN-ACK packet to confirm success of receiving.
- After which, the client again sends a ACK packet, concluding a connection establishment – this is also commonly referred to as a 3-way handshake.
- In addition, the client sends a HTTP request to the server for a resource and waits for it to respond to a request.
- Then the web server will process the request, find the resource and send the response to the client. If no more resources are required by the client, it sends a FIN packet to close the TCP connection.





HTTP Applications

- HTTP protocol is used for bootstrap the World Wide Web to transmit data in the form of text, audio, images, and video from the Web Server to the user's web browser and vice versa.
- HTTP is currently the data transmission platform of today's web browsing application and is widely used in Internet of Things systems. Even though Http protocol has many disadvantages in transmitting data and is not as suitable as those proficient protocols such as MQTT, CoAP, AMQP using for IoT, this protocol is still popular in smart-home industry as well as many advanced microcontrollers and microprocessor.

Advantages of applying HTTP:

1. **Search capabilities:** Although HTTP is a simple messaging protocol, it includes the **ability to search a database with a single request**. This allows the protocol to be used to carry out SQL searches and return results conveniently formatted in an HTML document.

2. **Ease of programming:** HTTP is coded in **plain text** and therefore is easier to follow and implement than protocols that make use of codes that require lookups. Data is formatted in lines of text and not as strings of variables or fields.

3. **Security:** HTTP 1.0 downloads each file over an independent connection and then closes the connection. So this reduces the risk of interception during transmission significantly

HTTP..

Disadvantages of applying HTTP protocol:

1. **Not suitable for small devices:** As small devices, such as wireless sensor, do not require much interaction and they consume very little power, HTTP is too heavy to be a good fit for these devices. An HTTP request requires a minimum of nine TCP packets, even more when you consider packet loss from poor connectivity, and plain text headers can get very verbose(containing more words than necessary)

2. **Not designed for event-based communication:** Most of the **IOT applications are event based**. The sensor devices measure for some variable like temperature, air quality and might need to take event driven decisions like turning off a switch **HTTP was designed for a request-response based communication rather than an event-driven communication.** Also, programming this event based systems using HTTP protocol becomes a big challenge especially because of the limited computing resources on the sensor devices.

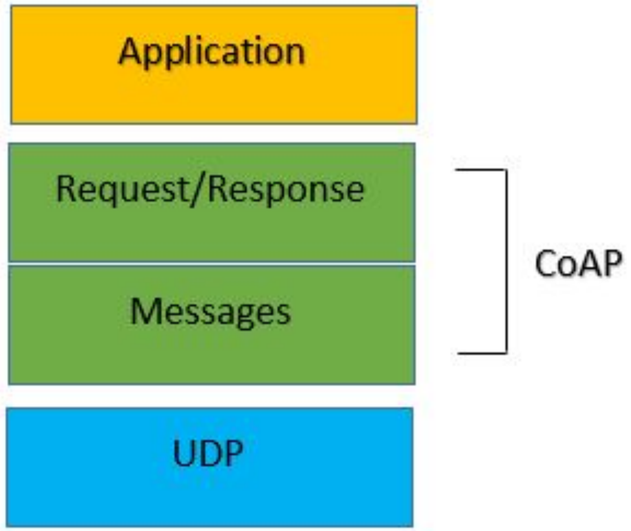
3. **Real-time problem:** After requesting a resource to the server, the **client has to wait for the server to respond**, leading to slow transfer of data. IOT sensors are small devices with **very limited computing resources and hence cannot work efficiently in a synchronous manner.** All the widely used IOT protocols are based on asynchronous models.

Constrained Application Protocol (CoAP)..

- CoAP is a simple protocol with low overhead specifically designed for constrained devices (such as microcontrollers) and constrained networks. This protocol is used in M2M data exchange and is very similar to HTTP, even if there are important differences that we will discuss later.
- CoAP has the following main features:
  - Constrained web protocol fulfilling M2M requirements.
  - Security binding to Datagram Transport Layer Security (DTLS).
  - Asynchronous message exchanges.
  - Low header overhead and parsing complexity.
  - URI and Content-type support.
  - Simple proxy and caching capabilities.
  - Optional resource discovery.
  - UDP (User Datagram Protocol) binding with optional reliability supporting unicast and multicast requests.

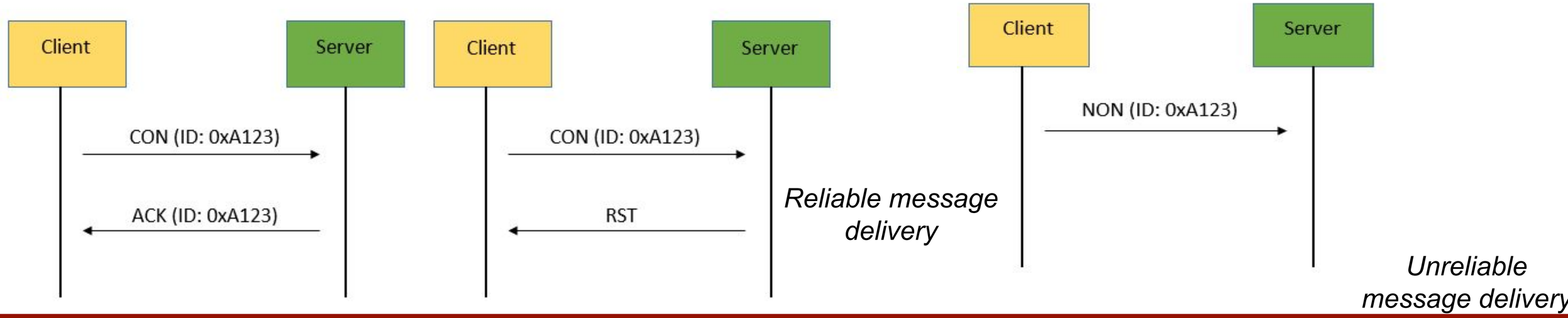
CoAP Structure Model

- CoAP interactive model is similar to HTTP's client/server model. CoAP employs a two layers structure. The **bottom layer** is a message layer that has been designed to deal with **UDP and asynchronous messages**. The **request/response layer** concerns **communication methods and deals with request/response messages.**



CoAP Messages Model

- Message Layer supports 4 types of messages: CON (Confirmable), NON (Non-confirmable), ACK (Acknowledgement), RST (Reset).
- **Reliable message transport:** A CON message is retransmitted until the recipient sends an ACK message with the same message ID. Using default timeout and decreasing counting time exponentially when transmitting a CON message. If a recipient is not able to process a message, it responses by replacing ACK message with RST message.
- **Unreliable message transport:** A message that does not require reliable delivery, can be sent as a NON message. These are not acknowledged, but still have a message ID for duplicate detection. Figure 3 shows unreliable message transport

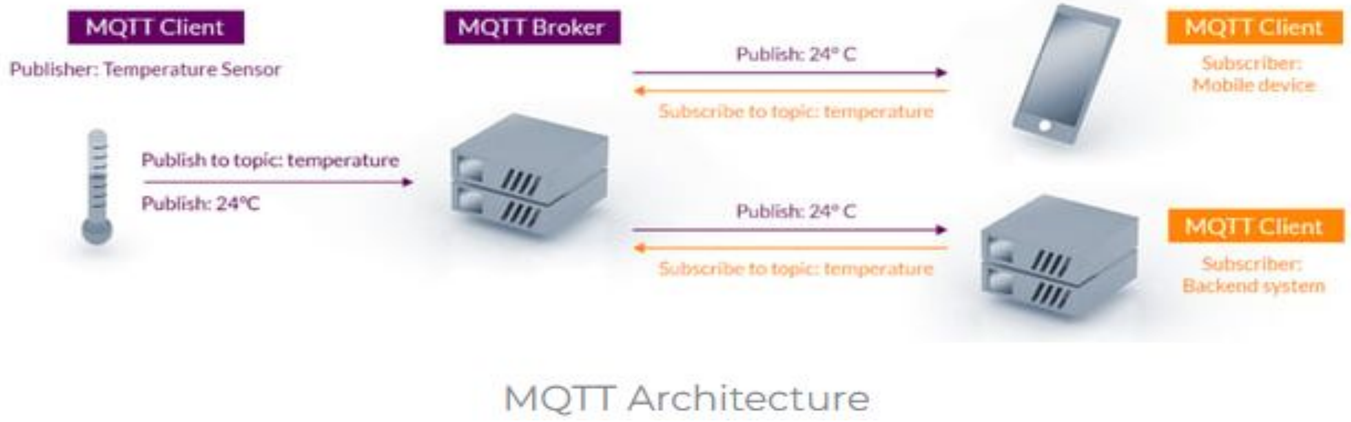


Advantages and Disadvantages of CoAP..

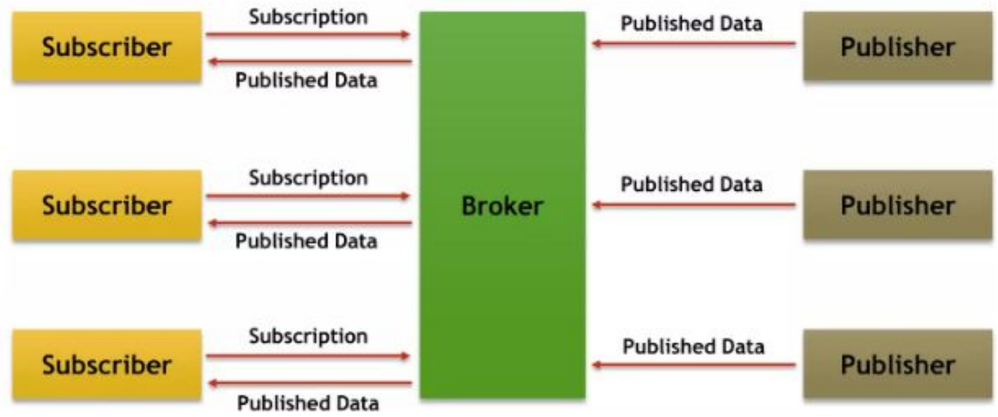
- It is a **simple protocol** and **uses less overhead** due to operation over UDP. It allows **short wake up times and long sleepy states**. This helps in achieving long battery life.
- It uses **IPSEC (IP Security) or DTLS (Datagram Transport Layer Security)** to provide secure communication.
- **Synchronous communication is not necessary** in CoAP protocol.
- It has **lower latency compared** to HTTP.
- It avoids unnecessary retransmissions so that it consumes **less power** than HTTP.
- CoAP protocol is used as the best protocol choice for home communication networks. It is used in information appliances, communication equipment and control equipment in smart home networks.
- **Disadvantages of CoAP protocol**
- CoAP is an **unreliable protocol** due to the use of UDP. Hence CoAP messages reach unordered or will get lost when they arrive at destination
- It **acknowledges each receipt** of the message and hence **increases processing time**. Moreover, it does not verify whether the received message has been decoded properly or not.
- It is an **unencrypted protocol like MQTT and uses DTLS to provide security** at the cost of implementation overhead.
- CoAP has **communication issues** for devices behind **NAT** (Network Address Translation).

MQTT(Message Queing Telementry Transport)

- It is a publish and subscribe system where we can publish and receive the messages as a client. It makes it easy for communication between multiple devices.
- It is a simple messaging protocol designed for the constrained devices and with low bandwidth, so it's a perfect solution for the internet of things applications.
- Developed as an open OASIS standard and an ISO recommended protocol, the MQTT was aimed to operate on data transmissions with a small bandwidth and minimum resources (e.g. on microcontrollers).
- It usually uses the TCP/IP protocol suite, which runs by first establishing connections, then allows multiple exchanges of data until one party finally disconnects itself.
- The MQTT technology runs using the MQTT Publish/Subscribe architecture and establishes the network from 2 different component categories: Clients (Publisher and Subscriber) and Brokers.



MQTT Architecture



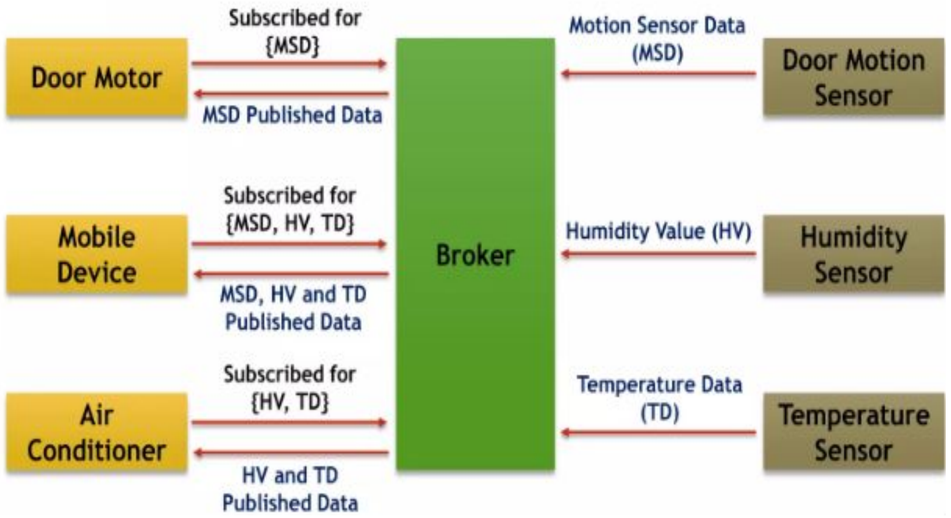
MQTT Publisher, Broker and Subscriber

- MQTT Publisher
  - System or sensors which collects data and send it to the broker which further sends it to multiple subscribers.
  - Example motion sensor, water level sensor, etc.
  - Publisher publish data in following formats
    - Binary
    - JSON
    - SDC Record
    - Text

MQTT Broker

- Broker is the component which take care of receiving data from Publisher and sending it to Subscriber accordingly.
- Broker has to filter messages, broker can filter messages in following ways.
  - Subject based
  - Content based
  - Type based
- Broker has a subscription table in which it store all the request from the subscriber for the publisher's data.
- Broker sends publish data to multiple subscriber according to this list.

- MQTT Subscriber
  - Subscriber can be a mobile device, data server, monitoring stations, etc. which receives publish data from broker so that it can act according to it or monitor it or store it.
  - Subscriber send request to broker to send required publisher's data.
  - Broker has the table in which it maintains all subscriptions request, and send publish data according to it.
  - Example Mobile devices, Monitoring system, etc.



Characteristics of MQTT..

- The MQTT has some unique features which are hardly found in other protocols. Some of the features of an MQTT are given below:
- It does not require that both the client and the server establish a connection at the same time.
- It allows the clients to subscribe to the narrow selection of topics so that they can receive the information they are looking for.
- It provides faster data transmission, like how WhatsApp/messenger provides a faster delivery. It's a real-time messaging protocol.
- It is designed as a simple and lightweight messaging protocol that uses a publish/subscribe system to exchange the information between the client and the server.
- It is a machine to machine protocol, it provides communication between the devices.

MQTT Architecture..

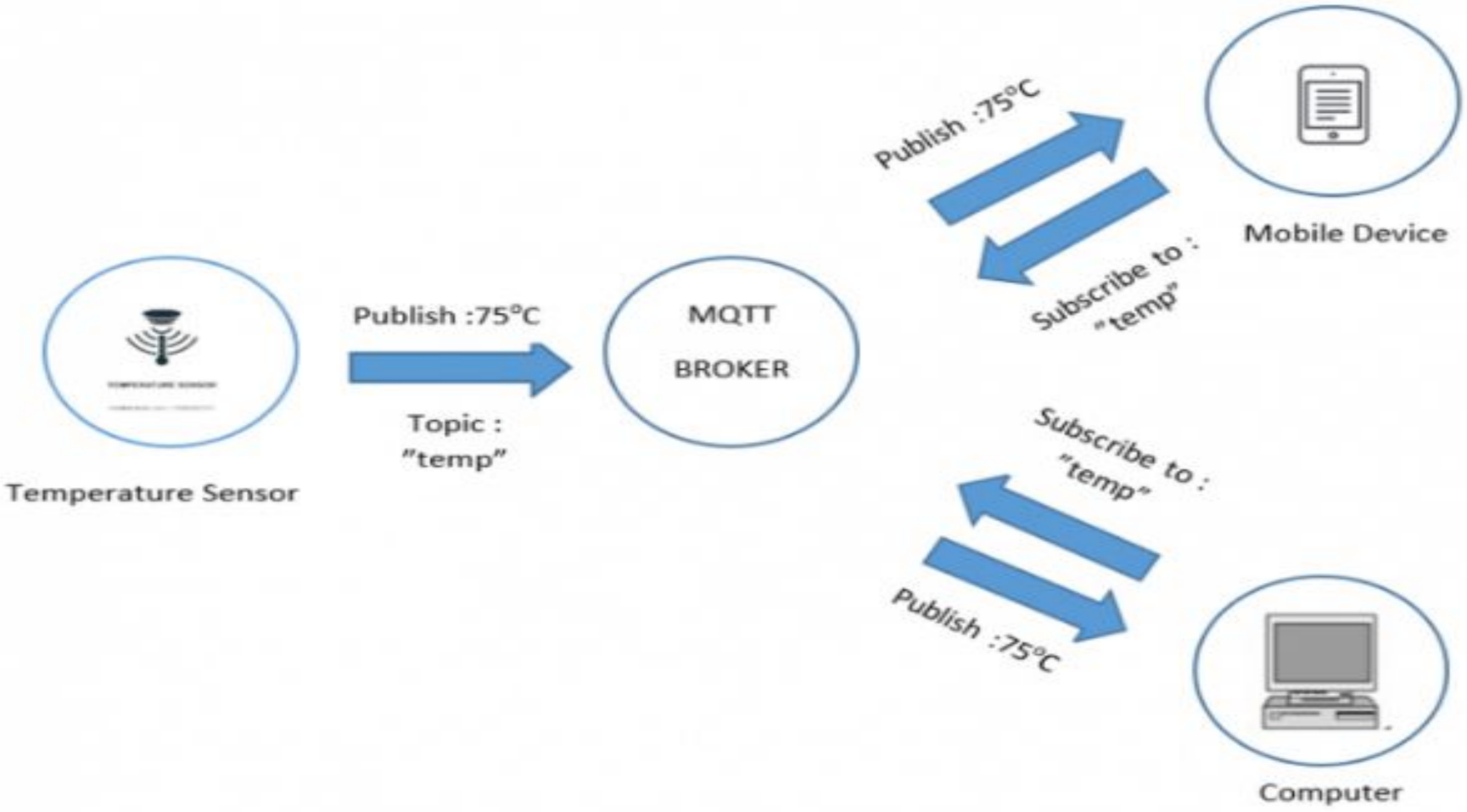
- To understand the MQTT architecture, we first look at the components of the MQTT: message, client, server and topic.
- Message: The message is the data that is carried out by the protocol across the network for the application. When the message is transmitted over the network, then the message contains the following parameters: Payload data, Quality of Service (QoS), Collection of Properties and Topic Name
- Client: In MQTT, the subscriber and publisher are the two roles of a client. The clients subscribe to the topics to publish and receive messages. In simple words, we can say that if any program or device uses an MQTT, then that device is referred to as a client. A device is a client if it opens the network connection to the server, publishes messages that other clients want to see, subscribes to the messages that it is interested in receiving, unsubscribes to the messages that it is not interested in receiving, and closes the network connection to the server.
- In MQTT, the client performs two operations:
  - Publish: When the client sends the data to the server, then we call this operation as a publish.
  - Subscribe: When the client receives the data from the server, then we call this operation a subscription.

Cont..

- Server: The device or a program that allows the client to publish the messages and subscribe to the messages. A server accepts the network connection from the client, accepts the messages from the client, processes the subscribe and unsubscribe requests, forwards the application messages to the client, and closes the network connection from the client.

- Topic: The label provided to the message is checked against the subscription known by the server is known as TOPIC.

Example..



Example illustrating data retrieval and transmission (temperature) in MQTT

Advantages and Disadvantages ..

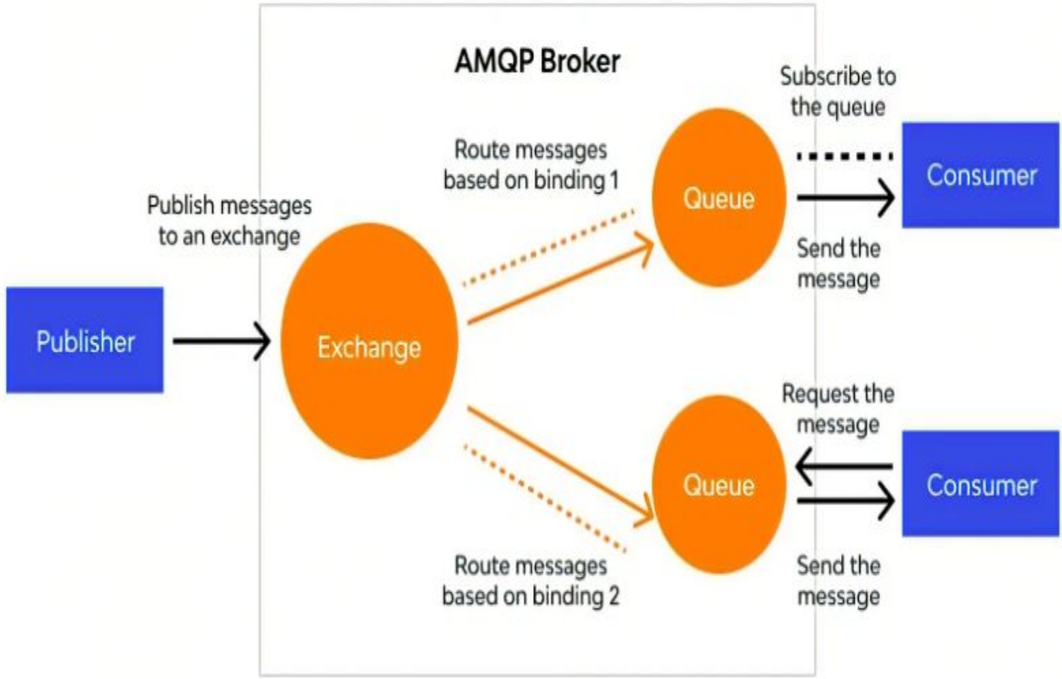
- Advantages of MQTT protocol:
  - Efficient data transmission and quick to implement due to its being a lightweight protocol;
  - Low network usage, due to minimize data packets;
  - Efficient distribution of data;
  - Successful implementation of remote sensing and control;
  - Fast and efficient message delivery;
  - Usage of small amounts of power, which is good for the connected devices;
  - Reduction of network bandwidth
- Disadvantages of MQTT protocol:
  - MQTT has slower transmit cycles compared to CoAP.
  - MQTT's resource discovery works on flexible topic subscription, whereas CoAP uses a stable resource discovery system.
  - MQTT is unencrypted. Instead, it uses TLS (Transport Layer Security)/SSL (Secure Sockets Layer) for security encryption.
  - It is difficult to create a globally scalable MQTT network.

Criteria	MQTT	HTTP	CoAP
Year	1999	1997	2010
Form	Message Queue Telemetry Transport	Hypertext Transfer Protocol	Constrained Application Protocol
Architecture	Client/Broker	Client/Server	Client/Server
Pattern	Publish/Subscribe	Request/Response	Request/Response
Header Size	2 Byte	Undefined	4 Byte
Message Size	Small and Undefined (up to 256 MB maximum size)	Large and Undefined (depends on the web server)	Small and Undefined (normally small to fit in single IP datagram)
Semantics/Methods	Connect, Disconnect, Publish, Subscribe, Unsubscribe, Close	Get, Post, Head, Put, Patch, Options, Connect, Delete	Get, Post, Put, Delete
Cache & Proxy Support	Partial	Yes	Yes
Quality of Services (QoS)/Reliability	QoS 0 – At most once (Fire and Forget) QoS 1 – At least once QoS 2 – Exactly once	Limited (via Transport Protocol – TCP)	Confirmable Message (similar to At most once) or Non-confirmable (similar to At least once)
Transport Protocol	TCP	TCP	UDP, (Stream Control Transmission Protocol)
Security	TLS /SSL	TLS/SSL	DTLS , IPsec
Default Port	1883/8883 (TLS/SSL)	80/443 (TLS/SSL)	5683 (UDP Port)
Encoding Format	Binary	Text	Binary
Licensing Model	Open Source	Free	Open Source
Organizational Support	IBM, Facebook, Eurotech, Cisco, Red Hat, Software AG, Tibco, ITSO, M2Mi, Amazon Web Services (AWS)	Global Web Protocol Standard	Large Web Community Support, Cisco, Contiki, Erika, IoTivity

AMQP (Advanced Message Queueing Protocol)

- AMQP, like MQPP, is a message queuing protocol. This means that the subscriber and publisher of the system communicate by sending and requesting messages from a '**message queue**'. This standard satisfies the need for IoT applications on asynchronous communication, ensuring that the system is flexible enough to enable communication across numerous 'things'.
- AMQP deals with publishers and consumers. The publishers produce the messages, the consumers pick them up and process them. It's the job of the message broker (such as RabbitMQ) to ensure that the messages from a publisher go to the right consumers.

- A **publisher sends messages** to a named **exchange** and a consumer pulls messages from a **queue** or the queue pushes them to the consumer depending on the configuration.
- It sends transaction message between servers
- **Broker** (or server) plays a crucial role in AMQP protocol enablement. It is responsible for connection building that ensure better data routing and queuing at the client-side.



DDS(Data Distribution service)

- DDS stands for Data Distribution Service, an open standard for **real-time applications.** The Object Management Group Data Distribution Service, is a **middleware protocol** and **API standard** that aims to **enable high-performance, interoperable, scalable data exchanges using a publish-subscribe pattern.**
- Its operation claims to provide a **secure and real-time data distribution.** Like MQTT, DDS works in a **Publisher/Subscriber architecture.**
- DDS is a machine-to-machine technology used for publish-subscribe middleware applications in real-time and embedded systems
- DDS protocol for real-time M2M communication enables scalable, reliable, high-performance, and interoperable data exchange between connected devices independent of the hardware and the software platform. DDS supports broker-less architecture and multicasting to provide high-quality QoS and ensure interoperability.

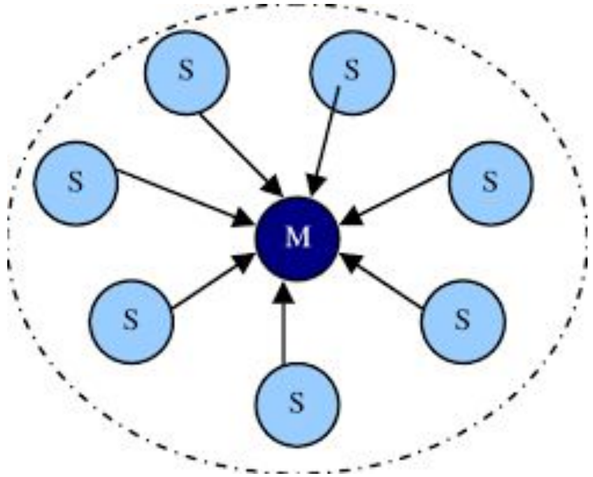
DDS Architecture

IOT Network Protocol-1) Bluetooth

- Bluetooth is used for short-range wireless voice and data communication.
- It is a Wireless Personal Area Network (WPAN) technology and is used for data communications over smaller distances.

Key Features of Bluetooth

- The transmission capacity of Bluetooth is 720 kbps.
- Bluetooth is a wireless device.
- Bluetooth is a Low-cost and short-distance radio communications standard.
- Bluetooth is robust and flexible.
- The basic architecture unit of Bluetooth is a piconet.



IOT Network Protocol-1) Bluetooth..

Types of Bluetooth

Various types of Bluetooth are available in the market nowadays. Let us look at them.

- **In-Car Headset:** One can make calls from the car speaker system without the use of mobile phones.
- **Stereo Headset:** To listen to music in car or in music players at home.
- **Webcam:** One can link the camera with the help of Bluetooth with their laptop or phone.
- **Bluetooth-equipped Printer:** The printer can be used when connected via Bluetooth with mobile phone or laptop.
- **Bluetooth Global Positioning System (GPS):** To use Global Positioning System (GPS) in cars, one can connect their phone with car system via Bluetooth to fetch the directions of the address.

Advantages of Bluetooth

- It is a low-cost and easy-to-use device.
- It can also penetrate through walls.
- It creates an Ad-hoc connection immediately without any wires.
- It is used for voice and data transfer.

IOT Network Protocol-1) Bluetooth..

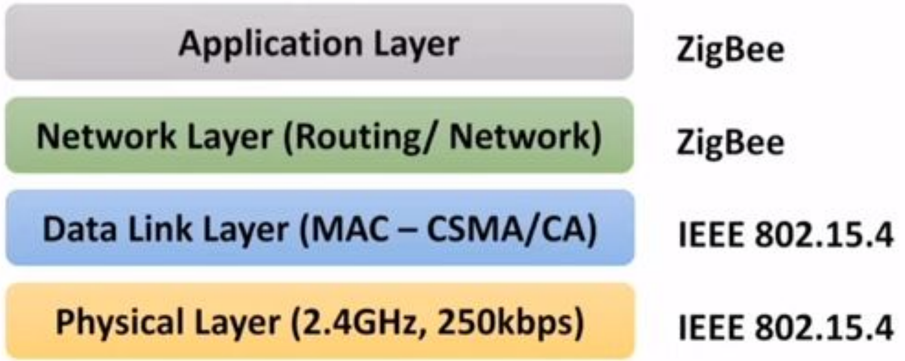
Disadvantages of Bluetooth

- It can be hacked and hence, less secure.
- It has a slow data transfer rate of 3 Mbps.
- Bluetooth communication does not support routing.

Applications of Bluetooth

- It can be used in wireless headsets, wireless PANs, and LANs.
- It can connect a digital camera wireless to a mobile phone.
- It can transfer data in terms of videos, songs, photographs, or files from one cell phone to another cell phone or computer.
- It is used in the sectors of Medical healthcare, sports and fitness, Military.

IOT Network Protocol-2) ZigBee

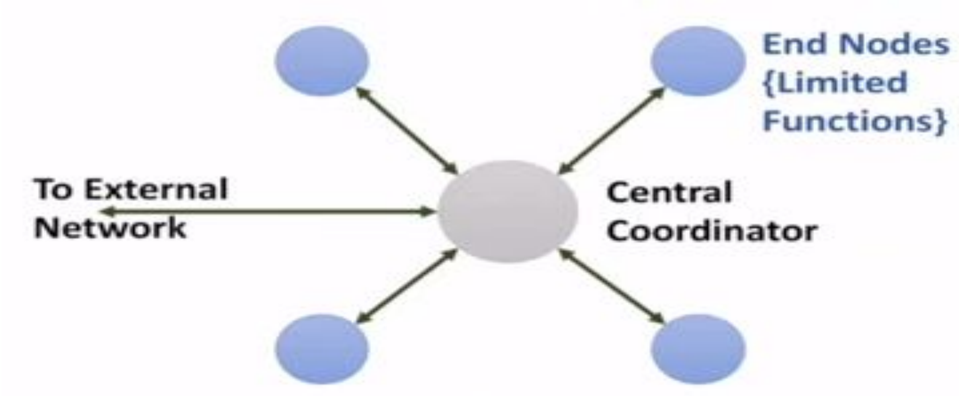


- ZigBee is developed by ZigBee Alliance, ZigBee is a competitor of 6LOWPAN.
- ZigBee uses IEEE 802.15.4 at MAC and Physical Layer.
- ZigBee is designed for low-cost and low-power wireless IoT Networks.
- ZigBee is used in low data rate applications that requires long battery life and secure networking.
- ZigBee is simpler and less expensive than other WPANs such as Bluetooth and Wi-Fi.
- ZigBee operates at short range around 10m to 20m and using mesh networking range can be extended up to 500m.

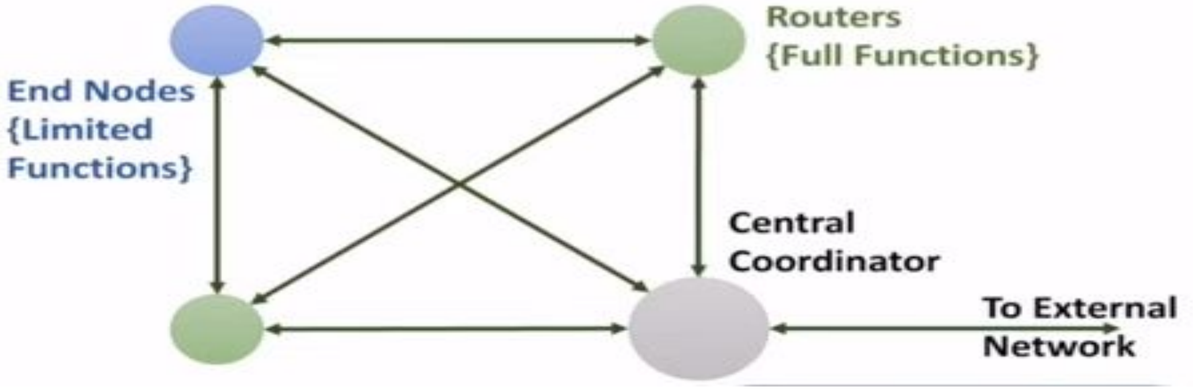
IOT Network Protocol-2) ZigBee…

- ZigBee Supports different network topologies like :
  - STAR
  - Peer to peer (Mesh)
  - Cluster Tree
- ZigBee can be classified as three different devices:
  - ZigBee Coordinator
  - ZigBee Router (full Function Device)
  - ZigBee End Devices(Reduced Function Device)

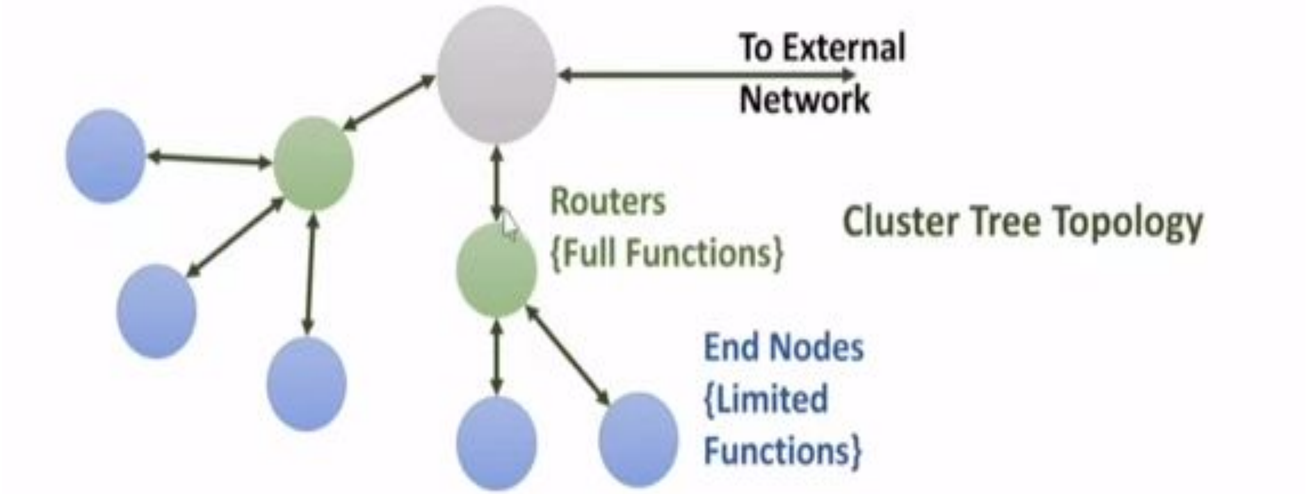
IOT Network Protocol-2) ZigBee… ZigBee Topology-



Star Topology



Peer to Peer {Mesh}



Cluster Tree Topology

IOT Network Protocol-2) ZigBee…

ZigBee Advantages-

- Easy to install and implement.
- It has low cost, low power, and long battery life.
- It supports many nodes (around 6500).
- It is more reliable and self-healing.

ZigBee Disadvantages-

- It has a low data rate. {250kbps MAX}
- It is not as secure as Wi-Fi and Bluetooth.
- It requires additional devices ZCs and ZRs, which increases the cost.
- It lacks internet protocol support.
- ZigBee Networks are incompatible with other networks.

IOT Network Protocol-3) Sigfox

- Long Range, Low Data Rate, Low Power Consumption
- Sigfox is used when wide area coverage is required with minimum power consumption.
- It aims at connecting billions of IoT devices.
- This protocol’s frequency range is 900MHZ, covering a range of 3km to 50km.
- The maximum data rate is very low, which is 1KBPS.

IOT Network Protocol-4) LoRaWAN

- Long Range Communication, High Data Rate, Low power
- This stands for Long Range Wide Area Network.
- Its range is approximately 2.5km and can go up to 15km.
- The data rate is very low, which is 03 KBPS and goes up to a maximum of 50KBPS.
- It can support many connected devices and is used in applications like Smart City, Supply Chain Management, etc.

RFID (Radio Frequency Identification)

- Radio Frequency Identification (RFID) is a technology that uses radio waves to passively identify a tagged object.
- RFID belongs to a group of technologies called automatic identification and data collection .


IntelliStride
Retail
Healthcare
Manufacturing
RFID Applications
Asset Management
Automotive
Transportation
Parking Management

RFID Use Scenarios

<u>These are just examples of RFID use:</u>

- Asset Tracking
- Retail
- Books Tracking (Library)
- Toll Gates fare collection
- Public Transport fare collection (AFC)
- Healthcare
- Animal Identification & Tracking
- Electronic Passport
- Luggage tracking
- Sport
- Anti-Theft
- Parking Systems
- Manufacturing line
- Inventory Management
- Brand Protection
- Access control systems

RFID Inventory Tracking

RFID Parking

RFID in Luggage tracking

RFID in Sports

SPPU Question

Q3)	a)	Draw and Explain WSN architecture?	[9]
	b)	Explain any four IoT network protocols?	[8]
		OR	
Q4)	a)	Explain Machine to Machine Architecture?	[9]
	b)	Explain any four applications of RFID?	[8]