2012 .

UNIT I FUNDAMENTALS OF IOT

Introduction - Definition and Characteristics of IoT - Physical design - IoT Protocols - Logical design - IoT communication models, IoT Communication APIs - Enabling technologies - Wireless Sensor Networks, Cloud Computing, Big data analytics, Communication protocols, Embedded Systems, IoT Levels and Templates - Domain specific IoTs - IoT Architectural view.

1.1 Introduction

- The Internet of Things represents the whole way from collecting data, processing it, taking an action corresponding to the signification of this data to storing everything in the cloud. All this is made possible by the internet
- The Internet of things has become a very widely spread concept in the last few years. The reason for this is mainly the need to computerize and control most of the surrounding objects and have access to data in real time.
- Example: Parking sensors, about phones which can check the weather and so on

1.1.1 Definition & Characteristics of IoT Definition:

A dynamic global n/w infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual ―things‖ have identities, physical attributes and virtual personalities and use intelligent interfaces, and are seamlessly integrated into information n/w, often communicate data associated with users and their environments.

Characteristics of IoT

i)**Dynamic & Self Adapting**:

IoT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, user‘s context or sensed environment.

Eg: The surveillance system comprising of a number of surveillance cameras. The surveillance camera can adapt modes based on whether it is day or night. The surveillance system is adapting itself based on context and changing conditions. ii)**Self Configuring:**

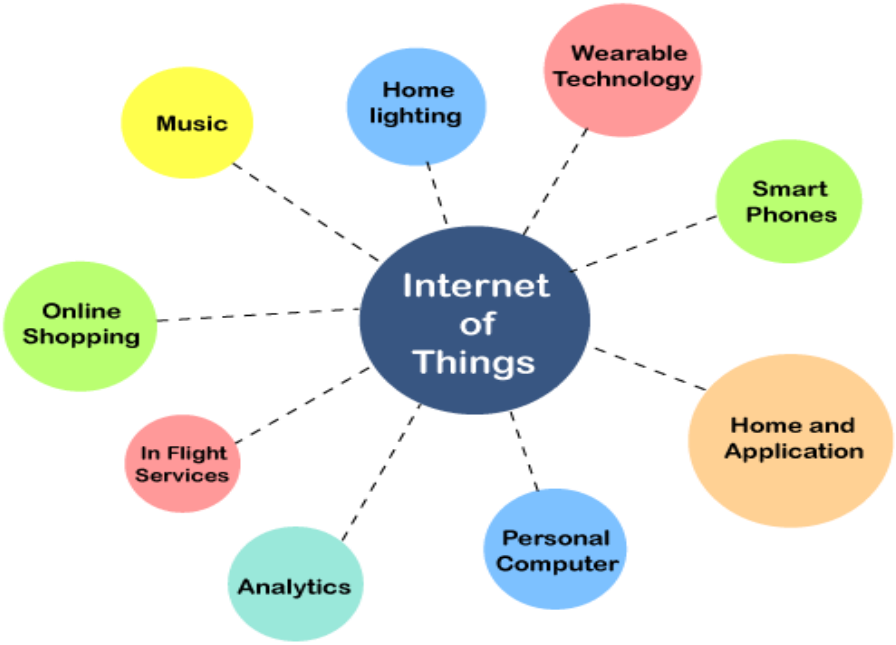
IOT devices have self configuring capability,allowing a large number of devices to work together to provide certain functionality. These devices have the ability configure themselves setup networking, and fetch latest software upgrades with minimal manual or user interaction.

iii) **Inter Operable Communication Protocols:** support a number of interoperable communication protocols and can communicate with other devices and also with infrastructure.

iv) **Unique Identity:** Each IoT device has a unique identity and a unique identifier(IP address).

v) **Integrated into Information Network:** that allow them to communicate and exchange data with other devices and systems.

Applications of IoT:



1) Home
2) Cities
3) Environment
4) Energy
5) Retail
6) Logistics
7) Agriculture
8) Industry
9) Health &LifeStyle

Physical Design of IoT :

The "Things" in IoT usually refers to IoT devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities.

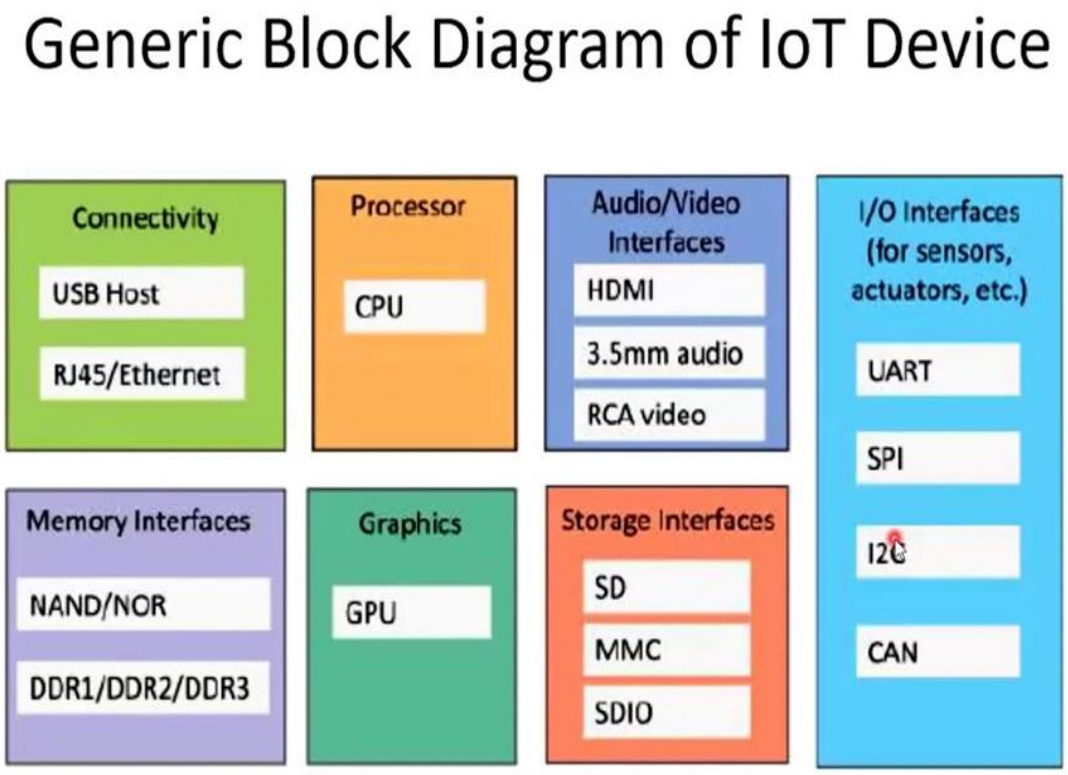
IoT devices can:

- Exchange data with other connected devices and applications (directly or indirectly), or
- Collect data from other devices and process the data locally or
- Send the data to centralized servers or cloud-based application back-ends for processing the data,
- Perform some tasks locally and other tasks within the IoT infrastructure, based on temporal and space constraints

Generic block diagram of an IoT Device

• An IoT device may consist of several interfaces for connections to other devices, both wired and wireless.
• I/O interfaces for sensors
• Interfaces for Internet connectivity

• Memory and storage interfaces
• Audio/video interfaces.



- HDMI: High definition multimedia Interface.
- 3.5mm: Audio Jack which headphone adapter.
- RCA: Radio corporation of America.
- UART: Universal Asynchronous Receiver Transmitter.
- SPI: Serial Peripheral Interface.
- I2C: Inter integrated circuit
- CAN: Controller Area Network used for Micro-controllers and devices to communicate.
- SD: Secure digital (memory card)
- MMC: multimedia card
- SDIO: Secure digital Input Output
- GPU: Graphics processing unit.
- DDR: Double data rate

IoT Protocols:

a) **Link Layer** :
Protocols determine how data is physically sent over the network‘s physical layer or medium. Local network connect to which host is attached. Hosts on the same link exchange data packets over the link layer using link layer protocols. Link layer determines how packets are coded and signalled by

the h/w device over the medium to which the host is attached.

Protocols:

- 802.3-Ethernet: IEEE802.3 is collection of wired Ethernet standards for the link layer. Eg: 802.3 uses co-axial cable; 802.3i uses copper twisted pair connection; 802.3j uses fiber optic connection; 802.3ae uses Ethernet overfiber.
- 802.11-WiFi: IEEE802.11 is a collection of wireless LAN(WLAN) communication standards including extensive description of link layer. Eg: 802.11a operates in 5GHz band, 802.11b and 802.11g operates in 2.4GHz band, 802.11n operates in 2.4/5GHz band, 802.11ac operates in 5GHz band, 802.11ad operates in 60Ghzband.
- 802.16 - WiMax: IEEE802.16 is a collection of wireless broadband standards including exclusive description of link layer. WiMax provide data rates from 1.5 Mb/s to 1Gb/s.
- 802.15.4-LR-WPAN: IEEE802.15.4 is a collection of standards for low rate wireless personal area network(LR-WPAN). Basis for high level communication protocols such as ZigBee. Provides data rate from 40kb/s to250kb/s.
- 2G/3G/4G-Mobile Communication: Data rates from 9.6kb/s(2G) to up to100Mb/s(4G). B)

b) Network/Internet Layer:

Responsible for sending IP datagrams from source n/w to destination n/w. Performs the host addressing and packet routing. Datagrams contains source and destination address.

Protocols:

- IPv4: Internet Protocol version4 is used to identify the devices on a n/w using a hierarchical addressing scheme. 32 bit address. Allows total of 2*32addresses.
- IPv6: Internet Protocol version6 uses 128 bit address scheme and allows 2*128 addresses.
- 6LOWPAN:(IPv6 over Low power Wireless Personal Area Network) operates in 2.4 GHz frequency range and data transfer 250 kb/s.

c) Transport Layer:

Provides end-to-end message transfer capability independent of the underlying n/w. Set up on connection with ACK as in TCP and without ACK as in UDP. Provides functions such as error control, segmentation, flow control and congestion control.

Protocols:

- TCP: Transmission Control Protocol used by web browsers(along with HTTP and HTTPS), email(along with SMTP, FTP). Connection oriented and stateless protocol. IP Protocol deals with sending packets, TCP ensures reliable transmission of protocols in order. Avoids n/w congestion and congestioncollapse.
- UDP: User Datagram Protocol is connectionless protocol. Useful in time sensitive applications, very small data units to exchange. Transaction oriented and stateless protocol. Does not provide guaranteed delivery.

d) Application Layer:

Defines how the applications interface with lower layer protocols to send data over the n/w. Enables process-to-process communication using ports.

Protocols:

- HTTP: Hyper Text Transfer Protocol that forms foundation of WWW. Follow requestresponse model

Stateless protocol.

- CoAP: Constrained Application Protocol for machine-to-machine(M2M) applications with constrained devices, constrained environment and constrained n/w. Uses client-server architecture.
- WebSocket: allows full duplex communication over a single socket connection.
- MQTT: Message Queue Telemetry Transport is light weight messaging protocol based on publish-subscribe model. Uses client server architecture. Well suited for constrained environment.
- XMPP: Extensible Message and Presence Protocol for real time communication and streaming XML data between network entities. Support client-server and server-server communication.
- DDS: Data Distribution Service is data centric middleware standards for device-to-device or machine-to-machine communication. Uses publish-subscribe model.
- AMQP: Advanced Message Queuing Protocol is open application layer protocol for business messaging. Supports both point-to-point and publish-subscribe model.

LOGICAL DESIGN of IoT

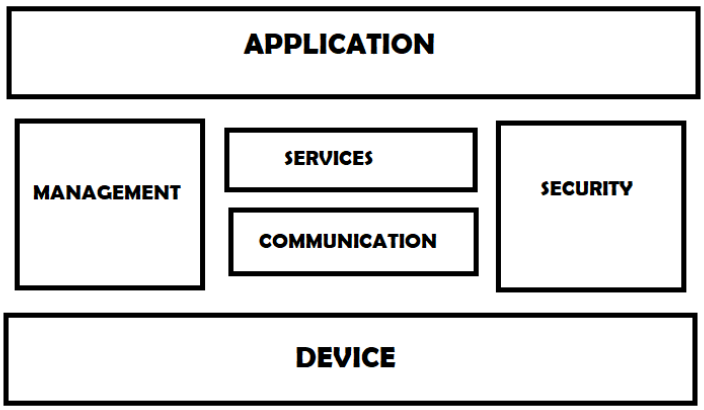
Refers to an abstract represent of entities and processes without going into the low level specifies of implementation.

1) IoT Functional Blocks
2) IoT Communication Models
3) IoT Comm. APIs

1) IoT Functional Blocks:

Provide the system the capabilities for identification, sensing, actuation, communication and management

- Device: An IoT system comprises of devices that provide sensing, actuation, monitoring and control functions.
- Communication: handles the communication for IoT system.
- Services: for device monitoring, device control services, data publishing services and services for device discovery.
- Management: Provides various functions to govern the IoT system.
- Security: Secures IoT system and priority functions such as authentication, authorization, message and context integrity and data security.
- Application: IoT application provide an interface that the users can use to control and monitor various aspects of IoT system.



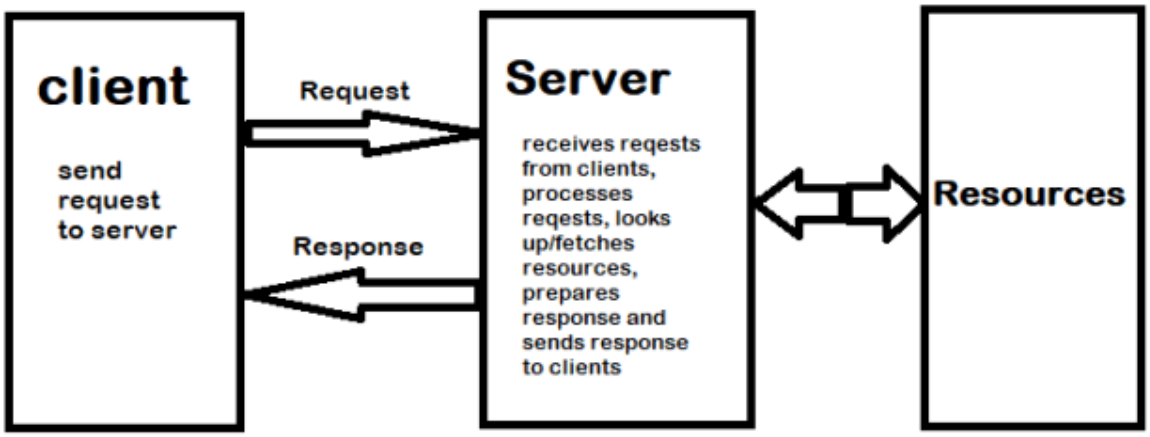
2) **IoT Communication Models:**

A) Request-Response

B) Publish-Subscribe
C)Push-Pull
D) Exclusive Pair

A) Request-Response

Request-Response is a communication model in which the client sends requests to the server and the server responds to the requests. When the server receives a request, it decides how to respond, fetches the data, retrieves resource representations, prepares the response, and then sends the response to the client.



Request-Response Communication Model

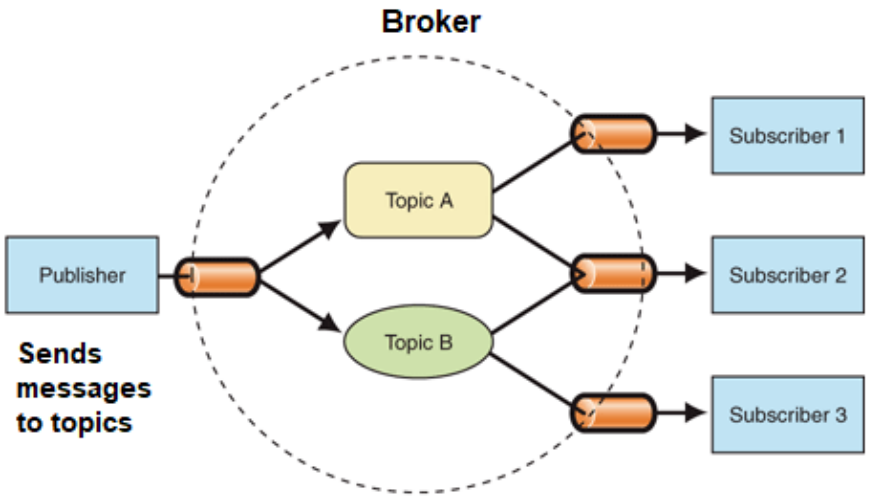
B) Publish-Subscribe communication model:

a. Publish-Subscribe is a communication model that involves publishers, brokers and consumers.

b. Publishers are the source of data. Publishers send the data to the topics which are managed by the broker. Publishers are not aware of the consumers.

c. Consumers subscribe to the topics which are managed by the broker.

d. When the broker receives data for a topic from the publisher, it sends the data to all the subscribed consumers

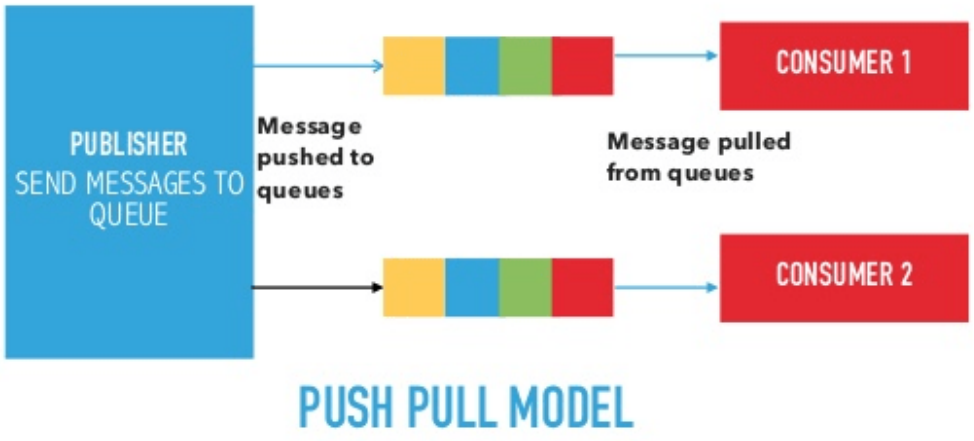


C) Push-Pull communication model:

a. Push-Pull is a communication model in which the data producers push the data to queues and the consumers pull the data from the queues. Producers do not need to be aware of the consumers.

b. Queues help in decoupling the messaging between the producers and consumers.

c. Queues also act as a buffer which helps in situations when there is a mismatch between the rate at which the producers push data and the rate at which the consumers pull.



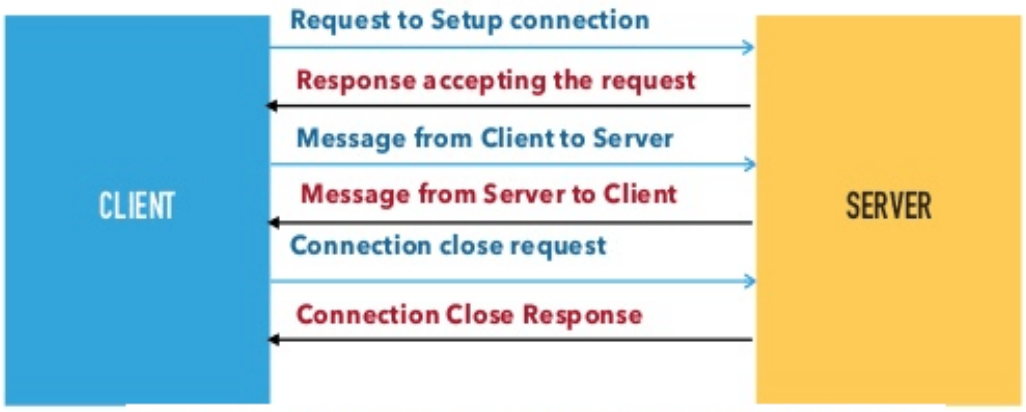
PUSH PULL MODEL

D) Exclusive Pair communication model:

a. Exclusive Pair is a bidirectional, fully duplex communication model that uses a persistent connection between the client and server.

b. Once the connection is setup it remains open until the client sends a request to close the connection.

c. Client and server can send messages to each other after connection setup.

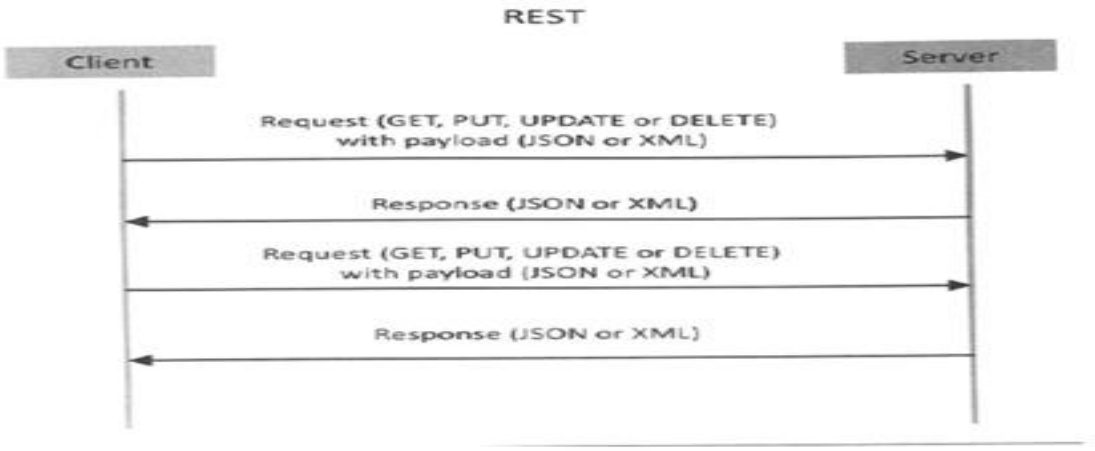


EXCLUSIVE PAIR COMMUNICATION MODEL

3)**IoT Communication APIs**: a) REST based communication APIs(Request-Response Based Model)
b) WebSocket based Communication APIs(Exclusive PairBasedModel)

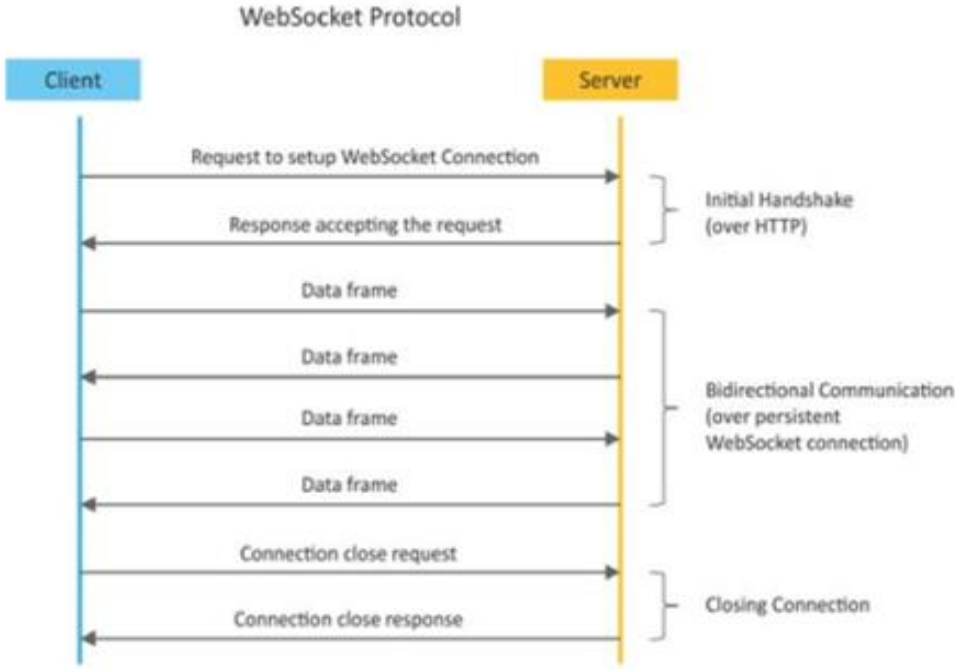
Request-Response model used by REST:

RESTful webservice is a collection of resources which are represented by URIs. RESTful web API has a base URI(e.g: http://example.com/api/tasks/). The clients and requests to these URIs using the methods defined by the HTTP protocol(e.g: GET, PUT, POST or DELETE). A RESTful web service can support various internet media types.



Request-response model used by REST

b) WebSocket Based Communication APIs: WebSocket APIs allow bi-directional, full duplex communication between clients and servers. WebSocket APIs follow the exclusive pair communication



model.

1.4 **IoT Enabling Technologies**

IoT is enabled by several technologies including Wireless Sensor Networks, Cloud Computing, Big Data

Analytics, Embedded Systems, Security Protocols and architectures, Communication Protocols, Web Services, Mobile internet and semantic search engines.

1.4.1 Wireless Sensor Networks

A wireless sensor network comprises of distributed devices with sensors which are used to monitor the environmental and physical conditions. A WSN consist of a number of end nodes and routers and a co-ordinator. The coordinator collects the data from all the nodes. Coordinator also acts as a gateway that connects the WSN to the internet.

WSNs used in IoT systems are described as follows:

- Weather Monitoring System: in which nodes collect temp, humidity and other data, which is aggregated and analyzed.
- Indoor air quality monitoring systems: to collect data on the indoor air quality and concentration of various gases.
- Soil Moisture Monitoring Systems: to monitor soil moisture at various locations.
- Surveillance Systems: use WSNs for collecting surveillance data(motion data detection).
- Smart Grids : use WSNs for monitoring grids at various points.
- Structural Health Monitoring Systems: Use WSNs to monitor the health of structures(building, bridges) by collecting vibrations from sensor nodes deployed at various points in the structure.

WSNs are enabled by wireless communication protocols such as IEEE 802.15.4. Zig Bee is one of the most popular wireless technologies used by WSNs .Zig Bee specifications are based on IEEE 802.15.4. Zig Bee operates 2.4 GHz frequency and offers data rates upto 250 KB/s and range from 10 to 100meters.

1.4.2 Cloud Computing

Cloud computing is a transformative computing paradigm that involves delivering applications and services over the internet. Cloud computing involves provisioning of computing, networking and storage resources on demand and providing these resources as metered services to the users, in a "pay as you go". Cloud computing resources can be provisioned on-demand by the users, without requiring interactions with the cloud service provider. The process of provisioning resources is automated.

Cloud computing services are offered to users in different forms.

- ***Infrastructure-as-a-service(IaaS):***Provides users the ability to provision computing and storage resources. These resources are provided to the users as a virtual machine instances and virtual storage.
- ***Platform-as-a-Service(PaaS):*** Provides users the ability to develop and deploy application in cloud using the development tools, APIs, software libraries and services provided by the cloud service provider.
- ***Software-as-a-Service(SaaS):*** Provides the user a complete software application or the user interface to the application itself. The cloud service provider manages the underlying cloud infrastructure including servers, network, operating systems, storage, and application software.

1.4.3 Big data Analysis

Big data is defined as collections of data sets whose volume , velocity or variety is so large that it is difficult to store, manage, process and analyze the data using traditional databases and data processing tools.

Some examples of big data generated by IoT are Sensor data generated by IoT systems.

- Machine sensor data collected from sensors established in industrial and energy systems.
- Health and fitness data generated IoT devices.
- Data generated by IoT systems for location and tracking vehicles.
- Data generated by retail inventory monitoring systems.

The underlying characteristics of Big Data are

Volume: There is no fixed threshold for the volume of data for big data. Big data is used for massive scale data.

Velocity: Velocity is another important characteristics of Big Data and the primary reason for exponential growth of data.

Variety: Variety refers to the form of data. Big data comes in different forms such as structured or unstructured data including test data, image , audio, video and sensor data .

1.4.4Communication Protocols:

Communication Protocols form the back-bone of IoT systems and enable network connectivity and coupling to applications.

- Allow devices to exchange data over network.
- Define the exchange formats, data encoding addressing schemes for device and routing of packets from source to destination.
- It includes sequence control, flow control and retransmission of lost packets.

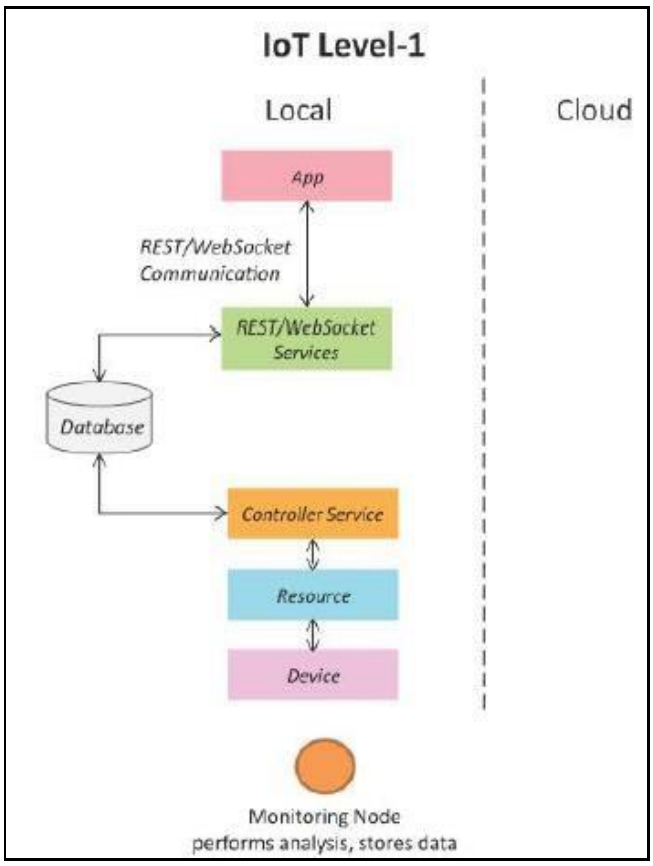
1.4.5 Embedded Systems:

Embedded Systemsis a computer system that has computer hardware and software embedded to perform specific tasks. Key components of embedded system include microprocessor or micro controller, memory (RAM, ROM, Cache), networking units (Ethernet Wi-Fi Adaptor), input/output units (Display, Keyboard, etc..,) and storage (Flash memory). Embedded System range from low cost miniaturized devices such as digital watches to devices such as digital cameras, POS terminals, vending machines, appliances etc.,

1.5 IOT Levels and Deployment Templates.

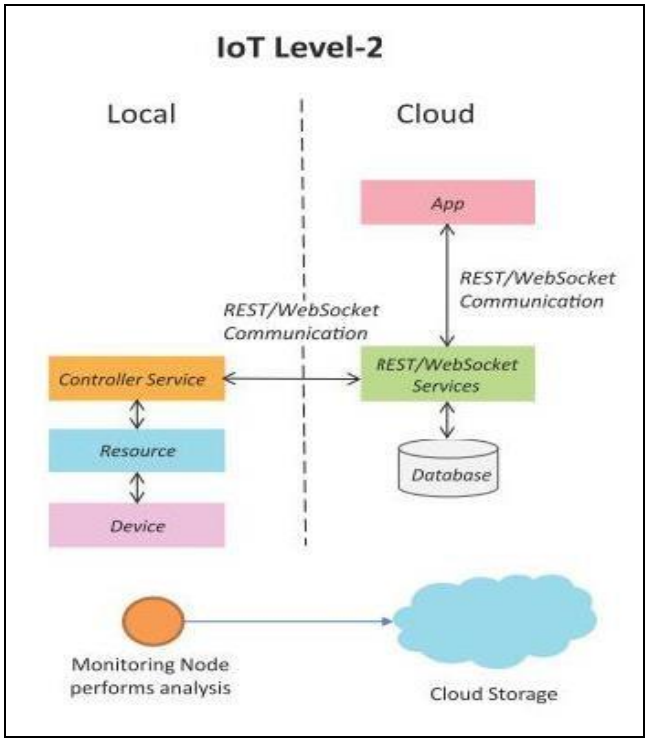
1.5.1 IoT Level-1

Level-1 IoT systems has a single node that performs sensing and/or actuation, stores data, performs analysis and host the application. Suitable for modeling low cost and low complexity solutions where the data involved is not big and analysis requirement are not computationally intensive. An e.g., of IoT Level1 isHomeautomation.The system consist of a single node that allows controlling the lights and appliances in a home the device used in this system interfaces with the lights and appliances using electronic rely switches. The status information of each light or appliances is maintained in a local database. REST services deployed locally allow retrieving and updating the state of each lighter appliance in the status database. The controller service continuously monitors the state of each light or appliance by retrieving the light from the database.



1.5.2 IoT Level 2

IoT Level2 has a single node that performs sensing and/or actuating and local analysis as shown in fig. Data is stored in cloud and application is usually cloud based. Level2 IoT systems are suitable for solutions where data are involved is big, however, the primary analysis requirement is not computationally intensive and can



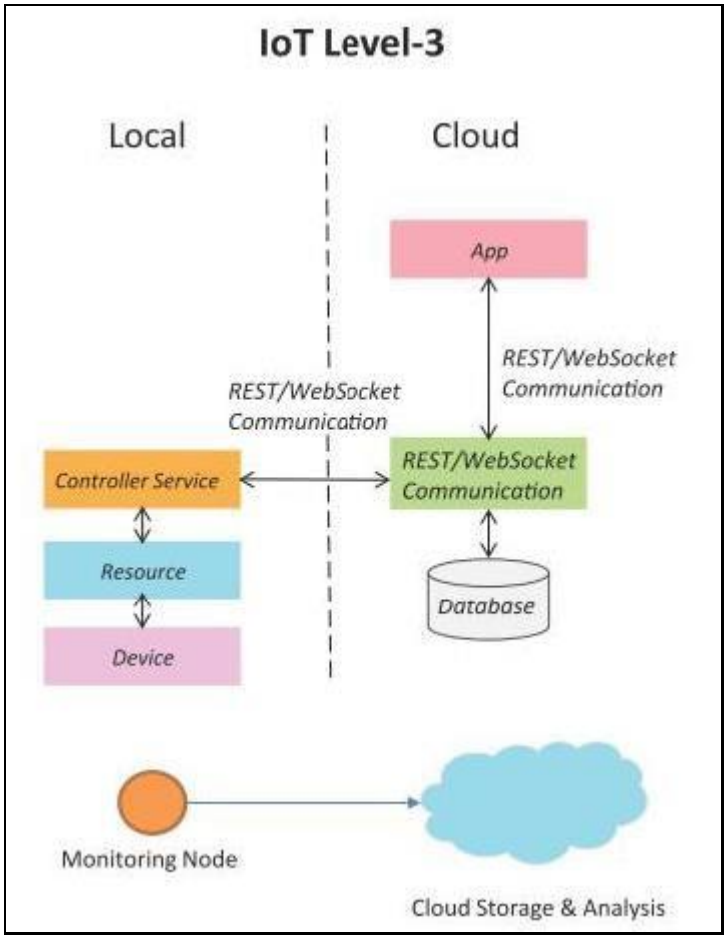
be done locally itself. An e,g., of Level2 IoT system for Smart Irrigation.

The system consists of a single node that monitors the soil moisture level and controls the irrigation system. The device used system collects soil moisture data from sensors. The controller service continuously monitors the moisture level. A cloud based REST web service is used for storing and retrieving moisture data which is stored in a cloud database. A cloud based application is used for visualizing the moisture level over a period of time which can help in making decision about irrigation schedule.

1.5.3 IoT Level 3

This System has a single node. Data is stored and analyzed in the cloud application is cloud based as shown in fig. Level3 IoT systems are suitable for solutions where the data involved is big and analysis requirements are computationally intensive.

The system consists of a single node that monitors the vibration levels for the package being shipped . The device in this system uses accelerometer and gyroscope sensor for monitoring vibration levels. The controller serves in the sensor data to the cloud in a real time using a websocket service. The data is stored in the cloud and also visualizing the cloud based applications . The analysis components in the cloud can trigger alerts if the vibration level becomes greater than the threshold.



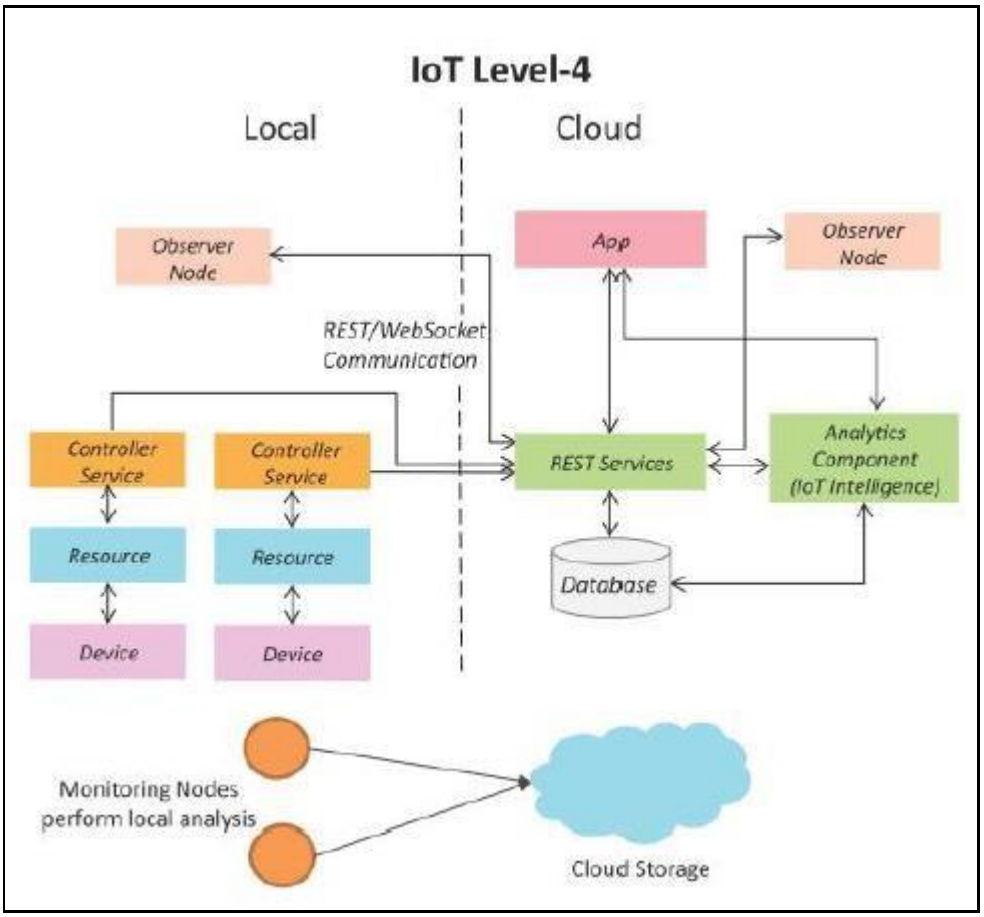
1.5.4 IoT Level 4

This System has multiple nodes that perform local analysis. Data is stored in the cloud and application is cloud based as shown in fig. Level4 contains local and cloud based observer nodes which can subscribe to and receive information collected in the cloud from IoT devices. Level 4 IoT systems are suitable for solutions where multiple nodes are required, the data involved in big and the analysis requirements are computationally intensive.

Example : IoT System for Noise Monitoring.

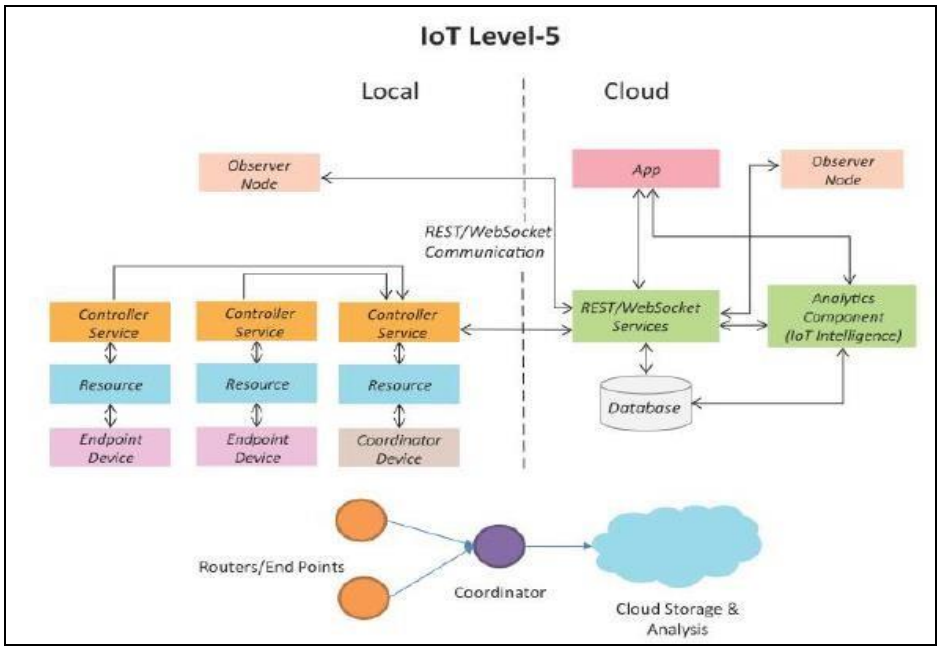
The system consists of multiple nodes placed in different locations for monitoring noise levels in an area. The nodes in this example are equipped with sound sensors. Nodes are independent of each other. Each

nodes runs its owner controller service that sends the data to the cloud . The data is stored in cloud database. The analysis of data collected from a number of nodes is done in the cloud. A cloud based application is used for visualizing the aggregated data.



1.5.5 IoT Level 5

System has multiple end nodes and one coordinator node as shown in fig. The end nodes that perform sensing and/or actuation. Coordinator node collects data from the end nodes and sends to the cloud. Data is stored and analyzed in the cloud and application is cloud based. Level5 IoT systems are suitable for solution based on wireless sensor network, in which data are high intensive.



Example :IoT system for Forest Fire Detection.

The system consists of multiple nodes placed in different locations for monitoring temperature, humidity and CO_2 levels in a forest. The end nodes in this example are equipped with various sensors such as temperature, humidity and CO_2. The coordinator node collects the data from the end nodes and act as a gateway that provides internet connectivity to the IoT system. The controller service on the coordinator device sends the collected data to the cloud. The data is stores in a cloud database. The analysis of data is done in the computing cloud to aggregate the data and make predictions. A cloud based applications is used for visualizing the data

1.5.6 IoT Level 6.

System has multiple independent end nodes that perform sensing and/or actuation and sensed data to the cloud. Data is stored in the cloud and application is cloud based as shown in fig. The analytics component analyses the data and stores the result in the cloud data base. The results are visualized with the cloud based applications. The centralized controller is aware of the status of all endnodes and sends control commands to the nodes.

Example weather monitoring system

The system consists of multiple nodes placed in different locations for monitoring temperatures,humidity and pressure in an area.the end nodes are equipped with various sensors(such as temperature,humidity and pressure).the end nodes send the data to the cloud realtime using a websocketservice.the data is stored in a cloud database. The analysis of data is done in a cloud to aggregate a data and make predictions.acloud based application is used for visualizing the data.

DOMAIN SPECIFIC IoTs

1) Home Automation:

a) **Smart Lighting:** helps in saving energy by adapting the lighting to the ambient conditions and switching on/off or diming the light when needed.

b) **Smart Appliances:** make the management easier and also provide status information to the users remotely.

c) **Intrusion Detection:** use security cameras and sensors(PIR sensors and door sensors) to detect intrusion and raise alerts. Alerts can be in the form of SMS or email sent to the user.

d) **Smoke/Gas Detectors:** Smoke detectors are installed in homes and buildings to detect smoke that is typically an early sign of fire. Alerts raised by smoke detectors can be in the form of signals to a fire alarm system. Gas detectors can detect the presence of harmful gases such as CO, LPGetc.,

2) Cities:

a) **Smart Parking:** make the search for parking space easier and convenient for drivers. Smart parking are powered by IoT systems that detect the no. of empty parking slots and send information over internet to smart application backends.

b) **Smart Lighting:** for roads, parks and buildings can help in saving energy.

c) **Smart Roads:** Equipped with sensors can provide information on driving condition, travel time estimating and alert in case of poor driving conditions, traffic condition and accidents.

d) **Structural Health Monitoring:** uses a network of sensors to monitor the vibration levels in the structures such as bridges and buildings.

e) **Surveillance:** The video feeds from surveillance cameras can be aggregated in cloud based scalable storage solution.

f) **Emergency Response:** IoT systems for fire detection, gas and water leakage detection can help in generating alerts and minimizing their effects on the critical infrastructures.

3) Environment:

a) **Weather Monitoring:** Systems collect data from a no. of sensors attached and send the data to cloud based applications and storage back ends. The data collected in cloud can then be analyzed and visualized by cloud based applications.

b) **Air Pollution Monitoring:** System can monitor emission of harmful gases(CO2, CO, NO, NO2 etc.,) by factories and automobiles using gaseous and meteorological sensors. The collected data can be analyzed to make informed decisions on pollutions control approaches.

c) **Noise Pollution Monitoring:** Due to growing urban development, noise levels in cities have increased and even become alarmingly high in some cities. IoT based noise pollution monitoring systems use a no. of noise monitoring systems that are deployed at different places in a city. The data on noise levels from the station is collected on servers or in the cloud. The collected data is then aggregated to generate noise maps.

d) **Forest Fire Detection:** Forest fire can cause damage to natural resources, property and human life. Early detection of forest fire can help in minimizing damage.

e) **River Flood Detection:** River floods can cause damage to natural and human resources and human life. Early warnings of floods can be given by monitoring the water level and flow rate. IoT based river flood monitoring system uses a no. of sensor nodes that monitor the water level and flow rate sensors.

4) Energy:

a) **Smart Grids:** is a data communication network integrated with the electrical grids that collects and analyze data captured in near-real-time about power transmission, distribution and consumption. Smart grid technology provides predictive information and recommendations to utilities, their suppliers, and their customers on how best to manage power. By using IoT based sensing and measurement technologies, the health of equipment and integrity of the grid can be evaluated.

b) **Renewable Energy Systems:** IoT based systems integrated with the transformers at the point of interconnection measure the electrical variables and how much power is fed into the grid. For wind energy systems, closed-loop controls can be used to regulate the voltage at point of interconnection which coordinate wind turbine outputs and provides power support.

c) **Prognostics:** In systems such as power grids, real-time information is collected using specialized electrical sensors called Phasor Measurment Units(PMUs) at the substations. The information received from PMUs must be monitored in real-time for estimating the state of the system and for predicting failures.

5) Retail:

a) **Inventory Management:** IoT systems enable remote monitoring of inventory using data collected by RFIDreaders.
b) **Smart Payments:** Solutions such as contact-less payments powered by technologies such as Near Field Communication(NFC) and Bluetooth.

c) **Smart Vending Machines:** Sensors in a smart vending machines monitors its operations and send the data to cloud which can be used for predictive maintenance.

6) Logistics:

a) **Route generation & scheduling:** IoT based system backed by cloud can provide first response to the route generation queries and can be scaled upto serve a large transportation network.

b) **Fleet Tracking:** Use GPS to track locations of vehicles inreal-time.

c) **Shipment Monitoring:** IoT based shipment monitoring systems use sensors such as temp, humidity, to monitor the conditions and send data to cloud, where it can be analyzed to detect foods poilage.

d) **Remote Vehicle Diagnostics:** Systems use on-board IoT devices for collecting data on Vehicle operations(speed, RPMetc.,) and status of various vehicle subsystems.

7) Agriculture:

a) **Smart Irrigation:** to determine moisture amount in the soil.

b) **Green House Control:** to improve productivity.

8) Industry:

a) Machine diagnosis and prognosis

b) Indoor Air Quality Monitoring **9) Health and Lifestyle:**

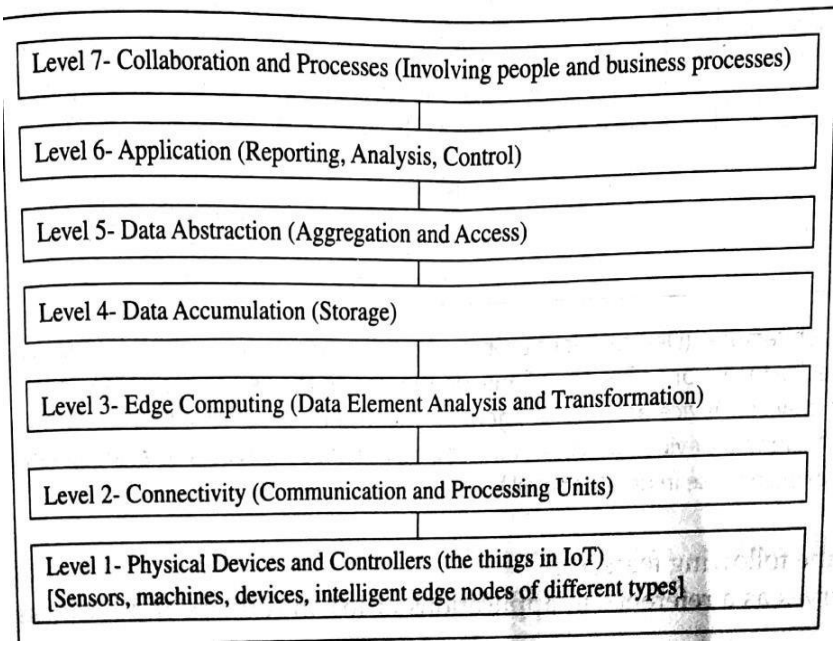
a) Health & Fitness Monitoring

b) Wearable Electronics

IoT Architectural View:

The IoT system is defined in different levels called as tiers. A model enables the conceptualisation of the framework.

A reference model can be used to depict the building blocks, successive interactions and integration.



The diagram below depicts the CISCO presentation of a reference model comprising of 7 levels and the functions of each level.

Features of the architecture:

- The architecture serves as a reference in the applications of IoT in services and business processes.
- A set of sensors which are smart, capture the data, perform necessary data element analysis and transformation as per device application framework and connect directly to a communication manager.
- The communication management subsystem consists of protocol handlers, message routers and access management.
- Data routes from gateway through the Internet and data centre to the application server or enterprise server which acquires that data.
- Organisation and analysis subsystems enable the services, business processes, enterprise integration and complex processes.

UNIT II ELEMENTS OF IOT

IoT and M2M- difference between IoT and M2M - Software Defined Networks - Network Function Virtualization - IoT systems management – Needs - NETCONF, YANG - IoT design methodology.

M2M Communication

- Machine-to-machine communication, or M2M, is exactly as it sounds: two machines "communicating," or exchanging data, without human interfacing or interaction.
- This includes serial connection, powerline connection (PLC), or wireless communications in the industrial Internet of Things (IoT).
- Switching over to wireless has made M2M communication much easier and enabled more applications to be connected. In general, when someone says M2M communication, they often are referring to cellular communication for embedded devices.
- Examples of M2M communication in this case would be vending machines sending out inventory information or ATM machines getting authorization to dispense cash. As businesses have realized the value of M2M, it has taken on a new name: The Internet of Things (IoT).
- IoT and M2M have similar promises: to fundamentally change the way the world operates. Just like IoT, M2M allows virtually any sensor to communicate, which opens up the possibility of systems monitoring themselves and automatically responding to changes in the environment, with a much reduced need for human involvement.
- M2M and IoT are almost synonymous—the exception is IoT (the newer term) typically refers to wireless communications, whereas M2M can refer to any two machines—wired or wireless—communicating with one another.

Traditionally, M2M focused on "industrial telematics," which is a fancy way of explaining data transfer for some commercial benefit. But many original uses of M2M still stand today, like smart meters. Wireless M2M has been dominated by cellular since it came out in the mid-2000's with 2G cell networks. Because of this, the cellular market has tried to brand M2M as an inherently cellular thing by offering M2M data plans. But cellular M2M is only one subsection of the market, and it shouldn't be thought of as a cellular-only area.

How M2M Works

As previously stated, machine-to-machine communication makes the Internet of Things possible. According to Forbes, M2M is among the fastest-growing types of connected device technologies in the market right now, largely because M2M technologies can connect millions of devices within a single network. The range of connected devices includes anything from vending machines to medical equipment to vehicles to buildings. Virtually anything that houses sensor or control technology can be connected to some sort of wireless network.

This sounds complex, but the driving thought behind the idea is quite simple. Essentially, M2M networks are very similar to LAN or WAN networks, but are exclusively used to allow machines, sensors, and controls, to communicate. These devices feed information they collect back to other devices in the network. This process allows a human (or an intelligent control unit) to assess what is going on across the whole network and issue appropriate instructions to member devices.

M2M Applications

The possibilities in the realm of M2M can be seen in four major use cases, which we've detailed below:

1. MANUFACTURING

Every manufacturing environment—whether it's food processing or general product manufacturing—relies on technology to ensure costs are managed properly and processes are executed efficiently. Automating manufacturing processes within such a fast-paced environment is expected to improve processes even more. In the manufacturing world, this could involve highly automated equipment maintenance and safety procedures.

For example, M2M tools allow business owners to be alerted on their smartphones when an important piece of equipment needs servicing, so they can address issues as quickly as they arise. Sophisticated networks of sensors connected to the Internet could even order replacement parts automatically.

2. HOME APPLIANCES

IoT already affects home appliance connectivity through platforms like Nest. However, M2M is expected to take home-based IoT to the next level. Manufacturers like LG and Samsung are already slowly unveiling smart home appliances to help ensure a higher quality of life for occupants.

For example, an M2M-capable washing machine could send alerts to the owners' smart devices once it finishes washing or drying, and a smart refrigerator could automatically order groceries from Amazon once its inventory is depleted. There are many more examples of home automation that can potentially improve quality of life for residents, including systems that allow members of the household to remotely control HVAC systems using their mobile devices. In situations where a homeowner decides to leave work early, he or she could contact the home heating system before leaving work to make sure the temperature at home will be comfortable upon arrival.

3. HEALTHCARE DEVICE MANAGEMENT

One of the biggest opportunities for M2M technology is in the realm of health care. With M2M technology, hospitals can automate processes to ensure the highest levels of treatment. Using devices that can react faster than a human healthcare professional in an emergency situation make this possible. For instance, when a patient's vital signs drop below normal, an M2M-connected life support device could automatically administer oxygen and additional care until a healthcare professional arrives on the scene. M2M also allows patients to be monitored in their own homes instead of in hospitals or care centers.

For example, devices that track a frail or elderly person's normal movement can detect when he or she has had a fall and alert a healthcare worker to the situation.

4. SMART UTILITY MANAGEMENT

In the new age of energy efficiency, automation will quickly become the new normal. As energy companies look for new ways to automate the metering process, M2M comes to the rescue, helping energy companies automatically gather energy consumption data, so they can accurately bill customers. Smart meters can track how much energy a household or business uses and automatically alert the energy company, which supplants sending out an employee to read the meter or requiring the customer to provide a reading. This is even more important as utilities move toward more dynamic pricing models, charging consumers more for energy usage during peak times. A few key analysts predict that soon, every object or device will need to be able to connect to the cloud. This is a bold but seemingly accurate statement. As more consumers, users, and business owners demand deeper connectivity, technology will need to be continually equipped to meet the needs and challenges of tomorrow. This will empower a wide range of highly automated processes, from equipment repairs and firmware upgrades to system diagnostics, data retrieval, and analysis. Information will be delivered to users, engineers, data scientists, and key decision-makers in real time, and it will eliminate the need for guesswork.

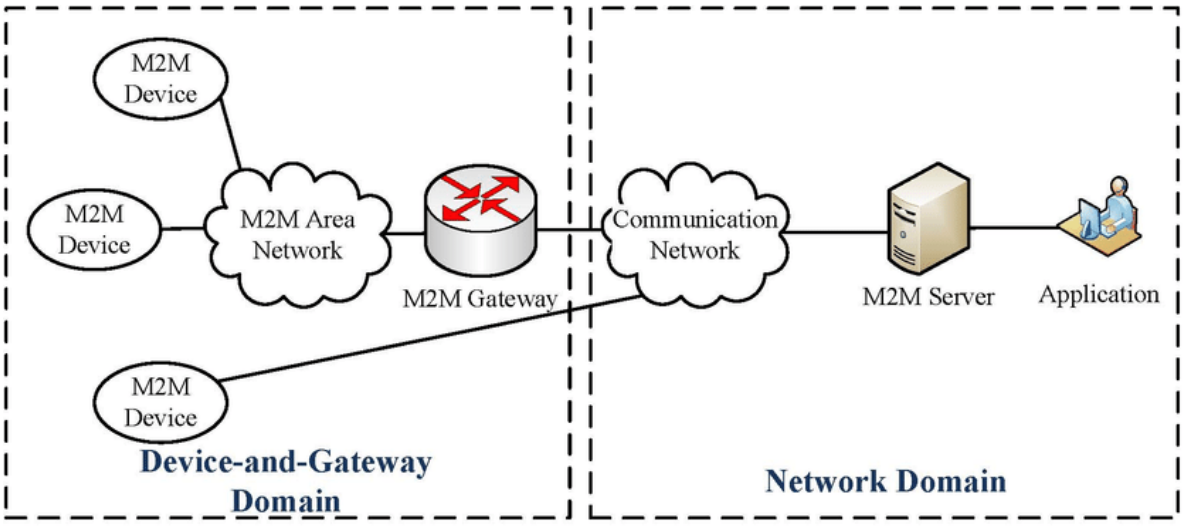
There are different M2M applications, environment monitoring, civil protection and public safety, supply chain management, energy and utility distribution as in smart grid, smart grid separately common. we have intelligent transportation systems, healthcare, automation of buildings, military applications, agriculture, home networks all these are different applications of M2M.

M2M features:

- Large number of nodes or devices
- Low cost
- Energy efficient
- Small traffic per device/machine
- M2M communication free from human intervention

General Architecture of M2M Systems:

- M2M device connects to the network domain via direct connectivity or M2M gateway. In the first case, the M2M device connects to the network domain via the access network, which performs the procedures such as registration, authentication, authorization, management, and provisioning with the network domain. In the second case, the M2M device connects to the M2M gateway using the M2M area network.
- M2M area network provides connectivity between M2M devices and M2M gateways.
- M2M gateway acts as a proxy between M2M devices and the network domain. As an example, an M2M gateway can run an application that collects and treats various information (e.g., contextual parameters) from sensors and meters.
- M2M communication network provides connection between the M2M gateways/devices and the M2M servers. Usually it contains two parts: the access network and the Internet.
- M2M server works as a middleware layer to pass data through various application services.



Difference Between IoT and M2M:

M2M, or machine-to-machine, is a direct communication between devices using wired or wireless communication channels. M2M refers to the interaction of two or more devices/machines that are connected to each other. These devices capture data and share with other connected devices, creating an intelligent network of things or systems. Devices could be sensors, actuators, embedded systems or other connected elements.

M2M technology could be present in our homes, offices, shopping malls and other places. Controlling electrical appliances like bulbs and fans using RF or Bluetooth from your smartphone is a simple example of M2M applications at home. Here, the electrical appliance and your smartphone are the two machines interacting with each other.
The Internet of Things (IoT) is the network of physical devices embedded with sensors, software and electronics, enabling these devices to communicate with each other and exchange data over a computer network. The things in the IoT refer to hardware devices uniquely identifiable through a network platform within the Internet infrastructure.

M2M versus the IoT	
M2M	**IoT**
M2M is about direct communication between machines.	The IoT is about sensors automation and Internet platform.
It supports point-to-point communication.	It supports cloud communication.
Devices do not necessarily rely on an Internet connection.	Devices rely on an Internet connection.
M2M is mostly hardware-based technology.	The IoT is both hardware- and software-based technology.
Machines normally communicate with a single machine at a time.	Many users can access at one time over the Internet.
A device can be connected through mobile or other network.	Data delivery depends on the Internet protocol (IP) network.

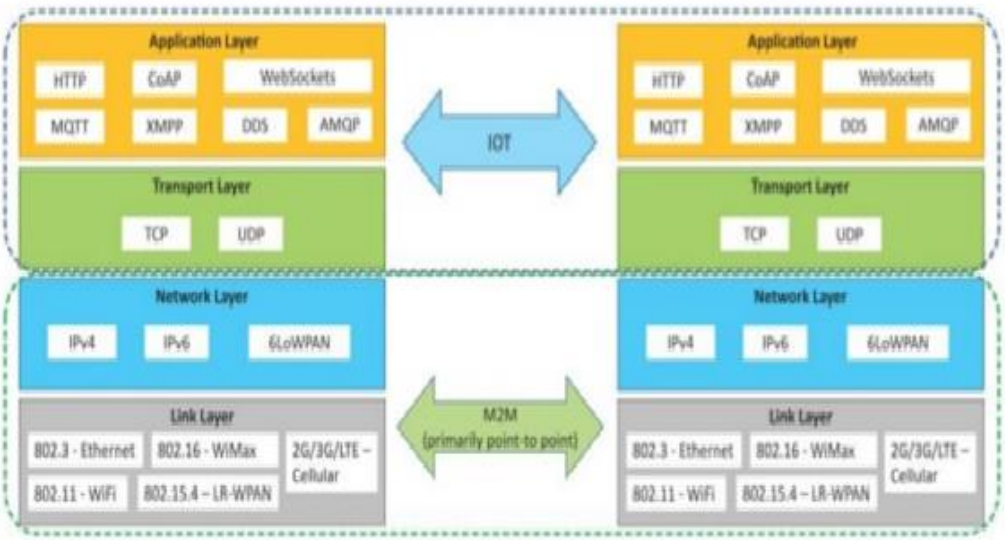
Some more differences like:

Communication Protocols:

• M2M and IoT can differ in how the communication between the machines ordevices happens.
• M2M uses either proprietary or non-IP based communication protocols for communication within the M2M area networks. IoT uses IP bases communication protococls.

Machines in M2M vs Things in IoT:

• The "Things" in IoT refers to physical objects that have unique identifiers and can sense and communicate with their external environment (and user applications) or their internal physical states.
• M2M systems, in contrast to IoT, typically have homogeneous machine types within an M2M area



network.

Hardware vs Software Emphasis:

• While the emphasis of M2M is more on hardware with embedded modules, the emphasis of IoT is more on software.

Data Collection & Analysis:

• M2M data is collected in point solutions and often in on-premises storage infrastructure.
• In contrast to M2M, the data in IoT is collected in the cloud (can be public, private or hybrid cloud).

Applications:

• M2M data is collected in point solutions and can be accessed by on premises applications such as diagnosis applications, service management applications, and on- premises enterprise applications.
• IoT data is collected in the cloud and can be accessed by cloud applications such as analytics applications, enterprise applications, remote diagnosis and management applications, etc

Software defined Networking(SDN)

SDN stands for Software Defined Network which is a networking architecture approach. It enables the control and management of the network using software applications. Through Software Defined Network (SDN) networking behavior of the entire network and its devices are programmed in a centrally controlled manner through software applications using open APIs.

To understand software-defined networks, we need to understand the various planes involved in networking.

1. Data Plane
2. Control Plane

Data plane:

All the activities involving as well as resulting from data packets sent by the end-user belong to this plane. This includes:

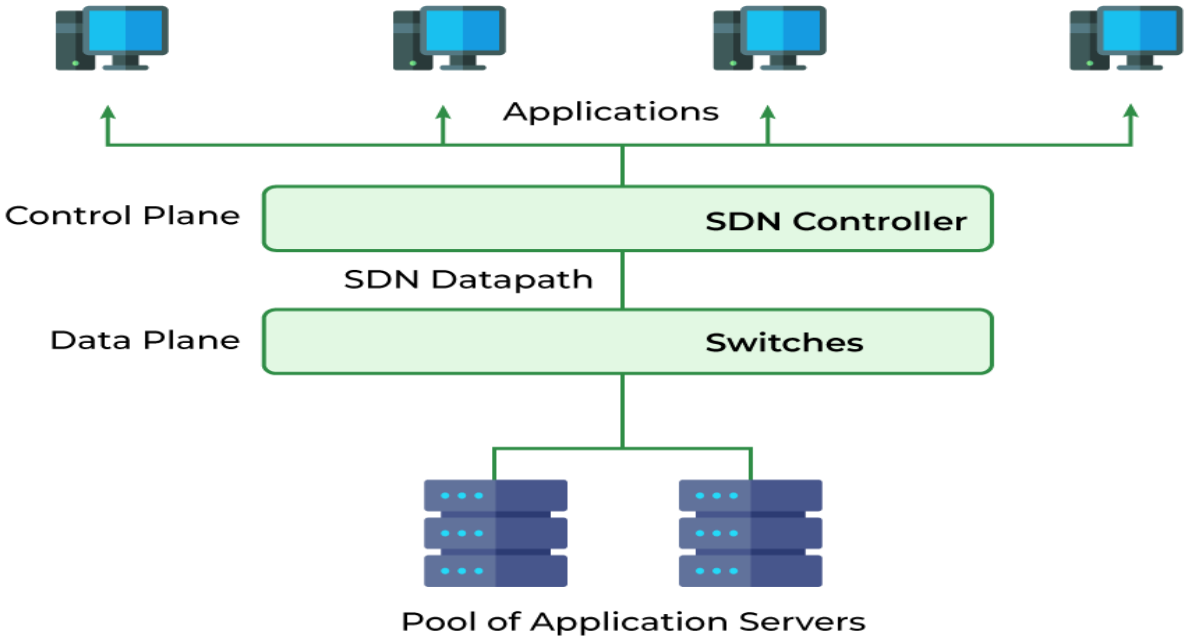
- Forwarding of packets.
- Segmentation and reassembly of data.
- Replication of packets for multicasting.

Control plane:

All activities necessary to perform data plane activities but do not involve end-user data packets belong to this plane. In other words, this is the brain of the network. The activities of the control plane include:

- Making routing tables.
- Setting packet handling policies.

Software Defined Networking (SDN)



Why SDN is Important?

- **Better Network Connectivity:** SDN provides very better network connectivity for sales, services, and internal communications. SDN also helps in faster data sharing.
- **Better Deployment of Applications:** Deployment of new applications, services, and many business models can be speed up using Software Defined Networking.
- **Better Security:** Software-defined network provides better visibility throughout the network. Operators can create separate zones for devices that require different levels of security. SDN networks give more freedom to operators.
- **Better Control with High Speed:** Software-defined networking provides better speed than other networking types by applying an open standard software-based controller.

In short, it can be said that- SDN acts as a "Bigger Umbrella or a HUB" where the rest of other networking technologies come and sit under that umbrella and get merged with another platform to bring out the best of the best outcome by decreasing the traffic rate and by increasing the efficiency of data flow.

Where is SDN Used?

- Enterprises use SDN, the most widely used method for application deployment, to deploy applications faster while lowering overall deployment and operating costs. SDN allows IT administrators to manage and provision network services from a single location.
- Cloud networking software-defined uses white-box systems. Cloud providers often use generic hardware so that the Cloud data center can be changed and the cost of CAPEX and OPEX saved.

Components of Software Defining Networking (SDN)

The three main components that make the SDN are:

1. **SDN Applications:** SDN Applications relay requests or networks through SDN Controller using API.
2. **SDN controller:** SDN Controller collects network information from hardware and sends this information to applications.
3. **SDN networking devices:** SDN Network devices help in forwarding and data processing tasks.

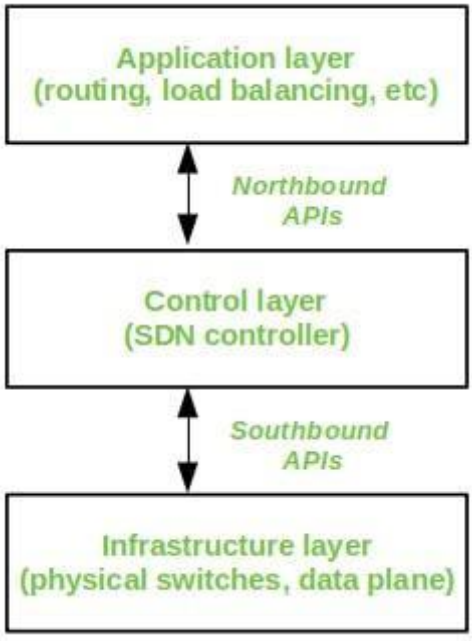
SDN Architecture

In a traditional network, each switch has its own data plane as well as the control plane. The control plane of various switches exchange topology information and hence construct a forwarding table that decides where an incoming data packet has to be forwarded via the data plane. Software-defined networking (SDN) is an approach via which we take the control plane away from the switch and assign it to a centralized unit called the SDN controller. Hence, a network administrator can shape traffic via a centralized console without having to touch the individual switches. The data plane still resides in the switch and when a packet enters a switch, its forwarding activity is decided based on the entries of flow tables, which are pre-assigned by the controller. A flow table consists of match fields (like input port number and packet header) and instructions. The packet is first matched against the match fields of the flow table entries. Then the instructions of the corresponding flow entry are executed. The instructions can be forwarding the packet via one or multiple ports, dropping the packet, or adding headers to the packet. If a packet doesn't find a corresponding match in the flow table, the switch queries the controller which sends a new flow entry to the switch. The switch forwards or drops the packet based on this flow entry.

A typical SDN architecture consists of three layers.

- **Application layer:** It contains the typical network applications like intrusion detection, firewall, and load balancing
- **Control layer:** It consists of the SDN controller which acts as the brain of the network. It also allows hardware abstraction to the applications written on top of it.
- **Infrastructure layer:** This consists of physical switches which form the data plane and carries out the actual movement of data packets.

The layers communicate via a set of interfaces called the north-bound APIs(between the application and control layer) and southbound APIs(between the control and infrastructure layer).



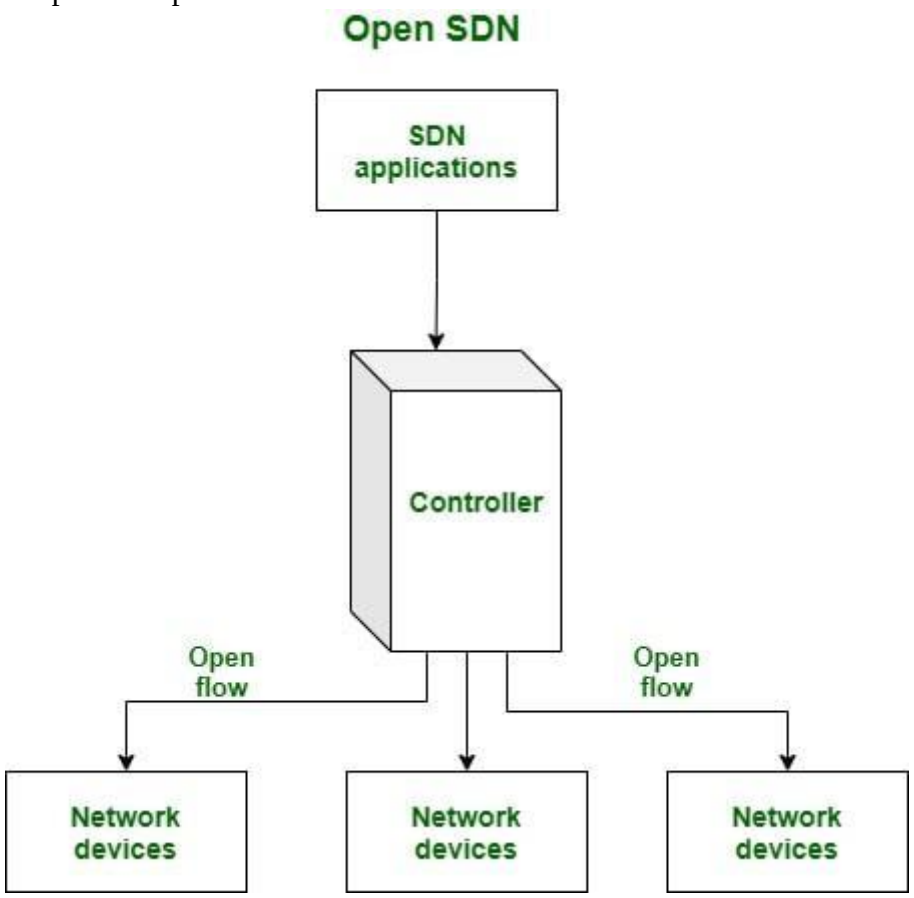
SDN Architecture

Different Models of SDN

There are several models, which are used in SDN:

1. Open SDN
2. SDN via APIs
3. SDN via Hypervisor-based Overlay Network
4. Hybrid SDN

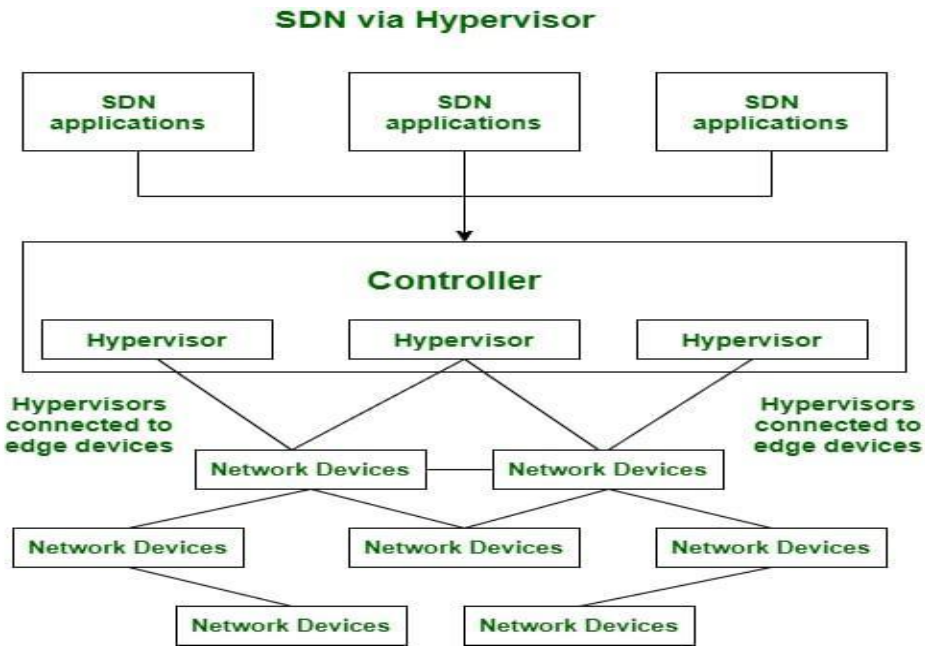
1. Open SDN: Open SDN is implemented using the OpenFlow switch. It is a straightforward implementation of SDN. In Open SDN, the controller communicates with the switches using south-bound API with the help of OpenFlow protocol.



Open SDN

2. SDN via APIs: In SDN via API, the functions in remote devices like switches are invoked using conventional methods like SNMP or CLI or through newer methods like Rest API. Here, the devices are provided with control points enabling the controller to manipulate the remote devices using APIs.

3. SDN via Hypervisor-based Overlay Network: In SDN via the hypervisor, the configuration of physical devices is unchanged. Instead, Hypervisor based overlay networks are created over the physical network. Only the devices at the edge of the physical network are connected to the virtualized networks, thereby concealing the information of other devices in the physical network.

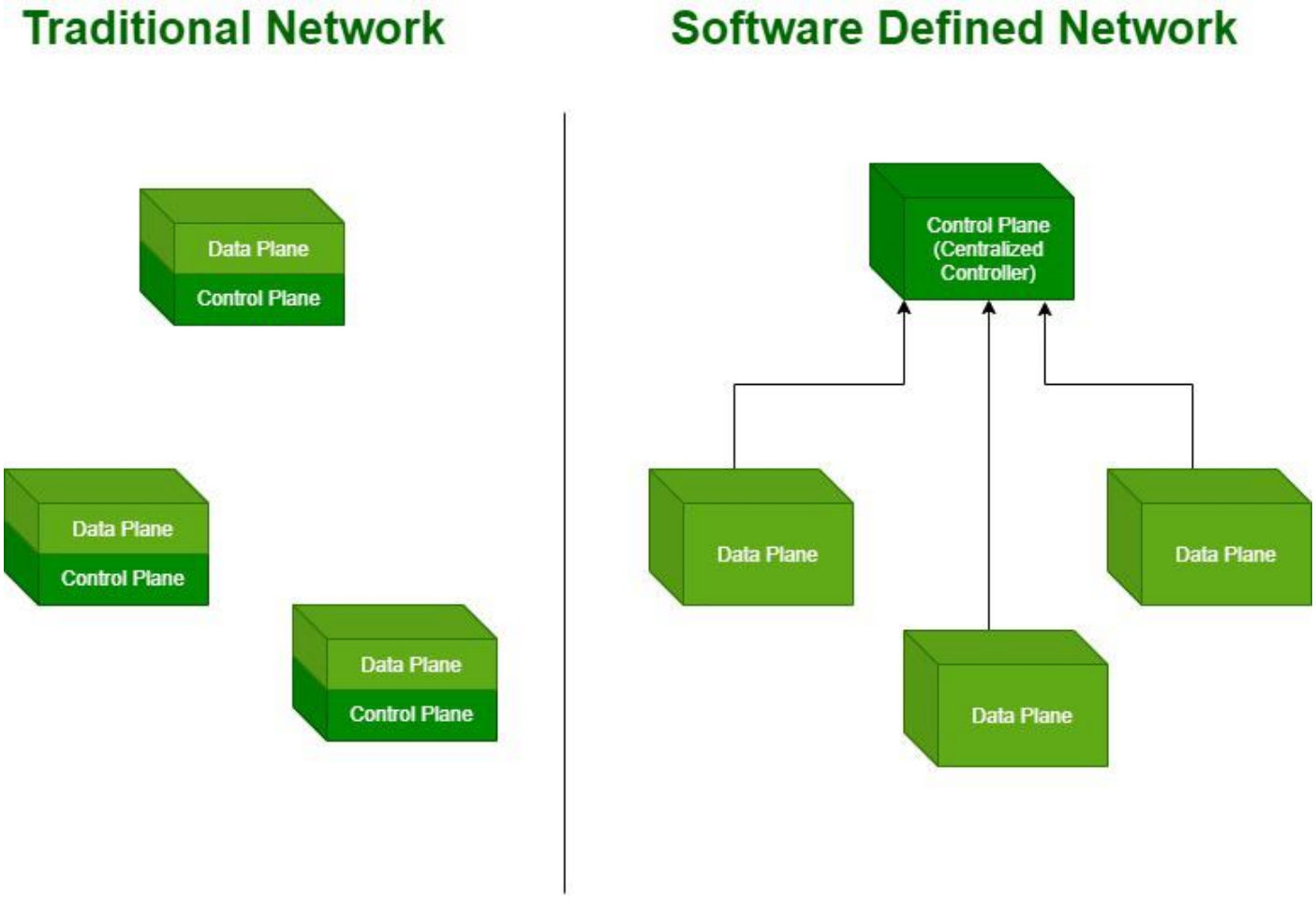


SDN via Hypervisor-based Overlay Network

4. Hybrid SDN: Hybrid Networking is a combination of Traditional Networking with software-defined networking in one network to support different types of functions on a network.
Difference between SDN and Traditional Networking

Software Defined Networking	**Traditional Networking**
Software Defined Network is a virtual networking approach.	A traditional network is the old conventional networking approach.
Software Defined Network is centralized control.	Traditional Network is distributed control.
This network is programmable.	This network is nonprogrammable.
Software Defined Network is the open interface.	A traditional network is a closed interface.
In Software Defined Network data plane and control, the plane is decoupled by software.	In a traditional network data plane and control plane are mounted on the same plane.

For more details you can refer differences between SDN and Traditional Networking article.



Difference between SDN and Traditional Networking

Advantages of SDN

- The network is programmable and hence can easily be modified via the controller rather than individual switches.
- Switch hardware becomes cheaper since each switch only needs a data plane.
- Hardware is abstracted, hence applications can be written on top of the controller independent of the switch vendor.
- Provides better security since the controller can monitor traffic and deploy security policies. For example, if the controller detects suspicious activity in network traffic, it can reroute or drop the packets.

Disadvantages of SDN

- The central dependency of the network means a single point of failure, i.e. if the controller gets corrupted, the entire network will be affected.
- The use of SDN on large scale is not properly defined and explored.

Network Functions Virtualization

The term "Network Functions Virtualization" (NFV) refers to the use of virtual machines in place of physical network appliances. There is a requirement for a hypervisor to operate networking software and procedures like load balancing and routing by virtual computers. A network functions virtualization standard was first proposed at the OpenFlow World Congress in 2012 by the European Telecommunications Standards Institute (ETSI), a group of service providers that includes AT&T, China Mobile, BT Group, Deutsche Telekom, and many more.

Need of NFV:

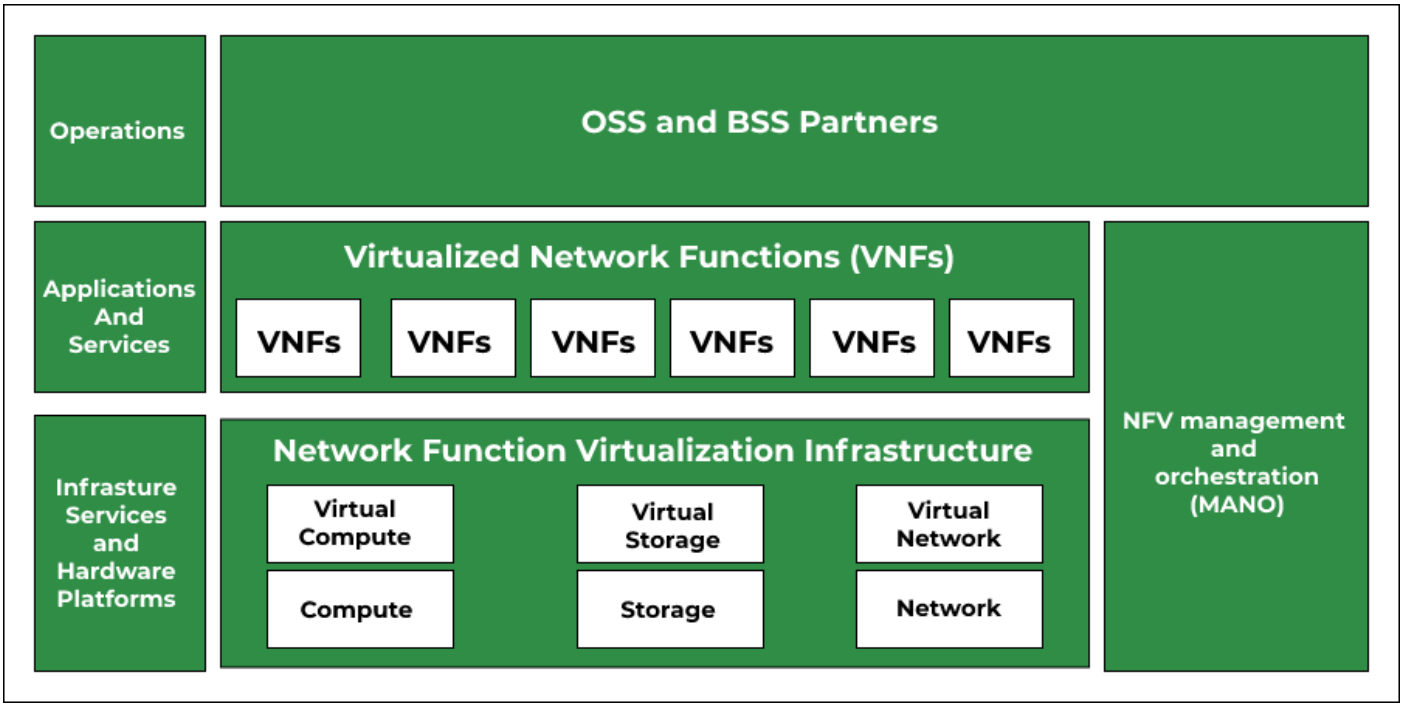
With the help of NFV, it becomes possible to separate communication services from specialized hardware like routers and firewalls. This eliminates the need for buying new hardware and network operations can offer new services on demand. With this, it is possible to deploy network components in a matter of hours as opposed to months as with conventional networking. Furthermore, the virtualized services can run on less expensive generic servers.

Advantages:

- Lower expenses as it follows Pay as you go which implies companies only pay for what they require.
- Less equipment as it works on virtual machines rather than actual machines which leads to fewer appliances, which lowers operating expenses as well.
- Scalability of network architecture is quite quick and simple using virtual functions in NFV. As a result, it does not call for the purchase of more hardware.

Working:

Usage of software by virtual machines enables to carry out the same networking tasks as conventional hardware. The software handles the task of load balancing, routing, and firewall security. Network engineers can automate the provisioning of the virtual network and program all of its various components using a hypervisor or software-defined networking controller.



Benefits of NFV:

- Many service providers believe that advantages outweigh the issues of NFV.
- Traditional hardware-based networks are time-consuming as these require network administrators to buy specialized hardware units, manually configure them, then join them to form a network. For this skilled or well-equipped worker is required.
- It costs less as it works under the management of a hypervisor, which is significantly less expensive than buying specialized hardware that serves the same purpose.
- Easy to configure and administer the network because of a virtualized network. As a result, network capabilities may be updated or added instantly.

Risks of NFV:
Security hazards do exist, though, and network functions virtualization security issues have shown to be a barrier to widespread adoption among telecom companies. The following are some dangers associated with implementing network function virtualization that service providers should take into account:

- **Physical security measures do not work:** Comparing virtualized network components to locked-down physical equipment in a data center enhances their susceptibility to new types of assaults.
- Malware is difficult to isolate and contain: Malware travels more easily among virtual components running on the same virtual computer than between hardware components that can be isolated or physically separated.
- **Network activity is less visible:** Because traditional traffic monitoring tools struggle to detect potentially malicious anomalies in network traffic going east-west between virtual machines, NFV necessitates more fine-grained security solutions.

NFV Architecture:

An individual proprietary hardware component, such as a router, switch, gateway, firewall, load balancer, or intrusion detection system, performs a specific networking function in a typical network architecture. A virtualized network substitutes software programs that operate on virtual machines for these pieces of hardware to carry out networking operations.

Three components make up an NFV architecture:

- **Centralized virtual network infrastructure:** The foundation of an NFV infrastructure can be either a platform for managing containers or a hypervisor that abstracts the resources for computation, storage, and networking.
- **Applications:** Software delivers many forms of network functionality by substituting for the hardware elements of a conventional network design (virtualized network functions).
- **Framework:** To manage the infrastructure and provide network functionality, a framework is required (commonly abbreviated as MANO, meaning Management, Automation, and Network Orchestration).

NeedforIoTSystems Management

Managingmultipledeviceswithinasinglesystem requiresadvancedmanagementcapabilitie.

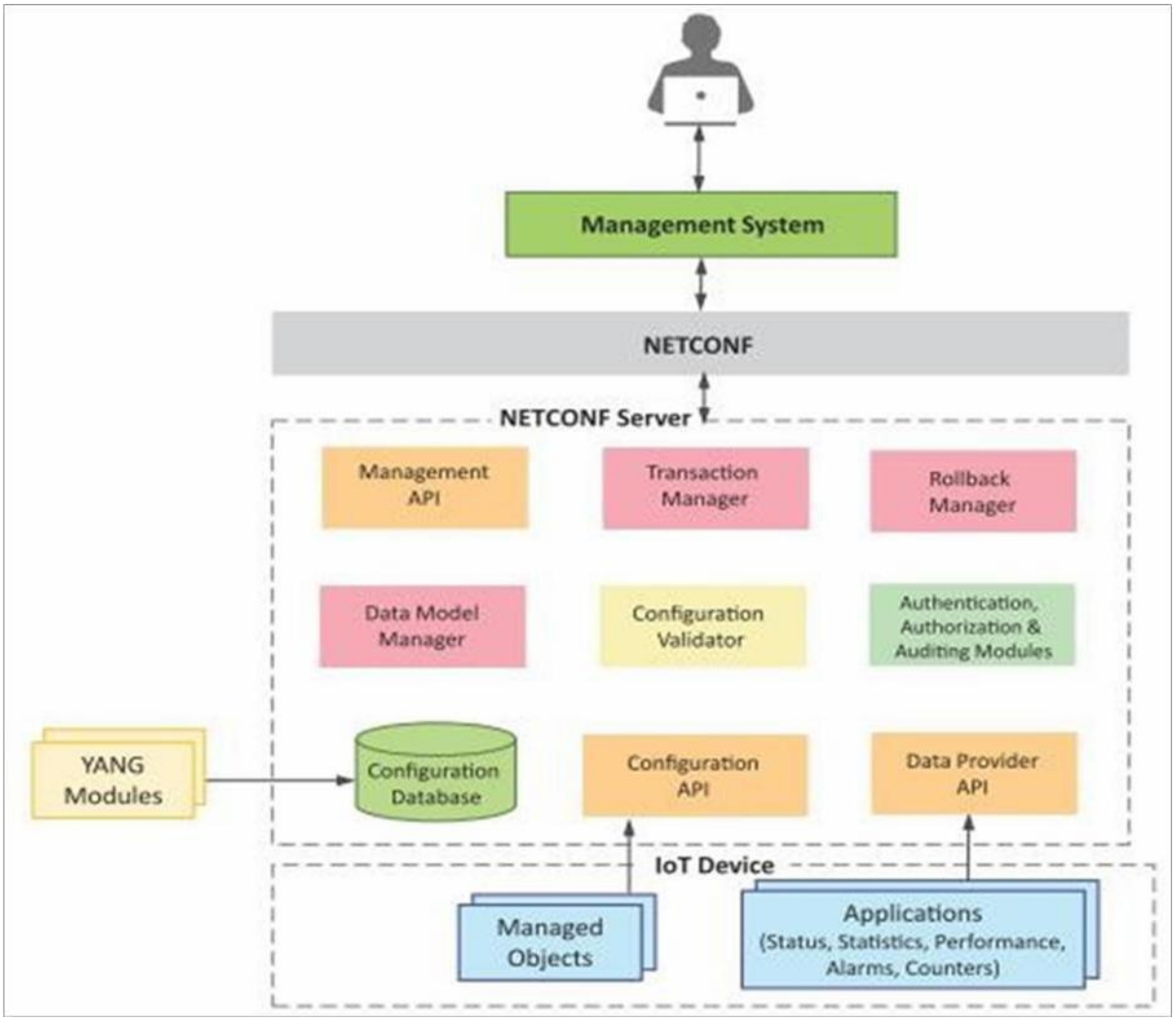
1) **AutomatingConfiguration:**IoTsystemmanagementcapabilitiescanhelpin automating the systemconfiguration.
2) **Monitoring Operational & Statistical Data :** Management systems can help in monitoring opeartional and statistical data of a system. This data can be used for fault diagnosis orprognosis.
3) **Improved Reliability:** A management system that allows validating the system configurationsbeforetheyareputinto effect canhelp inimprovingthe systemreliability.
4) **System Wide Configurations :** For IoT systems that consists of multiple devices or nodes, ensuring system wide configuration can be critical for the correct functioning of thesystem.
5) **Multiple System Configurations :** For some systems it may be desirable to have multiplevalidconfigurationswhichareappliedatdifferenttimesorin certainconditions.
6) **Retrieving&ReusingConfigurations:** Managementsystemswhichhavethecapability of retrieving configurations from devices can help in reusing the configurations for other devices of the sametype.

IoTSystemsManagementwithNETCONF-YANG

YANGisadatamodelinglanguageusedtomodelconfigurationandstatedatamanupulated by the NETCONF protocol.

ThegenericapproachofIoTdevicemanagement with NETCONF-YANG.
Rolesof various componentsare:

1) ManagementSystem
2) ManagementAPI
3) TransactionManager
4) RollbackManager
5) Data ModelManager
6) ConfigurationValidator
7) ConfigurationDatabase
8) ConfigurationAPI
9) Data ProviderAPI



1) **Management System :** The operator uses a management system to send NETCONF messages to configure the IoT device and receives state information and notifications from the device as NETCONFmessages.

2) **ManagementAPI :**allowsmanagementapplicationtostartNETCONFsessions.

3) **Transaction Manager:** executes all the NETCONF transactions and ensures that ACID properties hold true for thetrasactions.

4) **Rollback Manager :** is responsible for generating all the transactions necessary to rollback a current configuration to its original state.

5) **DataModelManager:** KeepstrackofalltheYANGdatamodelsandthecorresponding managed objects. Also keeps track oftheapplications which providedataforeach partof a datamodel.

6) **Configuration Validator :** checks if the resulting configuration after applying a transaction would be a validconfiguration.

7) **ConfigurationDatabase:**containsbothconfigurationandoperastionaldata.

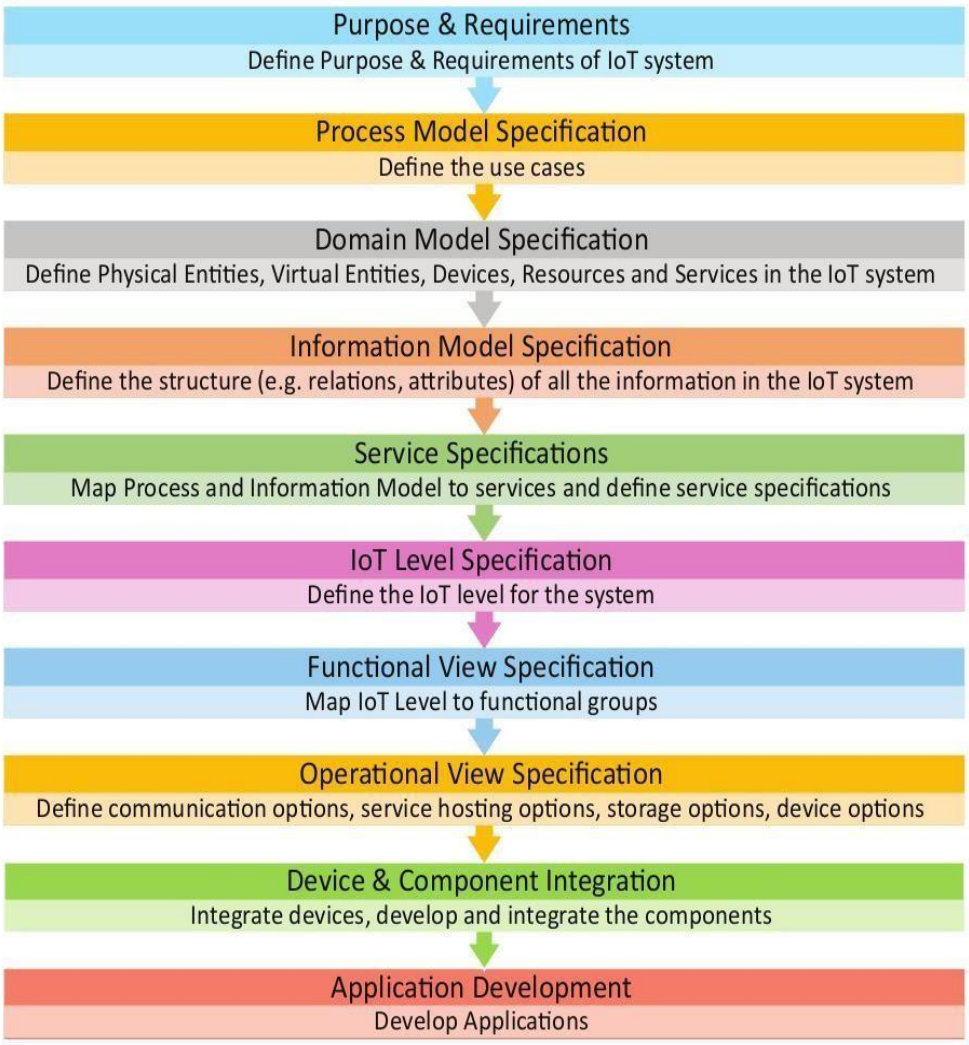
8) **Configuration API :** Using the configuration API the application on the IoT device can be read configuration data from the configuration datastore and write opeartional data to the opearationaldatastore.

9) **DataProviderAPI:** Applicationsonthe IoTdevicecanregisterforcallbacksforvarious events using the Data Provider API. Through the Data Provider API, the applications can report statistics and opeartionaldata.

StepsforIoTdeviceManagementwithNETCONF-YANG

1) Create a YANG model of the system that defines the configuration and state data of the system.
2) CompletetheYANGmodelwiththe_Inctool'whichcomeswithLibnetconf.
3) Fillinthe IoTdevicemangementcodeintheTransAPImodule.
4) BuildthecallbacksC filetogeneratethelibraryfile.
5) Load the YANG module and the TransAPImodule into the Netopeer server using Netopeermanagertool.
6) The operator can now connect from the management system to the Netopeer server using the NetopeerCLI.
7) Operator can issue NETCONF commands from the Netopeer CLI. Command can be issued to changew the configuration dsta, get operational dat or execute an RPC on the IoTdevice.

IoT Design Methodology – Steps



Step 1: Purpose & Requirements Specification:

The first step in IoT system design methodology is to define the purpose and requirements of the system. In this step, the system purpose, behavior and requirements (such as data collection requirements, data analysis requirements, system management requirements, data privacy and security requirements, user interface requirements, ...) are captured.

Step 2: Process Specification:

The second step in the IoT design methodology is to define the process specification. In this step, the use cases of the IoT system are formally described based on and derived from the purpose and requirement specifications.

Step 3: Domain Model Specification:

The third step in the IoT design methodology is to define the Domain Model. The domain model describes the main concepts, entities and objects in the domain of IoT system to be designed. Domain model defines the attributes of the objects and relationships between objects. Domain model provides an abstract representation of the concepts, objects and entities in the IoT domain, independent of any specific technology or platform. With the domain model, the IoT system designers can get an understanding of the IoT domain for which the system is to be designed.

Step 4: Information Model Specification:

The fourth step in the IoT design methodology is to define the Information Model. Information Model defines the structure of all the information in the IoT system, for example, attributes of Virtual Entities, relations, etc. Information model does not describe the specifics of how the information is represented or stored. To define the information model, we first list the Virtual Entities defined in the Domain Model. Information model adds more details to the Virtual Entities by defining their attributes and relations.

Step 5: Service Specifications:

The fifth step in the IoT design methodology is to define the service specifications. Service specifications define the services in the IoT system, service types, service inputs/output, service endpoints, service schedules, service preconditions and service effects.

Step 6: IoT Level Specification:

The sixth step in the IoT design methodology is to define the IoT level for the system.

Step 7: Functional View Specification:

The seventh step in the IoT design methodology is to define the Functional View. The Functional View (FV) defines the functions of the IoT systems grouped into various Functional Groups (FGs). Each Functional Group either provides functionalities for interacting with instances of concepts defined in the Domain Model or provides information related to these concepts.

Step 8: Operational View Specification:

The eighth step in the IoT design methodology is to define the Operational View Specifications. In this step, various options pertaining to the IoT system deployment and operation are defined, such as, service hosting options, storage options, device options, application hosting options, etc

Step 9: Device & Component Integration:

The ninth step in the IoT design methodology is the integration of the devices and components.

Step 10: Application Development:

The final step in the IoT design methodology is to develop the IoT application.

UNIT III IOT PROTOCOLS

Sensors and actuators - Communication modules – Zigbee - LoRa - RFID - Wi-Fi - Power sources.

Sensors:

- Generally speaking, a sensor is a device that is able to detect changes in an environment. By itself, a sensor is useless, but when we use it in an electronic system, it plays a key role. A sensor is able to measure a physical phenomenon (like temperature, pressure, and so on) and transform it into an electric signal. These three features should be at the base of a good sensor:
- It should be sensitive to the phenomenon that it measures
- It should not be sensitive to other physical phenomena
- It should not modify the measured phenomenon during the measurement process
- There is a wide range of sensors we can exploit to measure almost all the physical properties around us. A few common sensors that are widely adopted in everyday life include thermometers, pressure sensors, light sensors, accelerometers, gyroscopes, motion sensors, gas sensors and many more.

A sensor can be described using several properties, the most important being:

- **Range**: The maximum and minimum values of the phenomenon that the sensor can measure.
- **Sensitivity**: The minimum change of the measured parameter that causes a detectable change in output signal.
- **Resolution**: The minimum change in the phenomenon that the sensor can detect.

Sensor Classification:

Sensors can be grouped using several criteria:

Passive or Active: Passive sensors do not require an external power source to monitor an environment, while Active sensors require such a source in order to work. A passive sensor is one which just 'listens' to what is happening.

Examples include:

- A light sensor which detects if a light is shining on it.
- An infra-red sensor which detects the temperature of an object.

An active sensor is one which transmits a signal into the environment and then measures the response that comes back.
One example is an ultrasonic system:

- A pulse of ultrasound is emitted.
- If an object is in the way, the pulse is reflected back.
- The sensor detects it.
- The time taken between emission and detection gives an indication of the distance of the object.

Another classification is based on the method used to detect and measure the property (mechanical, chemical, etc.).

Analog and Digital: Analog sensors produce an analog, or continuous, signal while digital sensors produce a discrete signal.

There are different types of sensors that produce continuous analog output signal and these sensors are analog sensors. This continuous output signal produced by the analog sensors is proportional to the measurand. Generally, There are various types of analog sensors; practical examples of various types of analog sensors are as follows: accelerometers, pressure sensors, light sensors, sound sensors, temperature sensors, and so on.

Unlike analog sensor, Digital Sensor produce discrete values (0 and 1's). Discrete values often called digital or binary signals in digital communication.

Electronic sensors or electrochemical sensors in which data conversion and data transmission take place digitally are digital sensors. These digital sensors are replacing analog sensors as they are capable of overcoming the drawbacks of analog sensors. The digital sensor consists of majorly three components such as senor, cable, and transmitter. But, In digital sensors, the signal measured directly converted into digital signal output inside the digital sensor itself. So, this digital signal transmitted through cable digitally. There are different types of digital sensors that overcome the disadvantages of analog sensors.

Then, scaler sensors basically measure scalar variables which can measure only the changes in the magnitude whereas, the vector senses not only the magnitude, but also the direction. So, scalar sensor example would be temperature sensor is an example of scalar sensor because you know irrespective of which orientation you put, the sensor temperature sensor or in which direction you are taking it, it is going to give you the magnitude value. Only the changes in the magnitude of the temperature, on the contrary we have the vector sensor. For example, the camera sensor or the accelerometer sensor whose values are dependent on the orientation on the direction and so on direction in which the sensor is being put and the weight is measuring. Scalar sensors measure only the magnitude physical quantities, such as temperature colour, pressure, strain etcetera. These are scalar quantities and measurement of the change of magnitude is sufficient to convey the information.

On the other hand, vector sensors produce output signal of the voltage which is generally proportional to the magnitude as well as the direction and orientation of the quantity that is being measured. So, physical quantities such as the sound, image, velocity, acceleration orientation, these are all vector quantities and their measurement is not just dependent on the magnitude, but also on the direction. So, for example, accelerometer sensor, they give outputs in three dimensions x, y and z coordinate axis.

Some of the types of sensors:

1)Temperature Sensors

- Temperature sensors measure the amount of heat energy in a source, allowing them to detect temperature changes and convert these changes to data. Machinery used in manufacturing often requires environmental and device temperatures to be at specific levels. Similarly, within agriculture, soil temperature is a key factor for crop growth.

2) Humidity Sensors

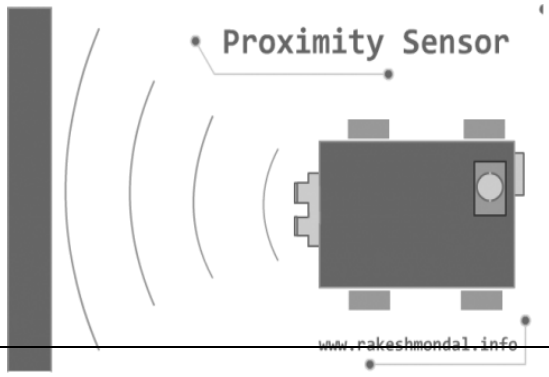
- These types of sensors measure the amount of water vapor in the atmosphere of air or other gases. Humidity sensors are commonly found in heating, vents and air conditioning (HVAC) systems in both industrial and residential domains. They can be found in many other areas including hospitals, and meteorology stations to report and predict weather.

3). Pressure Sensors

- A pressure sensor senses changes in gases and liquids. When the pressure changes, the sensor detects these changes, and communicates them to connected systems. Common use cases include leak testing which can be a result of decay. Pressure sensors are also useful in the manufacturing of water systems as it is easy to detect fluctuations or drops in pressure.

5. Proximity Sensors

- Proximity sensors are used for non-contact detection of objects near the sensor. These types of sensors often emit electromagnetic fields or beams of radiation such as infrared. Proximity sensors have some interesting use cases. In retail, a proximity sensor can detect the motion between a customer and a product in which he or she is interested. The user can be notified of any discounts or special offers of products located near the sensor. Proximity sensors are also used in the parking lots of malls, stadiums and airports to indicate parking availability. They can also be used on the assembly lines of chemical, food and many other types of industries.

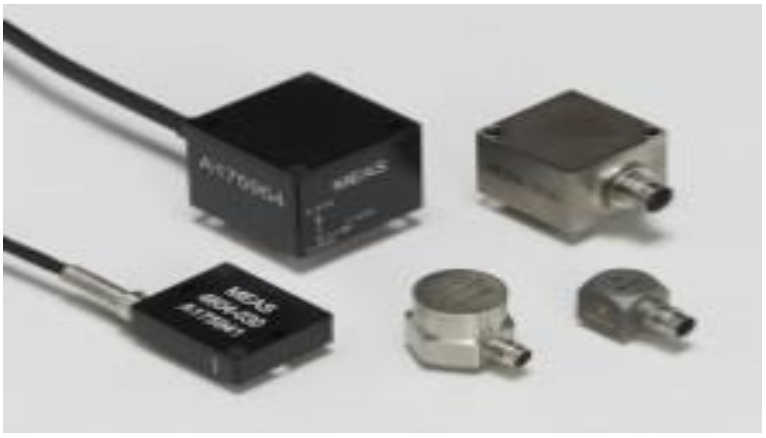


6. Level Sensors

- Level sensors are used to detect the level of substances including liquids, powders and granular materials. Many industries including oil manufacturing, water treatment and beverage and food manufacturing factories use level sensors. Waste management systems provide a common use case as level sensors can detect the level of waste in a garbage can or dumpster.

7. Accelerometers

- Accelerometers detect an object's acceleration i.e. the rate of change of the object's velocity with respect to time. Accelerometers can also detect changes to gravity. Use cases for accelerometers include smart pedometers and monitoring driving fleets. They can also be used as anti-theft protection alerting the system if an object that should be stationary is moved.



8. Gyroscope

- Gyroscope sensors measure the angular rate or velocity, often defined as a measurement of speed and rotation around an axis. Use cases include automotive, such as car navigation and electronic stability control (anti-skid) systems. Additional use cases include motion sensing for video games, and camera-shake detection systems.

9. Gas Sensors

- These types of sensors monitor and detect changes in air quality, including the presence of toxic, combustible or hazardous gasses. Industries using gas sensors include mining, oil and gas, chemical research and manufacturing. A common consumer use case is the familiar carbon dioxide detectors used in many homes**.**

10. Infrared Sensors

- These types of sensors sense characteristics in their surroundings by either emitting or detecting infrared radiation. They can also measure the heat emitted by objects. Infrared sensors are used in a variety of different IoT projects including healthcare as they simplify the monitoring of blood flow and blood pressure.
- Televisions use infrared sensors to interpret the signals sent from a remote control. Another interesting application is that of art historians using infrared sensors to see hidden layers in paintings to help determine whether a work of art is original or fake or has been altered by a restoration process.

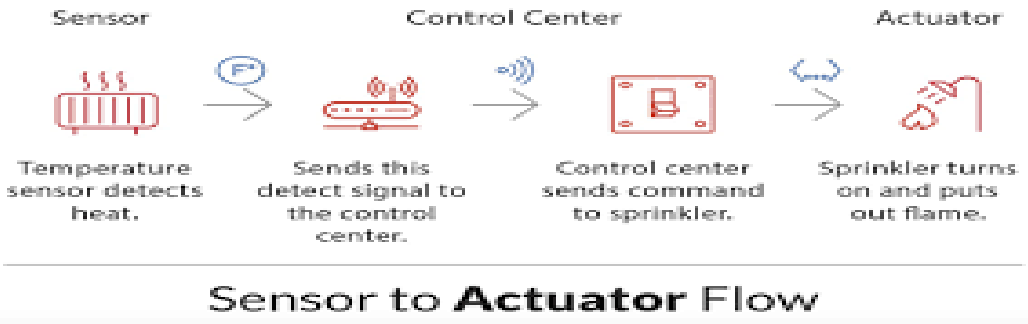
11. Optical Sensors

Optical sensors convert rays of light into electrical signals. There are many applications and use cases for optical sensors. In the auto industry, vehicles use optical sensors to recognize signs, obstacles, and other

things that a driver would notice when driving or parking. Optical sensors play a big role in the development of driverless cars. Optical sensors are very common in smart phones. For example, ambient light sensors can extend battery life. Optical sensors are also used in the biomedical field including breath analysis and heart-rate monitors**.**

Actuators:

- An IoT device is made up of a Physical object ("thing") + Controller ("brain") + Sensors + Actuators + Networks (Internet). An actuator is a machine component or system that moves or controls the mechanism or the system. Sensors in the device sense the environment, then control signals are generated for the actuators according to the actions needed to perform.
- A servo motor is an example of an actuator. They are linear or rotatory actuators, can move to a given specified angular or linear position. We can use servo motors for IoT applications and make the motor rotate to 90 degrees, 180 degrees, etc., as per our need.
- The following diagram shows what actuators do; the controller directs the actuator based on the sensor data to do the work.



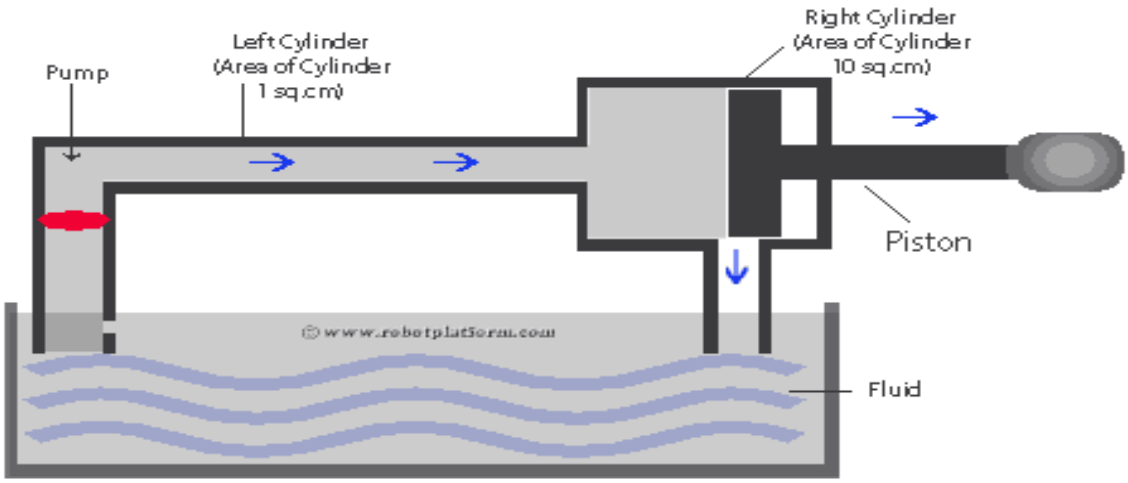
Sensor to **Actuator** Flow

- The control system acts upon an environment through the actuator. It requires a source of energy and a control signal. When it receives a control signal, it converts the source of energy to a mechanical operation. On this basis, on which form of energy it uses, it has different types given below.

Types of Actuators:

Hydraulic Actuators –

A hydraulic actuator uses hydraulic power to perform a mechanical operation. They are actuated by a cylinder or fluid motor. The mechanical motion is converted to rotary, linear, or oscillatory motion, according to the need of the IoT device. Example- construction equipment uses hydraulic actuators because hydraulic actuators can generate a large amount of force. So, this name suggests, these hydraulic actuators consist of a cylinder or fluid motor that uses hydraulic power to facilitate mechanical operation. The mechanical motion is converted to linear rotary or oscillatory motion. Basically when some fluid passes through, then you know that motion is converted to some linear motion or some oscillatory motion or rotary motion and since liquids are nearly impossible to compress, most of the hydraulic actuators basically exert considerable force which is the reason why liquid based actuators are typically used and these are quite popular because of this particular reason.

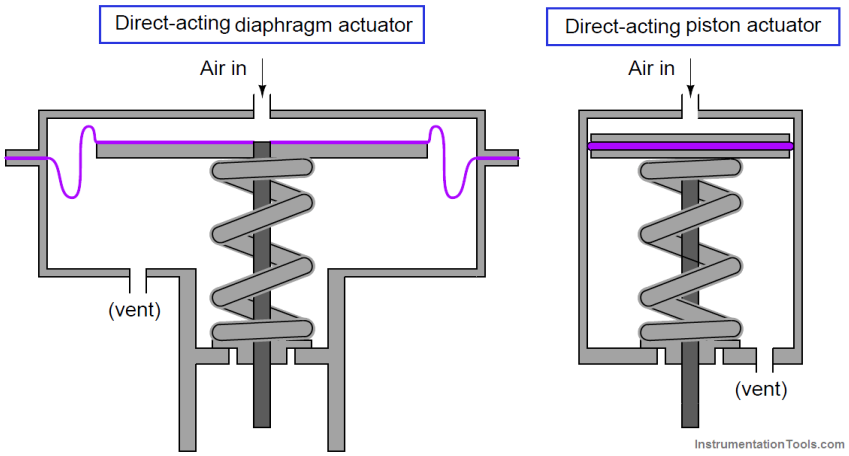


Hydraulic Actuator

Pneumatic Actuators –

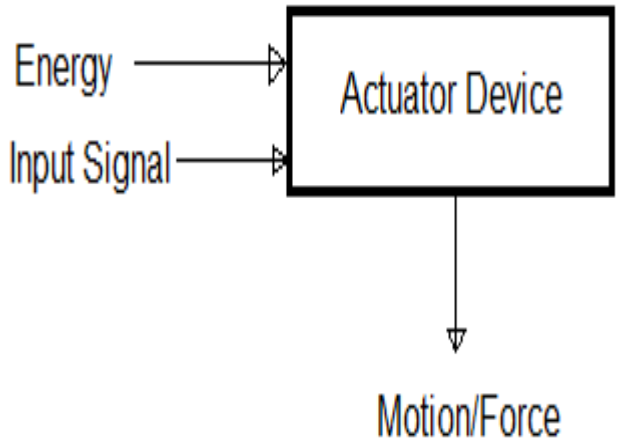
A pneumatic actuator uses energy formed by vacuum or compressed air at high pressure to convert into either linear or rotary motion. Example- Used in robotics, use sensors that work like human fingers by using compressed air. Pneumatic actuator, pneumatic means air based. A pneumatic actuator basically converts the energy formed by vacuum or compressed air at high pressure into either linear or rotatory motion. Pneumatic actuators basically exert a lot of force and for example, the pneumatic brakes can be very responsive to small changes in pressure that are applied by the driver.

Pneumatic brakes are quite common in different devices like trucks etc. They use pneumatic brakes. So, hydraulic brakes are more common in cars, in trucks pneumatic brakes are quite common. The advantage of pneumatic brakes, is that they are very responsive to small changes.



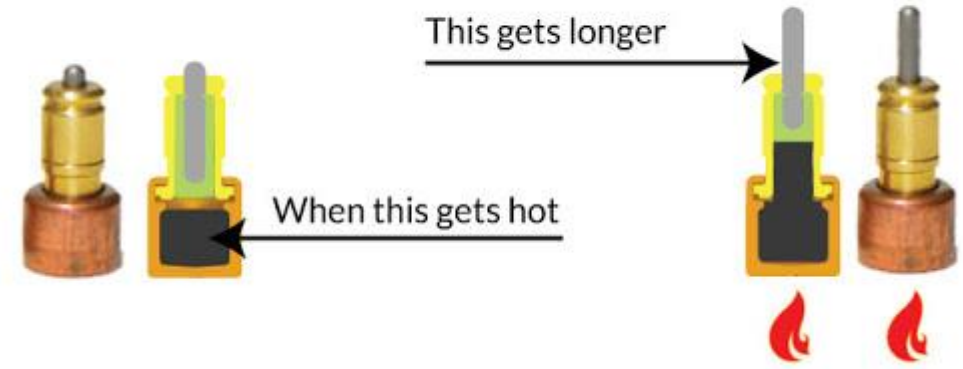
Electrical Actuators –

An electric actuator uses electrical energy, is usually actuated by a motor that converts electrical energy into mechanical torque. An example of an electric actuator is a solenoid based electric bell. An electric actuator is generally powered by a motor that converts electrical energy into mechanical torque. So, this electrical energy is used to actuate the equipment, such as the solenoid valve which control the flow of water in pipes in response to electrical signals.



Thermal /Magnetic Actuators –

- Actuators are simply devices used to transform energy into motion. A thermal actuator is a type of non-electric motor made of components such as a piston and a thermal sensitive material capable of producing linear motion in response to temperature changes.



- Magnetic Actuators: Magnetic Actuators use magnetic effects to generate forces which impact on the motion of a part in the actuator.

Mechanical Actuators –

- A mechanical actuator executes movement by converting rotary motion into linear motion. It involves pulleys, chains, gears, rails, and other devices to operate.

Communication modules:

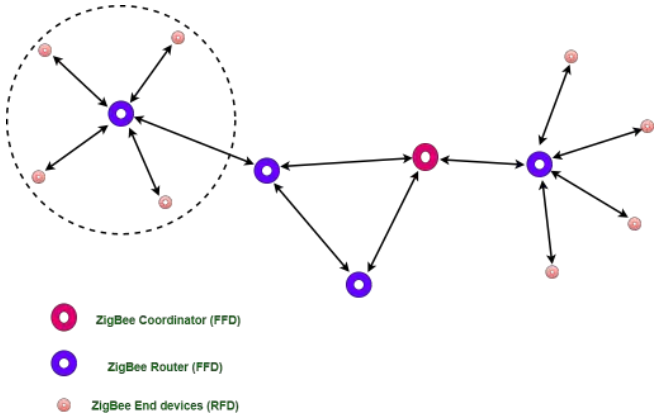
Zigbee Architecture

ZigBee is a Personal Area Network task group with low rate task group 4. It is a technology of home networking. ZigBee is a technological standard created for controlling and sensing the network. As we know that ZigBee is the Personal Area network of task group 4 so it is based on IEEE 802.15.4 and is created by Zigbee Alliance.

ZigBee is a standard that addresses the need for very low-cost implementation of Low power devices with Low data rates for short-range wireless communications.

Types of ZigBee Devices:

- **Zigbee Coordinator Device:** It communicates with routers. This device is used for connecting the devices.
- **Zigbee Router:** It is used for passing the data between devices.
- **Zigbee End Device:** It is the device that is going to be controlled.



General Characteristics of Zigbee Standard:

- Low Power Consumption
- Low Data Rate (20- 250 kbps)
- Short-Range (75-100 meters)
- Network Join Time (~ 30 msec)
- Support Small and Large Networks (up to 65000 devices (Theory); 240 devices (Practically))
- Low Cost of Products and Cheap Implementation (Open Source Protocol)
- Extremely low duty cycle.
- 3 frequency bands with 27 channels.

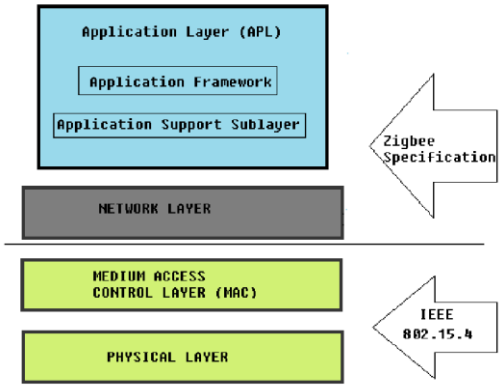
Operating Frequency Bands (Only one channel will be selected for use in a network):

1. **Channel 0**: 868 MHz (Europe)
2. **Channel 1-10**: 915 MHz (the US and Australia)
3. **Channel 11-26**: 2.4 GHz (Across the World)

Zigbee Network Topologies:

- **Star Topology** (ZigBee Smart Energy): Consists of a coordinator and several end devices, end devices communicate only with the coordinator.
- **Mesh Topology** (Self Healing Process): Mesh topology consists of one coordinator, several routers, and end devices.
- **Tree Topology**: In this topology, the network consists of a central node which is a coordinator, several routers, and end devices. The function of the router is to extend the network coverage.

Architecture of Zigbee:



Zigbee architecture is a combination of

1. Application Layer
2. Network Layer
3. Medium Access Control Layer
4. Physical Layer

- **Physical layer:** The lowest two layers i.e the physical and the MAC (Medium Access Control) Layer are defined by the IEEE 802.15.4 specifications. The Physical layer is closest to the hardware and directly controls and communicates with the Zigbee radio. The physical layer translates the data packets in the over-the-air bits for transmission and vice-versa during the reception.

- **Medium Access Control layer (MAC layer):** The layer is responsible for the interface between the physical and network layer. The MAC layer is also responsible for providing PAN ID and also network discovery through beacon requests.

- **Network layer:** This layer acts as an interface between the MAC layer and the application layer. It is responsible for mesh networking.

- **Application layer:** The application layer in the Zigbee stack is the highest protocol layer and it consists of the application support sub-layer and Zigbee device object. It contains manufacturer-defined applications.

Channel Access:

1. **Contention Based Method** (Carrier-Sense Multiple Access With Collision Avoidance Mechanism)
2. **Contention Free Method** (Coordinator dedicates a specific time slot to each device (Guaranteed Time Slot (GTS)))

Zigbee Applications:

1. Home Automation
2. Medical Data Collection
3. Industrial Control Systems
4. meter reading system
5. light control system

LoRa and LoRaWAN

The LoRaWAN protocol is a Low Power Wide Area Networking (LPWAN) communication protocol that functions on LoRa. The LoRaWAN specification is open so anyone can set up and operate a LoRa network.

LoRa is a wireless audio frequency technology that operates in a license-free radio frequency spectrum. LoRa is a physical layer protocol that uses spread spectrum modulation and supports long-range communication at the cost of a narrow bandwidth. It uses a narrow band waveform with a central frequency to send data, which makes it robust to interference.

Characteristics of LoRaWAN technology

- Long range communication up to 10 miles in line of sight.
- Long battery duration of up to 10 years. For enhanced battery life, you can operate your devices in class A or class B mode, which requires increased downlink latency.
- Low cost for devices and maintenance.
- License-free radio spectrum but region-specific regulations apply.
- Low power but has a limited payload size of 51 bytes to 241 bytes depending on the data rate. The data rate can be 0,3 Kbit/s – 27 Kbit/s data rate with a 222 maximal payload size.

Advantages:

8. Long Range: LoRaWAN can provide long-range communication, spanning several kilometers in urban areas and even greater distances in rural environments. This long-range capability is a significant advantage for applications that require wide-area coverage.

9. Low Power Consumption: IoT devices using LoRaWAN can operate on batteries for an extended period, often several years, before needing a battery replacement or recharge. This low power consumption is crucial for remote and battery-powered devices.

10. Scalability: LoRaWAN networks are highly scalable, allowing for the addition of a large number of devices to a single network without significant infrastructure changes.

11. Cost-Efficiency: Due to its low power requirements and long-range capabilities, LoRaWAN can be a cost-effective solution for many IoT applications. It reduces the need for frequent battery replacements and complex power infrastructure.

12. License-Free Spectrum: LoRaWAN operates in unlicensed ISM radio bands, reducing regulatory and licensing requirements. This simplifies deployment and lowers operational costs.

13. Wide Adoption: LoRaWAN has gained widespread adoption and support from various companies and organizations, creating a thriving ecosystem of devices, gateways, and network providers.

14. Security Features: LoRaWAN includes security features such as encryption and device authentication to protect data transmitted between devices and the network.

8. Use Cases: LoRaWAN is suitable for a wide range of IoT use cases, including smart agriculture, smart cities, industrial IoT, asset tracking, and environmental monitoring, among others.

Disadvantages:

15. Low Data Rate: LoRaWAN is designed for low-data-rate applications. If you need to transmit large amounts of data quickly, it may not be the best choice.

16. Limited Bandwidth: LoRaWAN networks have limited available bandwidth, which can lead to network congestion in areas with a high density of devices.

17. Latency: LoRaWAN is optimized for low power and long range, which can result in higher latency compared to other wireless technologies. This may not be suitable for applications requiring real-time data transmission.

18. Interference: In crowded radio frequency environments, interference from other devices operating in the same frequency bands can affect LoRaWAN communication quality.

19. Not Suitable for High Mobility: LoRaWAN is designed for stationary or slowly moving devices. It may not be suitable for applications that require high mobility, such as asset tracking on fast-moving vehicles.

20. Initial Deployment Complexity: Setting up a LoRaWAN network can be more complex than other wireless technologies, as it requires the installation of gateways and configuration of network servers.

21. Dependence on Gateways: LoRaWAN devices rely on gateways to relay data to the network. If gateways are unavailable or experience issues, communication can be disrupted.

8. Limited Use Cases: While LoRaWAN is versatile, it may not be the best choice for all IoT applications, especially those that require high bandwidth, low latency, or high mobility.

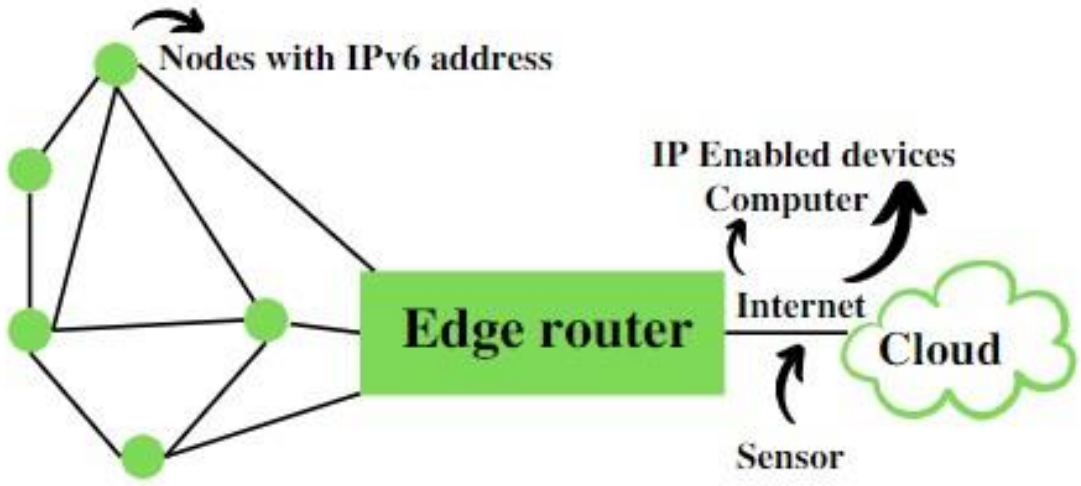
6LowPAN

6LoWPAN is an IPv6 protocol, and It's extended from is IPv6 over Low Power Personal Area Network. As the name itself explains the meaning of this protocol is that this protocol works on Wireless Personal Area Network i.e., WPAN.

WPAN is a Personal Area Network (PAN) where the interconnected devices are centered around a person's workspace and connected through a wireless medium. You can read more about WPAN at WPAN. 6LoWPAN allows communication using the IPv6 protocol. IPv6 is Internet Protocol Version 6 is a network layer protocol that allows communication to take place over the network. It is faster and more reliable and provides a large number of addresses.

6LoWPAN initially came into existence to overcome the conventional methodologies that were adapted to transmit information. But still, it is not so efficient as it only allows for the smaller devices with very limited processing ability to establish communication using one of the Internet Protocols, i.e., IPv6. It has very low cost, short-range, low memory usage, and low bit rate.

It comprises an Edge Router and Sensor Nodes. Even the smallest of the IoT devices can now be part of the network, and the information can be transmitted to the outside world as well. For example, LED Streetlights.



- It is a technology that makes the individual nodes IP enabled.
- 6LoWPAN can interact with 802.15.4 devices and also other types of devices on an IP Network. For example, Wi-Fi.
- It uses AES 128 link layer security, which AES is a block cipher having key size of 128/192/256 bits and encrypts data in blocks of 128 bits each. This is defined in IEEE 802.15.4 and provides link authentication and encryption.

Basic Requirements of 6LoWPAN:

1. The device should be having sleep mode in order to support the battery saving.
2. Minimal memory requirement.
3. Routing overhead should be lowered.

Features of 6LoWPAN:

1. It is used with IEEE 802.15,.4 in the 2.4 GHz band.
2. Outdoor range: ~200 m (maximum)
3. Data rate: 200kbps (maximum)
4. Maximum number of nodes: ~100

Advantages of 6LoWPAN:

1. 6LoWPAN is a mesh network that is robust, scalable, and can heal on its own.
2. It delivers low-cost and secure communication in IoT devices.
3. It uses IPv6 protocol and so it can be directly routed to cloud platforms.
4. It offers one-to-many and many-to-one routing.
5. In the network, leaf nodes can be in sleep mode for a longer duration of time.

Disadvantages of 6LoWPAN:

1. It is comparatively less secure than Zigbee.
2. It has lesser immunity to interference than that Wi-Fi and Bluetooth.
3. Without the mesh topology, it supports a short range.

Applications of 6LoWPAN:

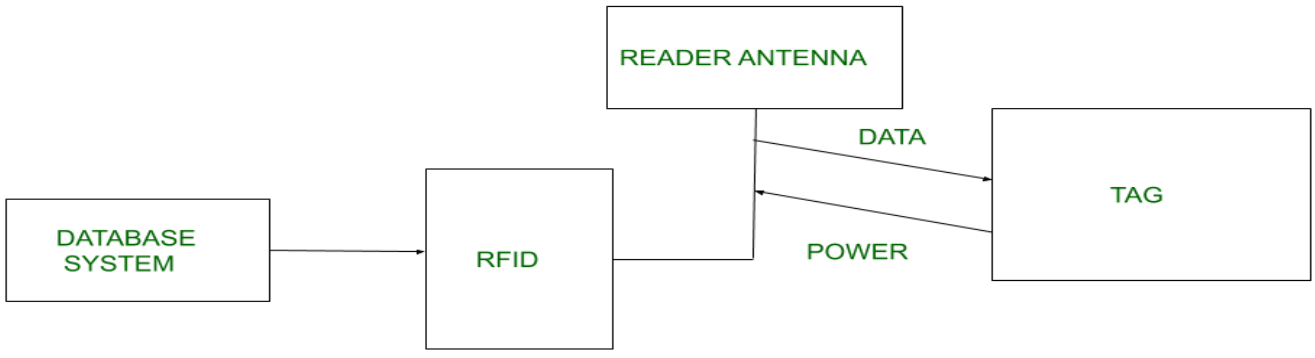
1. It is a wireless sensor network.
2. It is used in home-automation,
3. It is used in smart agricultural techniques, and industrial monitoring.

Security and Interoperability with 6LoWPAN:

- **Security**: 6LoWPAN security is ensured by the AES algorithm, which is a link layer security, and the transport layer security mechanisms are included as well.
- **Interoperability**: 6LoWPAN is able to operate with other wireless devices as well which makes it interoperable in a network.

Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person. It uses radio frequency to search ,identify, track and communicate with items and people. it is a method that is used to track or identify an object by radio transmission uses over the web. Data digitally encoded in an RFID tag which might be read by the reader. This device work as a tag or label during which data read from tags that are stored in the database through the reader as compared to traditional barcodes and QR codes. It is often read outside the road of sight either passive or active RFID.



Kinds of RFID :

There are many kinds of RFID, each with different properties, but perhaps the most fascinating aspect of RFID technology is that most RFID tags have neither an electric plug nor a battery. Instead, all of the energy needed to operate them is supplied in the form of radio waves by RFID readers. This technology is called passive RFID to distinguish it from the(less common) active RFID in which there is a power source on the tag.

UHF RHID (Ultra-High Frequency RFID).

It is used on shipping pallets and some driver's licenses. Readers send signals in the 902-928 MHz band. Tags communicate at distances of several meters by changing the way they reflect the reader signals; the reader is able to pick up these reflections. This way of operating is called backscatter.

HF RFID (High-Frequency RFID).

It operates at 13.56 MHz and is likely to be in your passport, credit cards, books, and noncontact payment systems. HF RFID has a short-range, typically a meter or less because the physical mechanism is based on induction rather than backscatter.
There are also other forms of RFID using other frequencies, such as LF RFID(Low-Frequency RFID), which was developed before HF RFID and used for animal tracking

There are two types of RFID :

1. **Passive RFID –**

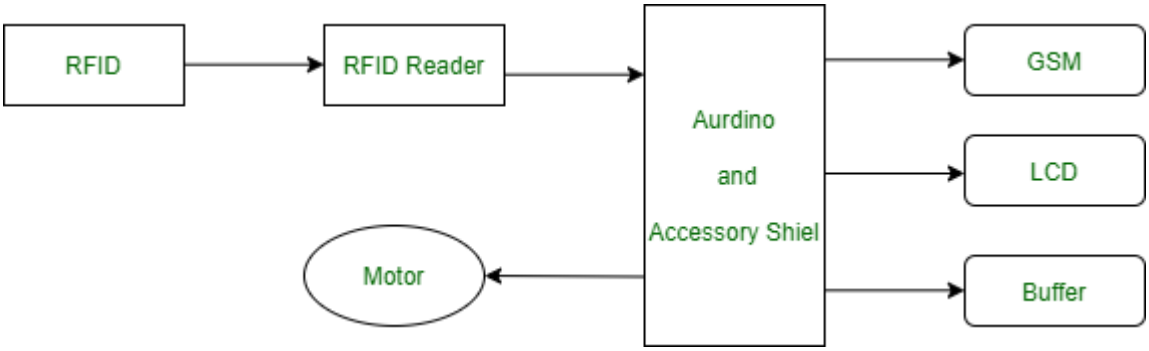
   Passive RFID tags does not have their own power source. It uses power from the reader. In this device, RF tags are not attached by a power supply and passive RF tag stored their power. When it is emitted from active antennas and the RF tag are used specific frequency like 125-134KHZ as low frequency, 13.56MHZ as a high frequency and 856MHZ to 960MHZ as ultra-high frequency.

2. **Active RFID –**

   In this device, RF tags are attached by a power supply that emits a signal and there is an antenna which receives the data. means, active tag uses a power source like battery. It has it's own power source, does not require power from source/reader.

Working Principle of RFID :

Generally, RFID uses radio waves to perform AIDC function. AIDC stands for Automatic Identification and Data Capture technology which performs object identification and collection and mapping of the data.
An antenna is an device which converts power into radio waves which are used for communication between reader and tag. RFID readers retrieve the information from RFID tag which detects the tag and reads or writes the data into the tag. It may include one processor, package, storage and transmitter and receiver unit.



Working of RFID System :

Every RFID system consists of three components: a scanning antenna, a transceiver and a transponder. When the scanning antenna and transceiver are combined, they are referred to as an RFID reader or interrogator. There are two types of RFID readers — fixed readers and mobile readers. The RFID reader is a network-connected device that can be portable or permanently attached. It uses radio waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data.

The transponder is in the RFID tag itself. The read range for RFID tags varies based on factors including the type of tag, type of reader, RFID frequency and interference in the surrounding environment or from other RFID tags and readers. Tags that have a stronger power source also have a longer read range.

Features of RFID :

- An RFID tag consists of two-part which is an microcircuit and an antenna.
- This tag is covered by protective material which acts as a shield against the outer environment effect.
- This tag may active or passive in which we mainly and widely used passive RFID.

Application of RFID :

- It utilized in tracking shipping containers, trucks and railroad, cars.
- It uses in Asset tracking.
- It utilized in credit-card shaped for access application.
- It uses in Personnel tracking.
- Controlling access to restricted areas.
- It uses ID badging.
- Supply chain management.
- Counterfeit prevention (e.g., in the pharmaceutical industry).

Advantages of RFID :

- It provides data access and real-time information without taking to much time.
- RFID tags follow the instruction and store a large amount of information.
- The RFID system is non-line of sight nature of the technology.
- It improves the Efficiency, traceability of production.
- In RFID hundred of tags read in a short time.

Disadvantages of RFID :

- It takes longer to program RFID Devices.
- RFID intercepted easily even it is Encrypted.
- In an RFID system, there are two or three layers of ordinary household foil to dam the radio wave.

- There is privacy concern about RFID devices anybody can access information about anything.
- Active RFID can costlier due to battery.

Wi-Fi

- **Wi-Fi**, a brand name given by the Wi-Fi Alliance (formerly Wireless Ethernet Compatibility Alliance), is a generic term that refers to the communication standard for the wireless network which works as a Local Area Network to operate without using the cable and any types of wiring.
- It is known as **WLAN**. The communication standard is **IEEE 802.11**. Wi-Fi works using Physical Data Link Layer.
- Nowadays in all mobile computing devices such as laptops, mobile phones, also digital cameras, smart TVs has the support of Wi-Fi. The Wi-Fi connection is established from the access point or base station to the client connection or any client-to-client connection within a specific range, the range depends on the router which provides the radio frequency through Wi-Fi. These frequencies operate on 2 types of bandwidth at present, 2.4 GHz and 5 GHz.

All the modern laptops and mobiles are capable of using both bandwidths, it depends on the Wi-Fi adapter which is inside the device to catch the Wi-Fi signal. 2.4 GHz is the default bandwidth supported by all the devices. 2.4 GHz can cover a big range of areas to spread the Wi-Fi signal but the frequency is low, so in simple words, the speed of the internet is less and 5 GHz bandwidth is for a lower range of area but the frequency is high so the speed is very high.

Let's say, if there is an internet connection of 60 MB/s bandwidth, then for 2.4 GHz bandwidth, it provides approx 30 to 45 MB/s of bandwidth connection and for 5 GHz bandwidth, it provides approx 50 to 57 MB/s bandwidth.

History:

The concept of Wi-Fi is very old but its implementation is not so old. At first **ALOHA System** is a wireless network system that is used to connect Hawaii island via a network in the year 1971. Where the protocol is used for this was ALOHA protocol and the network used packet transfer. Later it's converted to IEEE 802.11 protocol.
Then in 1985, the Federal Communications Commission (FCC) released a new network for general uses which works on 900 Mhz, 2.4 GHz, and 5.8 GHz bandwidth. This is known as the *ISM band*. Also, IBM introduced a *Token Ring LAN* network for connecting several computers, it can transfer data at 4 Mb/s speed. Then in 1988, a wireless cashier system was invented based on the Token Ring LAN network known as *waveLAN*, it operates at 900MHz or 2.4 GHz band and offers speeds of 1 to 2 Mbps. Then it was converted to *IEEE 802.11LAN/MAN* standards in 1989. ?Then in 1990, IEEE 802.11 Working Group for Wireless LANs is established by **Vic Hayes**, who was known as the **"Father of WiFi"**.
Then in 1994, *Dr. Alex Hills* introduced a research project on the wireless network, which provided coverage of the network to 7 buildings wirelessly.
Then in 1996 *Commonwealth Scientific and Industrial Research Organization (CSIRO)* introduced a wireless network based on the same protocol 802.11, later it was known as IEEE 802.11a standards.
Then after all this in 1997 the first version of Wi-Fi is released officially which is 802.11 and it can support a maximum of 2 Mb/s link speed. Then in 1999, the link speed is increased to 11 Mb/s over the 2.4 GHz frequency band, this version is known as *802.11b*
Then after a month, the IEEE 802.11a standard is approved officially, which provides up to 54 Mb/s link speed over the 5 GHz band, but the signal range is weaker than the 2.4 GHz band.

Then in 2003, the speed is increased in a new version, known as *802.11g*. The speed offers up to 54 to 108 Mb/s over 2.4 GHz.
After this two more versions were introduced that are, *802.11i and 802.11e*. In 802.11i, the security mechanism was increased and in 802.11e, Voice over Wireless LAN and multimedia streaming are involved.
Then in 2009, 802.11n is developed, which supports both 2.4 GHz and 5 GHz radiofrequency. And these are used simultaneously by dual-band routers and can reach maximum speeds of 600 Mbps.

Then in 2014, a new version was introduced that offers a potential speed of 1733 Mb/s in the 5 GHz band. This version is known as *802.11ac*. Till now this is the latest version of Wi-Fi.

Applications of Wi-Fi :

Wi-Fi has many applications, it is used in all the sectors where a computer or any digital media is used, also for entertaining Wi-Fi is used. Some of the applications are mentioned below –

- Accessing Internet: Using Wi-Fi we can access the internet in any Wi-Fi-capable device wirelessly.
- We can stream or cast audio or video wirelessly on any device using Wi-Fi for our entertainment.
- We can share files, data, etc between two or more computers or mobile phones using Wi-Fi, and the speed of the data transfer rate is also very high. Also, we can print any document using a Wi-Fi printer, this is very much used nowadays.
- We can use Wi-Fi as **HOTSPOTS** also, it points Wireless Internet access for a particular range of area. Using Hotspot the owner of the main network connection can offer temporary network access to Wi-Fi-capable devices so that the users can use the network without knowing anything about the main network connection. Wi-Fi adapters are mainly spreading radio signals using the owner network connection to provide a hotspot.
- Using Wi-Fi or WLAN we can construct simple wireless connections from one point to another, known as Point to point networks. This can be useful to connect two locations that are difficult to reach by wire, such as two buildings of corporate business.
- One more important application is **VoWi-Fi**, which is known as **voice-over Wi-Fi**. Some years ago telecom companies are introduced VoLTE (Voice over Long-Term Evolution). Nowadays they are introduced to VoWi-Fi, by which we can call anyone by using our home Wi-Fi network, only one thing is that the mobile needs to connect with the Wi-Fi. Then the voice is transferred using the Wi-Fi network instead of using the mobile SIM network, so the call quality is very good. Many mobile phones are already getting the support of VoWi-Fi.
- Wi-Fi in offices: In an office, all the computers are interconnected using Wi-Fi. For Wi-Fi, there are no wiring complexities. Also, the speed of the network is good. For Wi-Fi, a project can be presented to all the members at a time in the form of an excel sheet, ppt, etc. For Wi-Fi, there is no network loss as in cable due to cable break.
- Also using W-Fi a whole city can provide network connectivity by deploying routers at a specific area to access the internet. Already schools, colleges, and universities are providing networks using Wi-Fi because of its flexibility.
- Wi-Fi is used as a *positioning system* also, by which we can detect the positions of Wi-Fi hotspots to identify a device location.

Types of Wi-Fi:

Wi-Fi has several types of standards, which are discussed earlier, here just the name of the standards are defined,

Standards	Year of Release	Description
Wi-Fi-1 (802.11b)	**1999**	**This version has a link speed from 2Mb/s to 11 Mb/s over a 2.4 GHz frequency band**
Wi-Fi-2 (802.11a)	**1999**	**After a month of release previous version, 802.11a was released and it provide up to 54 Mb/s link speed over 5 Ghz band**
Wi-Fi-3 (802.11g)	**2003**	**In this version the speed was increased up to 54 to 108 Mb/s over 2.4 GHz**

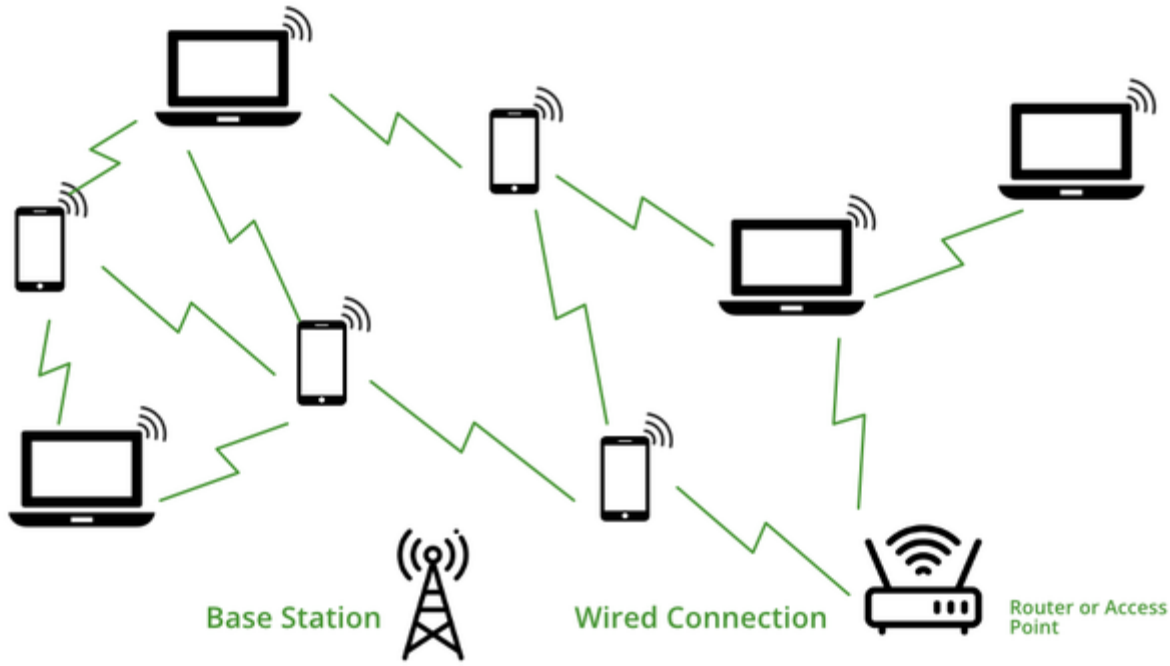
802.11i	**2004**	**This is the same as 802.11g but only the security mechanism was increased in this version**
802.11e	**2004**	**This is also the same as 802.11g, only Voice over Wireless LAN and multimedia streaming are involved**
Wi-Fi-4 (802.11n)	**2009**	**This version supports both 2.4 GHz and 5 GHz radio frequency and it offers up to 72 to 600 Mb/s speed**
Wi-Fi-5 (802.11ac)	**2014**	**It supports a speed of 1733 Mb/s in the 5 GHz band**

A new version will release in 2020 named *802.11ax* developed by **Huawei**, which can support, a maximum of 3.5 Gb/s. it will know **Wi-Fi 6**.

How does Wi-Fi work?

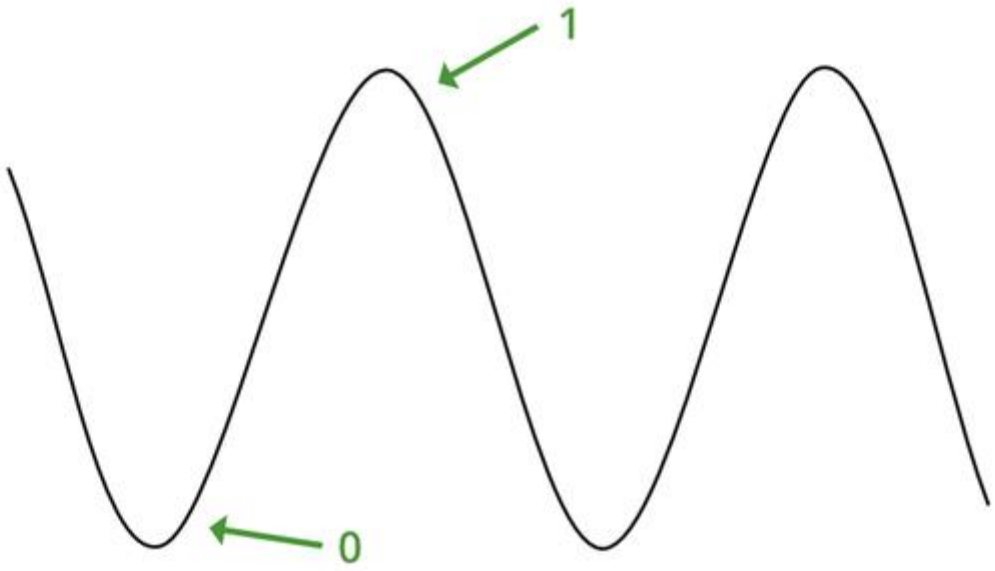
Wi-Fi is a wireless technology for networking, so it uses Electromagnetic waves to transmit networks. We know that there are many divisions of Electromagnetic waves according to their frequency such as X-ray, Gamma-ray, radio wave, microwave, etc, in Wi-Fi, the radio frequency is used. For transmitting Wi-Fi signal there is three medium,

- **Base station network or an Ethernet(802.3) connection:** It is the main host network from where the network connection is provided to the router.
- **Access point or router:** it is a bridge between a wired network and a wireless network. It accepts a wired Ethernet connection and converts the wired connection to a wireless connection and spreads the connection as a radio wave.
- **Accessing devices:** It is our mobile, computer, etc from where we use the Wi-Fi and surfing internet.



Working of Wi-Fi

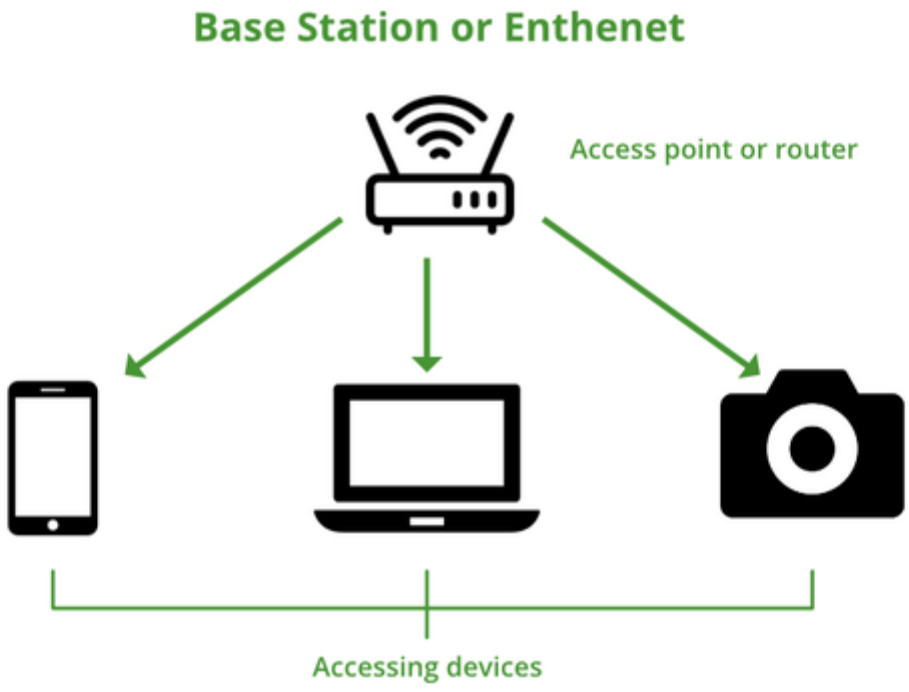
All the electronics devices read data in binary form, also router or our devices, here routers provide radio waves and those waves are receive by our devices and read the waves in binary form. We all know how a wave looks like, the upper pick of the wave is known as 1 and the lower pick of the wave is known as 0 in binary. Like below:



*Data transmission*Some more terminologies

- **SSID (Service Set Identifier)**: It is a 32 character name that identifies the Wi-Fi network and differentiates one Wi-Fi from another Wi-Fi. All the devices are attempting to connect a particular SSID. Simply, SSID is the name of the wireless network.
- **WPA-PSK (Wi-Fi Protected Access- Pre-Shared Key):** It is a program developed by the Wi-Fi Alliance Authority to secure wireless networks with the use of Pre-Shared Key(PSK) authentication. WPA has 3 types, such as WPA. WPA2, WPA3. It is a way of encrypting the Wi-Fi signal to protect from unwanted users.
- Wi-Fi uses **Ad-Hoc** networks to transmit. It is a point-to-point network without any interface.

How signals are reached to our devices?



Base Station

Advantages of Wi-Fi

- It is a flexible network connection, no wiring complexities. Can be accessed from anywhere in the Wi-Fi range.
- It does not require regulatory approval for individual users.
- It is salable, can be expanded by using Wi-Fi Extenders.
- It can be set up in an easy and fast way. Just need to configure the SSID and Password.
- Security in a high in Wi-Fi network, its uses **WPA** encryption to encrypt radio signals.
- It is also lower in cost.
- It also can provide Hotspots.
- it supports roaming also.

Disadvantages of Wi-Fi

- Power consumption is high while using Wi-Fi in any device which has a battery, such as mobile, laptops, etc.
- Many times there may be some security problems happening even it has encryption. Such as many times has known devices become unknown to the router, Wi-Fi can be hacked also.
- Speed is slower than a direct cable connection.
- It has lower radiation like cell phones, so it can harm humans.
- Wi-Fi signals may be affected by climatic conditions like thunderstorms.
- Unauthorized access to Wi-Fi can happen because it does not have a firewall.
- To use Wi-Fi we need a router, which needs a power source, so at the time of power cut, we cannot access the internet.

Power Source

- Power sources in IoT (Internet of Things) devices are a critical consideration as they directly impact the device's functionality, longevity, and deployment options.

Here are some important notes about power sources in IoT:

1. Battery Power:

- Advantages:

- Portability: Battery-powered IoT devices are highly portable and can be placed virtually anywhere without the need for a power outlet.
- Low Maintenance: Batteries can provide power for extended periods (months to years) without the need for frequent maintenance.

- Disadvantages:

- Limited Lifetime: Batteries have a finite lifespan, and their replacement or recharging can be costly and impractical for certain deployments.
- Size and Weight: Batteries can add bulk and weight to IoT devices, which may not be suitable for small or lightweight applications.
- Environmental Impact: Battery disposal and the environmental impact of disposable batteries are concerns.

2. Solar Power:

- Advantages:

- Renewable Energy: Solar panels harness energy from the sun, providing a renewable and eco-friendly power source.

- Extended Lifespan: Solar-powered IoT devices can operate for extended periods without the need for battery replacement.

- Disadvantages:

- Sunlight Dependency: Solar power is dependent on sunlight, which can be limited in certain geographic locations or during cloudy days.
- Initial Costs: Solar panel installation can have high upfront costs, although it can lead to long-term savings.

3. Energy Harvesting:

- Advantages:

- Energy from the Environment: Energy harvesting technologies, such as vibration, thermal, or kinetic energy, allow IoT devices to capture energy from their environment.
- Continuous Operation: When implemented effectively, energy harvesting can enable continuous device operation without the need for battery replacement.

- Disadvantages:

- Variable Energy Availability: The availability of environmental energy sources can vary, making it challenging to ensure consistent device operation.
- Energy Storage: Energy harvested must be stored efficiently for later use, which may require specialized components.

4. Wired Power:

- Advantages:

- Reliable and Stable: Wired power sources, such as AC or DC power outlets, provide a stable and reliable source of energy.
- High Power Capacity: Wired connections can support high-power IoT devices and applications.

- Disadvantages:

- Limited Mobility: Devices relying on wired power sources are typically fixed and cannot be easily moved.
- Installation Complexity: Installing wired power connections may be labor-intensive and costly, especially in remote or outdoor locations.

5. Hybrid Power:

- Advantages:

- Combining Sources: Hybrid power systems can combine multiple power sources, such as batteries and solar panels, to provide redundancy and extended operation.
- Flexibility: Hybrid systems can adapt to changing environmental conditions and energy availability.

- Disadvantages:

- Complexity: Designing and managing hybrid power systems can be complex and may require specialized knowledge.

6. Ultra-Low Power Consumption:

- Reducing power consumption through efficient hardware design and software optimization is crucial for extending the lifespan of battery-powered IoT devices**.**

7. Energy-Efficient Communication Protocols:

- Choosing energy-efficient communication protocols like LoRaWAN or MQTT-SN can minimize the power required for data transmission.

8. Energy Monitoring and Management:

- Implementing energy monitoring and management features in IoT devices can help optimize power usage and extend battery life.