IoT Gateways

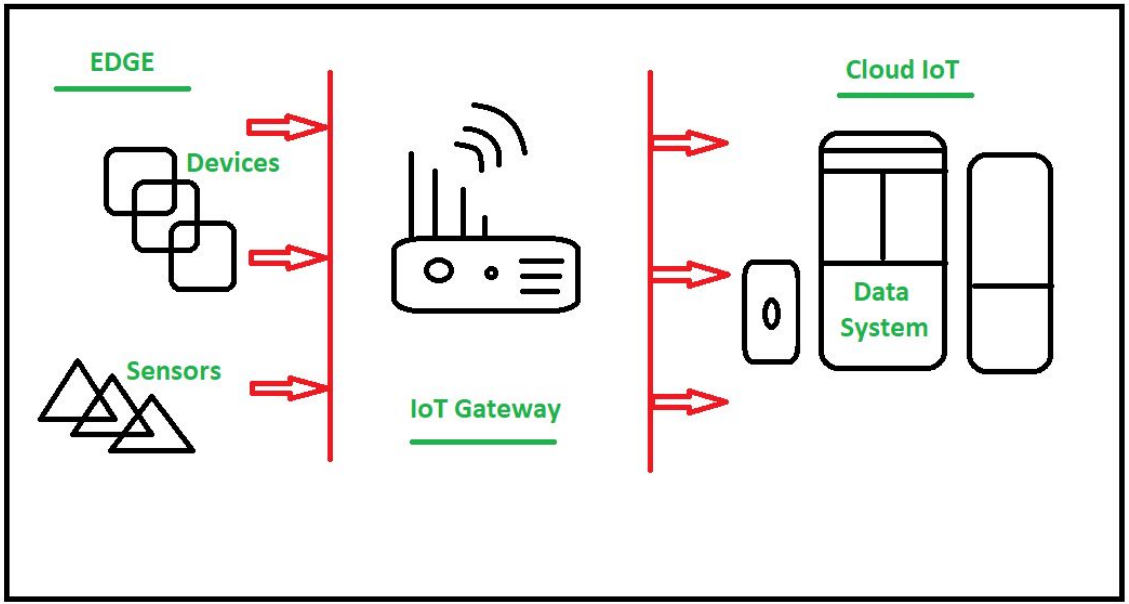
By - Monu Kumar (JRF)

Definition

1. Gateway provides a bridge between different communication technologies which means we can say that a Gateway acts as a medium to open up connections between the cloud and controller(sensors/devices) in Internet of Things (IoT).
2. With the help of gateways, it is possible to establish device-to-device or device-to-cloud communication.
3. A gateway can be a typical hardware device or software program. It enables a connection between the sensor network and the Internet along with enabling IoT communication.
4. As IoT devices work with low power consumption(Battery power) in other words they are energy constrained so if they will directly communicate to cloud/internet it won't be effective in terms of power. So they communicate with Gateway first using short range wireless transmission modes/network like ZigBee, Bluetooth, etc as they consume less power or they can also be connected using long range like Cellular and WiFi etc.

IoT Gateways Figure

The below figure shows how IoT Gateways establish communication between sensors and the cloud (Data System)



Key functionalities of IoT Gateways

1. Establishing communication bridge
2. Provides additional security.
3. Performs data aggregation.
4. Pre processing and filtering of data.
5. Provides local storage as a cache/ buffer.
6. Data computing at edge level.
7. Ability to manage entire device.
8. Device diagnostics.
9. Adding more functional capability.
10. Verifying protocols.

Working of IoT Gateway

1. Receives data from sensor network.
2. Performs Pre processing, filtering and cleaning on unfiltered data.
3. Transports into standard protocols for communication.
4. Sends data to cloud.

IoT Gateways are key element of IoT infrastructure as Gateways establish connection for communication and also performs other task as described above. So IoT Gateway is one of most essential thing when we start think about an IoT ecosystem.

Advantages of Gateway

1. **Protocol translation:** IoT devices typically use different communication protocols and a gateway can translate between these protocols to enable communication between different types of devices.
2. **Data aggregation:** A gateway can collect data from multiple IoT devices and aggregate it into a single stream for easier analysis and management.
3. **Edge computing:** Gateways can perform edge computing tasks such as data processing, analytics, and machine learning, enabling faster and more efficient decision-making.
4. **Security:** Gateways can act as a secure access point for IoT devices, providing a layer of protection against cyber threats.
5. **Scalability:** Gateways can support a large number of IoT devices and can be easily scaled up or down to meet changing needs.
6. **Improved reliability:** Gateways can help to improve the reliability of IoT devices by managing network connectivity and providing a backup mechanism in case of network failure.
7. **Cost-effective:** Gateways can be a cost-effective way to manage and control a large number of IoT devices, reducing the need for expensive infrastructure and IT resources.

Internet of Things
Unit - II

By - Monu Kumar (JRF)

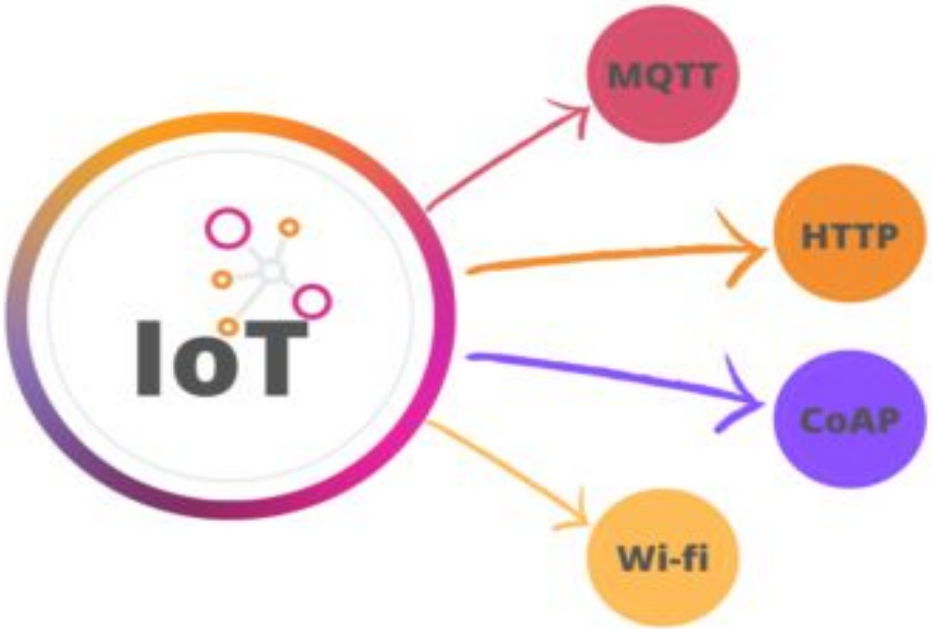
IoT Protocols

1. The Internet of Things (IoT) is about the network of sensor devices to the web in real-time. IoT devices communicate with each other over the network, so certain standards and rules need to be set to determine how data is exchanged.
2. These rules are called IoT Network Protocols. Today, a wide variety of IoT devices are available and therefore different protocols have been designed.
3. Depending on the IoT application's functionality, its workflow or architecture varies. Basic architecture involves four layers, i.e.
    a. Sensing layer
    b. Network layer
    c. Data processing layer
    d. Application layer
4. The Sensing layer contains all the hardware, like sensors, actuators, chips, etc., that collect information.

IoT Protocols

1. This layer is connected to the successive layer, which is the network layer, through protocols.
2. The Network layer allows communications among devices using network protocols like cellular, Wi-Fi, Bluetooth, Zigbee, etc.
3. The data collected by IoT devices is processed in the Data processing layer using technologies like data analytics and machine learning algorithms. This processed data can be displayed to the user through web portals, apps or interfaces provided by the application layer.
4. Users can directly interact and visualize the data obtained from IoT devices through these interfaces.
5. As IoT devices have very few components-little batteries and sensors, there is a small amount of power available. Hence, it is tough to design protocols for IoT. Also, we need to perform everything (construct topological structures, do address assignments, etc.) on wireless.

IoT Protocols



Short Range Communication, Low Data Rate, Low Power

1. **Bluetooth:** Bluetooth works in a frequency range of 2.4GHz. It covers a range of 10m to 100m and its data rate goes up to 1MBPS. It supports two network topologies – point-to-point and mesh. It is suitable to send a small amount of data to personal devices like speakers, earphones, smart watches, smart shoes etc. This protocol can also be used for Smart Homes, including Alarms, HVAC, lighting etc.
2. **Zigbee:** This is based on the IEEE802.15.4 standard. Its frequency range is the same as that of Bluetooth, which is 2.4GHz. Its range is up to 100 meters, and the data rate is a maximum of 250KBPS. Zigbee protocol can transmit small amounts of data within a short range. This can be used in systems that require high authentication and robustness. It supports star topology, mesh topology, and cluster tree topology. Major applications observed are sensing device health in industries, smart homes, etc.
3. **6LoWPAN:** PAN stands for Personal Area Network, and 6LoWPAN refers to IPV6 Low Power PAN. It works in a frequency ranging from 900 to 2400MHz. The data rate is 250KBPS, supporting two network topologies - star and mesh.

Short Range Communication, High Data Rate, Low Power

Wireless LAN - Wi-Fi:

Wi-Fi has high bandwidth and allows a data rate of 54MBPS and goes up to 600MBPS. Covers a range of 50 m in the local area where providing private antennas goes to 30 km. IoT devices can be easily connected using Wi-Fi and share a large amount of data. This protocol is used in smart homes, smart cities, offices, etc

Low Range Communication, High Data Rate, Low Power

1. **LoRaWAN**

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

2. **LTE-M**

   LTE-M stands for Long Term Evolution for Machines. This is a type of LPWAN – Low Power Wide Area Network. This is used along with cellular networks to provide security. LTE-M works in a frequency range of 1.4MHz-5 MHz, and the data rate can go up to 4MBPS.

Long Range, Low Data Rate, Low Power Comsumption

Sigfox

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

Long Range, Low Data Rate, High Power Consumption

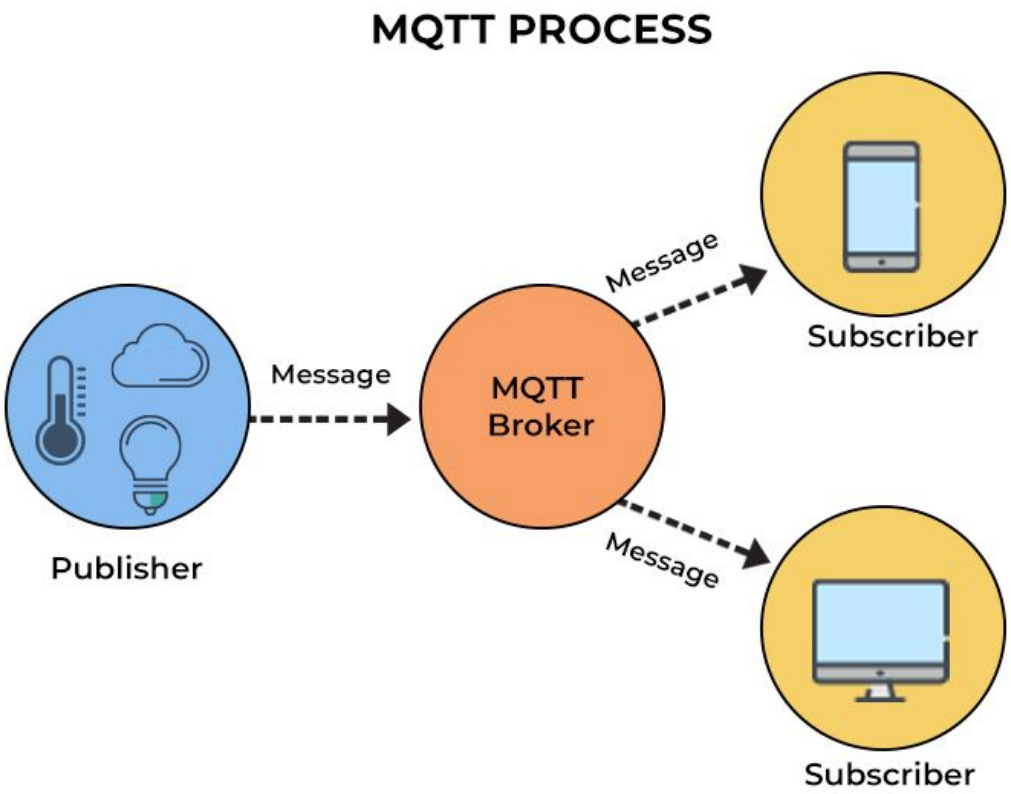
Cellular

This is also known as a mobile network. Cellular networks are 2G, 3G, 4G, and 5G. It Has frequency ranges – 900MHz, 1.8/1.9/2.1 GHz. The range is approximately 35 km and goes up to 200 km. The average data rate is 35 MBPS – 170KBPS. Cellular networks consume high power. This protocol is not used for most IoT devices due to frequency and security issues. It can be used with IoT applications like connected cars.

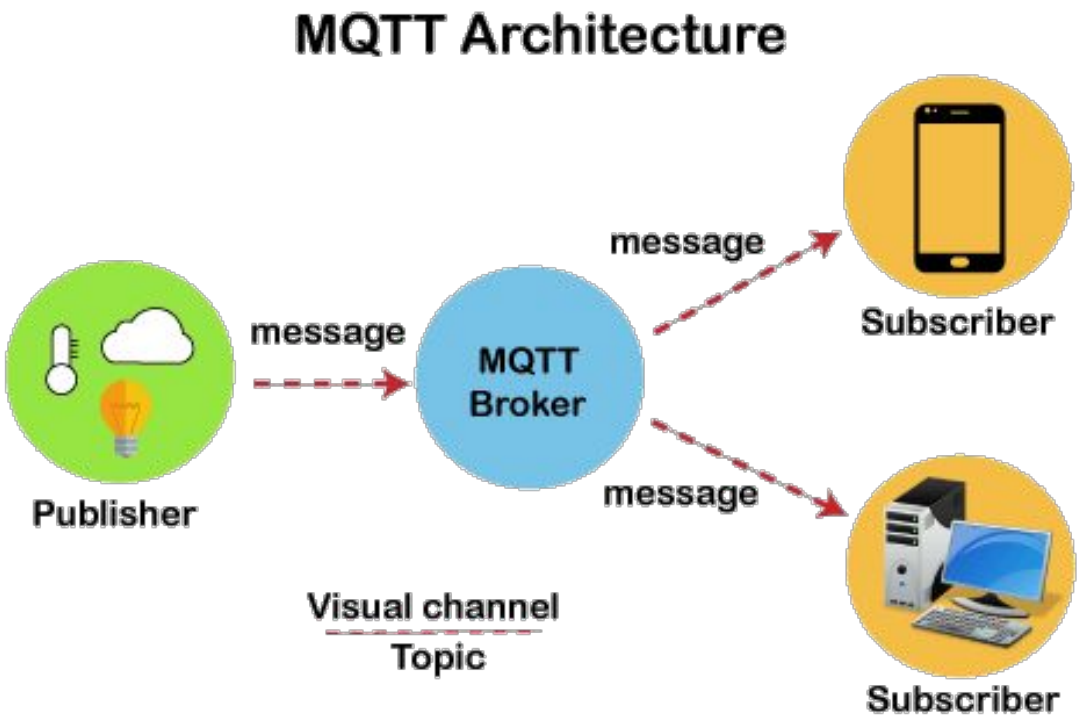
MQTT(Message Queue Telemetry Transport)

1. MQTT is a standards-based messaging protocol, or set of rules, used for machine-to-machine communication.
2. Smart sensors, wearables and other Internet of Things (IoT) devices typically have to transmit and receive data over a resource-constrained network with limited bandwidth.
3. These IoT devices use MQTT for data transmission, as it is easy to implement and can communicate IoT data efficiently.
4. MQTT supports messaging between devices to the cloud and the cloud to the device.
5. It is TCP-based protocol relying on the publish-subscribe model.
6. This communication protocol is suitable for transmitting data between resource-constrained devices having low bandwidth and low power requirements.
7. Hence this messaging protocol is widely used for communication in IoT Framework.

MQTT(Message Queue Telemetry Transport)



MQTT(Message Queue Telemetry Transport)



How does MQTT Work?

An overview of how MQTT works is given below.

1. An MQTT client establishes a connection with the MQTT broker.
2. Once connected, the client can either publish messages, subscribe to specific messages or do both.
3. When the MQTT broker receives a message, it forwards it to subscribers who are interested.

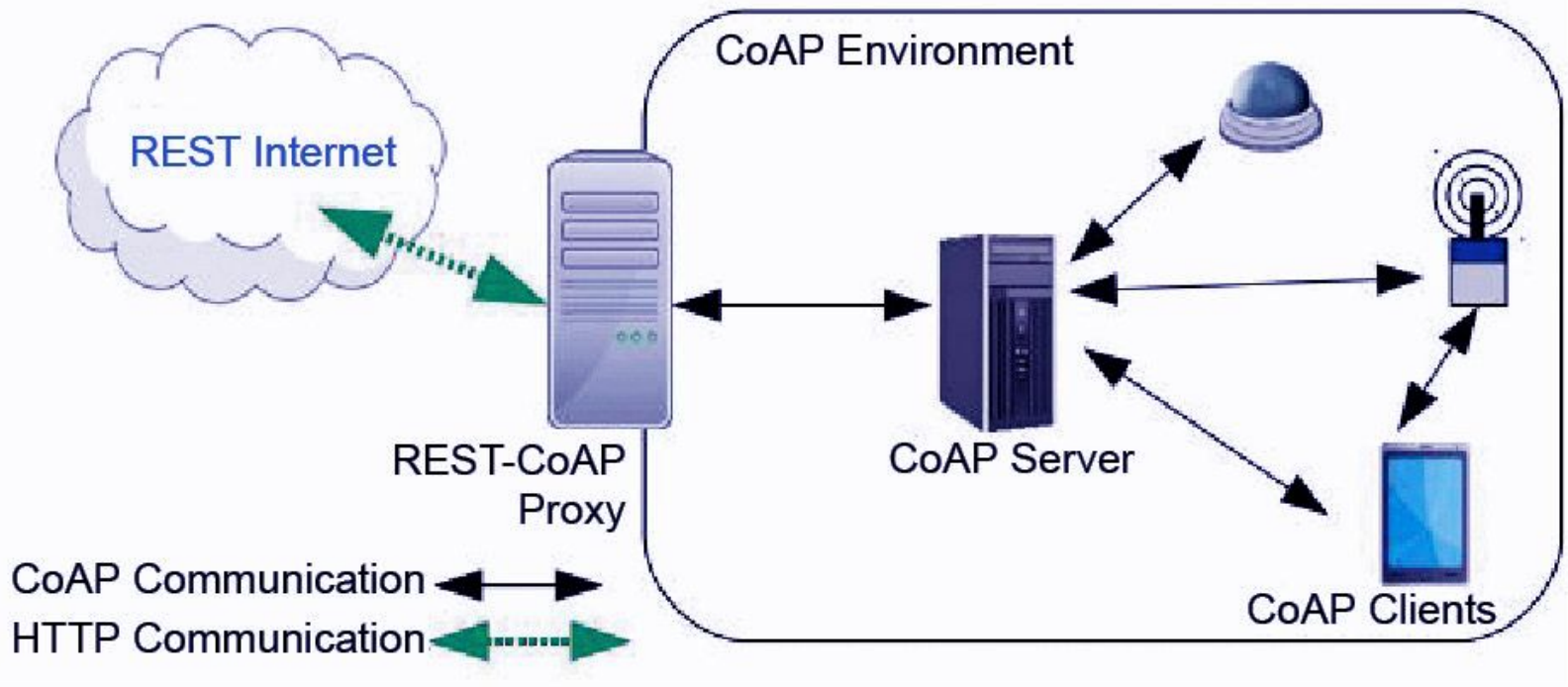
SMQTT(Secure Message Queue Telemetry Transport)

1. **SMQTT (Secure Message Queue Telemetry Transport) is an extension of MQTT protocol which uses encryption based on lightweight attribute encryption.**
2. **The main advantage of this encryption is that it has a broadcast encryption feature.**
3. **In this features, one message is encrypted and delivered to multiple other nodes.**
4. **The process of message transfer and receiving consists of four major stages:**
   a. **Setup:** In this phase, the publishers and subscribers register themselves to the broker and get a secret master key.
   b. **Encryption:** When the data is published to broker, it is encrypted by broker.
   c. **Publish:** The broker publishes the encrypted message to the subscribers.
   d. **Decryption:** Finally the received message is decrypted by subscribers with the same master key.
5. **SMQTT is proposed only to enhance MQTT security feature.**

CoAP(Constrained Application Protocol)

1. CoAP (Constrained Application Protocol) is a session layer protocol that provides the RESTful (HTTP) interface between HTTP client and server.
2. It is designed by IETF Constrained RESTful Environment (CoRE) working group.
3. It is designed to use devices on the same constrained network between devices and general nodes on the Internet.
4. CoAP enables low-power sensors to use RESTful services while meeting their low power constraints.
5. This protocol is specially built for IoT systems primarily based on HTTP protocols.
6. This network is used within the limited network or in a constrained environment.
7. The whole architecture of CoAP consists of CoAP client, CoAP server, REST CoAP proxy, and REST internet.

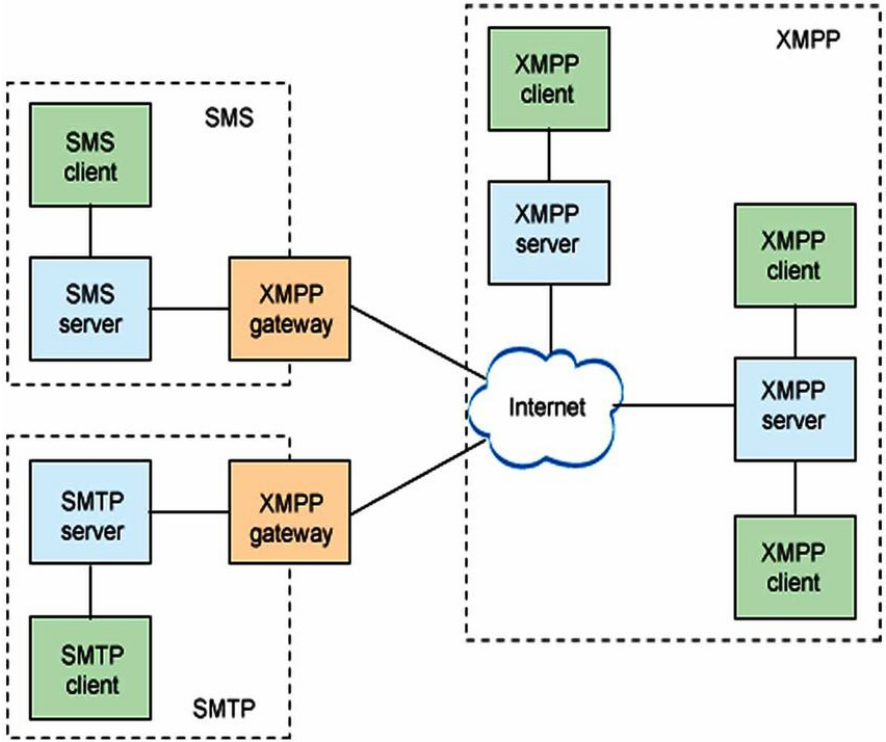
Architecture of CoAP



XMPP(Extensible Messaging and Presence Protocol)

1. XMPP is an open XML technology for real-time communication, which powers a wide range of applications including instant messaging, presence and collaboration
2. The Jabber open-source community developed XMPP in the late 1990s. It’s an open communication protocol for instant messaging (IM), presence information, and real-time applications that’s part of the Jabber technologies and XMPP.org family.
3. It enables the exchange of XML-based messages between clients and servers in a decentralized manner.
4. This means that, unlike other messaging protocols, XMPP doesn't rely on a central server to facilitate communication. Instead, it follows a federated model where users or organizations can operate their own XMPP server and communicate with users server-side.

XMPP Protocol Overview



Some Common XMPP Protocols

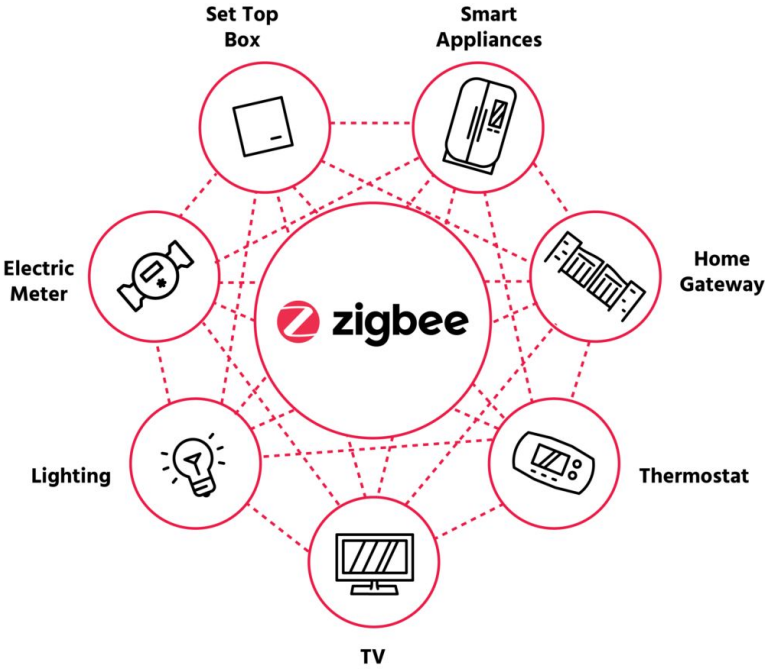
XMPP is a widely used protocol for real-time communication, particularly in instant messaging, voice-over IP, and social networking applications. Here are some of the common XMPP protocols:

1. XMPP Core
2. XMPP IM
3. XMPP Presence
4. XMPP MUC: MUC stands for Multi-User Chat
5. XMPP PubSub
6. XMPP File Transfer
7. XMPP Jingle
8. XMPP XEPs: XMPP Extension Protocols (XEPs)

Zigbee

1. Zigbee is a standards-based wireless technology developed to enable low-cost, low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks.
2. Zigbee is for low-data rate, low-power applications and is an open standard.
3. ZigBee is a Personal Area Network task group with low rate task group 4.
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.
5. ZigBee is an open, global, packet-based protocol designed to provide an easy-to-use architecture for secure, reliable, low power wireless networks. Flow or process control equipment can be place anywhere and still communicate with the rest of the system.
6. It can also be moved, since the network doesn't care about the physical location of a sensor, pump or valve.

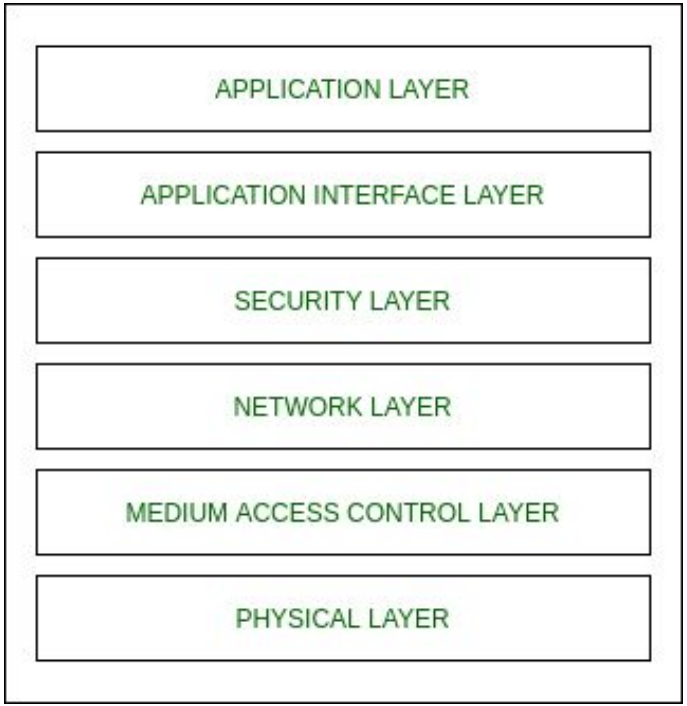
Zigbee Complete IoT Solution



Smart Home

Architecture of Zigbee

Zigbee architecture is a combination of 6 layers.



Zigbee Applications

1. Home Automation
2. Medical Data Collection
3. Industrial Control Systems
4. meter reading system
5. light control system
6. Commercial
7. Government Markets Worldwide
8. Home Networking

Zigbee Network Topologies

1. **Star Topology (ZigBee Smart Energy):**

   Consists of a coordinator and several end devices, end devices communicate only with the coordinator.
2. **Mesh Topology (Self Healing Process):**

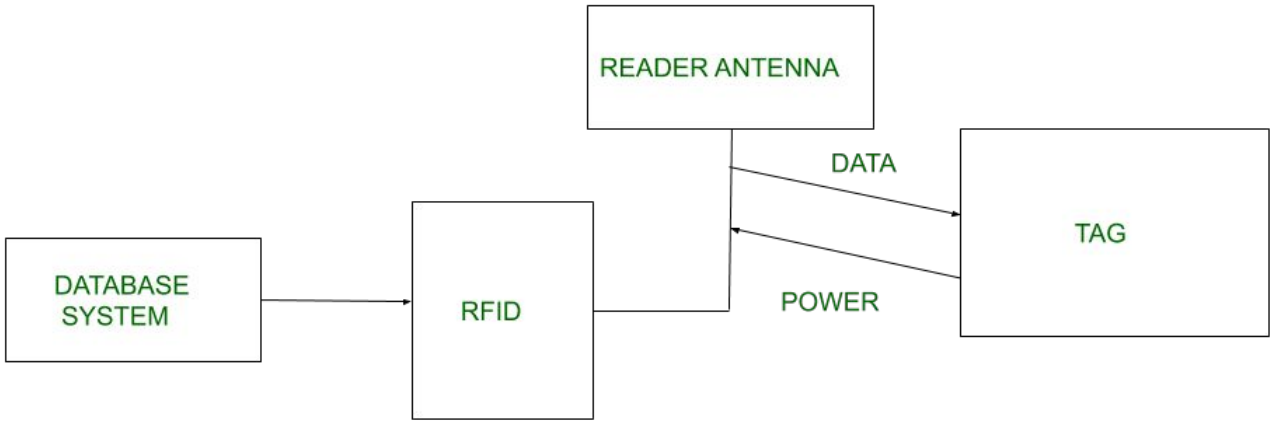
   Mesh topology consists of one coordinator, several routers and end devices.
3. **Tree Topology:**

   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.

RFID(Radio Frequency Identification)

1. 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.
2. It uses radio frequency to search, identify, track and communicate with items and people.
3. It is a method that is used to track or identify an object by radio transmission uses over the web.
4. Data digitally encoded in an RFID tag which might be read by the reader.
5. 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.
6. It is often read outside the road of sight either passive or active RFID.

RFID Block Diagram



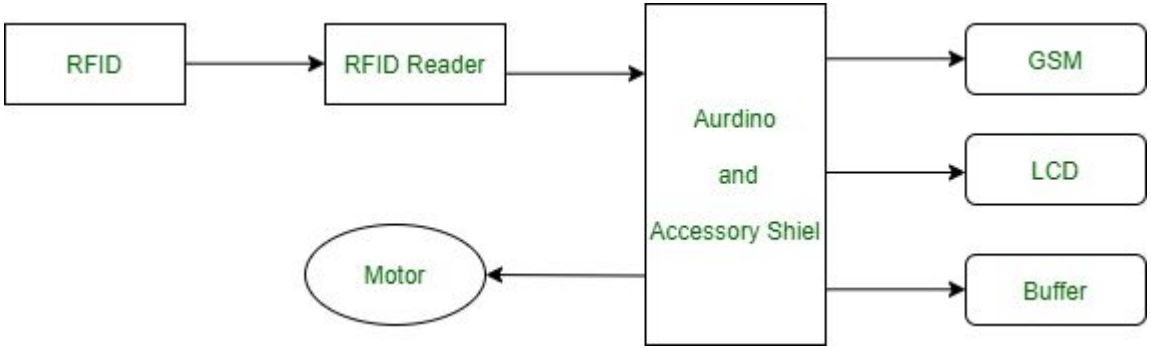
Types of RFID

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 125-134 KHZ as low frequency, 13.56MHZ as a high frequency and 856 MHZ to 960 MHZ 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

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



Applications of RFID

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

Advantages of RFID

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

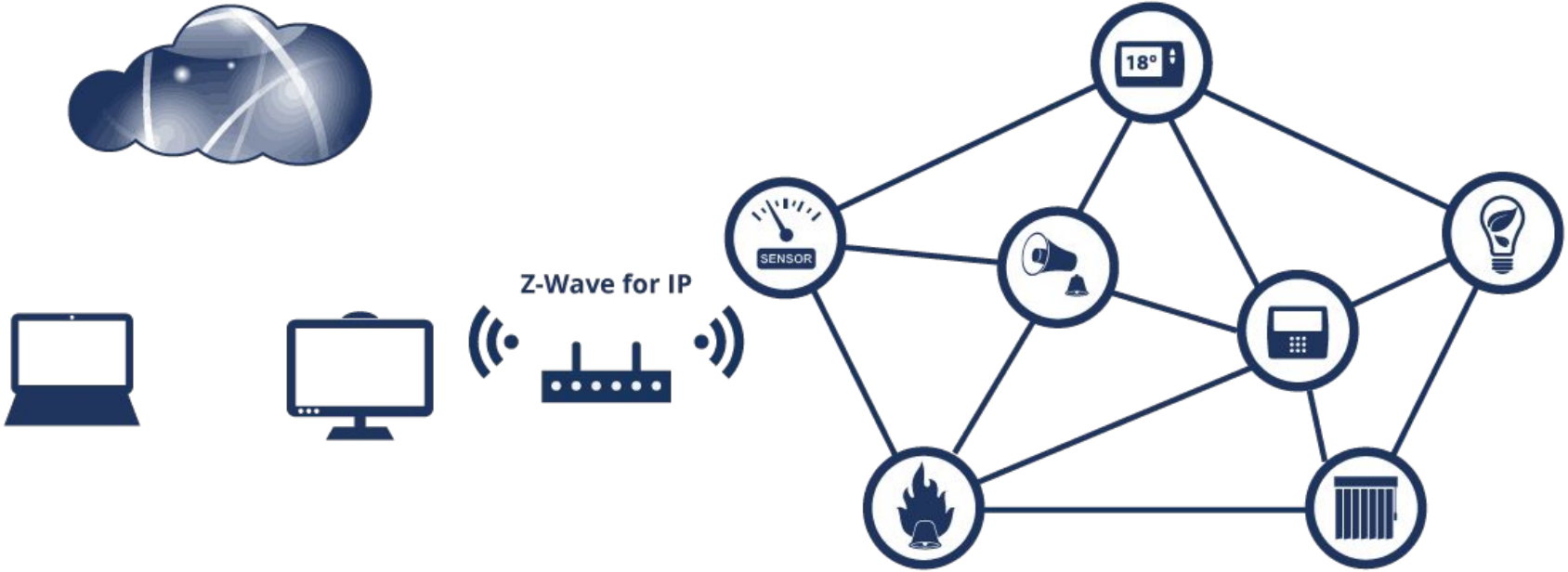
Disadvantages of RFID

1. It takes longer to program RFID Devices.
2. RFID intercepted easily even it is Encrypted.
3. In an RFID system, there are two or three layers of ordinary household foil to dam the radio wave.
4. There is privacy concern about RFID devices anybody can access information about anything.
5. Active RFID can costlier due to battery.

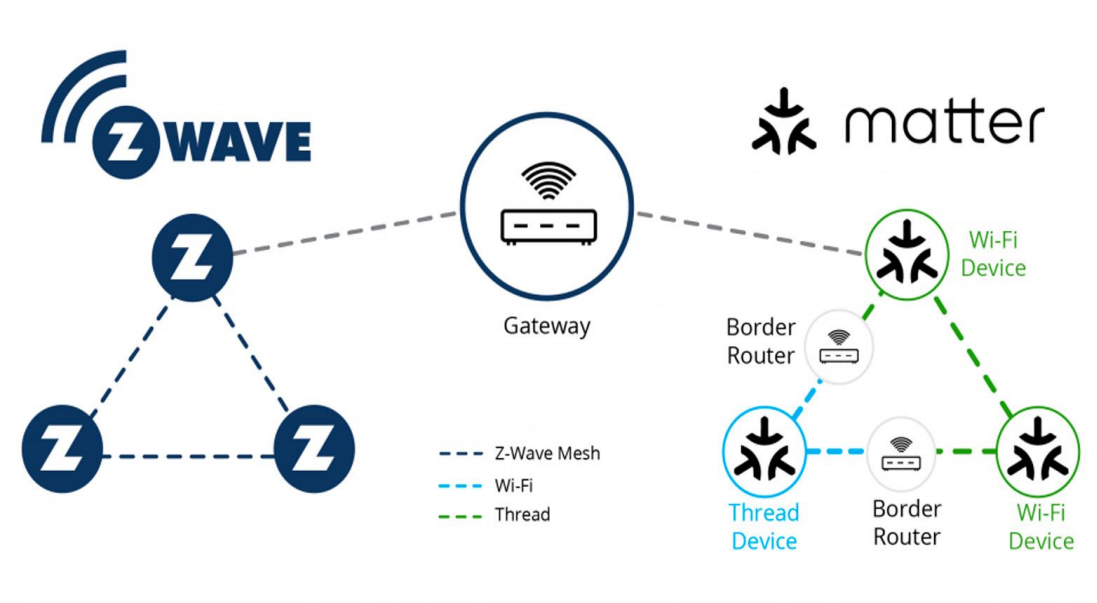
Z - Wave Protocol

1. It is a wireless communication protocol used by automatic or automotive appliances for the purpose of connection and communication.
2. It is invented in 1999 by Zensys a Danish-American company.
3. Zensys (later acquired by Sigma Designs) created the Z-Wave protocol, including its encryption. Open-zwave, an open-source version of the Z-Wave protocol stack, is also available, although it does not support the security layer.
4. It is primarily used in home automation technology. It has become a communications standard for the Internet of Things (IoT).

Z - Wave Protocol - Home Automation



Z - Wave Protocol - Home Automation



Advantages of Z - Wave

1. Mesh architecture allows users to centralise the entire network. All Z-Waves can be controlled from a phone application on the user's phone.
2. Z-Waves need significantly lower transmission power, ensuring lower power costs and longer battery life.
3. Any Z-Wave device must use AES 128 encryption, which means security is unbreakable, and a compromise is exceedingly unlikely.
4. Z-Wave uses the 900 MHz frequency spectrum to reduce interference and increase penetration.

Disadvantages of Z - Wave

1. Z-Wave frequency varies by region. As a result, gadgets that operate in one area of the world may not work in another.
2. Network maintenance is complex since the controller's network architecture must be replicated to all secondary units or nodes.

Future Scope of Z - Waves

1. With the acquisition of Z-Wave technology by Sigma Labs in 2018, Z-Waves have seen a massive increase in the scope of its applications.
2. Sigma Labs have merged Z-Waves with Insteon tech that can instantly detect Z-Waves and make processing it much faster.
3. The Z-Wave acquisition has also led to an increase in corporate partnerships that increased the adoption of the Z-Wave technology.
4. Companies like Amazon, Alarm.com, Comcast, ADT, Google Home and Samsung Smart Thing shave collaborated with Sigma Labs to innovate and expand the reach of the Z-Waves.