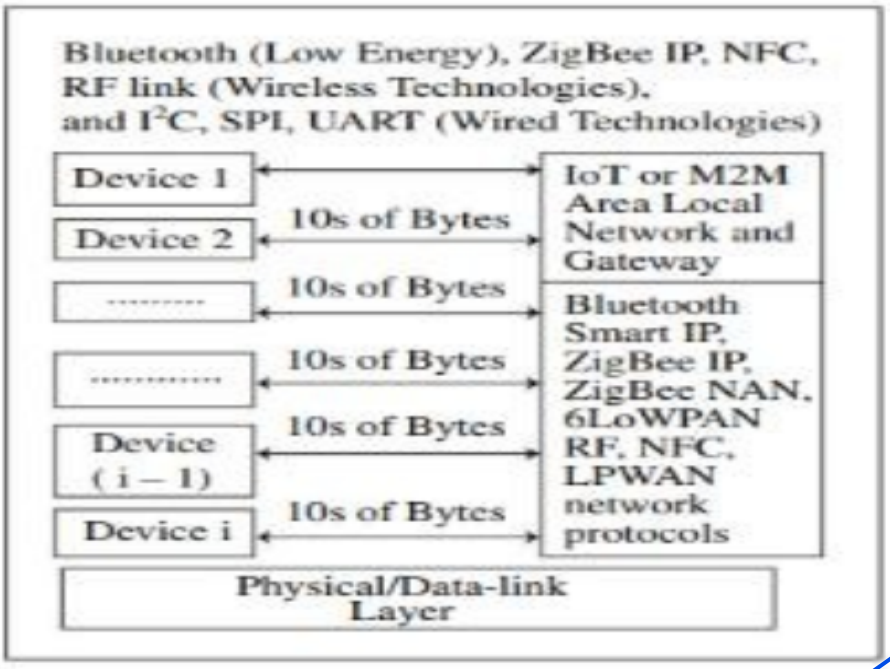
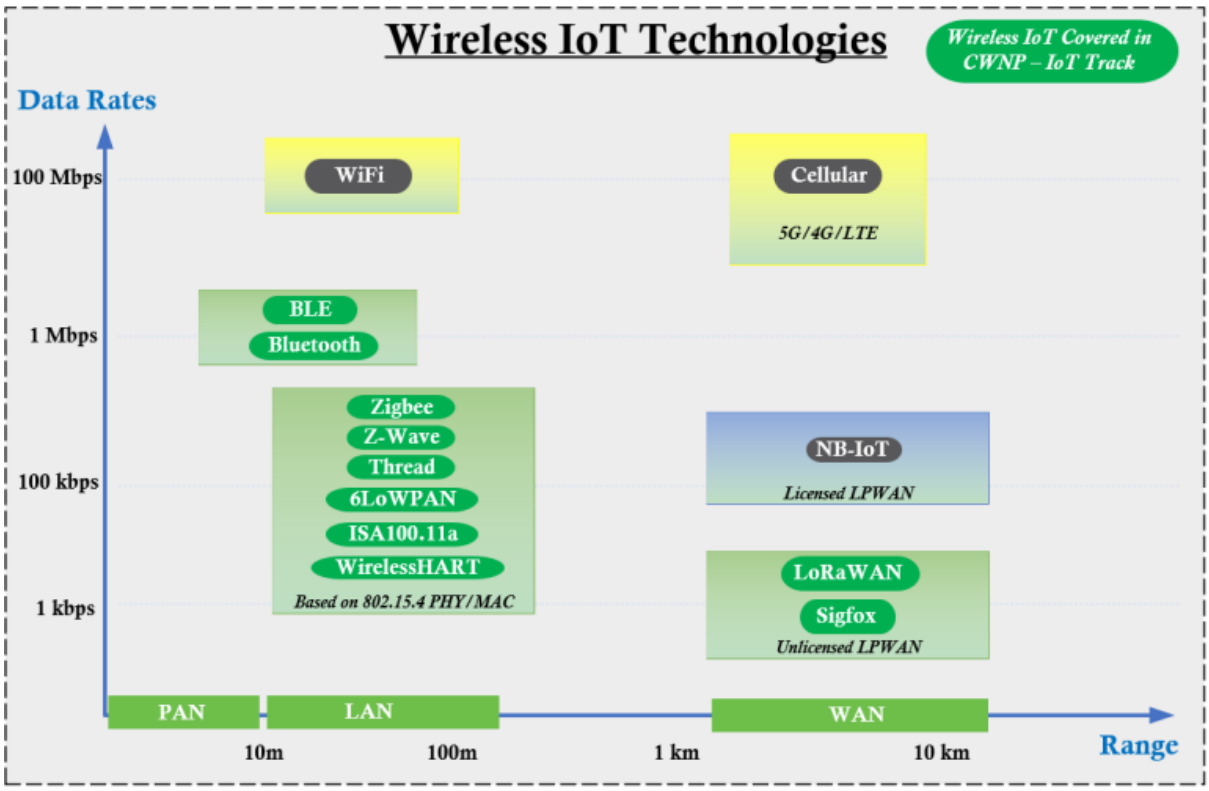
Communication Technologies

Physical cum data-link layer in the model consists of a local area network/personal area network. A local network of IoT or M2M device deploys one of the two types of technologies—wireless or wired communication technologies. The following figure shows connected devices (1st to ith) connectivity using different technologies for communication of data from and to devices to the local network connectivity to a gateway. It shows number of devices present in an IoT or M2M devices network. The figure shows the local area network of devices. The connectivity between the devices (left-hand side) is by using RF, Bluetooth Smart Energy, ZigBee IP, ZigBee NAN (neighbourhood area network), NFC or 6LoWPAN or mobile. Tens of bytes communicate at an instance between the device and local devices network.



\



Wireless Communication Technology for connected devices Near-Field communication (NFC):

NFC is a short distance (20 cm) wireless communication technology. It enables data exchange between cards in proximity and other devices. Examples of applications of NFC are proximity-card reader/RFID/IoT/M2M/mobile device, mobile payment wallet, electronic keys for car, house, office entry keys and biometric passport readers.

NFC devices transmit and receive data at the same instance and the setup time (time taken to start the communication) is 0.1 s. The device or its reader can generate RF fields for the nearby passive devices such as passive RFID. An NFC device can check RF field and detect collision of transmitted signals. The device can check collision when the received signal bits do not match with the transmitted signal bits.

Uses for Contactless Technology in the IoT

The long-range contactless technologies, referred to as **RFID**, are often used to track objects for logistics purposes. Their capabilities are often limited to transmitting a simple data, like a tracking or an ID code. On the other hand, **Near Field Communication** uses a different technology to communicate over a much shorter range, but with some interesting advantages.

Advantages of Near Field Communication in IoT Applications

NFC is a special type of contactless technology in the IoT because:

- It communicates over a very short range (0 - 5 cm) for security
- It is present in most iOS and Android mobile phones
- Users simply approach a mobile to a tag to connect (no codes, or addresses)

- An NFC tag is powered by the mobile phone during communication
- An NFC tag can harvest energy to power other circuits or devices
- An NFC tag can also execute its own software, process data, and communicate with other components.

Disadvantages –

- Low range.
- Expensive.
- Low speed.
- Less data transfer.

What are the Common Uses of NFC?

1. NFC Payments

- **Contactless payments:** NFC technology enables secure, NFC payments using smartphones and wearables.
- **Digital wallets:** Platforms like Google Pay and Apple Pay leverage NFC for seamless transactions.
- **Convenience and security:** Eliminates the need for physical cards and reduces the risk of card fraud.

2. Data Sharing

- **Nearby Share:** Android's Nearby Share feature, while not strictly NFC-based, utilizes NFC for initial connection and then switches to Bluetooth or Wi-Fi Direct for data transfer.
- **Content sharing:** Allows users to easily share files, images, or other content between NFC-enabled devices.

3. Smart Posters and Marketing

- **Interactive experiences:** NFC tags embedded in posters, packaging, or physical media can trigger actions when tapped by NFC-enabled devices.
- **Enhanced engagement:** Provides a more interactive way for brands to connect with consumers.

4. Public Transportation

- **Streamlined fare payment:** NFC-enabled smartphones or wearables can be used to tap in and out of public transportation systems.
- **Elimination of physical tickets:** Reduces the need for paper tickets or passes, providing a more efficient and environmentally friendly experience.

5. Access Control

- **Contactless authentication:** NFC technology offers secure access to buildings, events, and restricted areas.
- **Enhanced security:** Provides a more convenient and secure alternative to traditional access control methods.
- **Data tracking:** Can capture information such as time, location, and duration of access for security management.

6. NFC Business Cards

- **Digital exchange:** NFC-enabled business cards allow for quick and easy exchange of contact information.
- **Enhanced engagement:** Provides a more interactive and memorable way to network.

7. Automate Sleep Mode with NFC

- **Proximity-based activation:** NFC tags can be used to automatically activate or deactivate sleep mode on devices when they are placed in specific locations.
- **Enhanced battery life:** Helps conserve battery power by automatically activating sleep mode when the device is not in use.

8. Bluetooth Pairing Information

- **Simplified pairing:** NFC can be used to initiate Bluetooth pairing between devices, streamlining the process.

9. Connect/Disconnect Wi-Fi

- **Automated network switching:** NFC tags can be used to automatically connect or disconnect devices from Wi-Fi networks based on location or other criteria.

10. Program NFC Tags

- **Customizable functionality:** NFC tags can be programmed to perform various tasks, such as opening URLs, launching apps, or providing specific information.
- **Versatile applications:** Can be used in various industries and scenarios, from retail to manufacturing.

11. Authentication

- **Secure access control:** NFC technology can be used for authentication purposes, such as verifying identity or granting access to restricted areas.
- **Enhanced security:** Provides a more secure alternative to traditional authentication methods.

12. Automate Common Phone Tasks:

- **Task automation:** NFC tags can be used to automate common phone tasks, such as launching specific apps, sending messages, or making calls.
- **Increased efficiency:** Simplifies everyday tasks and improves productivity.

RFID (Radio Frequency Identification System)

It is the technology that uses electromagnetic waves to capture digital data and to identify or track the tags. It consists of a transponder(tags), a reader, and an antenna. There are mainly two types of tags active and passive. The passive tags lack computational capacity whereas active tags can sense channels easily.

The reader consists of an interrogator or a transceiver that sends signals which activate the tags. The antenna is used for transmitting and receiving the data. It has various applications in agricultural sectors, defence, tracking, cashless transaction, etc.

It is a technology used for automatically identifying and recording data about an object via a tiny, uniquely identifiable microchip tag connected to the object. A built-in antenna on the RFID tag interacts with a scanning device that can remotely read the tag's data.

The scanning device scans the tag when it comes in range. After that, the data is sent from the scanning equipment to an application program. With the help of the application, the user will store and send it wherever he desires.

Working of RFID

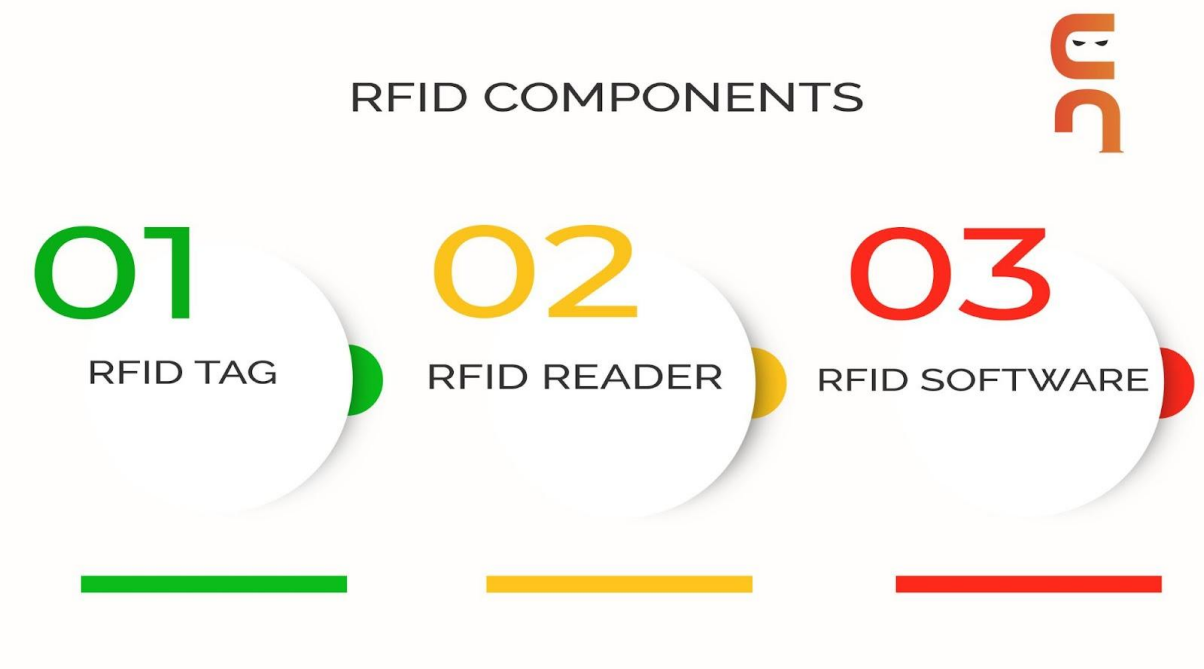
RFID, or radio frequency identification, is a technique for automatically identifying and capturing data about an object that has been stored in a small microchip tag attached to the object. An antenna built into the RFID tag communicates with a scanning device that reads the data remotely.

This data is then transferred from the scanning device to the data-housing enterprise application software. Each RFID tag has a unique identification number.

RFID can be used to track and control asset and personnel movement. RFID tags can be found on the back of library books and even in the new biometric passports. It simplifies the management of assets contained in boxes or pallets.

Components of RFID

Radio Frequency Identification technology consists of three main components:



1. **The RFID tag**: The RFID tag comprises an integrated circuit, a substrate, and an antenna. If the tag has an active power source and thus can support a sensor, it is called an active RFID tag. If the tag doesn't have an active power source, it is called a passive RFID tag.

2. **The RFID reader:** It is a device that reads RFID tags and gathers data about the connected object. It can be both wired and wireless. It can use many technologies to communicate with the software, including USBs and Bluetooth connections.

3. **The RFID software**: The software monitors and tracks the object connected to the RFID tags. It can be called data exchange and management software.

Advantages-

- Multiple usages at a time.
- Durable also.
- Much secure than barcodes.

Disadvantages-

- High cost.
- Metals used may create interference of the signal.
- Overhead reading.

Applications of RFID in IoT

- RFID has seen applications since the 1940s when they were first introduced. Its use rapidly increased to mainstream levels during the 70s. With the rise of IoT, it has threatened barcodes and NFCs as the most efficient technology to identify and track objects, livestock and humans uniquely.

- RFID tags are useful in cameras, GPS, and other smart sensors when utilised in the IoT. They can help with identifying and locating items. It's a low-cost approach to make household items seem "smart", as many companies are now entering the smart home market.

- Healthcare institutions also use RFID tags to track patients and their medical information. They are being used in transportation systems to read passenger data, regulate traffic, and update transportation systems.

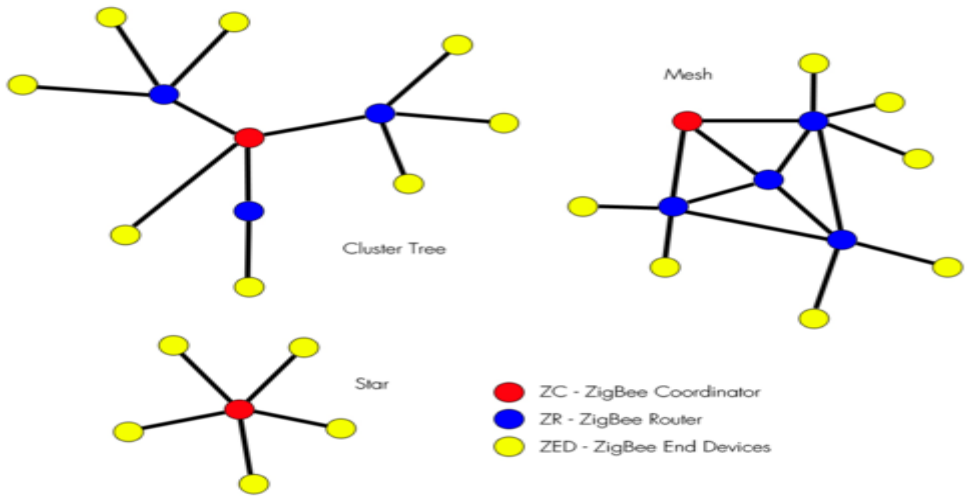
ZigBee

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.

IEEE 802.15.4 supports star and peer-to-peer topologies. The ZigBee specification supports star and two kinds of peer-to-peer topologies, mesh and cluster tree. ZigBee-compliant devices are sometimes specified as supporting point-to-point and point-to-multipoint topologies.

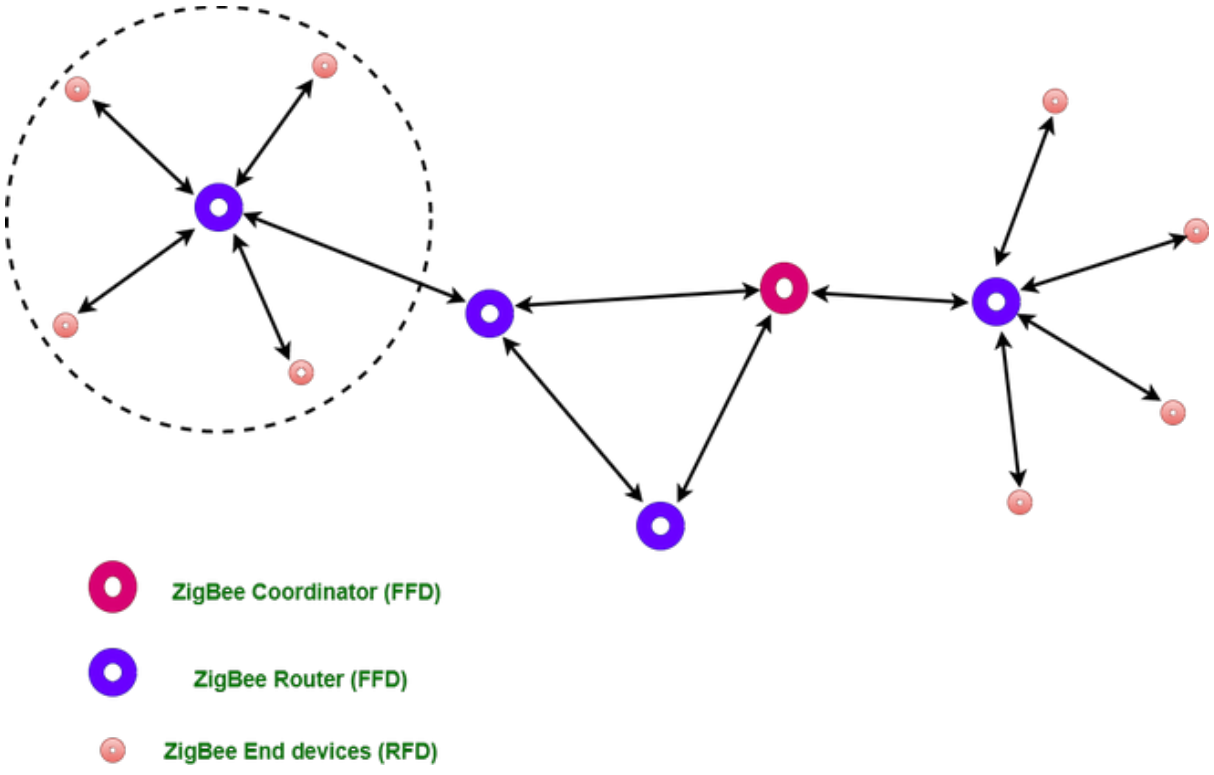
Zigbee network topologies



Why another short-range communication standard??

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.
-

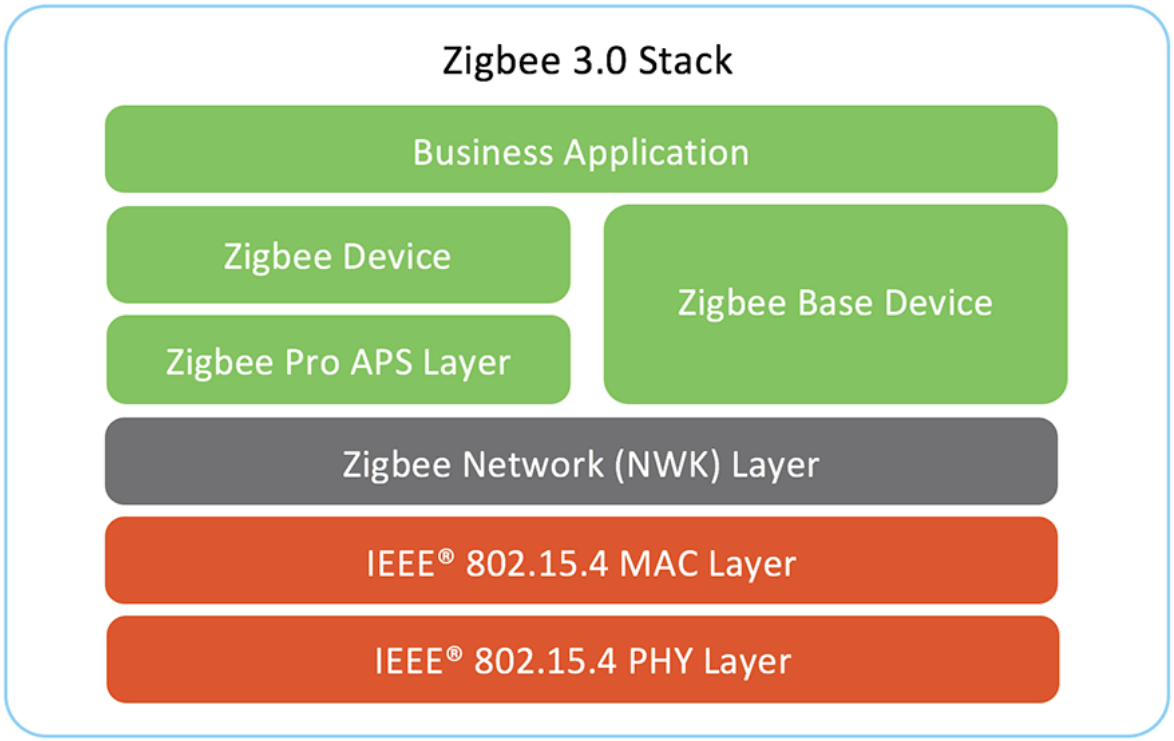


- **Zigbee Coordinator (ZC)** - This will typically be the Smart Home Controller (sometimes referred to as a hub, gateway or bridge). Its job is to establish the network itself, setup and maintain security, add devices to the network and manage communications between them. There can be only one Coordinator in the Zigbee network and it must be permanently powered.

- **Zigbee Router (ZR)** - Zigbee routers are permanently powered mains devices and these provide the back-bone of the Zigbee network. They direct communications between devices to create a literal route from one device to another. There can be many Routers within the Zigbee network and these are typically Smart Devices such as light bulbs, sockets, plugs, light switches and appliance modules - usually any Zigbee device that is AC mains powered.

- **Zigbee End Device (ZED)** - End Devices are the most basic device on the network, they can only send or receive data, they can't carry out routing tasks. This means they can only communicate with Zigbee Routers or direct to the Zigbee Coordinator. End Devices are usually battery powered and are typically Smart Devices such as motion sensors, door sensors, temperature sensors and door locks.

Zigbee devices seamlessly form a mesh network, enabling efficient data backhaul through a central node connected to a gateway for remote Internet access. A Zigbee app allows a user to control smart devices from anywhere. Zigbee is built on the Physical layer and Medium Access Control sub-layer defined in the IEEE 802.15.4 standard which manages low-level network operations. The Zigbee Network layer manages the network structure, routing and security. The application layer includes the Application Support sub-layer, the Zigbee device objects and user-defined applications.



Common Wireless Applications for Zigbee

With low latency and support for many devices, Zigbee works well for home automation, industrial control, and sensor networks. Zigbee can also cost less for manufacturers to build with because there are no license fees or royalties. Here are some prominent use cases:

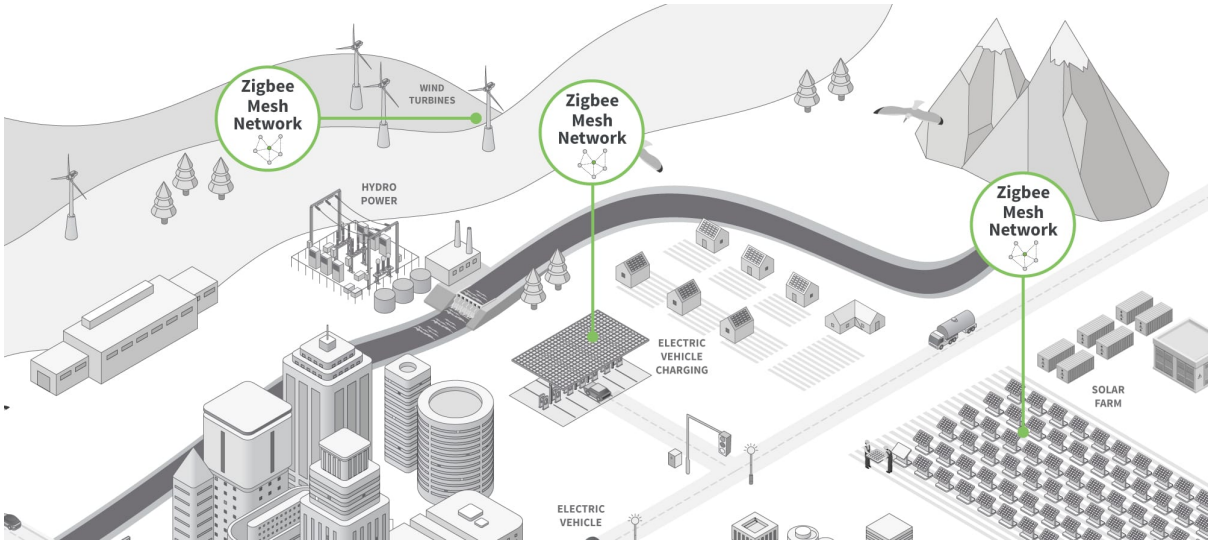
Green tech applications - Zigbee mesh is an excellent choice for green technology applications such as solar and wind farms and EV charging networks.

Smart home - In a smart home, a Zigbee network can control lights, door locks, smoke detectors, fans, appliances and more. In fact, Zigbee is employed by most large smart home ecosystem providers, including the Amazon Echo Plus, Samsung SmartThings and Signify (formerly Philips Lighting). Worldwide, there are hundreds of millions of Zigbee products in smart homes and buildings.

Smart energy - Zigbee devices built to Zigbee Pro 2023 specifications can now share the same network as Smart Energy devices to improve the control and use of these devices.

Medical - In a medical scenario, a patient can wear sensors that collect and communicate vitals such as heart rate, blood pressure and blood glucose levels wirelessly to a hospital.

Industrial automation - Inside a building, Zigbee can be used to automate lighting control, HVAC, security and access control systems.



What Devices Use Zigbee?

There are thousands of devices from hundreds of different manufacturers using Zigbee so you can be sure that there's a high likelihood of finding a device to suit most requirements.

Garage door controls, locks, lights, motion sensors, door sensors, smoke detectors, thermostats, remote controls, sirens and appliances are all covered extensively.

Backed by some of the worlds biggest companies, including Philips, Nest, Samsung, Texas, Siemens & Whirlpool, Zigbee technology is currently being built into millions of Smart Home Devices worldwide. Lights, thermostats, alarms, fridges, doors, appliances, utility meters - all are being Zigbee enabled.

Recently the likes of Amazon, Apple and Google have all begun to integrate Zigbee into their Smart Speakers and Smart Screens too!

Pros:

- Very low power consumption, ideal for battery-powered devices.
- Mesh networking capability allows devices to relay data through each other to extend the range.
- Designed for low data rate and intermittent communication.
- Good security features.

Cons:

- The limited data rate (up to 250 kbps) is unsuitable for high-bandwidth applications.
- Relatively short range (10-100 meters, depending on conditions).
- Requires a Zigbee hub or gateway for internet connectivity.

LoRaWAN (Long Range Wide Area Network)

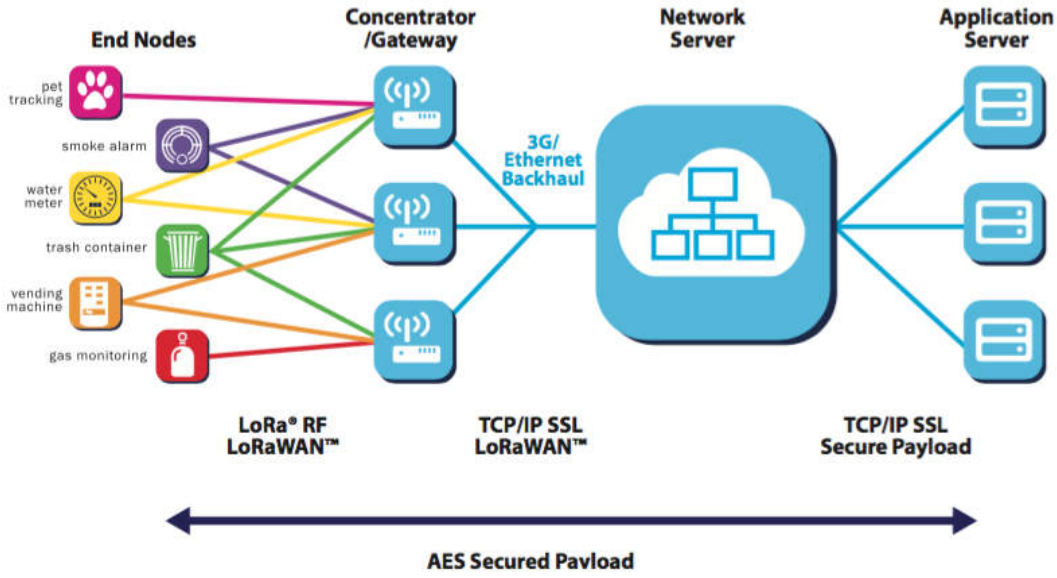
Long Range Wide Area Network helps define communication protocol as well as system architecture. It is a point to the multipoint communication network. acts as a gateway that does encryption as well as identification. It has a wide range of applications like smart cities, smart industrial control, home security systems, etc.

LoRaWAN technology consists of a low-power, wide-area network protocol built onto LoRa modulation useful for securing dependable bi-directional IoT communications. The LoRaWAN protocol provides end-to-end encryption to deliver advanced security features at scale. With LoRaWAN ranges reaching up to ten miles, this technology supplies a more economical choice compared to cellular technologies in remote areas.

How LoRa and LoRaWAN Work in IoT

In LoRa modulation, a chirp signal spreads the signal spectrum. By increasing the chirp rate, the signal spreads over a range of frequencies allowing it to travel farther without error. As a result, the LoRa communication protocol resists signal interference. This makes LoRa especially useful for urban and suburban areas where signal interference happens frequently.

LoRaWAN Architecture



- **End Devices** - sensors or actuators send LoRa modulated wireless messages to the gateways or receive messages wirelessly back from the gateways. .
- **Gateways** - receive messages from end devices and forward them to the Network Server.
- **Network Server** - a piece of software running on a server that manages the entire network.
- **Application servers** - a piece of software running on a server that is responsible for securely processing application data.

The interplay between these components forms a cohesive and dynamic system. Data collected by End-Devices is transmitted to nearby Gateways, which then forward this information to the Network Server. The Network Server filters and routes these data packets to the relevant Application Servers. This streamlined flow allows for efficient management of data and resources across vast networks, enabling IoT devices to function seamlessly across large distances without compromising on battery life or data integrity.

Common Applications for Long Range Communication

LoRa technology provides a unique combination of qualities that add utility and value to a broad array of industries and sectors. From agriculture and manufacturing to environmental monitoring and logistics, the combination of secure, scalable, low-cost networks provides bi-directional communication across many different environments.

- **Smart agriculture:** Getting data from sensors attached to fields and animals means farmers can act quickly to identify and correct pests and diseases
- **Smart buildings:** Smart meters inside buildings help managers optimize lighting and temperature management and reduce energy usage
- **Industrial IoT:** Machinery monitoring, safety alerts and asset tracking allow operators to respond more quickly to or even in advance of an incident.

- **Manufacturing:** Manufacturers prize LoRa technology for its ability to enable predictive maintenance across many factories
- **Logistics:** LoRaWAN provides the perfect balance of numerous sensor communications in places such as warehouses and equipment yards without radio frequency interference issues
- **Environmental monitoring:** Combined with satellite communications, LoRaWAN provides sensor monitoring for everything from smoke detection in remote forests to ocean temperatures on buoys
- **Oil and gas:** To meet regulatory requirements, oil and gas companies use LoRaWAN technology to monitor emissions from well operations

Classes of Devices:

  - Class A: Bidirectional communication where devices have scheduled receive windows after sending data.All LoRaWAN end-devices must support Class A implementation. A Class A device can send an uplink message at any time. Once the uplink transmission is completed, the device opens two short receive windows for receiving downlink messages from the network.
  - Class B: Adds synchronized receive windows at scheduled times in addition to Class A capabilities. Class B devices extend Class A capabilities by periodically opening receive windows called **ping slots** to receive downlink messages. The battery life is shorter in Class B compared to Class A because the devices spend more time in active mode due to receiving beacons and having open ping slots.
  - Class C: Continuous listening for downlink messages except when transmitting. Class C devices can receive downlink messages at almost any time, thus having very low latency for downlinks. These downlink messages can be used to activate certain functions of a device, such as reducing the brightness of a street light or turning on the cut-off valve of a water meter.

Compared to Class A and Class B devices, Class C devices have the lowest latency. However, they consume more power due to the need for opening continuous receive slots. As a result, these devices cannot be operated with batteries for long time therefore they are often mains powered.

Pros:

- Very long range (up to 15-20 kilometers in rural areas).
- Extremely low power consumption, enabling years of operation on a single battery.
- Suitable for environments with limited infrastructure (e.g., rural areas).
- Good scalability, capable of supporting thousands of devices.

Cons:

- Low data rate (up to 50 kbps), making it unsuitable for high-bandwidth applications.
- Typically, it requires a gateway for internet access.

- Limited interoperability with other networks.

IEEE 802.15.4(LR-WPANs) Technology

IEEE 802.15.4 is a low-cost, low-data-rate wireless access technology for devices that are operated or work on batteries. This describes how low-rate wireless personal area networks (LR-WPANs) function.

IEEE 802.15.4 is a wireless networking technology that provides the technical specifications for low-rate wireless personal area networks (LR-WPANs), allowing networked devices to communicate with one another in a variety of industrial and commercial settings, including healthcare, environmental monitoring, smart energy, home automation, and more.

Low power wide area networks (LPWAN) provide long-range communication using small, inexpensive batteries. This family of technologies is ideal for supporting large-scale IoT networks where a significant range is required. However, LPWANs can only send small blocks of data at a low rate.

LPWANs are ideally suited for use cases that don't require time sensitivity or high bandwidth, like a water meter for example. They can be quite effective for asset tracking in a manufacturing facility, facility management, and environmental monitoring. Keep in mind that standardization is important to ensure the network's security, interoperability, and reliability.

Definition and key features

IEEE 802.15.4 is a wireless networking standard developed for low-power, low-data-rate applications in Personal Area Networks (PANs) for IoT, embedded systems, and wireless sensor networks. It is known for its low power consumption, extended battery life, mesh networking capabilities, and cost-effectiveness. This RF-based technology operates on various frequencies such as 2.4 GHz band while supporting data transmission rates up to a maximum of 250 kbps. IEEE 802.15.4 also offers robust network security using encryption methods like Advanced Encryption Standard (AES) to ensure secure communication between connected devices within a PAN ecosystem.

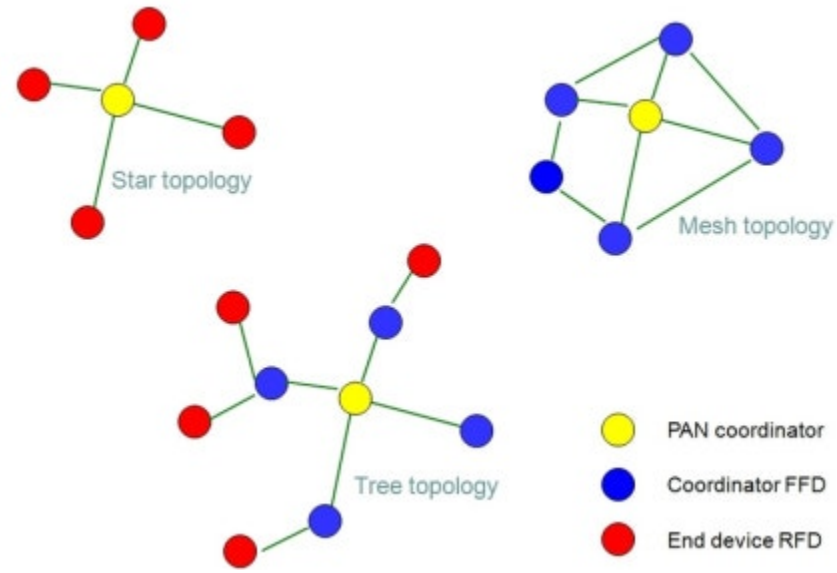
Basic architecture and network topology

The IEEE 802.15.4 technology's basic architecture consists of three layers, including the physical layer, media access control (MAC) layer, and networking layer. Mesh and star network topologies are used to connect devices. Mesh topology enables direct communication between devices without the need for a central hub or node, while star topology has all devices communicate with a central node. The technology offers versatile options for designing networks based on specific requirements and constraints of various applications such as industrial automation, healthcare monitoring systems, smart homes, and environmental monitoring systems, while keeping low-power consumption costs in mind due to their energy-efficient features.

Types of devices in IEEE 802.15.4 Technology

IEEE 802.15.4 technology includes various types of devices that can be used for wireless communication and networking. These devices are −

- **Coordinator** − This device is responsible for initiating the PAN (Personal Area Network) and managing the network.
- **Full Function Device (FFD)** − This device has the ability to act as a coordinator or a router, and can also host other devices.
- **Reduced Function Device (RFD)** − A device that can only communicate with FFDs, but not capable of hosting other devices or working as a coordinator.



Pros:

- Very long range (up to 15-20 kilometers in rural areas).
- Extremely low power consumption, enabling years of operation on a single battery.
- Suitable for environments with limited infrastructure (e.g., rural areas).
- Good scalability, capable of supporting thousands of devices.

Cons:

- Low data rate (up to 50 kbps), making it unsuitable for high-bandwidth applications.
- Typically, it requires a gateway for internet access.
- Limited interoperability with other networks.

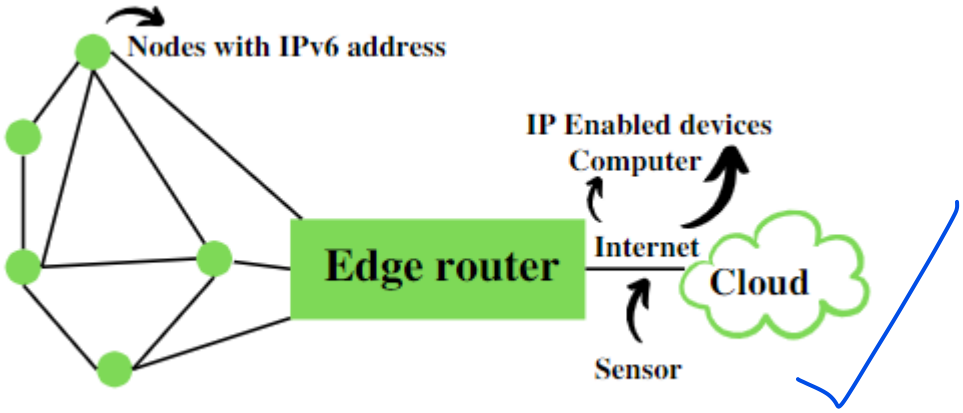
Applications:

- Agricultural IoT (e.g., soil moisture sensors, livestock monitoring).
- Smart cities (e.g., parking sensors, waste management).
- Environmental monitoring (e.g., air quality sensors, flood detection)

6LoWPAN

IPv6 over Low Power Personal Area Network or 6LoWPAN is an IP-Also Based protocol that ensures connectivity of even low data rate networks. It ensures that even the smallest or low power device should be a part of IoT. It helps provide end-to-end IP and is widely used in home automation systems.

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 minimal 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.



Core Elements: Building Blocks of the Network

A typical 6LoWPAN network consists of several key players working in concert:

- **6LoWPAN Devices:** These are the heart of the network, encompassing various resource-constrained devices with limited power budgets. Examples include sensors, actuators, wearables, and smart home appliances. These devices can be further categorized as:
    - **Hosts (End Devices):** These devices primarily collect or transmit data and lack the capability to route it for other devices. They operate in a low-power mode, periodically waking up to exchange data with the router.
    - **Routers:** As the name suggests, these devices route data packets within the 6LoWPAN network, ensuring it reaches the intended recipient. Routers typically have more processing power and battery capacity compared to hosts.
- **Edge Router:** This is the bridge between the 6LoWPAN network and the wider internet (or other IPv6 networks). It performs three crucial functions:
    - **Data Exchange:** It facilitates the exchange of data between devices within the 6LoWPAN network and the internet or other external networks.

    - **Local Data Routing:** It handles the routing of data packets between devices solely within the 6LoWPAN network.
    - **Radio Subnet Management:** It oversees the creation and maintenance of the 6LoWPAN network, which acts as a radio subnet within the broader network infrastructure.
- **Access Point (AP):** While not directly part of the 6LoWPAN network itself, the AP serves as the connection point for devices within the broader network, typically including PCs, servers, and other internet-connected devices. The AP often functions as an IPv6 router, facilitating communication between these devices and the internet.

Basic Requirements of 6LoWPAN

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

Features of 6LoWPAN

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

Applications of 6LoWPAN

Smart Homes:

When implemented in home settings, for instance, 6LoWPAN effectively links smart thermostats, light sensors, and security systems so that all the home's operations can be controlled from a distance using applications, and voice commands.

Industrial Automation:

In manufacturing industries, 6LoWPAN allows various sensors and control devices that govern equipment within factories to be connected, and effective management of such equipment is enhanced by monitoring and predictive maintenance applications.

Agriculture:

In **smart irrigation using IoT** and farming, 6LoWPAN can facilitate the placement of habilitating sensors that measure aspects of the environment that may include moisture and temperature of the soil for purposes of determining the best farming practices to use.

Smart Cities:

6LoWPAN in IoT involves low-energy solutions with a connection at scale, thereby making it particularly suitable for use in urban environments where traffic lights, public transport informing, and environmental sensors are put to use.

Advantages of 6LoWPAN over Alternative Solutions

Several network architectures cater to low-power wireless communication, but 6LoWPAN offers distinct advantages:

- **Native IP Communication:** 6LoWPAN leverages the well-established IPv6 protocol, allowing direct communication with internet devices without complex gateways. This simplifies network integration and management.
- **Scalability:** 6LoWPAN networks are inherently scalable, readily accommodating a large number of devices within a limited range. This is crucial for large-scale IoT deployments.
- **Security:** By utilizing the security features of IPv6, 6LoWPAN offers robust security mechanisms to protect data within the network.
- **Reduced Processing Power:** The edge router handles the heavy lifting of data translation and routing, freeing up resources on the resource-constrained devices within the 6LoWPAN network. This allows for simpler and more energy-efficient devices.

NBIOT

The Internet of Things enables applications to connect and communicate with large numbers of wireless communication devices. It promises to power smart cities, utilities, manufacturing facilities, agricultural applications, remote industrial machinery and more. Any of these applications may use Narrowband Internet of Things (NB-IoT) network protocols.

For example, a smart city might use NB-IoT to monitor street lighting, utility meters and waste management systems across its municipality. A solar or wind farm could use Narrowband IoT (NB-IoT) to monitor each of the units across the deployment. Industrial

operations may rely on NB-IoT to remotely monitor all machines across distributed sites.

NB-IoT stands for narrowband IoT. It is a low-power wide-area network (LPWAN) technology deployed on cellular networks over a limited range of frequencies. For IoT applications that don't require lots of data communications or high-speed transmission and need to transmit over long distances, NB-IoT might fit your needs.

It can even send data indoors and underground while using very little battery power. This means it is a scalable, cost-effective and energy-efficient network option for devices even if they aren't connected to the Internet.

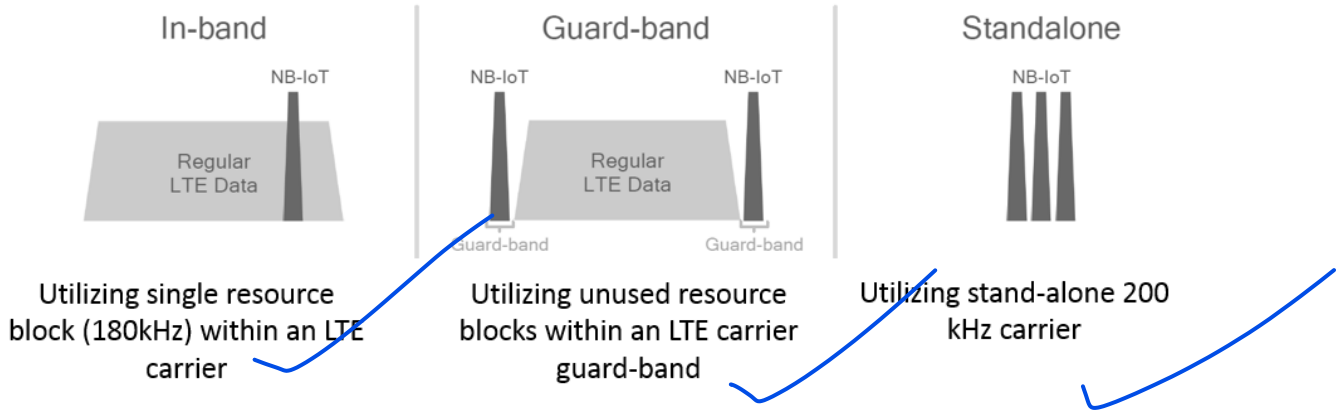
Energy efficiency is an important aspect of NB-IoT. The NB-IoT protocol was designed from the ground up to power ultra-low power devices for a very long span of time. This means that expensive batteries for massive numbers of devices won't need to be recharged or replaced very often.

How Does Narrowband IoT Work?

LTE and NB-IoT pair well together.

Deploying Narrowband IoT Technology

- **In-band** — Uses resource blocks in a normal LTE carrier
- **Guard band** — Uses unused resource blocks within an LTE carrier
- **Standalone** — Spectrum currently used by GSM EDGE Radio Access Network systems in place of GSM carriers when cellular services are not available



Important Industrial Narrowband Examples

- **Remote asset tracking** — Businesses can use NB-IoT to remotely trace, track, and monitor assets and receive status updates
- **Sustainable agriculture** — From moisture and pressure sensors to pH sensors, NB-IoT efficiently and cost-effectively help farmers continuously monitor and alert when soil conditions change
- **Smart vending** — NB-IoT-equipped smart vending machines alert service providers about empty vending machine items
- **Gas leak detection** — NB-IoT works perfectly for continuous monitoring of air quality and automatically sends alerts when levels surpass thresholds

NB-IoT Applications and Use Cases

- Smart Metering

NB-IoT can be utilized in the employment of advanced metering infrastructure, which enables two-way communication between the meter and the user, without the involvement of the physical presence of a monitor. NB-IoT can facilitate direct controlling and monitoring of devices from any specific location as per the convenience of the owner of the equipment.

- Smart Cities

The scope of NB-IoT is unlimited when the application involves smart cities. From Automatic Street Lighting to Smart Waste Management to Smart Parking, the opportunities opened up to employ NB-IoT are innumerous. Other applications include connected emergency services, weather monitoring, and traffic monitoring.

- Smart Homes And Commercial Properties

NB-IoT can be connected to sensors that are designed to alert the users whenever there are disruptions in the optimally set parameters, like access control & identity management, room temperature, smoke detectors, lighting controls, oxygen levels in confined rooms, intruder alerts, and fire alarms.

- Healthcare/E-health

NB-IoT technology can materialize the idea of connected personal appliances that measure health parameters. These appliances, mostly in the form of wearables, are proving to be a great boon for the elderly, who require constant monitoring of their health parameters. NB-IoT is the most reliable and feasible option when parameters such as Blood Pressure and Heart rate are to be measured and analyzed at regular intervals.

- Industries

NB-IoT as an underlying technology is used in industrial appliances ranging from precision farming tools in the agriculture sector to smart shelves in the connected retail sector. NB-IoT enables automation in manufacturing and real-time monitoring of equipment. This technology's advanced performance can enable factories and warehouses to achieve efficient integration of processes and equipment through real-time decision making and enhanced efficiency.

Bluetooth and BLE (Bluetooth Low Energy)

Another well-known wireless technology in consumer circles is Bluetooth. This wireless personal area network (WPAN) is a short-range communication technology with optimization

for power consumption (**Bluetooth Low Energy**) positioned to support small-scale consumer IoT applications.

Bluetooth and BLE are used for everything from fitness and medical wearables like smartwatches to smart home devices like home security systems, where data is communicated to smartphones. They work quite effectively with very short-range communications.

It is the most common wireless technology used for short-range communication. Device to device file transfer, wireless speakers, earphones, headsets can be some of the applications of Bluetooth. It is the best alternative for cables used to connect printers, fax, keyboard, etc. The PAN (Personal Area Network) Also Based Bluetooth technology in Fitness Trackers, smartwatches, home automation devices are much used these days. It works with operating systems like Android, IOs, windows, etc.

Key Features of Bluetooth

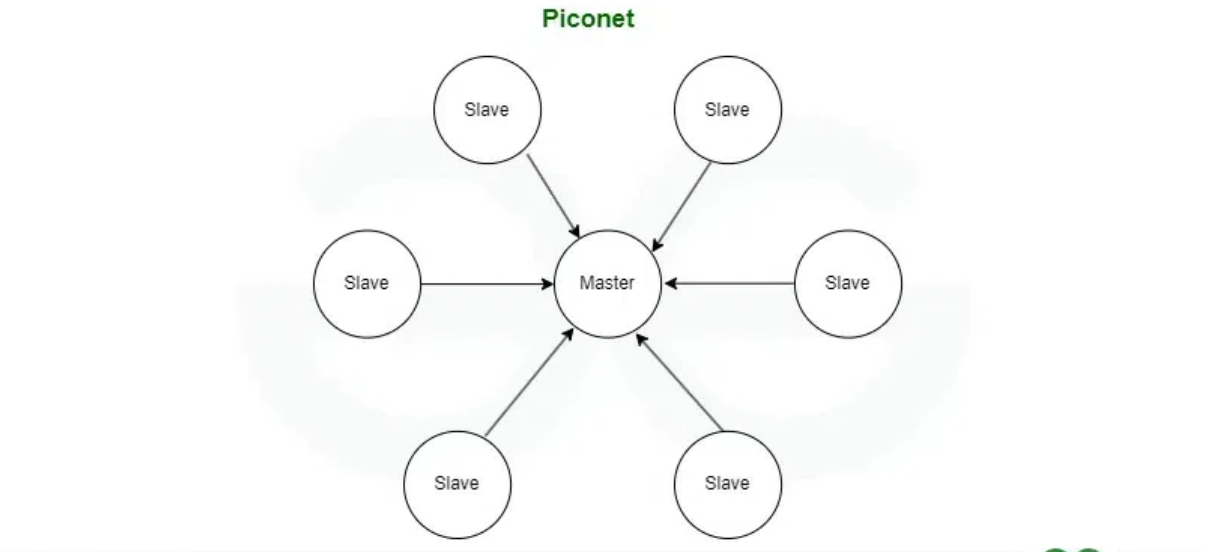
- The transmission capacity of Bluetooth is 720 kbps.
- Bluetooth is a wireless technology.
- Bluetooth is a Low-cost and short-distance radio communications standard.
- Bluetooth is robust and flexible.
- The basic architecture unit of Bluetooth is a piconet.

Architecture of Bluetooth

The architecture of Bluetooth defines two types of networks:

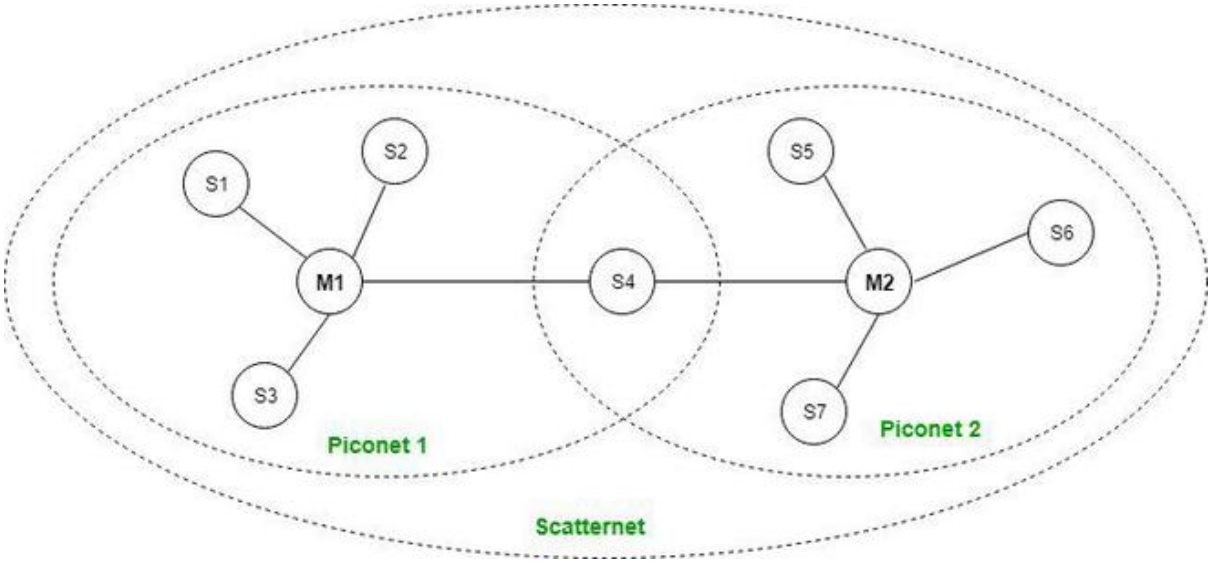
Piconet

Piconet is a type of Bluetooth network that contains one primary node called the master node and seven active secondary nodes called slave nodes. Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also has 255 parked nodes, these are secondary nodes and cannot take participation in communication unless it gets converted to the active state.



Scatternet

It is formed by using various piconets. A slave that is present in one piconet can act as master or we can say primary in another piconet. This kind of node can receive a message from a master in one piconet and deliver the message to its slave in the other piconet where it is acting as a master. This type of node is referred to as a bridge node. A station cannot be mastered in two piconets.



Types of Bluetooth

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

- **In-Car Headset:** One can make calls from the car speaker system without the use of mobile phones.
- **Stereo Headset:** To listen to music in car or in music players at home.
- **Webcam:** One can link the camera with the help of Bluetooth with their laptop or phone.

- **Bluetooth-Equipped Printer:** The printer can be used when connected via Bluetooth with mobile phone or laptop.
- **Bluetooth Global Positioning System (GPS):** To use Global Positioning System (GPS) in cars, one can connect their phone with car system via Bluetooth to fetch the directions of the address.

Applications of Bluetooth

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

Advantages

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

Disadvantages

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

Wi-Fi(Wireless Fidelity)

Wireless Fidelity is one of the most hassle-free and fast wireless communication technology. It is the choice of many developers due to its various advantages. It allows access to the internet as well as to connect devices in a specific range. Personal computers, smartphones, laptops, printers, and cars use this protocol.

Wi-Fi relies on IEEE 802.11 standards, which define the specifications for wireless communication. Devices communicate through a wireless access point (AP) or router, which acts as a bridge to the wired network or the Internet. Wi-Fi utilizes various modulation techniques, like OFDM (Orthogonal Frequency-Division Multiplexing), to efficiently transmit data, while security protocols such as WPA3 (Wi-Fi Protected Access) ensure encrypted communication.

Pros:

- High data rates (up to gigabit speeds with newer standards like Wi-Fi 6).
- Widely available with extensive infrastructure support.

- Secure, with support for strong encryption (WPA3).
- Suitable for devices requiring constant, high-bandwidth connections (e.g., video streaming).

Cons:

- High power consumption, making it less ideal for battery-operated IoT devices.
- Limited range (typically 50-100 meters indoors).
- Network congestion in densely populated areas can reduce performance.

Applications:

- Smart home devices (e.g., smart thermostats, security cameras).
- Industrial IoT for real-time monitoring (e.g., factory automation systems).
- Connected appliances and entertainment systems.

Wired Communication Protocols In IoT

Communication protocols are of two types: –

1. External system protocols:- USB, UART, Ethernet.
2. Internal system protocols:- I2C, SPI.

EXTERNAL SYSTEM

External system protocols are used to communicate between two communicating devices. For example, between a laptop and development boards. Hence communication is through the inter bus system.

INTERNAL SYSTEMS

Internal system protocols are use to communicate between devices within the same circuit.

1. I2C

I2C stands for Inter-Integrated Circuit bus. It is an internal communication protocol that uses one wire SCL (serial clock) for clock and the other wire SDA (serial data) for transmission. It can connect many slave devices to master devices. Since communication is half-duplex, it can either send or receive messages at a time. There are 3 types of I2C based on speed : Slow (under 100 Kbps) ,Fast (400 Kbps) ,High-speed (3.4 Mbps).

Working of I2C Communication Protocol

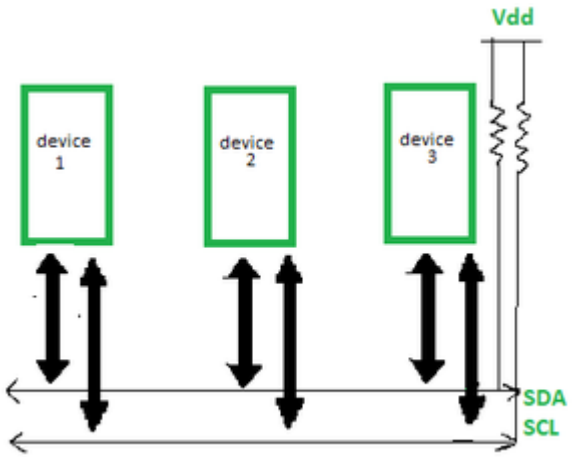
It uses only 2 bi-directional open-drain lines for data communication called SDA and SCL. Both these lines are pulled high.

Serial Data (SDA) : Transfer of data takes place through this pin. **Serial Clock (SCL) :** It carries the clock signal.

I2C operates in 2 modes

- Master mode
- Slave mode

Each data bit transferred on SDA line is synchronized by a high to the low pulse of each clock on the SCL line.



According to I2C protocols, the data line can not change when the clock line is high, it can change only when the clock line is low. The 2 lines are open drain, hence a pull-up resistor is required so that the lines are high since the devices on the I2C bus are active low. The data is transmitted in the form of packets which comprises 9 bits. The sequence of these bits are –

1. **Start Condition:** 1 bit
2. **Slave Address:** 8 bit
3. **Acknowledge:** 1 bit

Steps of I2C Data Transmission?

Here are the steps of I2C (Inter-Integrated Circuit) data transmission

- **Start Condition**: The master device sends a start condition by pulling the SDA line low while the SCL line is high. This signals that a transmission is about to begin.
- **Addressing the Slave:** The master sends the 7-bit address of the slave device it wants to communicate with, followed by a read/write bit. The read/write bit indicates whether it wants to read from or write to the slave.
- **Acknowledge Bit (ACK):** The addressed slave device responds by pulling the SDA line low during the next clock pulse (SCL). This confirms that the slave is ready to communicate.
- **Data Transmission:** The master or slave (depending on the read/write operation) sends data in 8-bit chunks. After each byte, an ACK is sent to confirm that the data has been received successfully.

- **Stop Condition:** When the transmission is complete, the master sends a stop condition by releasing the SDA line to high while the SCL line is high. This signals that the communication session has ended.

Advantages:

- I2C Protocol supports multi-master, multi-slave communication
- It uses only two wires
- Adaptable as it can adapt to the needs of various slave device
- In I2C Protocol the addressing is very simple
- It uses flow control

Disadvantages:

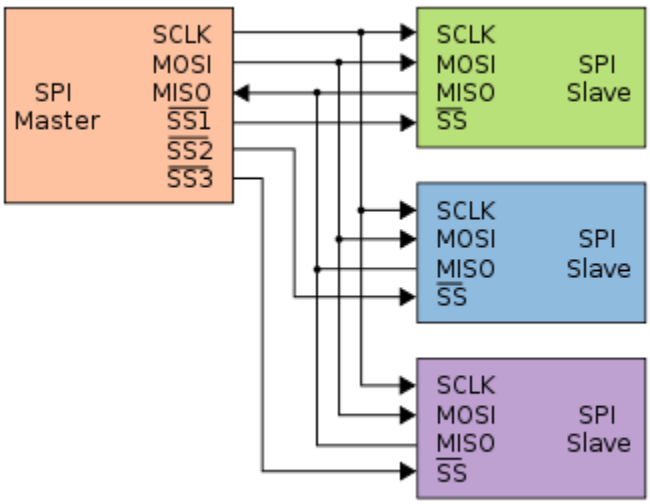
- I2C Protocol is a half-duplex mode of communication
- The hardware complexity increases when the number of master/slave devices is more in the circuit
- Many devices have multiple addresses stored which can cause conflicts

Applications of I2C Protocol:

- Accessing DACs and ADCs
- Reading certain memory ICs
- Reading hardware sensors
- Communicating with multiple micro-controller
- Transmitting and controlling user-directed actions

2.SPI :

The **Serial Peripheral Interface bus** (**SPI**) is a synchronous serial communication interface specification used for short distance communication, primarily in embedded systems. The interface was developed by Motorola in the late 1980s. Typical applications include Secure Digital cards and liquid crystal displays.



As you can see in the image above that slave devices have 4 connections i.e SCLK(Serial Clock) ,MOSI(Master Output Slave Input) ,MISO(Master Input Slave Output) ,SS(Slave Select).First 3 pins share same line from controller but SS pin controls which slave device is active.

1. SCLK (Serial Clock): The Serial Clock wire carries the clock signal from the master device to other devices on the serial bus.
2. MOSI (Master Output, Slave Input): The MOSI wire carries data output from the master device to the slave devices on the serial bus
3. MISO (Master Input, Slave Output): The MISO wire carries data output from the selected slave device to the master device or micro controller on the serial bus
4. SS (Slave Select): On an SPI bus, there must be one master device, but there can be multiple slave devices. The master device can exchange data with all of the slave devices, but the slave devices can only send data to the master - not to each other. The master device uses the Slave Select wire to select which slave device on the bus it will be communicating with before sending a data transmission.

Advantages of SPI

1. The main advantage of the SPI is to transfer the data without any interruption.
2. It is simple hardware.
3. It provides full-duplex communication.
4. There is no need for a unique address of the slave in this protocol.
5. This protocol does not require precise oscillation of slave devices because it uses the master's clock.
6. In this, software implementation is very simple.
7. It provides high transfer speed.
8. Signals are unidirectional.

9. It has separate lines of MISO and MOSI, so the data can be sent and received at the same time.

Disadvantages of SPI

1. Usually, it supports only one master.
2. It does not check the error like the UART.
3. It uses more pins than the other protocol.
4. It can be used only from a short distance.
5. It does not give any acknowledgment that the data is received or not.

Applications of SPI

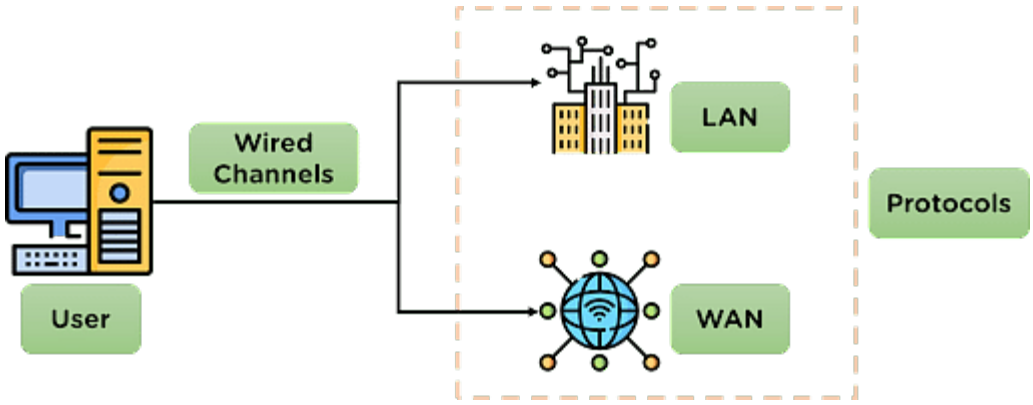
- Memory: SD Card, MMC, EEPROM, and Flash.
- Sensors: Temperature and Pressure.
- Control Devices: ADC, DAC, digital POTS, and Audio Codec.
- Others: Camera Lens Mount, Touchscreen, LCD, RTC, video game controller, etc.

I^2C Protocol	**SPI Protocol**
There are two bus lines required as a serial data line (SDA) and a serial clock line (SCL).	Three bus lines are needed; a data input line (SI1), a data output line (SO1) and a serial clock line (SCK1) [plus 1 Chip Select (CS)].
It can support transfer speeds of around 100kHz (original standard, or 400kHz using the most recent standard)	It is used at higher data rates (up to 10 MHz or more).
It is used to be more efficient in multi-master, multi-slave applications.	It is used to be more efficient in point-to-point (single master, single slave) applications.
It is used for a built-in addressing scheme, and straightforward.	It can lack built-in device addressing.
It is used for more overhead when handling point-to-point applications.	It can take less overhead when running a point-to-point application.
It can be suited better for communication with onboard devices that are accessed on an occasional basis.	It can be served better for applications that are naturally thought of as data streams.

I^2C Protocol	SPI Protocol
It has an acknowledgement mechanism to confirm receipt of data.	It does not have an acknowledgement mechanism to confirm receipt of data.

3.Ethernet

A system connecting a number of systems to form a LAN (Local Area Network) having protocols to control the data transfer and avoid data transmission by two or more systems simultaneously. Every Ethernet network interface card (NIC) is apply a unique identifier – a MAC address which is a 48-bit number. The first 24 bits identify the manufacturer and it is the manufacturer ID or Organizational Unique Identifier (OUI) which is assign along the registration authority.



Ethernet is designed for the transmission of data over the channel using wired technology and is used for high-speed data transmission. It is also responsible for applying some protocols for smooth and efficient data transmission over the network.

Ethernet uses cables to transmit data in a network model, such as LAN and, in some cases, WAN. It is more reliable and secure, providing better network connectivity.

Types of Ethernet

Depending on the network requirements, the type of ethernet networks applied in the communication also varies. The different types of ethernet connections are mentioned below:

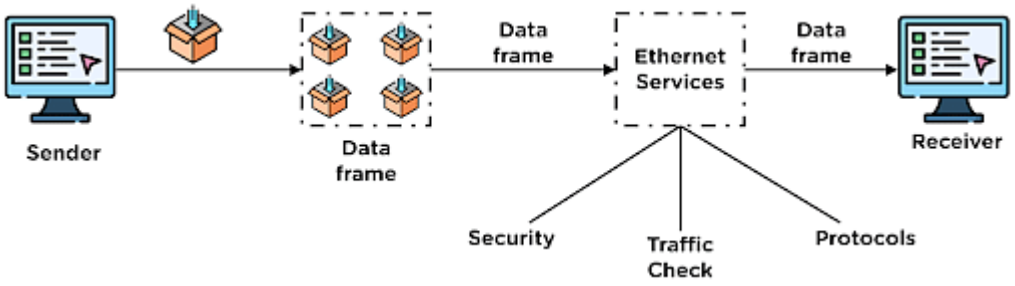
- Fast Ethernet: This Ethernet type is used for transferring data around the network at a speed of 100 Mbps through twisted-pair cables or optical cables. This type of data transmitted can be done without applying protocols.
- Gigabit Ethernet: This type of Ethernet also uses optical and twisted pair cables for data transmission at 1000 Mbps. This is also one of the most preferred Ethernet networks.
- Switched Ethernet: This Ethernet type installs network devices such as switches or hubs to improve the network transmission. The transmission range for this type ranges from 1000Mbps to 10Gbps.

Working of Ethernet Network

The Ethernet network is designed to work in the 1st layer (physical layer) and 2nd layer (Data Link Layer) of the OSI model.

Ethernet divides the transmission of data into two parts: packets and frames.

- Packet–Refers to a unit of data in the network.
- Frame–Refers to the collection of data packets being transmitted.



The data to be transmitted is converted into data packets in the network and then transferred to the channel. At a point, multiple data packets are collected to form a data frame, which is then transmitted further in the network channel.

During data transmission, Ethernet applies various services over the data being transmitted, such as security checks, traffic control services & other protocols.

Application of Ethernet :

- Cloud Computing
- Site to Site Access
- Video Applications
- Distributed Storage Area Networks
- CCTV
- Copper cable
- Fiber optic cable

Pros:–

1. The network starts and ends with it.
2. needs a switch to keep a network.
3. can be in use in a building.

Cons:-

1. Can’t be in use for long distances as Fibre should be in use.
2. It includes too many wires while connecting it in a building which is tough to manage.

3. UART

UART stands for Universal Asynchronous Receiver Transmitter and USART also means for Universal Synchronous Asynchronous Receiver Transmitter.

UART converts data into serial data. though, UARTs communicate directly by converting data into serial form and transmits it into the receiving UART that converts serial data into parallel data for the receiving device.

The flow of data is from the Tx pin of the transmitting UART to the Rx pin of the receiving UART. Hence only two wires are required. UART is asynchronous and hence doesn't require a clock for synchronisation whereas USART uses a clock for synchronisation in case of synchronous communication. It can be used in asynchronous communication also. Hence, it is a dual-type of serial communication.

UART is generally used in serial ports used with personal computers connected to modems use 8 data bits and low cost embedded systems.

UART is a Universal Asynchronous Receiver Transmitter protocol that is used for serial communication. Two wires are established here in which only one wire is used for transmission whereas the second wire is used for reception. Data format and transmission speeds can be configured here. So, before starting with the communication define the data format and transmission speed. Data format and transmission speed for communication will be defined here and we do not have a clock over here that's why it is referred to as asynchronous communication with UART protocol. Here we will see how this protocol is designed physically.

Pros:-

1. No clock signal required.
2. Only requires two wires.

Cons:-

1. Data frame size is limited only to a maximum of 9 bits.
2. Multiple master/slaves are not possible.

Application of UART :

- Transmitting and receiving UARTs must be set for the same bit speed, character length, parity, and stop bits for proper operation.

- Very low-cost home computers or embedded systems dispense with a UART and use the CPU to sample the state of an input port or directly manipulate an output port for data transmission.
- Typical serial ports used with personal computers connected to modems use eight data bits.

4.USB：

It is a representative peripheral interface.USB stands for **Universal Serial Bus**.It provides a serial bus standard for connecting devices,usually to a computer, but it also is in use on other devices such as set-top boxes, game consoles and PDAs.

Advantages :

- Flash drives use little power, have no fragile moving parts, and for most capacities are small and light.
- Data stored on flash drives is impervious to mechanical shock, magnetic fields, scratches and dust.
- Simple and fast.
- Almost acceptable everywhere.

Disadvantages :

- Flash drives can sustain only a limited number of write and erase cycles before the drive fails.
- A drawback to the small size is that they are easily misplaced, left behind, or otherwise lost.