FUNDAMENTALS OF INTERNET OF THINGS

(III-CSE, SEMESTER-II, R-22)

PREPARED BY-MAGANTI APPARAO

HEAD OF THE DEPARTMENT

ST. MARY'S ENGINEERING COLLEGE

UNIT – I

INTRODUCTION TO INTERNET OF THINGS

- **Definition and Characteristics of IoT**
- **Physical Design of IoT**
- **Functional blocks of IoT**
- **Sensing**
- **Actuation**
- **Basics of Networking**
- **Communication Protocols**
- **Sensor Networks**

INTRODUCTION

The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold.

Kevin Ashton (born 1968) is a British technology pioneer who is known for inventing the term "the Internet of Things" to describe a system where the Internet is connected to the physical world via ubiquitous sensors.

IoT is able to interact without human intervention. Some preliminary IoT applications have been already developed in healthcare, transportation, and automotive industries.

IoT technologies are at their infant stages; however, many new developments have occurred in the integration of objects with sensors in the Internet.

The development of IoT involves many issues such as infrastructure, communications, interfaces, protocols, and standards.

The objective of this paper is to give general concept of IoT, the architecture and layers in IoT, some basic terms associated with it and the services provided.

The below fig 1.1 give an example things connected to internet. The IOT concept was coined by a member of the Radio Frequency Identification (RFID) development community in 1999, and it has recently become more relevant to the practical world largely because of the growth of mobile devices, embedded and ubiquitous communication, cloud computing and data analytics.

IOT comprises things that have unique identities and are connected to the Internet.

The focus on IOT is in the configuration, control and networking via Internet devices or Things that are traditionally not associated with the Internet.

Fig 1.1: Things connected to Internet.

DEFINITION OF IOT

The Internet of Things (IoT) is the network of physical objects—devices, instruments, vehicles, buildings and other items embedded with electronics, circuits, software, sensors and network connectivity that enables these objects to collect and exchange data.

The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency and accuracy.

IoT refers to the interconnection via the internet of computing devices embedded in everyday objects, enabled them to send and receive the data.

A **dynamic global network** infrastructure with **self-configuring capabilities** based on standard and **interoperable communication protocols,** where physical and virtual "things" have **identities,** physical attributes, and use intelligent interfaces, and are seamlessly **integrated into information network** that communicate data with users and environments.

CHARACTERISTICS OF IOT

1) Dynamic & Self-Adapting: IoT device and system 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.

For example, consider a surveillance adapt their modes based on the weather it is day or night, cameras could switch from lower resolution to higher resolution modes when any motion is detected and alert nearby cameras to do the same.

2. Self-Configuring: IoT devices may have self-configuring capability, allowing a large number of devices to work together to provide certain functionality (such as weather monitoring). These devices have the ability configure themselves, setup the networking and fetch latest software upgrades with minimal manual or user intervention.

3. Interoperable Communication Protocols: IoT devices may support a number of interoperable communication protocols and can communicate with other devices and also with the infrastructure.

4. Unique Identity: Each IoT device has a unique identity and a unique identifier (such as an IP address). IoT systems may have intelligent interface which adapt based on the context, allow communicating with user and the environmental contexts, IoT device interfaces allow users to query the devices, monitor their status and control them remotely.

5. Integrated into Information Network: IoT devices are usually integrated into the information network that allows them to communicate and exchange data with other devices and systems, IoT devices can be dynamically discovered in the network, by other devices and/or the network, and have the capability to describe themselves to other devices or user applications.

Applications of IoT

1) Home

2) Cities

3) Environment

4) Energy

5) Retail

6) Logistics

7) Agriculture

8) Industry

9) Health & Life Style

PHYSICAL DESIGN OF IOT

A physical design of an IoT system refers to the individual node devices and their protocols that are utilized to create a functional IoT ecosystem.

Physical design knowledge is crucial for selecting suitable devices and sensors, ensuring seamless integration, and optimizing connectivity options in IoT systems.

Things in IoT

Refers to IoT devices which have unique identities that can perform sensing, actuating and monitoring capabilities.

IoT devices can exchange data with other connected devices or collect data from other devices and process the data either locally or send the data to centralized servers or cloud – based application back-ends for processing the data.

Generic Block Diagram of an IoT Device

An IoT device may consist of several interfaces for connections to other devices,

both wired and wireless. The below Fig 1.2 shows the block diagram of an IoT

Device.

- I/O interfaces for sensors
- Interfaces for internet connectivity

◦ Memory and storage interfaces

◦ Audio/video interfaces

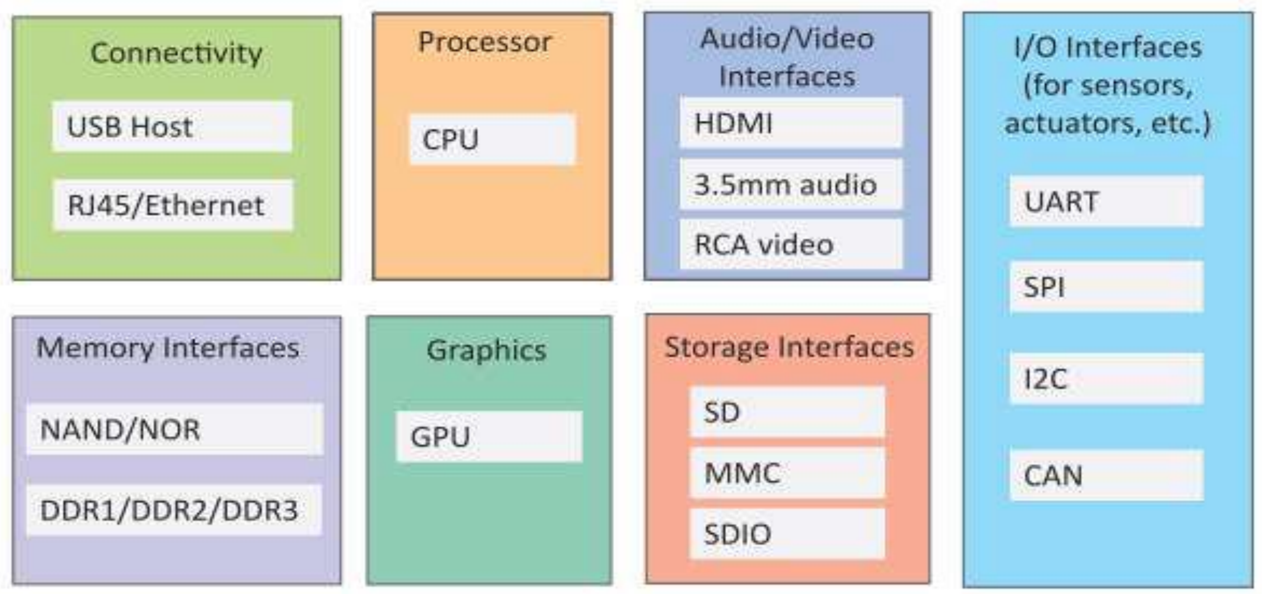


Fig 1.2: Block Diagram of an IoT Device

IOT PROTOCOLS /COMMUNICATION PROTOCOLS

The IoT devices are typically connected to the Internet via an IP (Internet Protocol) network.

However, devices such as Bluetooth and RFID allow IoT devices to connect locally.

In these cases, there’s a difference in power, range, and memory used.

Connection through IP networks are comparatively complex, requires increased memory and power from the IoT devices while the range is not a problem.

On the other hand, non-IP networks demand comparatively less power and memory but have a range limitation.

As far as the IoT communication protocols or technologies are concerned, a mix of both IP and non-IP networks can be considered depending on usage.

LIST OF PROTOCOLS

- Transmission Control Protocol (TCP)
- Internet Protocol (IP)
- User Datagram Protocol (UDP)
- Post office Protocol (POP)
- Simple mail transport Protocol (SMTP)
- File Transfer Protocol (FTP)
- Hyper Text Transfer Protocol (HTTP)
- Hyper Text Transfer Protocol Secure (HTTPS)
- Telnet
- Gopher

Fig 1.3 shows Four Layer of IoT Protocol

1. Link Layer
2. Network Layer
3. Transport Layer
4. Application Layer

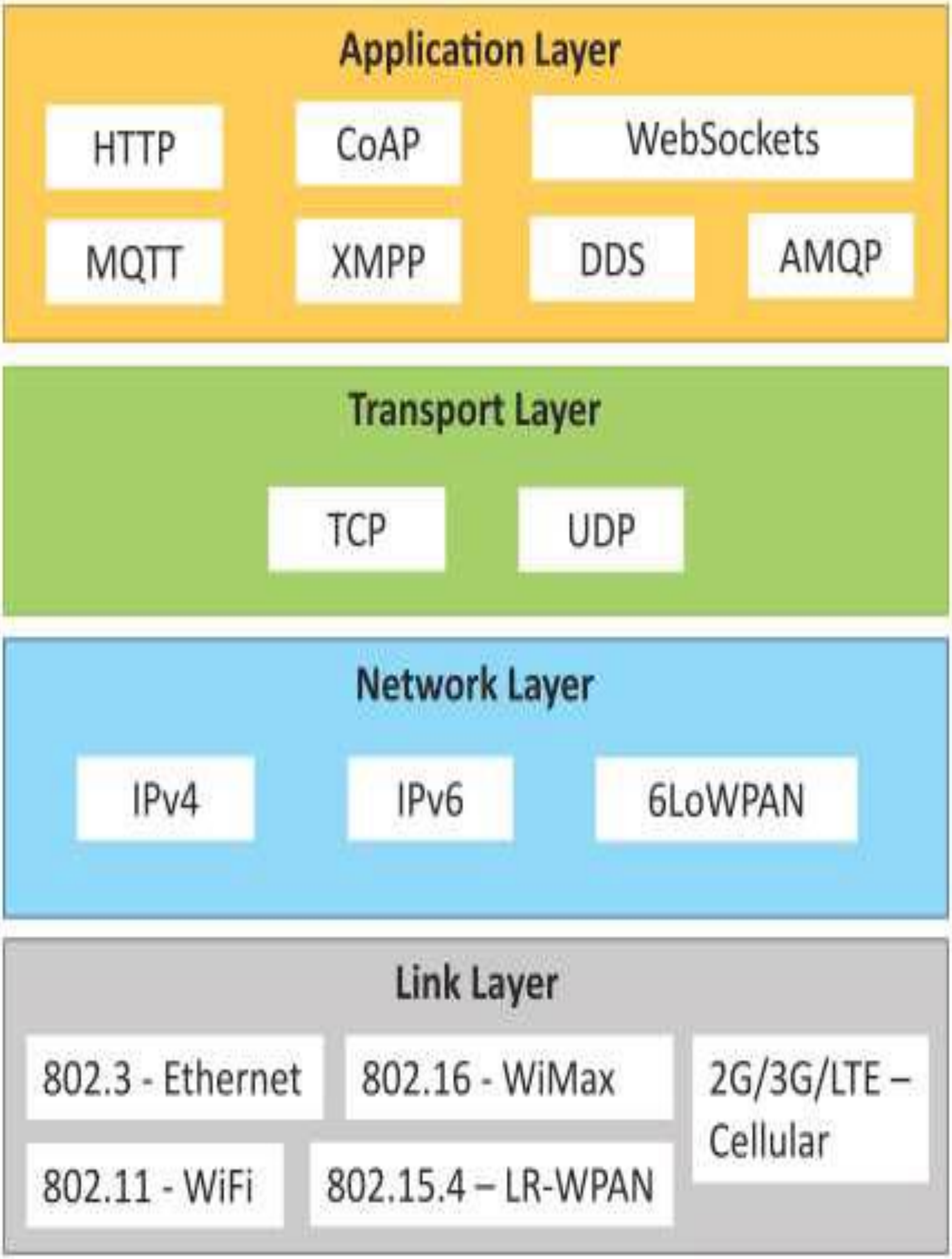


Fig 1.3 Four Layer IoT Protocol

1. Link Layer

In computer networking, the link layer is the lowest layer in the Internet protocol suite, the networking architecture of the Internet. The link layer is the group of methods and communications protocols confined to the link that a host is physically connected.

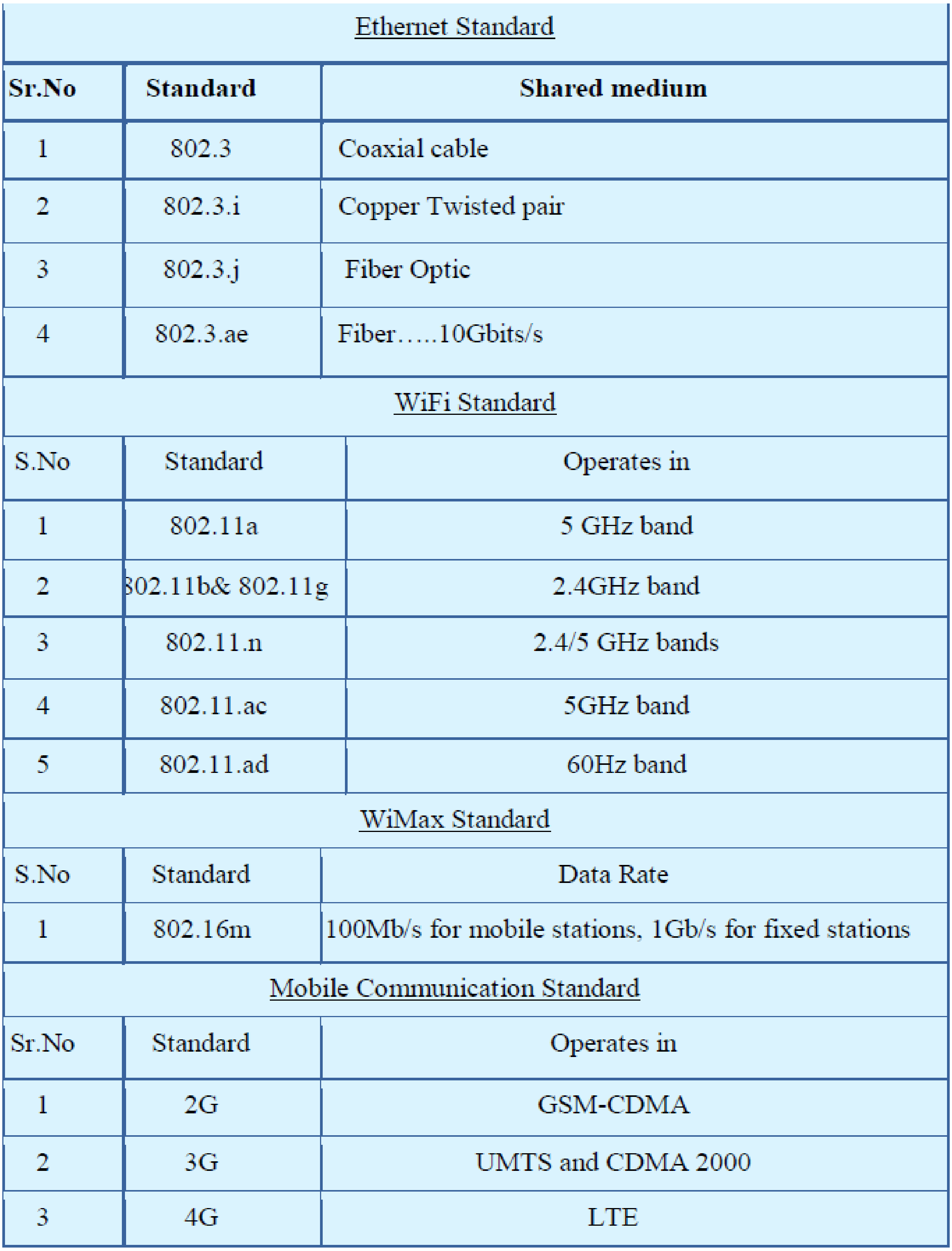
The link is the physical and logical network component used to interconnect hosts or nodes in the network and a link protocol is a suite of methods and standards that operate only between adjacent network nodes of a network segment.

The below Table 1.1 shows the different method of link layer with different standards. For Ethernet method Data Rates are provided from 10Gbit/s to 40Gb/s and higher.

Collection of Wireless LAN Data Rates from 1Mb/s to 6.75 Gb/s. Collection of Wireless Broadband Standards Data Rates from 1.5Mb/s to 1 Gb/s.

LR-WPAN: Collection of standards for low-rate wireless personal area networks, Basis for high level communication protocols such as ZigBee, Data Rates from 40Kb/s to 250Kb/s.

2G/3G/4G –Mobile Communication: Data Rates from 9.6Kb/s (for 2G) to up to 100Mb/s (for 4G).



Ethernet Standard

Sr.No	Standard	Shared medium
1	802.3	Coaxial cable
2	802.3.i	Copper Twisted pair
3	802.3.j	Fiber Optic
4	802.3.ae	Fiber…..10Gbits/s

WiFi Standard

S.No	Standard	Operates in
1	802.11a	5 GHz band
2	802.11b& 802.11g	2.4GHz band
3	802.11.n	2.4/5 GHz bands
4	802.11.ac	5GHz band
5	802.11.ad	60Hz band

WiMax Standard

S.No	Standard	Data Rate
1	802.16m	100Mb/s for mobile stations, 1Gb/s for fixed stations

Mobile Communication Standard

Sr.No	Standard	Operates in
1	2G	GSM-CDMA
2	3G	UMTS and CDMA 2000
3	4G	LTE

Table 1.1: different methods of link layer with standards.

2. Network/Internet Layer

The internet layer is a group of internetworking methods, protocols, and specifications in the Internet protocol suite that are used to transport network packets from the originating host across network boundaries; if necessary, to the destination host specified by an IP address.

The internet layer derives its name from its function facilitating internetworking, which is the concept of connecting multiple networks with each other through gateways.

- Responsible for sending of IP datagrams from source to destination network
- Performs the host addressing and packet routing
- Host identification is done using hierarchical IP addressing schemes such as IPV4 or IPV6

IPV4

Used to identify the devices on a network using hierarchical addressing scheme. Uses 32-bit address scheme

IPV6

Uses 128-bit address scheme

6LoWPAN (IPV6 over Low Power Wireless Personal Area Network)

Used for devices with limited processing capacity, Operates in 2.4 Ghz, Data Rates of 250Kb/s.

3. Transport Layer

In computer networking, the transport layer is a conceptual division of methods in the layered architecture of protocols in the network stack in the Internet protocol suite and the OSI model.

The protocols of this layer provide host-to-host communication services for applications.

It provides services such as connection-oriented communication, reliability, flow control, and multiplexing.

The best-known transport protocol of the Internet protocol suite is the Transmission

Control Protocol (TCP). It is used for connection-oriented transmissions, whereas the connectionless User Datagram Protocol (UDP) is used for simpler messaging transmissions.

- Provide end-to-end message transfer capability independent of the underlying network
- It provides functions such as error control, segmentation, flow-control and congestion control.

Transmission Control Protocol (TCP):

- Connection Oriented
- Ensures Reliable transmission

- Provides Error Detection Capability to ensure no duplicity of packets and retransmit lost packets
- Flow Control capability to ensure the sending data rate is not too high for the receiver process
- Congestion control capability helps in avoiding congestion which leads to degradation of n/w performance

User Datagram Protocol (UDP):

- Connectionless
- Does not ensures Reliable transmission
- Does not do connection before transmitting
- Does not provide proper ordering of messages
- Transaction oriented and stateless

4. Application Layer:

An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communications network.

The application layer abstraction is used in both of the standard models of computer networking: The Internet Protocol Suite (TCP/IP) and the OSI model.

Although both models use the same term for their respective highest level layer, the detailed definitions and purposes are different.

Hyper Transfer Protocol:

- Forms foundation of World Wide Web(WWW)
- Includes commands such as GET, PUT, POST, HEAD, OPTIONS, TRACE etc.
- Follows a request-response model
- Uses Universal Resource Identifiers(URIs) to identify HTTP resources.

Constrained Application Protocol (CoAP):

- Used for Machine to machine (M2M) applications meant for constrained devices and n/w’s
- Web transfer protocol for IoT and uses request-response model
- Uses client –server architecture
- Supports methods such as GET, POST, PUT and DELETE

Web Socket:

□ Allows full-duplex communication over single socket, based on TCP, Client can be a browser, IoT device or mobile application

Message Queue Telemetry Transport (MQTT):

□ light-weight messaging protocol, based on publish-subscribe model, well suited for constrained environments where devices have limited processing, low memory and n/w bandwidth requirement.

XMPP:

• Extensible messaging and presence protocol, For Real time communication and streaming XML data between n/w entities, Used for Applications such as Multi-party chat and voice/video calls.

FUNCTIONAL BLOCKS OF IOT

□ An IoT system comprises a number of functional blocks that provide the system the capabilities for identification, sensing, actuation, communication and management.

□ Fig 1.4 shows the functional block diagram of IoT. Below is the individual block explanation.

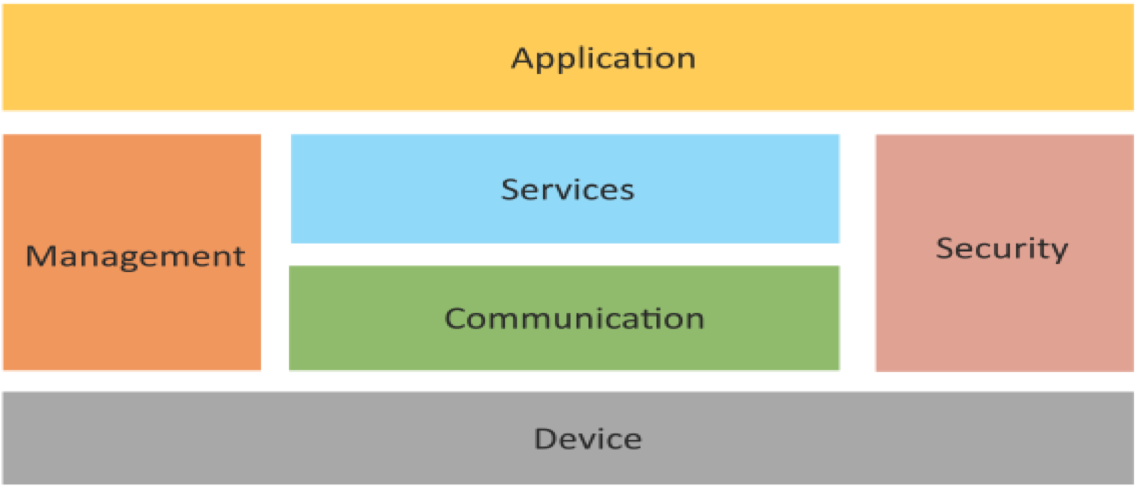


Fig 1.4: Functional Block Diagram of IoT.

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.

SENSING

Sensors play an important role in creating solutions using **IoT**. **Sensors** are devices that detect external information, replacing it with a signal that humans and machines can distinguish.

The main **purpose of sensors** is to collect data from the surrounding environment. **Sensors**, or 'things' of the **IoT** system, form the front end.

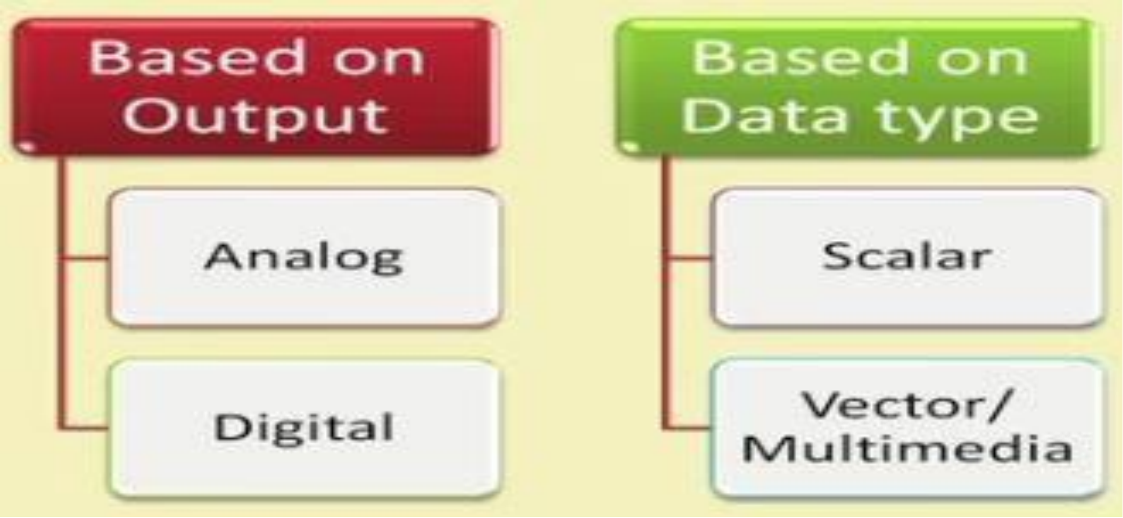
These are connected directly or indirectly to **IoT** networks after signal conversion and processing.

Sensors measure or identify a particular quantity i.e Convert physical quantities to electrical signals understood by machines.

An **IoT** system consists of **sensors**/**devices** which “talk” to the cloud through some kind of connectivity. Once the data gets to the cloud, software processes it and then might decide to perform an action, such as sending an alert or automatically adjusting the **sensors**/**devices** without the need for the user.

For example, heat is converted to electrical signals in a temperature sensor, or atmospheric pressure is converted to electrical signals in a barometer.

SENSOR CLASSES



Analog Sensors

Analog Sensors produces a continuous output signal or voltage which is generally proportional to the quantity being measured. Physical quantities such as Temperature, speed, Pressure, Displacement, Strain etc. are all analog quantities as they tend to be continuous in nature.

For example, the temperature of a liquid can be measured using a thermometer or thermocouple (e.g. in geysers) which continuously responds to temperature changes as the liquid is heated up or cooled down.

Digital Sensors

Digital Sensors produce discrete output voltages that are a digital representation of the quantity being measured.

Digital sensors produce a binary output signal in the form of a logic "1" or a logic "0”, ("ON" or "OFF).

Scalar Sensors

Scalar Sensors produce output signal or voltage which generally proportional to the magnitude of the quantity being measured.

Physical quantities such as temperature, color, pressure, strain, etc. are all scalar quantities as only their magnitude is sufficient to convey an information.

For example, the temperature of a room can be measured using thermometer or thermocouple, which responds to temperature changes irrespective of the orientation of the sensor or its direction.

Vector Sensors

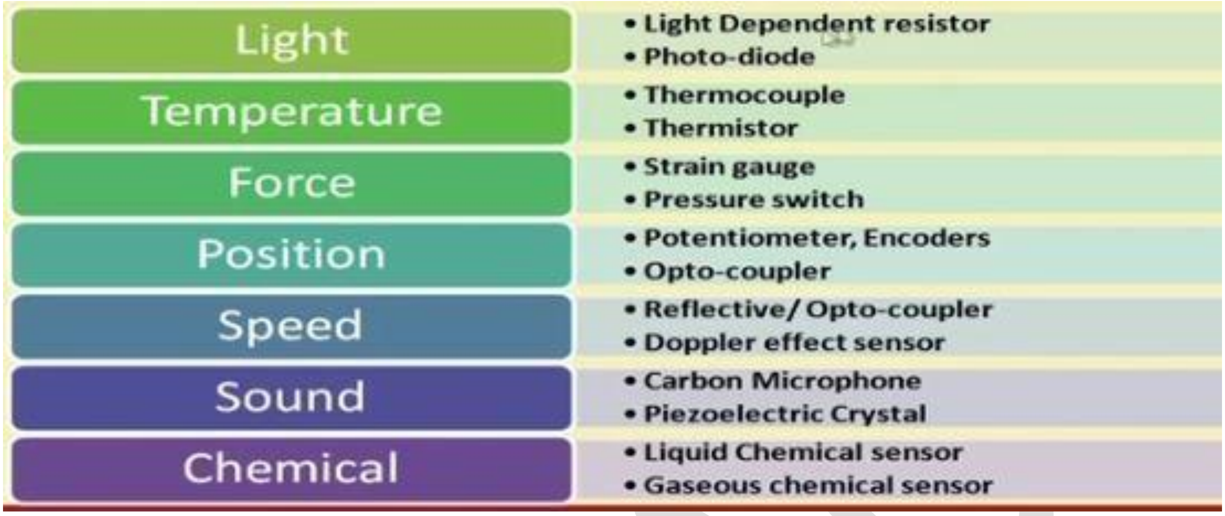
Vector Sensors produce output signal or voltage which generally proportional to the magnitude, direction, as well as the orientation of the quantity being measured.

Physical quantities such as sound, image, velocity, acceleration, orientation, etc. are all vector quantities, as only their magnitude is not sufficient to convey the complete information. For example, the acceleration of a body can be measured using an accelerometer, which gives the components of acceleration of the body with respect to the x, y, z coordinate axes.

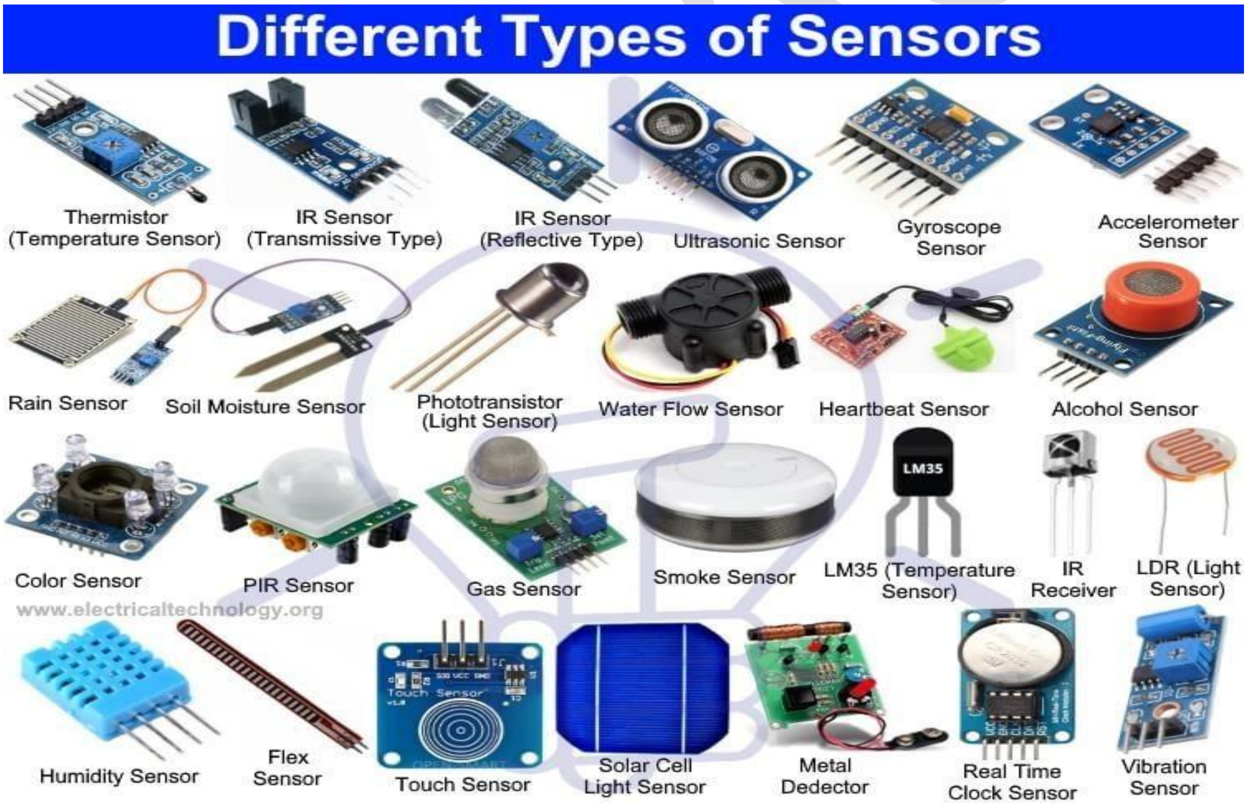
TYPES OF SENSOR:

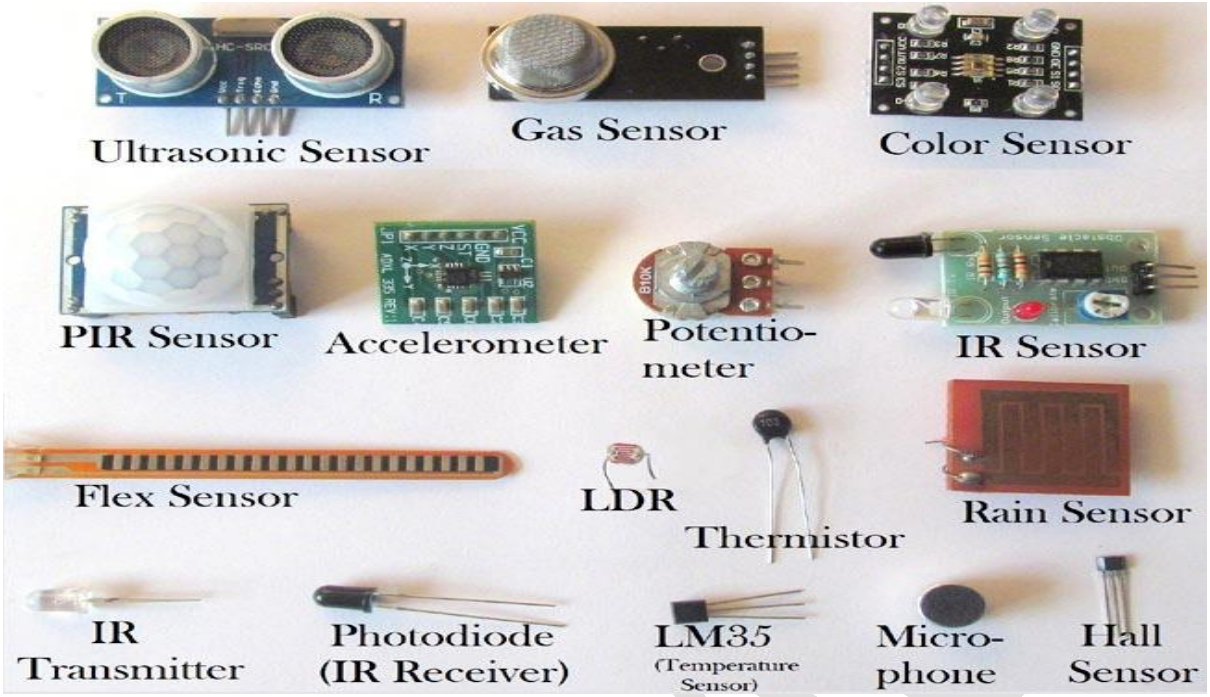
- Temperature Sensor.
- Proximity Sensor.
- Accelerometer.
- IR Sensor (**Infrared** Sensor)
- Pressure Sensor.
- Light Sensor.
- Ultrasonic Sensor.

- Smoke, Gas and **Alcohol** Sensor.



Light	• Light Dependent resistor • Photo-diode
Temperature	• Thermocouple • Thermistor
Force	• Strain gauge • Pressure switch
Position	• Potentiometer, Encoders • Opto-coupler
Speed	• Reflective/ Opto-coupler • Doppler effect sensor
Sound	• Carbon Microphone • Piezoelectric Crystal
Chemical	• Liquid Chemical sensor • Gaseous chemical sensor





Applications of Sensors

- Automotive
- Braking and Traction control
- Air Bags
- Engine Data
- Heating
- ventilation
- Air-condition
- Navigation
- Safety Features
- Security
- Remote locking

ACTUATION

Sensor generates electrical signals while an **actuator** results in the production of energy in the form of heat or motion. Magnetometer, cameras, microphones are some of the examples in which the **sensor** is used. In contrast, **actuators** are used in the LED, loudspeaker, motor controllers, laser etc...

An **actuator** is a component of a machine that is responsible for moving and controlling a mechanism or system, for example by opening a valve. In simple terms, it is a "mover". An **actuator** requires a control signal and a source of energy.

In simple terms, an actuator operates in the reverse direction of a sensor.

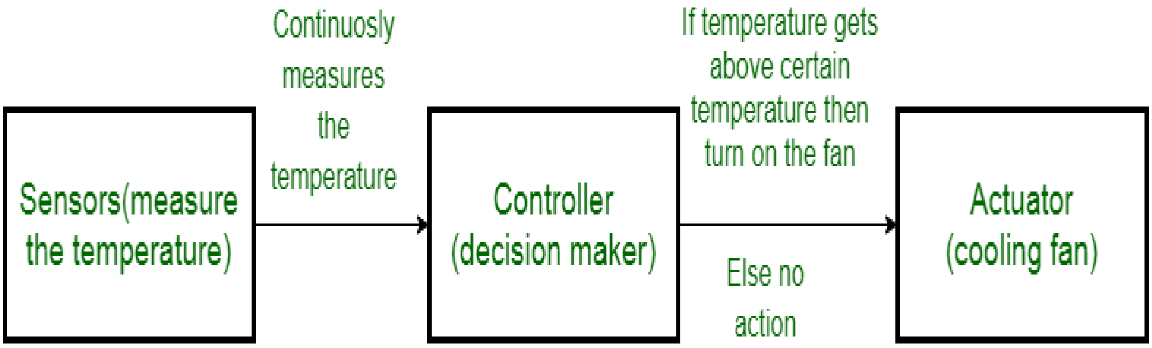
It takes an electrical input and turns it into physical action. For instance, an electric motor, a hydraulic system, and a pneumatic system are all different types of actuators.

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.

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.


Sensors(measure the temperature)
Continuosly measures the temperature
Controller (decision maker)
If temperature gets above certain temperature then turn on the fan
Else no action
Actuator (cooling fan)

IOT ACTUATOR TYPES

Actuators, as the name itself suggests, can act on their immediate environment to enable correct operation of the machines or devices they are embedded into.

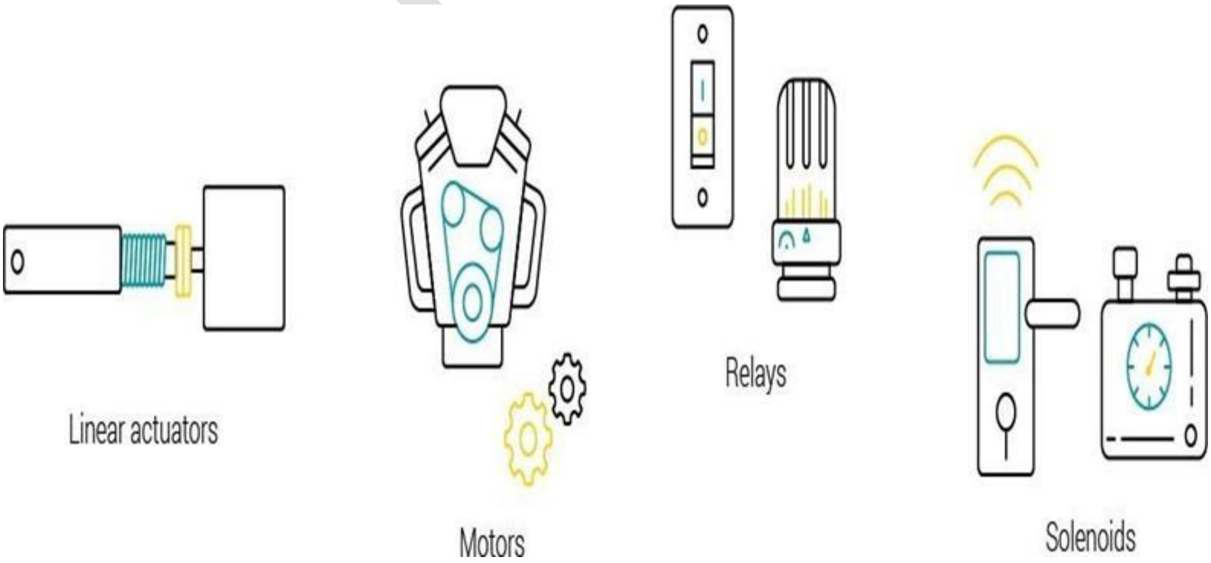
Small as they are, they are rarely visible during operation, but the effects of their work can be felt in vehicles, industrial machines or any other electronic equipment involving automation technologies. They can be separated into four main categories based on their construction pattern and the role they play in a specific IoT environment:

Linear actuators – these are used to enable motion of objects or elements in a straight line.

Motors – they enable precise rotational movements of device components or whole objects.

Relays – this category includes electromagnet-based actuators to operate power switches in lamps, heaters or even smart vehicles.

Solenoids – most widely used in home appliances as part of locking or triggering mechanisms, they also act as controllers in IoT-based gas and water leak monitoring systems.



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. Ex- construction equipment uses hydraulic actuators because hydraulic actuators can generate a large amount of force.

Advantages:

Hydraulic actuators can produce a large magnitude of force and high speed.

Used in welding, clamping, etc.

Used for lowering or raising the vehicles in car transport carriers.

Disadvantages:

Hydraulic fluid leaks can cause efficiency loss and issues of cleaning.

It is expensive.

It requires noise reduction equipment, heat exchangers, and high maintenance systems.

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.

Advantages:

They are a low-cost option and are used at extreme temperatures where using air is a safer option than chemicals.

They need low maintenance, are durable, and have a long operational life.

It is very quick in starting and stopping the motion.

Disadvantages:

Loss of pressure can make it less efficient.

The air compressor should be running continuously.

Air can be polluted, and it needs maintenance.

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.

Advantages:

It has many applications in various industries as it can automate industrial valves.

It produces less noise and is safe to use since there are no fluid leakages.

It can be re-programmed and it provides the highest control precision positioning.

Disadvantages

It is expensive.

It depends a lot on environmental conditions.

Other actuators are

Thermal/Magnetic Actuators –

These are actuated by thermal or mechanical energy. Shape Memory Alloys (SMAs) or Magnetic

Shape-Memory Alloys (MSMAs) are used by these actuators. An example of a thermal/magnetic actuator can be a piezo motor using SMA.

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. Example – A crankshaft.

BASICS OF NETWORKING

Switches, routers, and wireless access points are the essential **networking basics**. Through them, devices connected to your **network** can communicate with one another and with other **networks**, like the Internet. Switches, routers, and wireless access points perform very different functions in a **network**.

SWITCHES

Switches are the foundation of most business networks. A switch acts as a controller, connecting computers, printers, and servers to a network in a building or a campus.

Switches allow devices on your network to communicate with each other, as well as with other networks, creating a network of shared resources. Through information sharing and resource allocation, switches save money and increase productivity.

There are two basic types of switches to choose from as part of your networking basics: on-premises and cloud-managed.

A managed on-premises switch lets you configure and monitor your LAN, giving you tighter control of your network traffic.

Have a small IT team.

A cloud-managed switch can simplify your network management. You get a simple user interface, multisite full-stack management, and automatic updates delivered directly to the switch.

ROUTERS

Routers connect multiple networks together. They also connect computers on those networks to the Internet. Routers enable all networked computers to share a single Internet connection, which saves money.

A router acts a dispatcher. It analyzes data being sent across a network, chooses the best route for data to travel, and sends it on its way.

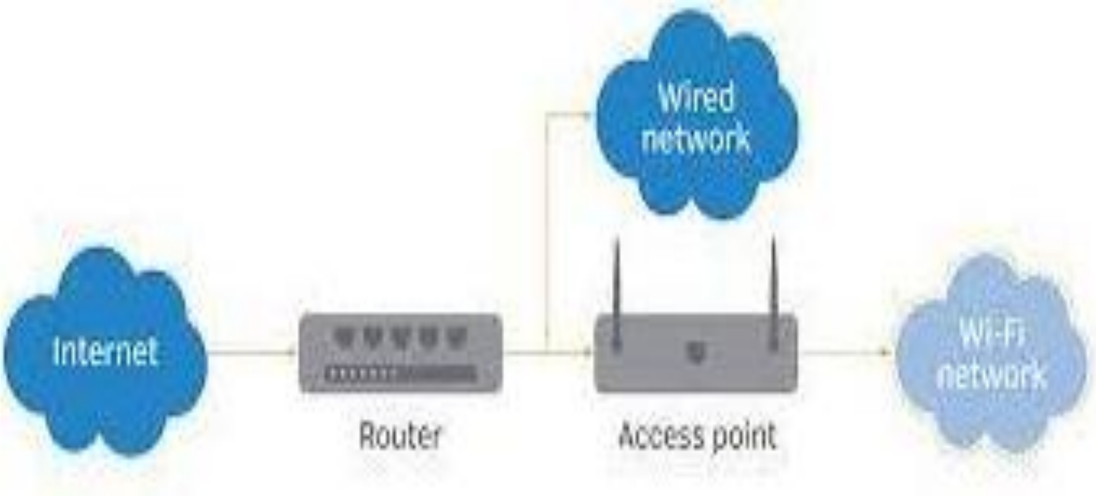
Routers connect your business to the world, protect information from security threats, and can even decide which computers receive priority over others.

Beyond those basic networking functions, routers come with additional features to make networking easier or more secure. Depending on your security needs, for example, you can choose a router with a firewall, a virtual private network (VPN), or an Internet Protocol (IP) communications system.

ACCESS POINT

An access point allows devices to connect to the wireless network without cables. A wireless network makes it easy to bring new devices online and provides flexible support to mobile workers.

An access point acts like an amplifier for your network. While a router provides the bandwidth, an access point extends that bandwidth so that the network can support many devices, and those devices can access the network from farther away.

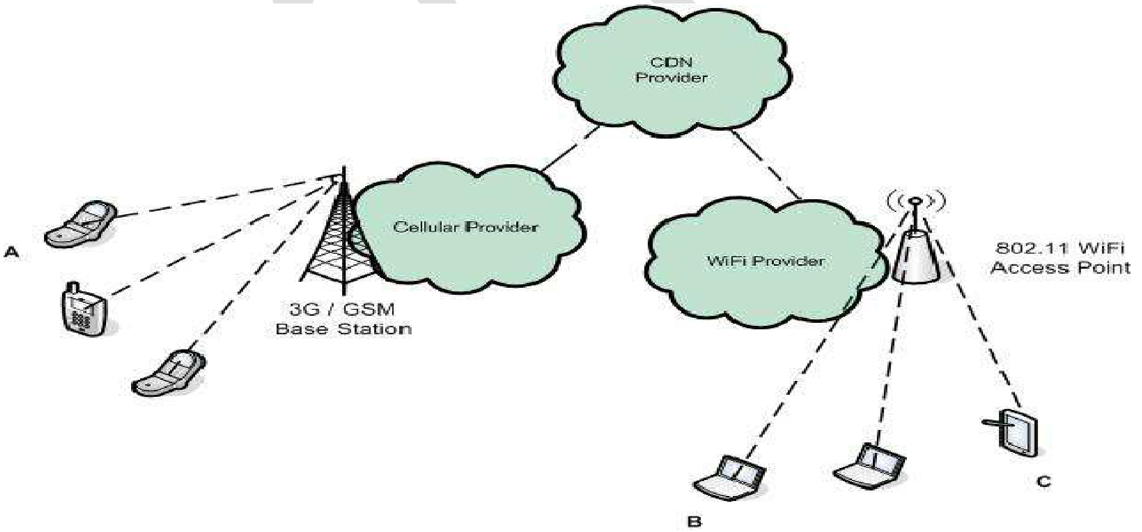


WIRELESS NETWORKING

To create your wireless network, you can choose between three types of deployment: centralized deployment, converged deployment, and cloud-based deployment

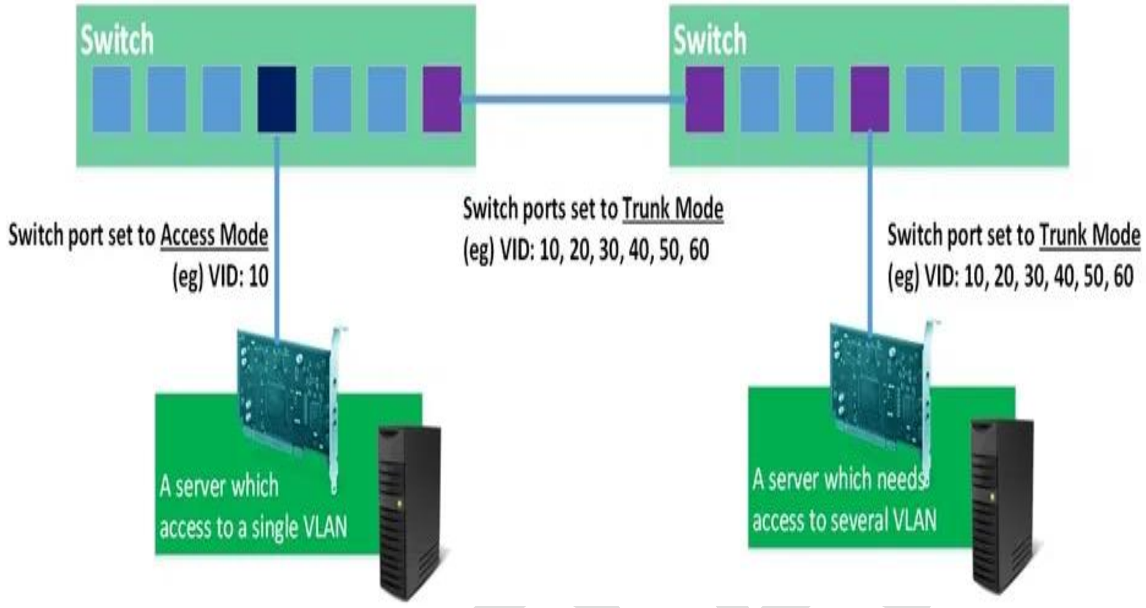
Centralized deployment

The most common type of wireless network system, centralized deployments are traditionally used in campuses where buildings and networks are in close proximity. This deployment consolidates the wireless network, which makes upgrades easier and facilitates advanced wireless functionality. Controllers are based on-premises and are installed in a centralized location.



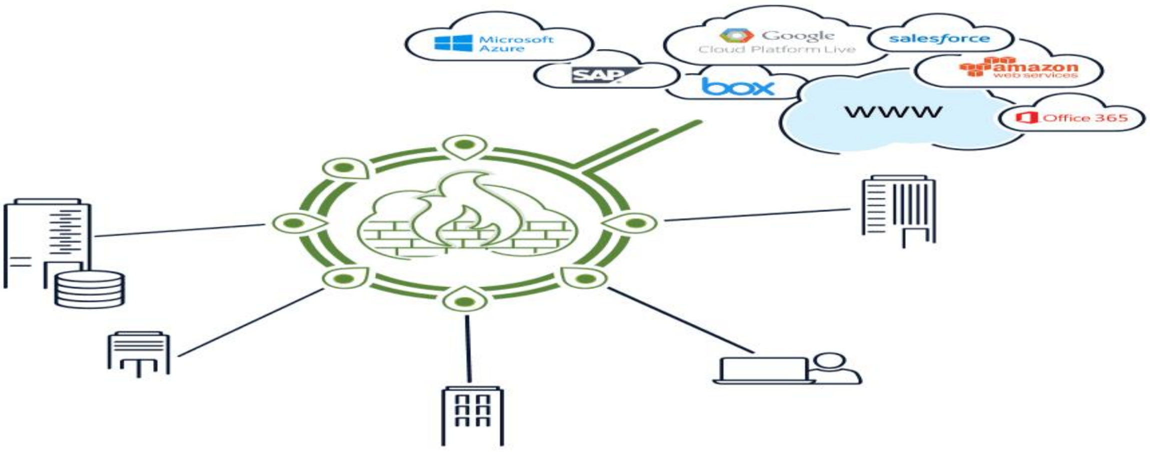
Converged deployment

For small campuses or branch offices, converged deployments offer consistency in wireless and wired connections. This deployment converges wired and wireless on one network device—an access switch—and performs the dual role of both switch and wireless controller.

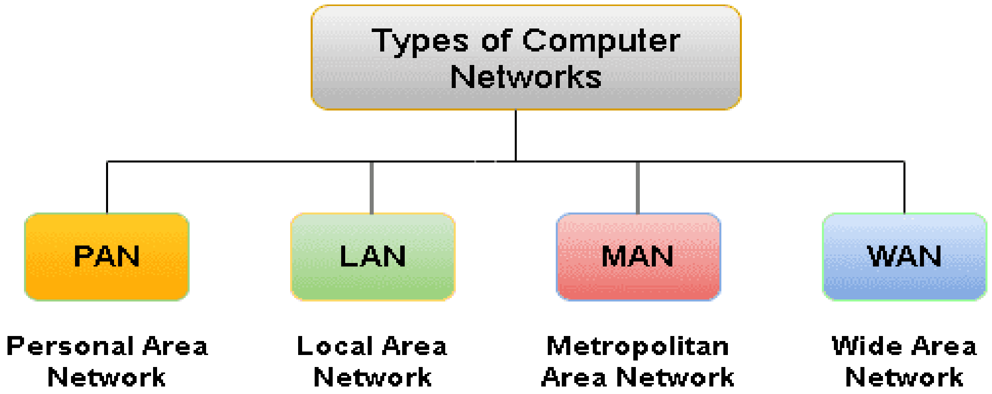

Switch
Switch
Switch port set to Access Mode
(eg) VID: 10
Switch ports set to Trunk Mode
(eg) VID: 10, 20, 30, 40, 50, 60
Switch port set to Trunk Mode
(eg) VID: 10, 20, 30, 40, 50, 60
A server which
access to a single VLAN
A server which needs
access to several VLAN

Cloud-based deployment

This system uses the cloud to manage network devices deployed on-premises at different locations. The solution requires Cisco Meraki cloud-managed devices, which provide full visibility of the network through their dashboards.



TYPES OF NETWORKS

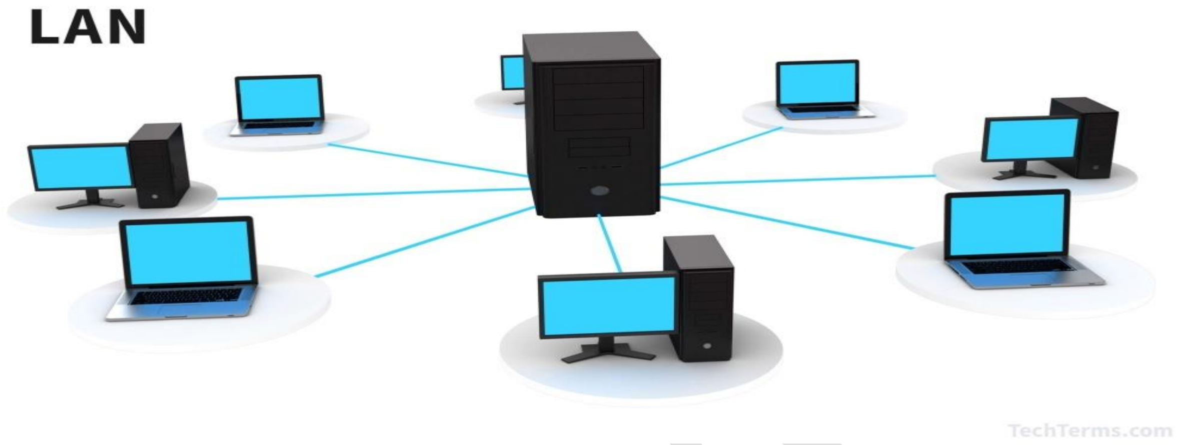


PERSONAL AREA NETWORK (PAN)

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

LOCAL AREA NETWORK (LAN)

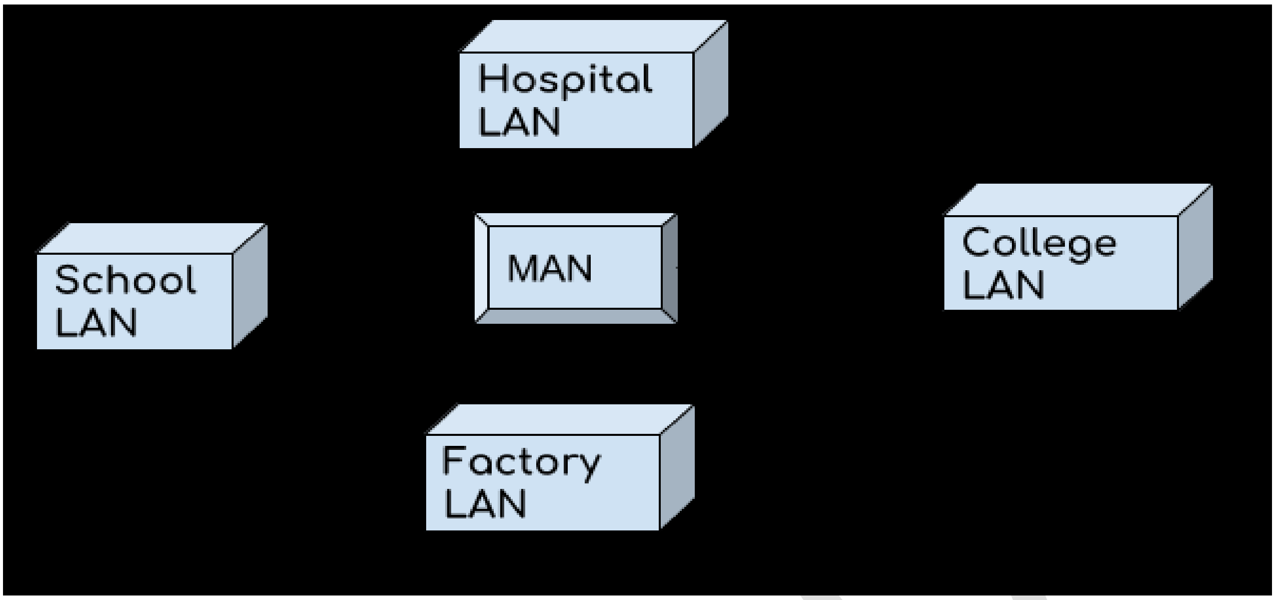
LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs.



Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidly and safely transfer data.

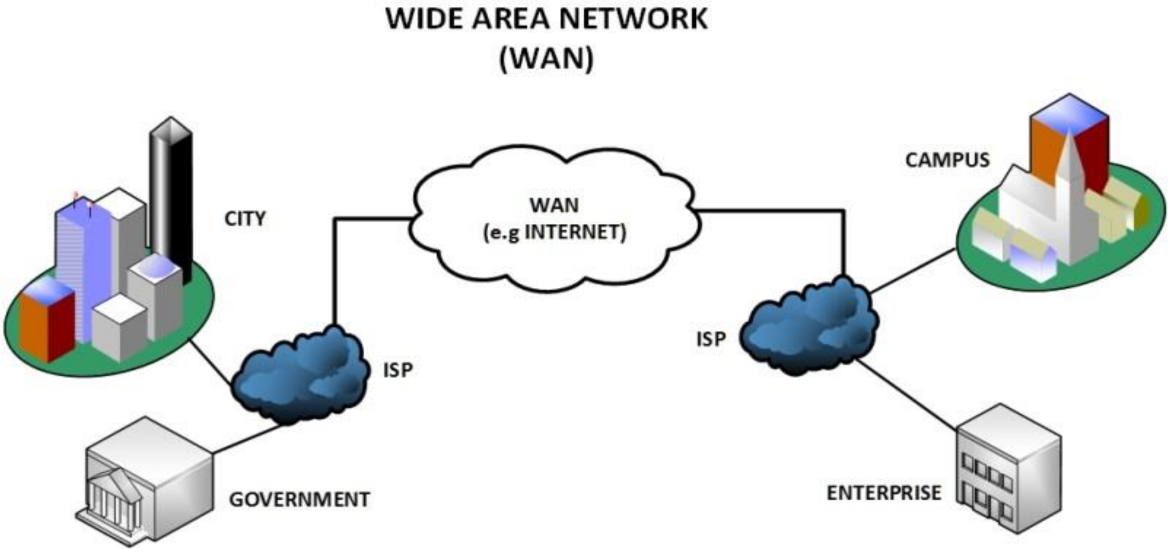
METROPOLITAN AREA NETWORK (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either a single person or company (a local council, a large company, etc.).



WIDE AREA NETWORK (WAN)

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're miles apart.



OTHER TYPES OF NETWORKS

1.Wireless Local Area Network (WLAN)

Functioning like a LAN, WLANs make use of wireless network technology, such as Wi-Fi. Typically seen in the same types of applications as LANs, these types of networks don’t require that devices rely on physical cables to connect to the network.

2. Campus Area Network (CAN)

Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large K-12 school districts or small businesses.

3. Storage-Area Network (SAN)

As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don’t rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network

4. System-Area Network (also known as SAN)

This term is fairly new within the past two decades. It is used to explain a relatively local network that is designed to provide high-speed connection in server-to-server applications (cluster environments), storage area networks (called “SANs” as well) and processor-to-processor applications

5. Passive Optical Local Area Network (POLAN)

As an alternative to traditional switch-based Ethernet LANs, POLAN technology can be integrated into structured cabling to overcome concerns about supporting traditional Ethernet protocols and network applications such as PoE (Power over Ethernet.

6. Enterprise Private Network (EPN)

These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.

SENSOR NETWORKS

A sensor network comprises a group of small, powered devices, and a wireless or wired networked infrastructure.

They record conditions in any number of environments including industrial facilities, farms, and hospitals. The sensor network connects to the internet or computer networks to transfer data for analysis and use.

Sensor network nodes cooperatively sense and control the environment. They enable interaction between persons or computers and the surrounding environment.

A wireless **sensor network** (WSN) is a **network** formed by a large number of **sensor** nodes where each node is equipped with a **sensor** to detect physical phenomena such as light, heat, pressure, etc.... With the rapid technological development of **sensors**, WSNs will become the key technology for **IoT**.

Operation of a Sensor Network

Sensor networks typically include sensor nodes, actuator nodes, gateways, and clients. Sensor nodes group inside the sensor field and form networks of different topologies.

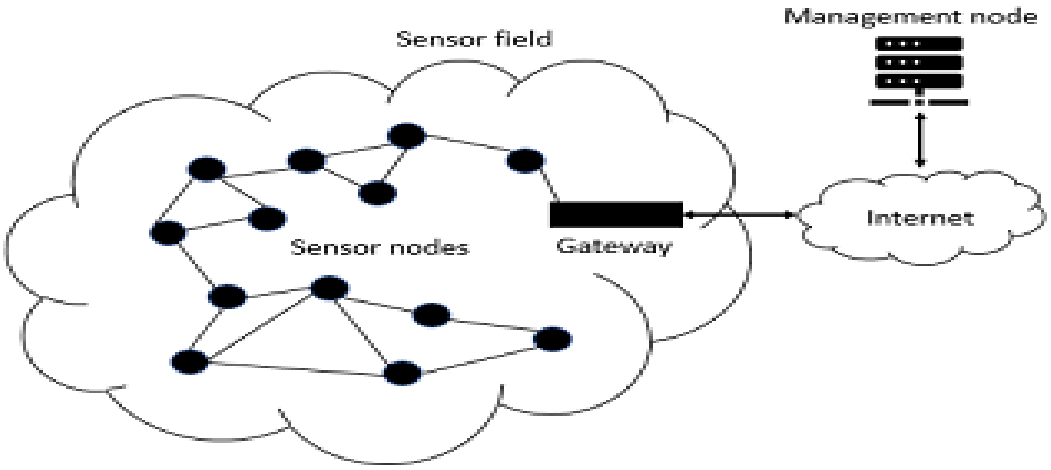
The following process describes how sensor networks operate:

A sensor node monitors the data collected by the sensor and transmits this to other sensor nodes.

During the transmission process, data may be handled by multiple nodes as it reaches a gateway node.

The data is then transferred to the management node.

The management node is managed by the user and determines the monitoring required and collects the monitored data.



SENSOR NODES

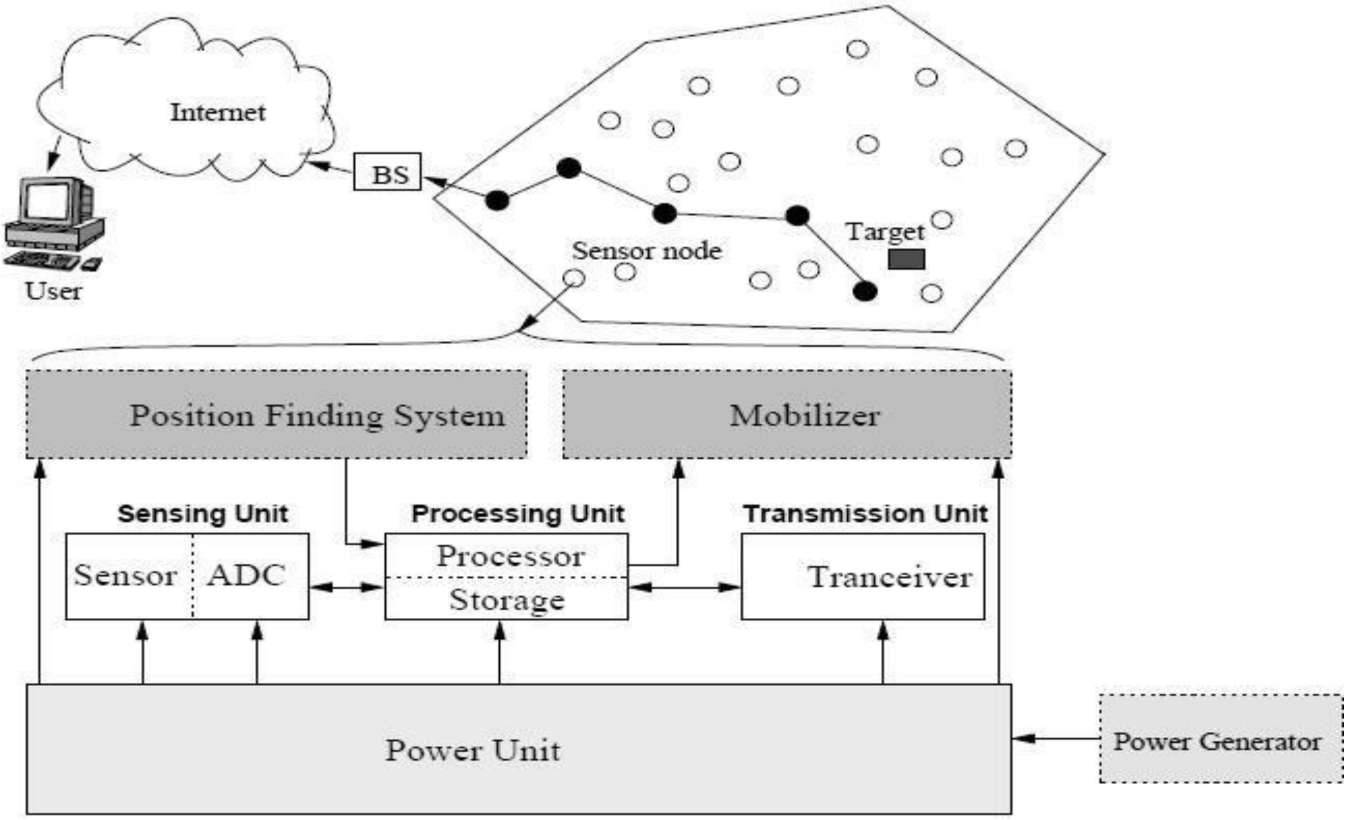
There are many nodes in a sensor network. These nodes are the detection stations. There is a sensor/transducer, microcontroller, transceiver, and power source:

A sensor senses the physical condition, and if there is any change, it generates electrical signals.

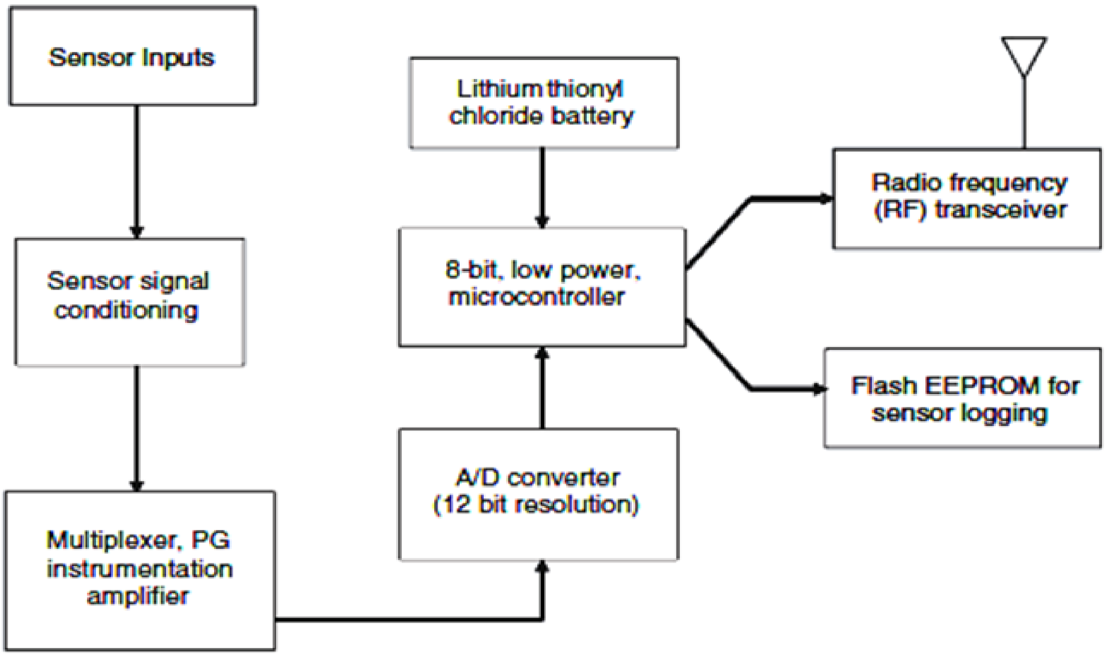
The signals go to the microcontroller for processing.

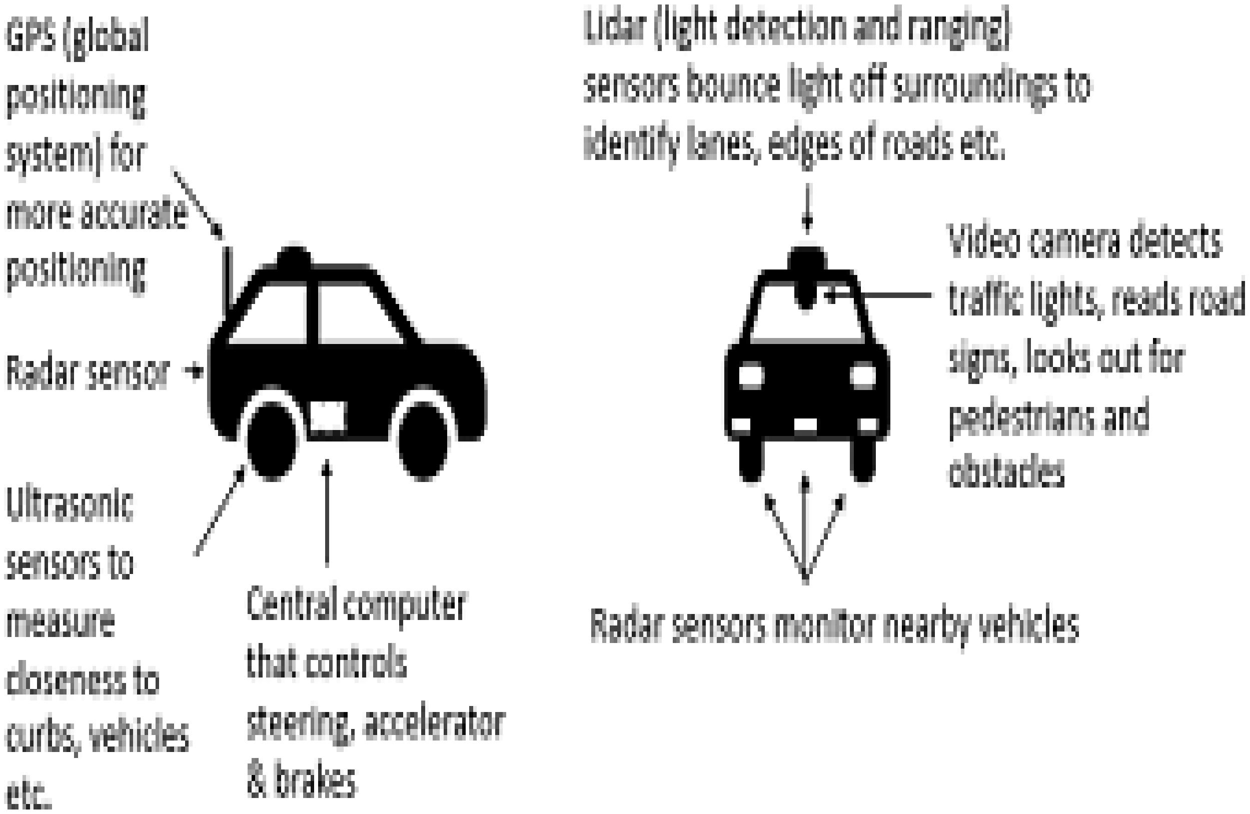
A central processor sends commands to the transceiver and data is transmitted to a computer.

The components of a sensor node



Functional block diagram of a sensor node


Sensor Inputs
Sensor signal conditioning
Multiplexer, PG instrumentation amplifier
Lithium thionyl chloride battery
8-bit, low power, microcontroller
A/D converter (12 bit resolution)
Radio frequency (RF) transceiver
Flash EEPROM for sensor logging


GPS (global positioning system) for more accurate positioning
Radar sensor
Ultrasonic sensors to measure closeness to curbs, vehicles etc.
Central computer that controls steering, accelerator & brakes
Lidar (light detection and ranging) sensors bounce light off surroundings to identify lanes, edges of roads etc.
Video camera detects traffic lights, reads road signs, looks out for pedestrians and obstacles
Radar sensors monitor nearby vehicles

Sensors Using Self –Driving Car