UNIT-1

Introduction to Internet of Things

Internet of things (IoT)

The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data.

Characteristics:

Things-related services: The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things

Connectivity: Things in I.O.T. should be connected to the infrastructure, without connection nothing makes sense.

Intelligence: Extraction of knowledge from the generated data is important, sensor generate data and this data and this data should be interpreted properly.

Scalability: The no. of things getting connected to the I.O.T. infrastructure is increased day by day. Hence, an IOT setup shall be able to handle the massive expansion.

Unique Identity: Each IOT device has an I.P. address. This identity is helpful in tracking the equipment and at times to query its status.

Dynamic and Self-Adapting: The IOT device must dynamically adopt itself to the changing context. Assume a camera meant for surveillance, it may have to work in different conditions and at different light situations (morning, afternoon, night).

Heterogeneity: The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices different networks.

Safety: Having got all the things connected with the Internet possess a major threat, as our personal data is also there and it can be tampered with, if proper safety measures are not taken.

Application areas of IoT:

Smart Home: The smart home is one of the most popular applications of IoT. The cost of owning a house is the biggest expense in a homeowner's life. Smart homes are promised to save the time, money and energy.

Smart cities: The smart city is another powerful application of IoT. It includes smart surveillance, environment monitoring, automated transformation, urban security, smart traffic management, water distribution, smart healthcare etc.

Wearables: Wearables are devices that have sensors and software installed which can collect data about the user which can be later used to get the insights about the user. They must be energy efficient and small sized.

Connected cars: A connected car is able to optimize its own operation, maintenance as well as passenger's comfort using sensors and internet connectivity.

Smart retail: Retailers can enhance the in-store experience of the customers using IoT. The shopkeeper can also know which items are frequently bought together using IoT devices.

Smart healthcare: People can wear the IoT devices which will collect data about user's health. This will help users to analyze themselves and follow tailor-made techniques to combat illness. The doctor also doesn't have to visit the patients in order to treat them.

IoT Categories

IOT can be classified into two categories:

1. Consumer IoT(CIOT): The Consumer IoT refers to the billions of physical personal devices, such as smartphones, wearables, fashion items and the growing number of smart home appliances, that are now connected to the internet, collecting and sharing data.

A Consumer IoT network typically entails few consumer devices, each of which has a limited lifetime of several years.

The common connectivity used in this kind of solutions are Bluetooth, WiFi, and ZigBee. These technologies offer short-range communication, suitable for applications deployed in limited spaces such as houses, or small offices.

2. industrial internet of things (IIoT): It refers to interconnected sensors, instruments, and other devices networked together with computers' industrial applications, including manufacturing and energy management. This connectivity allows for data collection, exchange, and analysis, potentially facilitating improvements in productivity and efficiency as well as other economic ben

BASELINE TECHNOLOGIES

There are various baseline technologies that are very closely related to IOT, They include: Machine-to-Machine (M2M)**,** Cyber-Physical Systems (CPS), Web Of Things(WOT)

a) Machine-to-Machine (M2M):

- Machine-to-Machine (M2M) refers to networking of machines (or devices) for the purpose of remote monitoring and control and data exchange.
- An M2M area network comprises of machines (or M2M nodes) which have embedded network modules for sensing, actuation and communicating various communication protocols can be used for M2M LAN such as ZigBee, Bluetooth, M-bus, Wireless M-Bus etc., These protocols provide connectivity between M2M nodes within an M2M area network.
- The communication network provides connectivity to remote M2M area networks. The communication network provides connectivity to remote M2M area network.
- The communication network can use either wired or wireless network (IP based). While the M2M are networks use either proprietary or non-IP based communication protocols, the communication network uses IP-based network. Since non-IP based protocols are used within M2M area network, the M2M nodes within one network cannot communicate with nodes in an external network.
- To enable the communication between remote M2M are network, M2M gateways are used

b) Cyber-Physical systems:

Cyber-Physical Systems (CPS) are integrations of computation, networking, and physical processes. Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa.

In cyber-physical systems, physical and software components are deeply intertwined, able to operate on different spatial and temporal scales, exhibit multiple and distinct behavioural modalities, and interact with each other in ways that change with context.

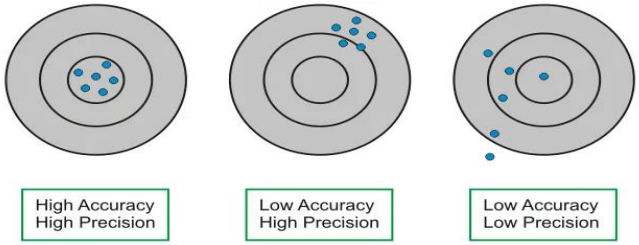
c) **Web of Things**: web of things is a term used to describe approaches, software architectural style of programming patterns that allow real world objects to be part of WWW. The major portion of the WoT specification is the Thing Description. Thing is an abstract representation of a physical or virtual entity. A Thing Description includes the metadata and interfaces of a Thing in a standardized way, with the aim to make the Thing able to communicate with other Things in a heterogeneous world.

SENSOR

Sensor is a device used for the conversion of physical events or characteristics into the electrical signals. This is a hardware device that takes the input from environment and gives to the system by converting it.
For example, a thermometer takes the temperature as physical characteristic and then converts it into electrical signals for the system.

Characteristics of Sensors

1. Range: It is the minimum and maximum value of physical variable that the sensor can sense or measure. For example, a Resistance Temperature Detector (RTD) for the measurement of temperature has a range of -200 to 800°C.
2. Span: It is the difference between the maximum and minimum values of input. In above example, the span of RTD is 800 – (-200) = 1000°C.
3. Accuracy: The error in measurement is specified in terms of accuracy. It is defined as the difference between measured value and true value. It is defined in terms of % of full scale or % of reading.
4. Precision: It is defined as the closeness among a set of values. It is different from accuracy.



5.Linearity: Linearity is the maximum deviation between the measured values of a sensor from ideal curve.

6.Hysteresis: It is the difference in output when input is varied in two ways- increasing and decreasing.

7. Resolution: It is the minimum change in input that can be sensed by the sensor.
8. Reproducibility: It is defined as the ability of sensor to produce the same output when same input is applied.
9. Repeatability: It is defined as the ability of sensor to produce the same output every time when the same input is applied and all the physical and measurement conditions kept the same including the operator, instrument, ambient conditions etc.
10. Response Time: It is generally expressed as the time at which the output reaches a certain percentage (for instance, 95%) of its final value, in response to a step change of the input.

Classification of sensors:

- Sensors based on the power requirement sensor is classified into two types: Active Sensors, Passive Sensors.

Active Sensors: Does not need any external energy source but directly generates an electric signal in response to the external.

Example: Thermocouple, Photodiode, Piezoelectric sensor.

Passive Sensors: The sensors require external power called excitation signal. Sensors modify the excitation signal to provide output.

Example: Strain gauge.

- Sensors based on output sensor is classified into two types: Analog Sensors, Digital Sensors.

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).
- Digital signal only produces discrete (non-continuous) values, which may be output as a signal "bit" (serial transmission), or by combing the bits to produce a signal "byte" output (parallel transmission).

- Based on type of data measured sensor is classified into two types: Scalar Sensors and Vector Sensors.

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.

ACTUATOR

Actuator is a device that converts the electrical signals into the physical events or characteristics. It takes the input from the system and gives output to the environment. For example, motors and heaters are some of the commonly used actuators.

Types of Actuators

1. Hydraulic Actuators: Hydraulic actuators operate by the use of a fluid-filled cylinder with a piston suspended at the centre. Commonly, hydraulic actuators produce linear movements, and a spring is attached to one end as a part of the return motion. These actuators are widely seen in exercise equipment such as steppers or car transport carriers.

2. Pneumatic Actuators: Pneumatic actuators are one of the most reliable options for machine motion. They use pressurized gases to create mechanical movement. Many companies prefer pneumatic-powered actuators because they can make very precise motions, especially when starting and stopping a machine. Examples of equipment that uses pneumatic actuators include: Bus brakes, Exercise machines, Vane motors, Pressure sensors

3.Electric Actuators : Electrical actuators, as you may have guessed, require electricity to work. Well-known examples include electric cars, manufacturing machinery, and robotics equipment. Similar to pneumatic actuators, they also create precise motion as the flow of electrical power is constant.

4.Thermal and Magnetic Actuators : Thermal and magnetic actuators usually consist of shape memory alloys that can be heated to produce movement. The motion of thermal or magnetic actuators often comes from the Joule effect, but it can also occur when a coil is placed in a static magnetic field. The magnetic field causes constant motion called the Laplace-Lorentz force. Most thermal and magnetic actuators can produce a wide and powerful range of motion while remaining lightweight.

5.Mechanical Actuators : Some actuators are mostly mechanical, such as pulleys or rack and pinion systems. Another mechanical force is applied, such as pulling or pushing, and the actuator will leverage that single movement to produce the desired results. For instance, turning a single gear on a set of rack and pinions can mobilize an object from point A to point B. The tugging movement applied on the pulley can bring the other side upwards or towards the desired location.

6. Soft Actuators: Soft actuators (e.g. polymer based) are designed to handle fragile objects like fruit harvesting in agriculture or manipulating the internal organs in biomedicine.

They typically address challenging tasks in robotics. Soft actuators produce flexible motion due to the integration of microscopic changes at the molecular level into a macroscopic deformation of the actuator materials.

IOT COMPONENTS

Four fundamental components of IoT system, which tells us how IoT works.

i. Sensors/Devices

First, sensors or devices help in collecting very minute data from the surrounding environment. All of this collected data can have various degrees of complexities ranging from a simple temperature monitoring sensor or a complex full video feed.

A device can have multiple sensors that can bundle together to do more than just sense things. For example, our phone is a device that has multiple sensors such as GPS, accelerometer, camera but our phone does not simply sense things.

ii. Connectivity

Next, that collected data is sent to a cloud infrastructure but it needs a medium for transport.

The sensors can be connected to the cloud through various mediums of communication and transports such as cellular networks, satellite networks, Wi-Fi, Bluetooth, wide-area networks (WAN), low power wide area network and many more.

iii. Data Processing

Once the data is collected and it gets to the cloud, the software performs processing on the acquired data.

This can range from something very simple, such as checking that the temperature reading on devices such as AC or heaters is within an acceptable range. It can sometimes also be very complex, such as identifying objects (such as intruders in your house) using computer vision on video.

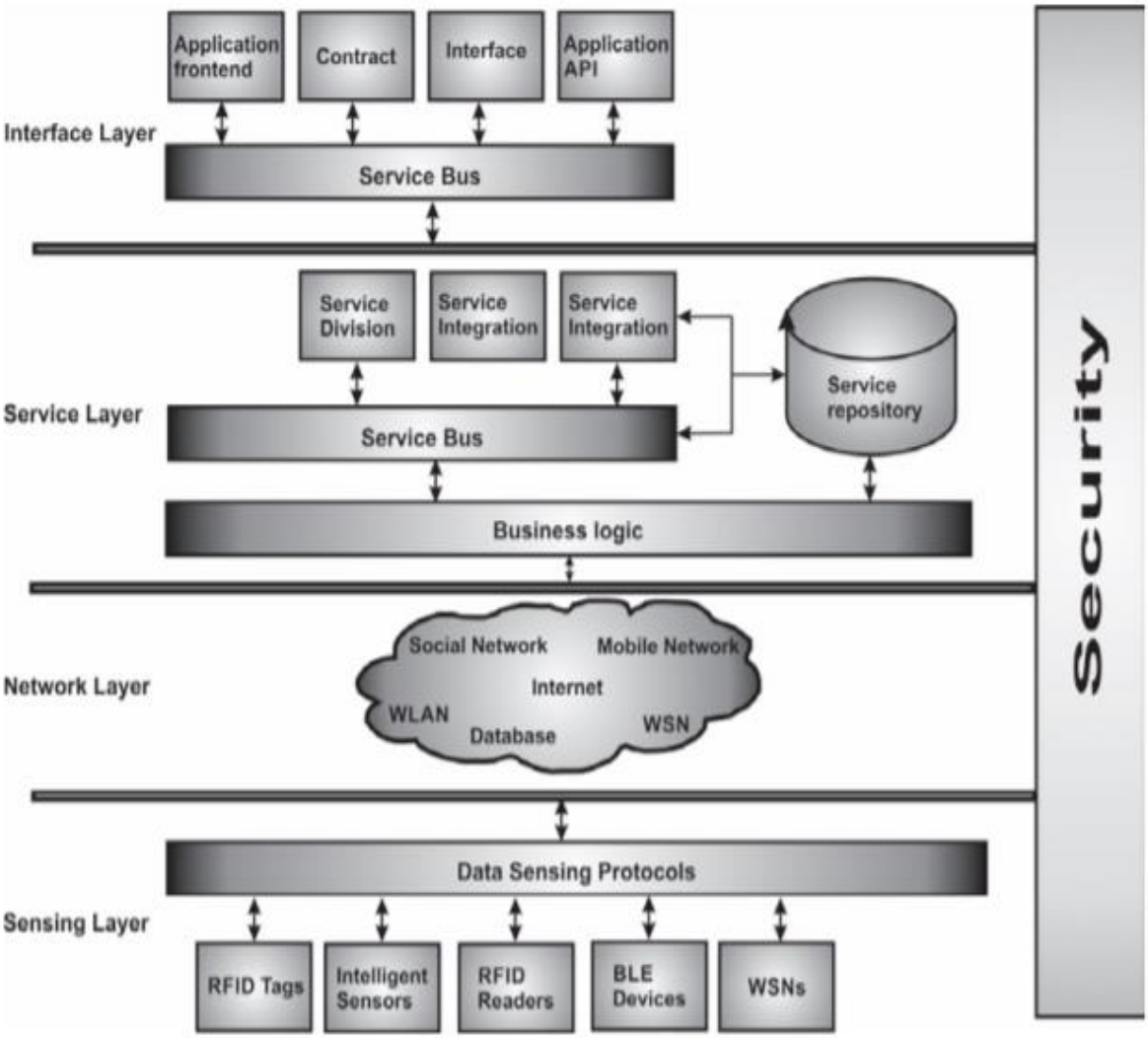
iv. User Interface

Next, the information made available to the end-user in some way. This can achieve by triggering alarms on their phones or notifying through texts or emails.

Also, a user sometimes might also have an interface through which they can actively check in on their IOT system. For example, a user has a camera installed in his house, he might want to check the video recordings and all the feeds through a web server.

Service Oriented Architecture of IoT

SOA can also use to support IoT as a main contributing technology in devices or heterogeneous systems.



Service-Oriented Architecture for IoT technologies.

1.Sensing Layer: IoT can be defined as a worldwide interconnected network, where things or devises are controlled remotely. Interconnected things or devices are become easier, as more and more things are furnished with sensors and RFID technologies.

2.Networking Layer: Networking Layer is responsible to connect all device or things together so that they can able to share the information with each other over the Internet. Moreover, network layer also collects data and information from the present IT infrastructure for example ICT systems, power grids, business systems, healthcare systems, and transportation systems.

3. Service Layer: This layer depends upon the technology used on the middleware layer which is responsible for functionalities incorporate between applications and services in IoT. This middleware technology also provides a cost-effective and efficient platform for IoT and this platform including software and hardware components which can be reused when needed.

4. Interface Layer: The core responsibility of the interface layer has also simplified the interconnection and management of things. Interface specific profile can be defined as the subset of services that support interaction with the application used in a network

Challenges for IoT

1. Security: Security is the most significant challenge for the IoT. Increasing the number of connected devices increases the opportunity to exploit security vulnerabilities, as do poorly designed devices, which can expose user data to theft by leaving data streams inadequately protected and in some cases people's health and safety can be put at risk.

2. Privacy: The IoT creates unique challenges to privacy, many that go beyond the data privacy issues that currently exist. Much of this stems from integrating devices into our environments without us consciously using them. This is becoming more prevalent in consumer devices, such as tracking devices for phones and cars as well as smart televisions.

3. Scalability: Billions of internet-enabled devices get connected in a huge network, large volumes of data are needed to be processed. The system that stores, analyses the data from these IoT devices needs to be scalable.

4. Interoperability: Technological standards in most areas are still fragmented. These technologies need to be converged. Which would help us in establishing a common framework and the standard for the IoT devices. As the standardization process is still lacking, interoperability of IoT with legacy devices should be considered critical. This lack of interoperability is preventing us to move towards the vision of truly connected everyday interoperable smart objects.

5. Bandwidth: Connectivity is a bigger challenge to the IoT than you might expect. As the size of the IoT market grows exponentially, some experts are concerned that bandwidth-intensive IoT applications such as video streaming will soon struggle for space on the IoT's current server-client model.

6. Standards: Lack of standards and documented best practices have a greater impact than just limiting the potential of IoT devices. Without standards to guide manufacturers, developers sometimes design products that operate in disruptive ways on the Internet without much regard to their impact. If poorly designed and configured, such devices can have negative consequences for the networking resources they connect to and the broader Internet.

7. Regulation: The lack of strong IoT regulations is a big part of why the IoT remains a severe security risk, and the problem is likely to get worse as the potential attack surface expands to include ever more crucial devices. When medical devices, cars and children's toys are all connected to the Internet, it's not hard to imagine many potential disaster scenarios unfolding in the absence of sufficient regulation

UNIT-2

IOT Networking

Connectivity Terminologies

IoT Node : These are machines , things or computers Connected to other nodes inside a LAN via the IoT LAN, May be sometimes connected to the internet through a WAN directly

IoT LAN : It is Local, Short range Comm, May or may not connect to Internet, Building or Organization wide

IoT WAN: Connection of various network segments, Organizationally and geographically wide, Connects to the internet

IoT Gateway : A router connecting the IoT LAN to a WAN to the Internet, Can implement several LAN and WAN, Forwards packets between LAN and WAN on the IP layer

IoT Proxy: Performs active application layer functions between IoT nodes and other entities

Gateway Prefix Allotment:

- ✓ One of the strategies of address conservation in IoT is to use local addresses which exist uniquely within the domain of the gateway. These are represented by the circles in this slide.
- ✓ The network connected to the internet has routers with their set of addresses and ranges.
- ✓ These routers have multiple gateways connected to them which can forward packets from the nodes, to the Internet, only via these routers. These routers assign prefixes to gateways under them, so that the gateways can be identified with them.

Impact of Mobility on Addressing

- ✓ The network prefix changes from 1 to 2 due to movement, making the IoT LAN safe from changes due to movements.
- ✓ IoT gateway WAN address changes without change in LAN address. This is achieved using ULA.
- ✓ The gateways assigned with prefixes, which are attached to a remote anchor point by using various protocols such as Mobile IPv6, and are immune to changes of network prefixes.
- ✓ This is achieved using LU. The address of the nodes within the gateways remain unchanged as the gateways provide them with locally unique address and the change in gateway's network prefix doesn't affect them.
- ✓ Sometimes, there is a need for the nodes to communicate directly to the internet. This is achieved by tunneling, where the nodes communicate to a remote anchor point instead of channeling their packets through the router which is achieved by using tunneling protocols such as IKEv2:internet key exchange version 2

Multihoming

Multihoming is the practice of connecting a host or a computer network to more than one network. This can be done in order to increase reliability or performance or to reduce cost. There are several different ways to perform multihoming.

Host multihoming

A single host may be connected to multiple networks. For example, a mobile phone might be simultaneously connected to a WiFi network and a 3G network, and a desktop computer might be connected to both a home network and a VPN. A multihomed host usually is assigned multiple addresses, one per connected network.

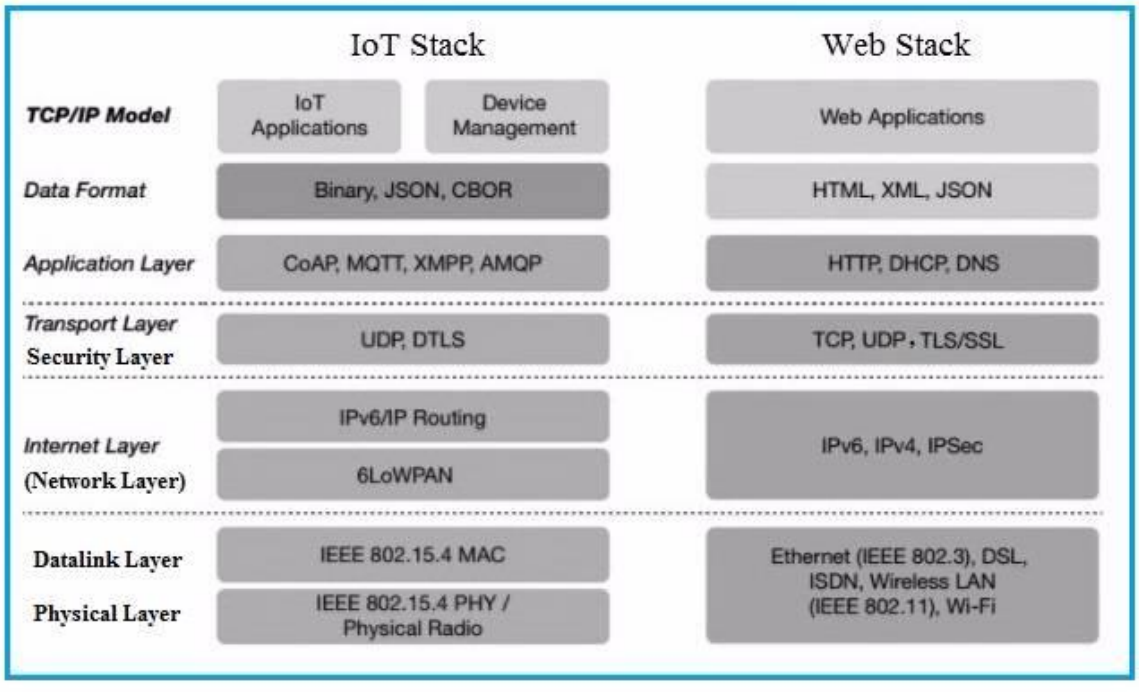
Classical multihoming

In classical multihoming a network is connected to multiple providers, and uses its own range of addresses (typically from a Provider Independent (PI) range). The network's edge routers communicate with the providers using a dynamic routing protocol, typically BGP, which announces the network's address range to all providers. If one of the links fails, the dynamic routing protocol recognizes the failure within seconds or minutes, and reconfigures its routing tables to use the remaining links, transparently to the hosts.

Multihoming with multiple addresses

In this approach, the network is connected to multiple providers, and assigned multiple address ranges, one for each provider. Hosts are assigned multiple addresses, one for each provider.

Deviation from regular Web



Features	IoT Stack	Web Stack
Function or application	It is used in constrained network having low power, low bandwidth and low memory requirements.	It is used in non-constrained network having no limits on power/BW/memory.
Size of data to be transported	tens of bytes	hundreds or thousands of bytes
Data format	It uses CBOR (Concise Binary Object Representation) format as IoT is used for tiny messages. CBOR is based on JSON though CBOR uses binary encoding while JSON uses text encoding.	It uses HTML, XML and JSON formats.
Application Layer	It uses CoAP protocol at application layer.	It uses HTTP protocol at application layer.
Transport layer	It uses UDP which is faster due to smaller header size compare to TCP. It is lighter protocol compare to TCP.	It uses TCP which is connection oriented and slower compare to UDP.
Security layer	It uses DTLS (Datagram Transport Layer Security) protocol for security.	It uses TLS/SSL protocols for the same.
Internet layer	It uses 6LoWPAN to convert large IPv6 packets into small size packets to be carried on wireless medium as per bluetooth, zigbee etc. standards. It does fragmentation and reassembly. It also does header compression to reduce packet size.	It does not require protocols like 6LoWPAN. Fragmentation and reassembly is taken care by transport layer (i.e. TCP) itself.
Datalink or MAC layer	It will have MAC layer as per IoT wireless technology used viz. bluetooth, zigbee, zwave etc. It takes care of medium access control and resource allocation and management.	It will have MAC layer as per LAN or WLAN or DSL or ISDN technologies.
Physical layer and Radio Frequency (RF) layer	It will have physical layer (baseband) as per IoT wireless technologies viz. bluetooth, zigbee, zwave etc. It uses frequencies as per cellular or indoor wireless technologies and country wide allocations for the same.	It will have PHY layer as per LAN or WLAN or DSL or ISDN technologies.

IoT identification and Data protocols

IPv4:

IP version four addresses are 32-bit integers which will be expressed in dotted decimal notation. Example- 192.0.2.126 could be an IPv4 address.

Characteristics of IPv4

- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields is twelve and the length of the header field is twenty.
- It has Unicast, broadcast, and multicast style of addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask).
- IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causing host.

IPv4 Datagram Header

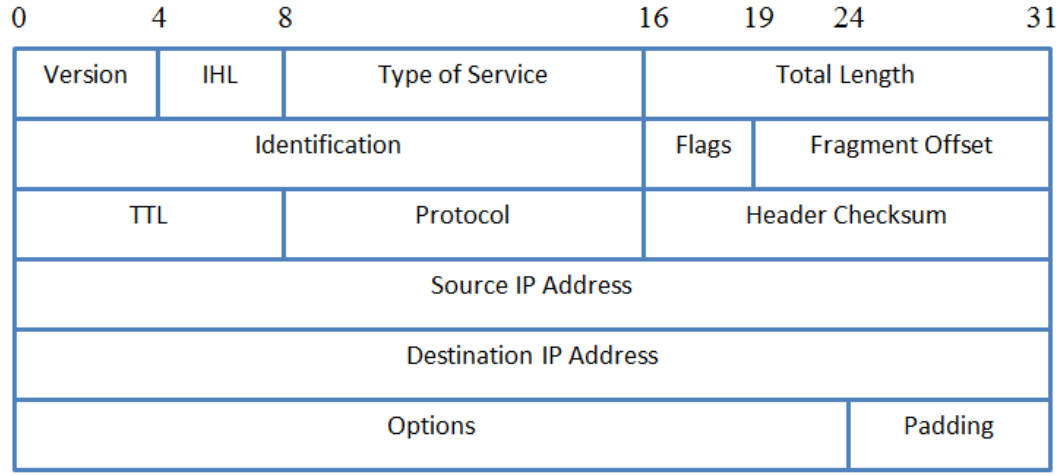


Fig: IPv4 Frame Format

Version:

This field indicates the version number of the IP packet so that the revised version can be distinguished from the previous version. The current IP version is 4.

Internet Header Length (IIHL):

It specifies the length of the IP header in unit 32 bits. In case of no option present in the IP header, IHL will have a value of 5. So, if the value of IHL is more than 5 then the length of the option field can be easily calculated.

Type of Service: This field specifies the priority of the packets based on delay, throughput, reliability and cost requirements. Three bits are assigned for priority level and four bits for specific requirements (delay, throughput, reliability and cost).

Total Length:

This field specifies the number of bytes of the IP packet including header and data. As 16 bits are assigned to this field, the maximum length of the packet is 65635 bytes.

Identification:

The identification field is used to identify which packet a particular fragment belongs to so that fragments for different packets don't get mixed up.

Flags:

The flag field has three bits:

1. Unused bit

2. Don't fragment (DF) bit

3. More fragment (MF) bit

Fragment Offset:

The fragment offset field identifies the location of the fragment in a packet. The value measures the offset in a unit of 8 bytes, between the beginning of the packet to be fragmented and the beginning of the fragment.

Time to live (TTL):

This field is used to indicate the amount of time in seconds a packet is allowed to remain in the network.

Protocol:

This field specifies the protocol that is to receive the IP data at the destination host.

Header Checksum:

This field verifies the integrity of the header of the IP packet. The integrity of the data part is left to the upper layer protocols. The checksum is generated by the source and it is sent along with the frame header to the next router.

Source IP address & Destination IP address:

These two fields contain the IP addresses of the source and destination hosts respectively.

Options:

Options fields are rarely used to include special features such as security level, the route to be taken and time stamp at each router. It is used in RSVP.

Padding:

This field is used to make the header a multiple of 32-bit words.

IPv6

Internet Protocol version 6 (IPv6) is also known as **Internet Protocol next generation** (**IPng**). It also accommodates more feature to meet the global requirement of growing Internet.
To allocate a sufficient number of network address, IPv6 allows 128 bits of IP address separated into 8 sections of 2 bytes each. Unlike IPv4 where the address is represented as dotted-decimal notation, IPv6 uses hexadecimal numbers and colon (**":"**) is used as a delimiter between the sections.
Example: IPv6 address may be like this :

FA20:B120:6230:0000:0000:CE12:0006:ABDF

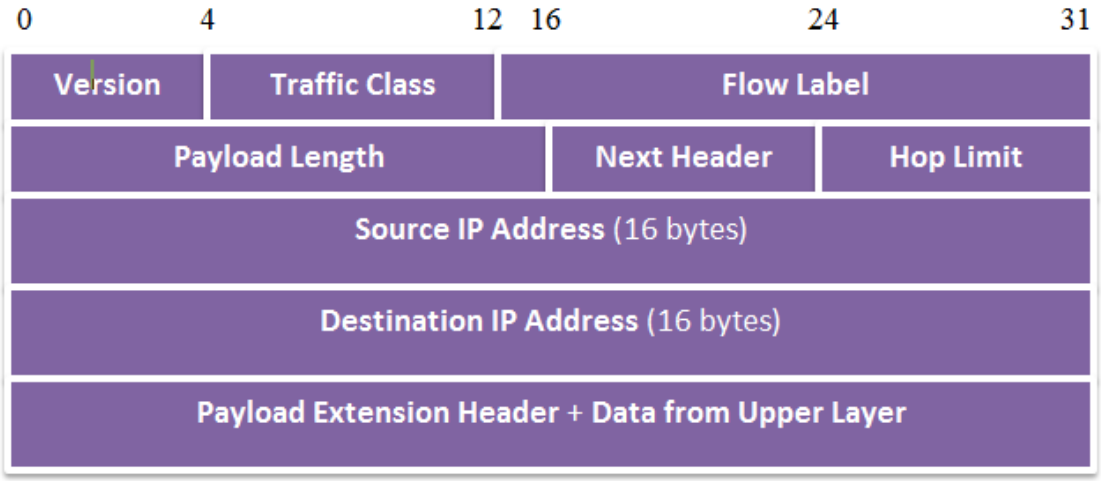


Fig: IPv6 Packet Format

Version: This field is 4 bits long and it defines the version of the IP packet. The value of it for IPv6 is 6 and IPv4 its value is 4. During the transition period from IPv4 to IPv6, the routers will be able to distinguish the two versions of the IP packets.
Traffic Class: This field is 20 bits long and it is used to distinguish between the different requirements for real-time delivery services.
Flow Label: This field is 20 bits long and it is used to allow the source and destination nodes to set up a pseudo connection with particular properties and requirements. It is designed to provide special handling of a particular flow of data.
Payload Length: It is of 2 bytes length and signifies the number of bytes that follow the 40 bytes base header. It is the length of the IP datagram excluding the base header.
Next Header: This field is of 1 bye length and it defines one of the extension headers that follow the base header. The extension headers also contain this field to indicate the next header. if this is the last IP header then Next header field tells which of the transport protocols (TCP or UDP) the packet is to be passed.
Hop Limit: This field contains 1 byte and it signifies the maximum number of hops a packet can travel. The time to live field in the IPv4 header did the same task, except that in IPv4 it was counted in time and in IPv6 it is counted in terms of the number of routers.
Source Address: It is 16 bytes long and contains the IP address of the source machine to the network interface.
Destination Address: It is 16 bytes long and usually contains the IP address of the ultimate destination machine to the network interface. In case of specific routing, it may contain the IP address of the next router.
Extension Header: Some of the fields Ipv4 that are missing in IPv6 is necessary in some of the cases. To handle this problem, IPv6 has introduced the concept of the extension header. There are be one or more of the six possible extension headers. These headers appear directly after the base header.

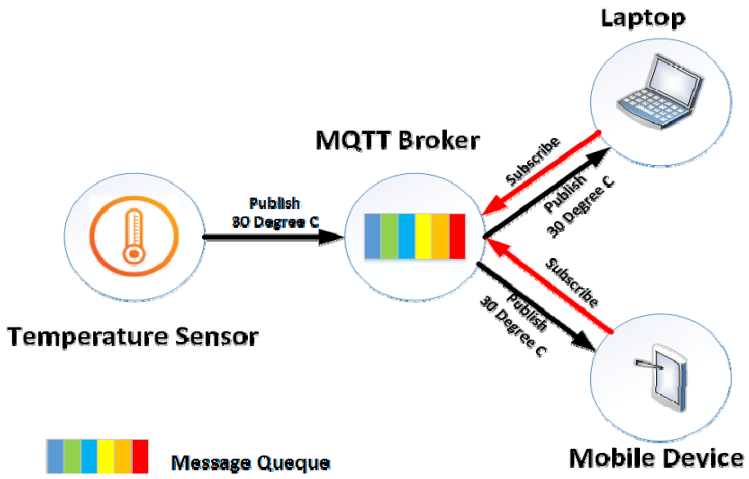
MQTT

- ✓ It is a publish-subscribe-based lightweight messaging protocol for use in conjunction with the TCP/IP protocol.
- ✓ Designed to provide connectivity (mostly embedded) between applications and middle-wares on one side and networks and communications on the other side.
- ✓ A message broker controls the publish-subscribe messaging pattern.
- ✓ A topic to which a client is subscribed is updated in the form of messages and distributed by the message broker.
- ✓ Designed for: Remote connections, Limited bandwidth, Small-code footprint

MQTT Components

- **Publishers:** Lightweight sensors
- **Subscribers:** Applications interested in sensor data
- **Brokers:** Connect publishers and subscribers and Classify sensor data into topics

Communication:



- ✓ The protocol uses a **publish/subscribe** architecture (HTTP uses a request/response paradigm).
- ✓ Publish/subscribe is **event-driven** and enables messages to be pushed to clients.
- ✓ The central **communication point is the MQTT broker**, which is in charge of dispatching all messages between the senders and the rightful receivers.
- ✓ Each client that publishes a message to the broker, includes a **topic** into the message. The **topic is the routing information for the broker.**
- ✓ Each client that wants to receive messages subscribes to a certain topic and the broker delivers all messages with the matching topic to the client.
- ✓ Therefore the clients don't have to know each other. They only communicate over the topic.

- ✓ This architecture enables highly scalable solutions without dependencies between the data producers and the data consumers.

Applications

- ✓ **Facebook Messenger** uses MQTT for online chat.
- ✓ **Amazon Web Services** use Amazon IoT with MQTT.
- ✓ **Microsoft Azure** IoT Hub uses MQTT as its main protocol for telemetry messages.
- ✓ The **EVRYTHNG IoT platform** uses MQTT as an M2M protocol for millions of connected products.
- ✓ **Adafruit** launched a free MQTT cloud service for IoT experimenters called Adafruit IO.

SMQTT

- ✓ **Secure MQTT** is an extension of MQTT which uses encryption based on lightweight attribute based encryption.
- ✓ The main advantage of using such encryption is the broadcast encryption feature, in which one message is encrypted and delivered to multiple other nodes, which is quite common in IoT applications.
- ✓ In general, the algorithm consists of four main stages: setup, encryption, publish and decryption.

CoAP

- ✓ CoAP – **Constrained Application Protocol**.
- ✓ **Web transfer protocol** for use with constrained nodes and networks.
- ✓ **Designed for Machine to Machine** (M2M) applications such as smart energy and building automation and Based on **Request-Response model** between end-points
- ✓ Client-Server interaction is **asynchronous over a datagram oriented transport protocol** such as UDP
- ✓ The Constrained Application Protocol (CoAP) is a session layer protocol designed by IETF Constrained RESTful Environment (CoRE) working group to provide lightweight RESTful (HTTP) interface.
- ✓ Representational State Transfer (REST) is the standard interface between HTTP client and servers.
- ✓ Lightweight applications such as those in IoT, could result in significant overhead and power consumption by REST.
- ✓ CoAP is designed to enable low-power sensors to use RESTful services while meeting their power constraints
- ✓ Built over UDP, instead of TCP (which is commonly used with HTTP) and has a light mechanism to provide reliability.
- ✓ CoAP architecture is divided into two main sub-layers:

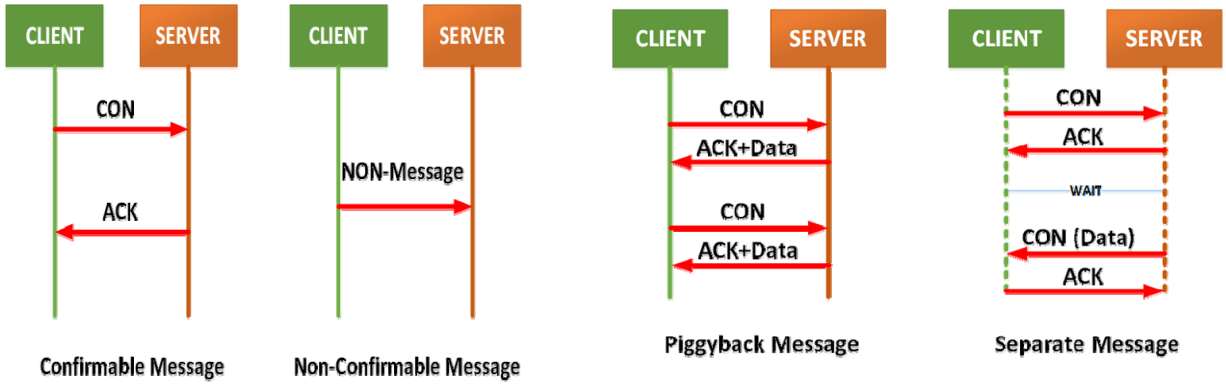
- Messaging
- Request/response.

✓ The messaging sub-layer is responsible for reliability and duplication of messages, while the request/response sub-layer is responsible for communication.

✓ CoAP has four messaging modes:

- Confirmable
- Non-confirmable
- Piggyback
- Separate

CoAP Request-Response Model



✓ Confirmable and non-confirmable modes represent the reliable and unreliable transmissions, respectively, while the other modes are used for request/response.

✓ Piggyback is used for client/server direct communication where the server sends its response directly after receiving the message, i.e., within the acknowledgment message.

✓ On the other hand, the separate mode is used when the server response comes in a message separate from the acknowledgment, and may take some time to be sent by the server.

✓ Similar to HTTP, CoAP utilizes GET, PUT, PUSH, DELETE messages requests to retrieve, create, update, and delete, respectively

XMPP

✓ XMPP – Extensible Messaging and Presence Protocol.

✓ A communication protocol for message-oriented middleware based on XML (Extensible Markup Language).

✓ Real-time exchange of structured data.

✓ It is an open standard protocol

✓ XMPP uses a client-server architecture.

- ✓ As the model is decentralized, no central server is required.
- ✓ XMPP provides for the discovery of services residing locally or across a network, and the availability information of these services.
- ✓ Well-suited for cloud computing where virtual machines, networks, and firewalls would otherwise present obstacles to alternative service discovery and presence-based solutions.
- ✓ Open means to support machine-to-machine or peer-to-peer communications across a diverse set of networks.

Applications:

- ✓ Publish-subscribe systems
- ✓ Signaling for VoIP
- ✓ Video
- ✓ File transfer
- ✓ Gaming
- ✓ Internet of Things applications: Smart grid and Social networking services

AMQP

- ✓ Advanced Message Queuing Protocol.
- ✓ Open standard for passing business messages between applications or organizations.
- ✓ Connects between systems and business processes.
- ✓ It is a binary application layer protocol.
- ✓ Basic unit of data is a *frame*

Components

Exchange:

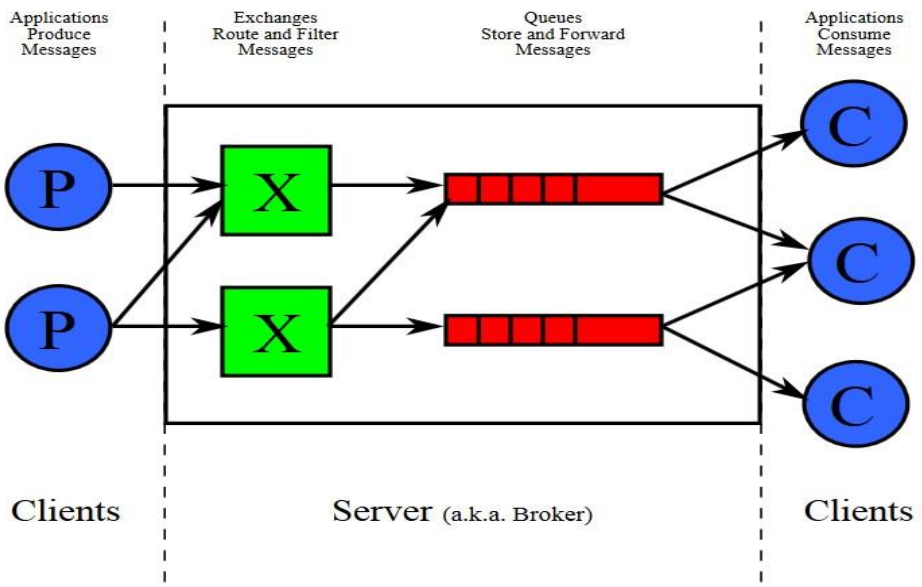
- ✓ Part of Broker
- ✓ Receives messages and routes them to Queues

Queue :

- ✓ Separate queues for separate business processes
- ✓ Consumers receive messages from queues

Bindings:

- ✓ Rules for distributing messages (who can access what message, destination of the message)



AMQP Features

- ✓ Targeted QoS (Selectively offering QoS to links)
- ✓ Persistence (Message delivery guarantees)
- ✓ Delivery of messages to multiple consumers
- ✓ Possibility of ensuring multiple consumption
- ✓ Possibility of preventing multiple consumption
- ✓ High speed protocol

Applications

- ✓ Monitoring and global update sharing.
- ✓ Connecting different systems and processes to talk to each other.
- ✓ Allowing servers to respond to immediate requests quickly and delegate time consuming tasks for later processing.
- ✓ Distributing a message to multiple recipients for consumption.
- ✓ Enabling offline clients to fetch data at a later time.
- ✓ Introducing fully asynchronous functionality for systems.
- ✓ Increasing reliability and uptime of application deployments.

UNIT-3

Connectivity Technologies

- Communication Protocols: The following communication protocols have immediate importance to consumer and industrial IoTs:
    - IEEE 802.15.4
    - Zigbee
    - 6LoWPAN
    - Wireless HART
    - Z-Wave
    - ISA 100
    - Bluetooth
    - NFC
    - RFID

IEEE 802.15.4

Features of IEEE 802.15.4:

- ✓ Well-known standard for low data-rate WPAN.
- ✓ Developed for low-data-rate monitoring and control applications and extended-life low-power-consumption uses.
- ✓ This standard uses only the first two layers (PHY, MAC) plus the logical link control (LLC) and service specific convergence sub-layer (SSCS) additions to communicate with all upper layers
- ✓ Uses direct sequence spread spectrum (DSSS) modulation.
- ✓ Highly tolerant of noise and interference and offers link reliability improvement mechanisms.
- ✓ Low-speed versions use Binary Phase Shift Keying (BPSK).
- ✓ High data-rate versions use offset-quadrature phase-shift keying (O-QPSK).
- ✓ Uses carrier sense multiple access with collision avoidance (CSMA-CA) for channel access.
- ✓ Multiplexing allows multiple users or nodes interference-free access to the same channel at different times.
- ✓ Networking topologies defined are -- Star, and Mesh.

IEEE 802.15.4 supports two types of network node:

1. **Full Function Device (FFD)**
   - Can talk to all types of devices
   - Supports full protocol
2. **Reduced Function Device (RFD)**
   - Can only talk to an FFD
   - Lower power consumption
   - Minimal CPU/RAM required

IEEE 802.15.4 Types:

1. Beacon Enabled Networks

- Periodic transmission of beacon messages
- Data-frames sent via Slotted CSMA/CA with a super frame structure managed by PAN coordinator. Beacons used for synchronization & association of other nodes with the coordinator
- Scope of operation spans the whole network**.**

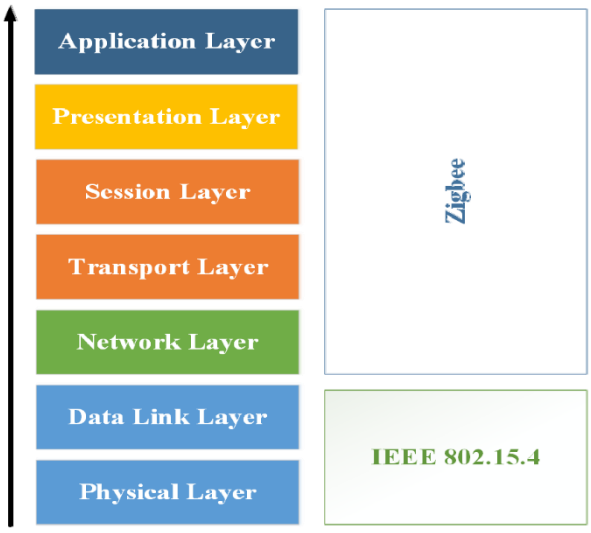
2. Non-Beacon Enabled Networks

- Data-frames sent via un-slotted CSMA/CA (Contention Based)
- Beacons used only for link layer discovery
- Requires both source and destination IDs.
- As 802.15.4 is primarily, a mesh protocol, all protocol addressing must adhere to mesh configurations
- De-centralized communication amongst nodes

ZigBee

Features of ZigBee

- ✓ Most widely deployed enhancement of IEEE 802.15.4.
- ✓ The ZigBee protocol is defined by layer 3 and above. It works with the 802.15.4 layers 1 and 2.
- ✓ The standard uses layers 3 and 4 to define additional communication enhancements.
- ✓ These enhancements include authentication with valid nodes, encryption for security, and a data routing and forwarding capability that enables mesh networking.



- ✓ The most popular use of ZigBee is wireless sensor networks using the mesh topology.

ZigBee has two important components:

- ZigBee Device Object(ZDO): ZDO responsible for Device management, Security, Policies
- Application Support Sub-layer(APS) :APS responsible for Interfacing and control services, bridge between network and other layers

ZigBee Types

***1.ZigBee Coordinator (ZC)*:**

- The Coordinator forms the root of the ZigBee network tree and might act as a bridge between networks.
- There is a single ZigBee Coordinator in each network, which originally initiates the network.
- It stores information about the network under it and outside it.
- It acts as a Trust Center & repository for security keys**.**

2. *ZigBee Router (ZR)*: Capable of running applications, as well as relaying information between nodes connected to it.

***3. ZigBee End Device (ZED)*:**

- It contains just enough functionality to talk to the parent node, and it cannot relay data from other devices.
- This allows the node to be asleep a significant amount of the time thereby enhancing battery life.
- Memory requirements and cost of ZEDs are quite low, as compared to ZR or ZC.

Applications:

- ✓ Building automation
- ✓ Remote control (RF4CE or RF for consumer electronics)
- ✓ Smart energy for home energy monitoring
- ✓ Health care for medical and fitness monitoring
- ✓ Home automation for control of smart homes
- ✓ Light Link for control of LED lighting
- ✓ Telecom services.

6LoWPAN

- ✓ Low-power Wireless Personal Area Networks over IPv6.
- ✓ Allows for the smallest devices with limited processing ability to transmit information wirelessly using an Internet protocol.
- ✓ Allows low-power devices to connect to the Internet.
- ✓ Created by the Internet Engineering Task Force (IETF) - RFC 5933 and RFC 4919.

Features of 6LoWPANs

- ✓ Allows IEEE 802.15.4 radios to carry 128-bit addresses of Internet Protocol version 6 (IPv6).
- ✓ Header compression and address translation techniques allow the IEEE 802.15.4 radios to access the Internet.
- ✓ IPv6 packets compressed and reformatted to fit the IEEE 802.15.4 packet format.
- ✓ Uses include IoT, Smart grid, and M2M applications.

Addressing in 6LoWPAN

- 64-bit addresses: globally unique
- 16 bit addresses: PAN specific; assigned by PAN coordinator

6LoWPAN Routing

- ✓ Mesh routing within the PAN space.
- ✓ Routing between IPv6 and the PAN domain
- ✓ Routing protocols in use:
    - LOADng
    - RPL

LOADng Routing

- ✓ Basic operations of LOADng include:
    - Generation of Route Requests (RREQs) by a LOADng Router (originator) for discovering a route to a destination,
    - Forwarding of such RREQs until they reach the destination LOADng Router,
    - Generation of Route Replies (RREPs) upon receipt of an RREQ by the indicated destination, and unicast hop-by-hop forwarding of these RREPs towards the originator.
    - If a route is detected to be broken, a Route Error (RERR) message is returned to the originator of that data packet to inform the originator about the route breakage.

RPL Routing

- ✓ Distance Vector IPv6 routing protocol for lossy and low power networks.
- ✓ Maintains routing topology using low rate beaconing.
- ✓ Beaconing rate increases on detecting inconsistencies (e.g. node/link in a route is down).
- ✓ Routing information included in the datagram itself.
- ✓ **Proactive:** Maintaining routing topology.
- ✓ **Reactive:** Resolving routing inconsistencies**.**

RFID

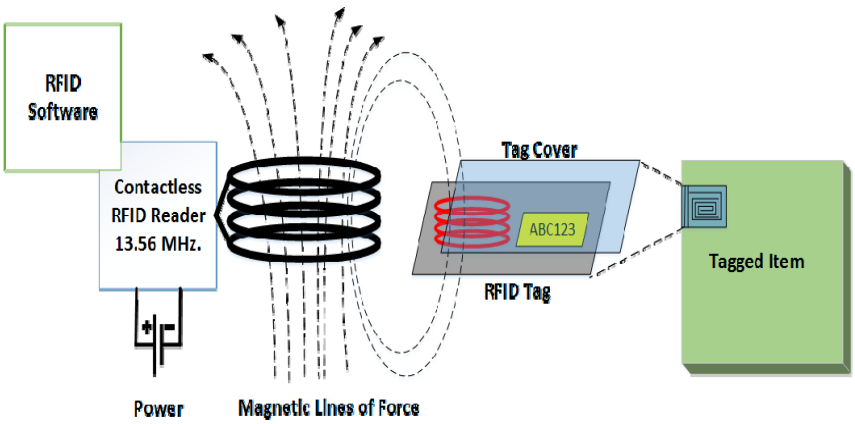
- ✓ RFID is an acronym for “radio-frequency identification”
- ✓ Data digitally encoded in RFID tags, which can be read by a reader.
- ✓ Somewhat similar to barcodes.
- ✓ Data read from tags are stored in a database by the reader.
- ✓ As compared to traditional barcodes and QR codes, RFID tag data can be read outside the line-of-sight.

RFID Features

- ✓ RFID tag consists of an integrated circuit and an antenna.
- ✓ The tag is covered by a protective material which also acts as a shield against various environmental effects.
- ✓ Tags may be passive or active.
- ✓ Passive RFID tags are the most widely used.
- ✓ Passive tags have to be powered by a reader inductively before they can transmit information, whereas active tags have their own power supply.

Working Principle

- ✓ Derived from Automatic Identification and Data Capture (AIDC) technology.
- ✓ AIDC performs object identification, object data collection and mapping of the collected data to computer systems with little or no human intervention.
- ✓ AIDC uses wired communication
- ✓ RFID uses radio waves to perform AIDC functions.
- ✓ The main components of an RFID system include an RFID tag or smart label, an RFID reader, and an antenna.



Applications

1. Inventory management 2. Asset tracking 3. Personnel tracking 4. Controlling access to restricted areas 5. ID badging 6. Supply chain management 7. Counterfeit prevention (e.g. in the pharmaceutical industry)

HART & Wireless HART

- ✓ WirelessHART is the latest release of Highway Addressable Remote Transducer (HART) Protocol.
- ✓ HART standard was developed for networked smart field devices.
- ✓ The wireless protocol makes the implementation of HART cheaper and easier.
- ✓ HART encompasses the most number of field devices incorporated in any field network.
- ✓ Wireless HART enables device placements more accessible and cheaper– such as the top of a reaction tank, inside a pipe, or at widely separated warehouses.
- ✓ Main difference between wired and unwired versions is in the physical, data link and network layers. Wired HART lacks a network layer.

HART Physic al Layer

- ✓ Derived from IEEE 802.15.4 protocol.
- ✓ It operates only in the 2.4 GHz ISM band.
- ✓ Employs and exploits 15 channels of the band to increase reliability.

HART Data Link Layer

- ✓ Collision free and deterministic communication achieved by means of super-frames and TDMA. Super-frames consist of grouped 10ms wide timeslots.
- ✓ Super-frames control the timing of transmission to ensure collision free and reliable communication.
- ✓ This layer incorporates channel hopping and channel blacklisting to increase reliability and security. Channel blacklisting identifies channels consistently affected by interference and removes them from use.

HART Network & Transport Layers

- ✓ Cooperatively handle various types of traffic, routing, session creation, and security.
- ✓ Wireless HART relies on Mesh networking for its communication, and each device is primed to forward packets from every other devices. Each device is armed with an updated network graph (i.e., updated topology) to handle routing.
- ✓ Network layer (HART)=Network + Transport + Session layers (OSI)

HART Application Layer

- ✓ Handles communication between gateways and devices via a series of command and response messages.
- ✓ Responsible for extracting commands from a message,

  executing it and generating responses.
- ✓ This layer is seamless and does not differentiate between wireless and wired versions of HART.

NFC

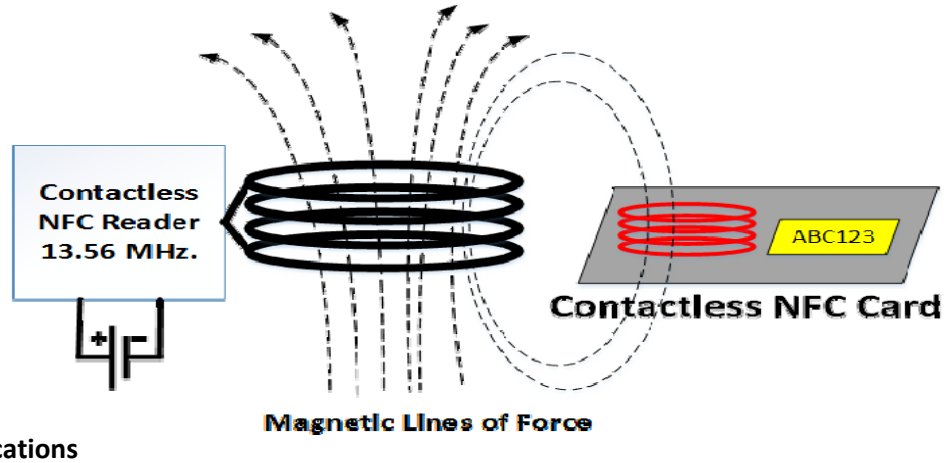
- ✓ Near field communication, or NFC for short, is an offshoot of radio-frequency identification (RFID).
- ✓ NFC is designed for use by devices within close proximity to each other.
- ✓ All NFC types are similar but communicate in slightly different ways.

NFC Types

- ✓ **Passive devices** contain information which is readable by other devices, however it cannot read information itself.
- ✓ NFC tags found in supermarket products are examples of passive NFC.
- ✓ **Active devices** are able to collect as well as transmit information.
- ✓ Smartphones are a good example of active devices.

Working Principle

- ✓ Works on the principle of magnetic induction.
- ✓ A reader emits a small electric current which creates a magnetic field that in turn bridges the physical space between the devices.
- ✓ The generated field is received by a similar coil in the client device where it is turned back into electrical impulses to communicate data such as identification number status information or any other information.
- ✓ 'Passive' NFC tags use the energy from the reader to encode their response while 'active' or 'peer-to-peer' tags have their own power source.



NFC Applications

- ✓ Smartphone based payments.
- ✓ Parcel tracking.
- ✓ Information tags in posters and advertisements.
- ✓ Computer game synchronized toys.
- ✓ Low-power home automation systems.

Bluetooth

- ✓ Bluetooth wireless technology is a short range communications technology.
- ✓ Intended for replacing cables connecting portable units
- ✓ Maintains high levels of security.
- ✓ Bluetooth technology is based on Ad-hoc technology also known as Ad-hoc Piconets

Features

- ✓ Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHZ.
- ✓ Uses spread spectrum hopping, full-duplex signal at a nominal rate of 1600 hops/sec.
- ✓ Bluetooth supports 1Mbps data rate for version 1.2 and 3Mbps data rate for Version 2.0 combined with Error Data Rate.
- ✓ Bluetooth operating range depends on the device:

  - Class 3 radios have a range of up to 1 meter or 3 feet
  - Class 2 radios are most commonly found in mobile devices have a range of 10 meters or 30 feet
  - Class 1 radios are used primarily in industrial use cases have a range of 100 meters or 300 feet.

Connection Establishment

- ✓ **Inquiry:** Inquiry run by one Bluetooth device to try to discover other devices near it.
- ✓ **Paging:** Process of forming a connection between two Bluetooth devices.
- ✓ **Connection:** A device either actively participates in the network or enters a low-power sleep mode

Piconets:

- ✓ Bluetooth enabled electronic devices connect and communicate wirelessly through short range networks known as Piconets.
- ✓ Bluetooth devices exist in small ad-hoc configurations with the ability to act either as master or slave. Provisions are in place, which allow for a **master** and a **slave** to switch their roles.
- ✓ The simplest configuration is a point to point configuration with one master and one slave.
- ✓ Devices in adjacent Piconets provide a bridge to support inner-Piconet connections, allowing assemblies of linked Piconets to form a physically extensible communication infrastructure known as Scatternet

Applications

- ✓ Audio players
- ✓ Home automation
- ✓ Smartphones
- ✓ Toys
- ✓ Hands free headphones
- ✓ Sensor networks

Z Wave

- ✓ Zwave is a protocol for communication among devices used for home automation.
- ✓ It uses RF for signaling and control.
- ✓ Operating frequency is 908.42 MHz in the US & 868.42 MHz in Europe.
- ✓ Mesh network topology is the main mode of operation, and can support 232 nodes in a network.
- ✓ Zwave utilizes GFSK modulation and Manchester channel encoding.
- ✓ A central network controller device sets-up and manages a Zwave network.
- ✓ Each logical Zwave network has 1 Home (Network) ID and multiple node IDs for the devices in it.
- ✓ Nodes with different Home IDs cannot communicate with each other.
- ✓ Network ID length=4 Bytes, Node ID length=1 Byte.

ISA 100.11A

- ✓ ISA is acronym International Society of Automation.
- ✓ Designed mainly for large scale industrial complexes and plants.
- ✓ More than 1 billion devices use ISA 100.11A
- ✓ ISA 100.11A is designed to support native and tunnelled application layers.
- ✓ Various transport services, including 'reliable,' 'best effort,' 'real-time' are offered.
- ✓ Network and transport layers are based on TCP or UDP / IPv6.
- ✓ Data link layer supports mesh routing and Frequency hopping.
- ✓ Physical and MAC layers are based on IEEE 802.15.4
- ✓ Topologies allowed are:
    - Star/tree
    - Mesh
- ✓ Permitted networks include:
    - Radio link
    - ISA over Ethernet
    - Field buses

UNIT-4

Wireless Sensor Networks

Wireless Sensor Networks (WSNs):

- WSN Consists of a large number of sensor nodes, densely deployed over an area.
- Sensor nodes are capable of collaborating with one another and measuring the condition of their surrounding environments (i.e. Light, temperature, sound, vibration).
- The sensed measurements are then transformed into digital signals and processed to reveal some properties of the phenomena around sensors.

Components of a Sensor Node:

In any wireless sensor network, sensor node consists of four basic components, a sensing unit, a processing unit, a transceiver unit, and a power unit. They may also have additional application dependent components such as a location finding system, power generator and mobilize

Challenges in WSN:

Energy: Power consumption can be allocated to three functional domains: sensing, communication, and data processing, each of which requires optimization. The sensor node lifetime typically exhibits a strong dependency on battery life. The constraint most often associated with sensor network design is that sensor nodes operate with limited energy budgets.

Limited bandwidth: Bandwidth limitation directly affects message exchanges among sensors, and synchronization is impossible without message exchanges. Sensor networks often operate in a bandwidth and performance constrained multi-hop wireless communications medium. These wireless communications links operate in the radio, infrared, or optical range.

Node Costs: A sensor network consists of a large set of sensor nodes. It follows that the cost of an individual node is critical to the overall financial metric of the sensor network. Clearly, the cost of each sensor node has to be kept low for the global metrics to be acceptable.

Deployment Node: A proper node deployment scheme can reduce the complexity of problems. Deploying and managing a high number of nodes in a relatively bounded environment requires special techniques. Hundreds to thousands of sensors may be deployed in a sensor region.

Security: One of the challenges in WSNs is to provide high security requirements with constrained resources. Many wireless sensor networks collect sensitive information. The remote and unattended operation of sensor nodes increases their exposure to malicious intrusions and attacks. The security requirements in WSNs are comprised of node authentication and data confidentiality. To identify both trustworthy and unreliable nodes from a security stand points, the deployment sensors must pass a node authentication examination by their corresponding manager nodes or cluster heads and unauthorized nodes can be isolated from WSNs during the node authentication procedure.

SENSOR WEB

the sensor web is a type of sensor network that is especially well suited for environmental monitoring. The sensor web is also associated with a sensing system which heavily utilizes the World Wide Web.

Sensor Web Enablement (SWE)

Sensor Web Enablement (SWE) is a suite of standards developed and maintained by Open Geospatial Consortium. SWE standards enable developers to make all types of sensors, transducers and sensor data repositories discoverable, accessible and usable via the Web.

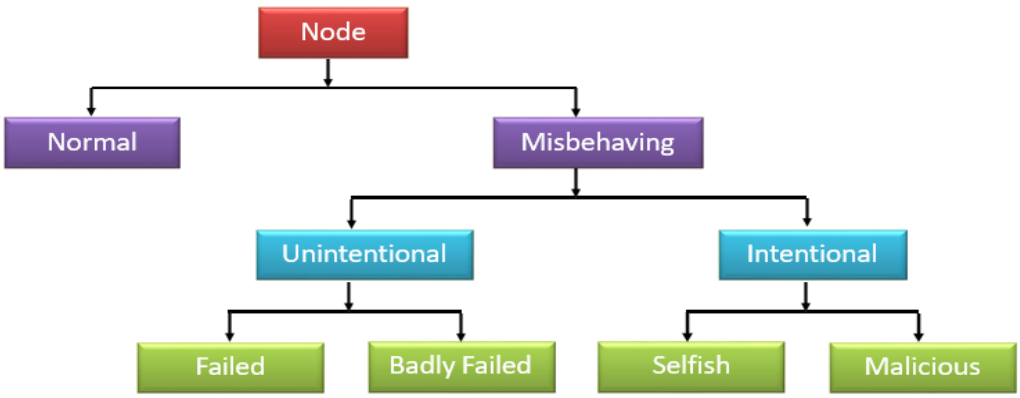
SWE Standards include:

- Sensor Observation Service
- Sensor Planning Service
- Observations and Measurements
- Sensor Model Language
- Sensor Things API

Cooperation in Wireless Ad Hoc and Sensor Networks

- Nodes communicate with other nodes with the help of intermediate nodes.
- The intermediate nodes act as relays.
- Wireless nodes are energy-constrained.
- Nodes may or may not cooperate.
- Two extremities for Cooperation:
    - **Total cooperation:** if all relay requests are accepted, nodes will quickly exhaust limited energy.
    - **Total non-cooperation:** if no relay requests are accepted, the network throughput will go down rapidly.

Node Behaviour in WSNs:



- Normal nodes work perfectly in ideal environmental conditions
- Failed nodes are simply those that are unable to perform an operation; this could be because of power failure and environmental events.
- Badly failed nodes exhibit features of failed nodes but they can also send false routing messages which are a threat to the integrity of the network.

- Selfish nodes are typified by their unwillingness to cooperate, as the protocol requires whenever there is a personal cost involved. Packet dropping is the main attack by selfish nodes.
- Malicious nodes aim to deliberately disrupt the correct operation of the routing protocol, denying network service if possible.

Dynamic Misbehaviour (Dumb behaviour):

- Detection of such temporary misbehaviour in order to preserve normal functioning of the network – coinage and discovery of dumb behaviour
- In the presence of adverse environmental conditions (high temperature, rainfall, and fog) the communication range shrinks
- A sensor node can sense its surroundings but is unable to transmit the sensed data
- With the resumption of favourable environmental conditions, dumb nodes work normally
- Dumb behaviour is temporal in nature (as it is dependent on the effects of environmental conditions)

Self-Management of Wireless Sensor Networks:

- A WSN is deployed with the intention of acquiring information
- The sensed information is transmitted in the form of packets
- Information theoretic self-management (INTSEM) controls the transmission rate of a node by adjusting a node's sleep time
- Benefits
    - Reduce consumption of transmission energy of transmitters
    - Reduce consumption of receiving energy of relay nodes

Social sensing WSN

- ✓ Social Sensing-based Duty Cycle Management for Monitoring Rare Events in Wireless Sensor Networks
    - ✓ WSNs are energy-constrained Scenario:
    - Event monitoring using WSNs
    - WSNs suffer from ineffective sensing for rare events
    - Event monitoring or sensing, even if there is no event to monitor or sense
    - Example: Submarine monitoring in underwater surveillance
- ✓ Challenges:
    - Distinguish rare events and regular events
    - Adapt the duty-cycle with the event occurrence probability.
- ✓ Contribution:
    - Probabilistic duty cycle (PDC) in WSNs

- Accumulates information from the social media to identify the occurrence possibility of rare events
- Adjusts the duty cycles of sensor nodes using weak estimation learning automata

Applications of WSNs:

1. Mines

- ✓ Fire Monitoring and Alarm System for Underground Coal Mines Bord-and-Pillar Panel Using Wireless Sensor Networks
  - WSN-based simulation model for building a fire monitoring and alarm (FMA) system for Bord & Pillar coal mine.
  - The fire monitoring system has been designed specifically for Bord & Pillar based mines
  - It is not only capable of providing real-time monitoring and alarm in case of a fire, but also capable of providing the exact fire location and spreading direction by continuously gathering, analysing, and storing real time information

2. Healthcare

- ✓ Wireless Body Area Networks
  - Wireless body area networks (WBANs) have recently gained popularity due to their ability in providing innovative, cost-effective, and user-friendly solution for continuous monitoring of vital physiological parameters of patients.
  - Monitoring chronic and serious diseases such as cardiovascular diseases and diabetes.
  - Could be deployed in elderly persons for monitoring their daily activities.

3.Internet of Things (IOT)
4. Surveillance and Monitoring for security, threat detection
5. Environmental temperature, humidity, and air pressure
6. Noise Level of the surrounding
7. Landslide Detection

Wireless Multimedia Sensor Networks (WMSNs)

- Incorporation of low-cost camera (typically CMOS) to wireless sensor nodes
- **Camera sensor (CS) nodes:** capture multimedia (video, audio, and the scalar) data, expensive and resource hungry, directional sensing range
- **Scalar sensor (SS) nodes:** sense scalar data (temperature, light, vibration, and so on), omni-directional sensing range, and low cost
- WMSNs consist of a smaller number of CS nodes and large number of SS nodes

WMSNs Application

- In security surveillance, wild-habitat monitoring, environmental monitoring, SS nodes cannot provide precise information
- CS nodes replace SS nodes to get precise information
- Deployment of both CS and SS nodes can provide better sensing and prolong network lifetime

Nanonetworks:

- Nanodevice has components of sizes in the order nano-meters.
- Communication options among nanodevices
  - Electromagnetic
  - Molecular

Molecular Communication:

- Molecule used as information
- Information packed into vesicles
- Gap junction works as mediator between cells and vesicles
- Information exchange between communication entities using molecules

Electromagnetic-based Communication

- Surface Plasmonic Polariton (SPP) generated upon electromagnetic beam
- EM communication for Nanonetworks centres around 0.1-10 Terahertz channel

Underwater Acoustic Sensor Networks

- In a layered shallow oceanic region, the inclusion of the effect of internal solitons on the performance of the network is important.
- Based on various observations, it is proved that non-linear internal waves, i.e., Solitons are one of the major scatters of underwater sound.
- If sensor nodes are deployed in such type of environment, inter-node communication is affected due to the interaction of wireless acoustic signal with these solitons, as a result of which network performance is greatly affected.
- The performance analysis of UWASNs renders meaningful insights with the inclusion of a mobility model which represents realistic oceanic scenarios.
- The existing works on performance analysis of UWASNs lack the consideration of major dominating forces, which offer impetus for a node's mobility.

WSN Coverage:

- ✓ Coverage – area-of-interest is covered satisfactorily
- ✓ Connectivity – all the nodes are connected in the network, so that sensed data can reach to sink node
- ✓ Sensor Coverage studies how to deploy or activate sensors to cover the monitoring area
    - Sensor placement
    - Density control
- ✓ Two modes
    - Static sensors
    - Mobile sensors
- ✓ Determine how well the sensing field is monitored or tracked by sensors
- ✓ To determine, with respect to application-specific performance criteria,
    - in case of static sensors, where to deploy and/or activate them
    - in case of (a subset of) the sensors are mobile, how to plan the trajectory of the mobile sensors.
- ✓ These two cases are collectively termed as the coverage problem in wireless sensor networks.
- ✓ The purpose of deploying a WSN is to collect relevant data for processing or reporting
- ✓ Two types of reporting
    - ✓ event driven: e.g., forest fire monitoring
    - ✓ on demand: e.g., inventory control system
- ✓ Objective is to use a minimum number of sensors and maximize the network lifetime
- ✓ The coverage algorithm proposed are either centralized or distributed and localized
- ✓ Distributed: Nodes compute their position by communicating with their neighbours only.
- ✓ Centralized: Data collected at central point and global map computed.
- ✓ Localized: Localized algorithms are a special type of distributed algorithms where only a subset of nodes in the WASN participate in sensing, communication, and computation.

Stationary Wireless Sensor Networks

- ✓ Sensor nodes are static
- ✓ Advantages:
    - Easy deployment
    - Node can be placed in an optimized distance—Reduce the total number of nodes

- Easy topology maintenance

✓ Disadvantages:

- Node failure may result in partition of networks
- Topology cannot be change automatically

Mobile Wireless Sensor Networks

- MWSN is Mobile Ad hoc Network (MANET)
- Let us remember from previous lectures: -
- MANET-Infrastructure less network of mobile devices connected wirelessly which follow the self-CHOP properties
  - Self-Configure
  - Self-Heal
  - Self-Optimize
  - Self-Protect
- Wireless Sensor Networks-
  - Consists of a large number of sensor nodes, densely deployed over an area.
  - Sensor nodes are capable of collaborating with one another and measuring the condition of their surrounding environments (i.e. Light, temperature, sound, vibration).

Components of MWSN:

Mobile Sensor Nodes: Sense physical parameters from the environment When these nodes come in close proximity of sink, deliver data.

Mobile Sink: Moves in order to collect data from sensor nodes. Based on some algorithm sink moves to different nodes in the networks

Data Mules: A mobile entity Collects the data from sensor nodes and Goes to the sink and delivers the collected data from different sensor nodes

UNIT-5

Machine to Machine Communication

M2M Communication: M2M, is the Communication between machines or devices with computing and communication facilities, without any human intervention.

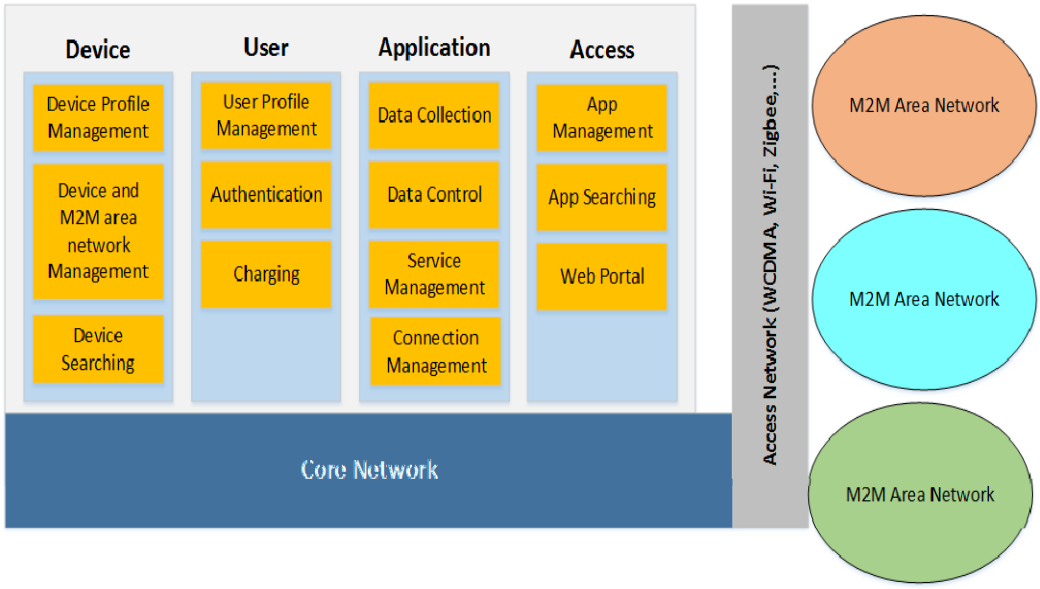
Features of M2M:

- Large number of nodes or devices.
- Low cost.
- Energy efficient.
- Small traffic per machine/device.
- Large quantity of collective data.
- M2M communication free from human intervention.
- Human intervention required for operational stability and sustainability

M2M Ecosystem: It comprises of Device Providers, Internet Service Providers (ISPs), Platform Providers, Service Providers and Service Users.

The device provider is basically the owner of these devices. M2M area network sends the data from M2M devices, through gateway to the internet which is handled by the internet service provider. RESTful architecture acts as an interface between the device provider and the internet service provider. . RESTful architecture is used in low resource environment. From the ISP the reaches the platform provider. The platform provider takes care of device management, user management, data Analytics and user access is the data is then through a RESTful architecture which takes care of the the business model to the service providers and users.

M2M Service Platform (M2SP)



M2M Device Platform:

- ✓ Enables access to objects or devices connected to the Internet anywhere and at any time.
- ✓ Registered devices create a database of objects from which managers, users and services can easily access information.
- ✓ Manages device profiles, such as location, device type, address, and description.
- ✓ Provides authentication and authorization key management functionalities.
- ✓ Monitors the status of devices and M2M area networks, and controls them based on their status.

M2M User Platform

- ✓ Manages M2M service user profiles and provides functionalities such as,
    - User registration
    - Modification
    - Charging
    - Inquiry.
- ✓ Interoperates with the Device-platform, and manages user access restrictions to devices, object networks, or services.
- ✓ Service providers and device managers have administrative privileges on their devices or networks.
- ✓ Administrators can manage the devices through device monitoring and control.

M2M Application Platform

- ✓ Provides integrated services based on device collected data- sets.
- ✓ Heterogeneous data merging from various devices used for creating new services.
- ✓ Collects control processing log data for the management of the devices by working with the Device-platform.
- ✓ Connection management with the appropriate network is provided for seamless services.

M2M Access Platform

- ✓ Provides app or web access environment to users.
- ✓ Apps and links redirect to service providers.
- ✓ Services actually provided through this platform to M2M devices.
- ✓ Provides App management for smart device apps.
- ✓ App management manages app registration by developers and provides a mapping relationship between apps and devices.
- ✓ Mapping function provides an app list for appropriate devices.

Interoperability in Internet of Things

Interoperability is a characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, present or future, in either implementation or access, without any restrictions.

Need of Interoperability:

- ✓ To fulfil the IoT objectives
    - Physical objects can interact with any other physical objects and can share their information
    - Any device can communicate with other devices anytime from anywhere
    - Machine to Machine communication(M2M), Device to Device Communication (D2D), Device to Machine Communication (D2M)
    - Seamless device integration with IoT network
- ✓ Heterogeneity
    - Different wireless communication protocols such as ZigBee (IEEE 802.15.4), Bluetooth (IEEE 802.15.1), GPRS, 6LowPAN, and Wi-Fi (IEEE 802.11)
    - Different wired communication protocols like Ethernet (IEEE 802.3) and Higher Layer LAN Protocols (IEEE 802.1)
    - Different programming languages used in computing systems and websites such as JavaScript, JAVA, C, C++, Visual Basic, PHP, and Python
    - Different hardware platforms such as Crossbow, NI, etc.
    - Different operating systems
    - As an example, for sensor node: TinyOS, SOS, Mantis OS, RETOS, and mostly vendor specific OS
    - As an example, for personal computer: Windows, Mac, Unix, and Ubuntu
    - Different databases: DB2, MySQL, Oracle, PostgreSQL, SQLite, SQL Server, and Sybase
    - Different data representations
    - Different control models
    - Syntactic or semantic interpretations

Types of Interoperability

User Interoperability: Interoperability problem between a user and a device

The following problems need to be solved

- ✓ Device identification and categorization for discovery:
- ✓ Syntactic interoperability for device interaction
- ✓ Semantic interoperability for device interaction

Device identific ation and categorization for discovery: There are different solutions for generating unique address like Electronic Product Codes (EPC), Universal Product Code (UPC), Uniform Resource Identifier (URI), IP Addresses (IPv6)

Syntactic Interoperability for Device Interaction:

- The interoperability between devices and device user in term of message formats
- The message format from a device to a user is understandable for the user's computer
- On the other hand, the message format from the user to the device is executable by the device

Semantic Interoperability for Device Interaction:

- The interoperability between devices and device user in term of message's meaning
- The device can understand the meaning of user's instruction that is sent from the user to the device.
- Similarly, the user can understand the meaning of device's response sent from the device

Device Interoperability: Interoperability problem between two different devices

Solution approach for device interoperability

✓ Universal Middleware Bridge (UMB)

- Solves seamless interoperability problems caused by the heterogeneity of several kinds of home network middleware
- UMB creates virtual maps among the physical devices of all middleware home networks, such as HAVI, Jini, LonWorks, and UPnP
- Creates a compatibility among these middleware home networks
- UMB consists of UMB Core (UMB-C) and UMB Adaptor (UMB-A)
- UMB-A converts physical devices into virtually abstracted one, as described by Universal Device Template (UDT)
- UDT consists of a Global Device ID, Global Function ID, Global Action ID, Global Event ID, and Global Parameters
- UMB Adaptors translate the local middleware's message into global metadata's message
- The major role of the UMB Core is routing the universal metadata message to the destination or any other UMB Adaptors by the Middleware Routing Table (MRT)