1. THE INTERNET OF THINGS AN OVERVIEW

1.1. THE FLAVORS OF THE INTERNET

My Train-Schedule Alarm Clock:

- The alarm rings.
- As we open our eyes dim, we see that it’s five minutes later than our usual wake-up time.
- It was just a simple state machine that slept until it got close to wake-up time, then it started Monitoring the departure boards.
- The clock has checked the train times online, and your train must be delayed, so it lets you sleep a little longer.

Vitality Glow Cap:

- Vitality Glow Cap is an easy-to-use, comprehensive medication adherence system consisting of a smart cap and bottle, Vitality Mobile Application, and the Vitality Medication Adherence Portal.
- Automated visual and audible alerts are scheduled during dosage windows which signals that it is time for the user to take his or her medications.
- A blinking light reminds you it’s time to take your tablets.
- If you forget, the medicine bottle cap goes online and emails your doctor, care managers, and trusted family and friends to let them know.

Umbrella with Weather-Forecasting

- A model for appropriate embedded technology, the Forecast umbrella provides information about the likelihood of rain so that users can make a simple decision about whether to take their umbrella with them as they leave for home.
- Using existing Wi-Fi technology to wirelessly pull information from the internet, Forecast’s lighted umbrella handle is lit up, which means that it has checked the BBC weather reports and predicted rain.

Nike + Health App:

- A pedometer in your training shoes and a heart monitor in your wrist band help track your run around the block.
- The wrist band’s large display also makes it easy to glance down and see how fast you are running and how many calories you’ve burned.
- All the data is automatically uploaded to your sports tracking site, which also integrates with your online supermarket shopping account to make it easy to compare with how many calories you’ve eaten.

Transport for London:

- The bus company first installed those displays, they ran on the expected timetable information only, but now that every bus has GPS tracking its location, they simply connect to the bus company’s online service and always give the updated information.
- As you pass the bus stop on the way to the station, you notice the large LCD display flash that the number 23 is due.

Where dial:

- Your phone checks you in automatically to a location-based service (such as Foursquare).
- On your mantelpiece at home, an ornament with a dial notices the change and starts to turn so that the text on it points to the word “Traveling”.
- Your family will also see later that you’ve arrived at “Work” safely.

1.2. THE INTERNET OF THINGS FAQ

1. Define and explain Internet Of Things and Ubiquitous Computing
2. Explain the components of the Internet of Things.
3. Define and Explain Internet of Things

1.2.1. Introduction

- IoT stands for Internet of Things.
- It refers to the interconnectedness of physical devices, such as appliances and vehicles that are embedded with software, sensors, and connectivity which enables these objects to connect and exchange data.
- This technology allows for the collection and sharing of data from a vast network of devices, creating opportunities for more efficient and automated systems.
- In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives.

1.2.2. Definition

IoT is a network of interconnected computing devices which are embedded in everyday objects, enabling them to send and receive data.

1.2.3. Working of IoT

- Devices have hardware, like sensors, that collect data.
- The data collected by the sensors is processed by the processors.
- The processed data is then shared via the cloud and integrated with software.
- The software then analyzes and transmits the data to users via an app or website.

1.2.4. Building blocks of IoT

- Five things form basic building blocks of the IoT system –Things or Device, gateways, cloud, analytics and user interface.
- Each of these nodes has to have its own characteristics in order to form a useful IoT system.

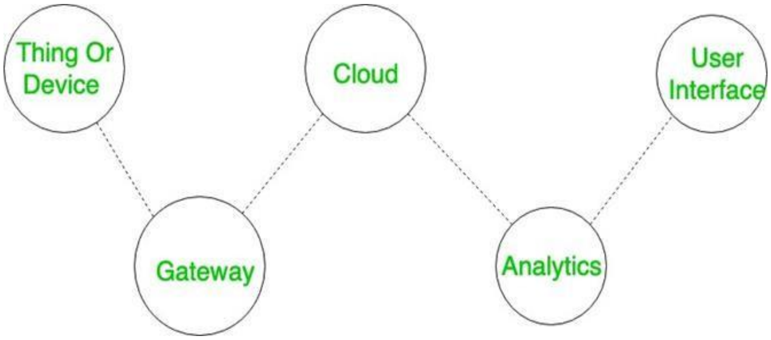


Figure 1: Building Blocks of IoT or Devices

Things or Device

- These are fitted with sensors and actuators.
- Sensors collect data from the environment and give it to the gateway whereas actuators perform the action (as directed after processing of data).

Gateway

- The sensors give data to Gateway and here some kind of pre-processing of data is even done.
- It also acts as a level of security for the network and for the transmitted data.

Cloud

- The data after being collected is uploaded to the cloud.
- Cloud in simple terms is basically a set of servers connected to internet 24*7.

Analytics

- The data after being received in the cloud processing is done.
- Various algorithms are applied here for proper analysis of data (techniques like Machine Learning etc. are even applied).

User Interface

- User end application where user can monitor or control the data.

1.2.5. Equation of Internet of Things

- Physical Object + Controllers, Sensors and Actuators + Internet = Internet of Things

1.2.6. Advantages of IoT

- It can assist in the smarter control of homes and cities via mobile phones. It enhances security and offers personal protection.
- By automating activities, it saves us a lot of time.
- Information is easily accessible, even if we are far away from our actual location, and it is updated frequently in real time.
- Electric Devices are directly connected and communicate with a controller computer, such as a cell phone, resulting in efficient electricity use. As a result, there will be no unnecessary use of electricity equipment.
- It minimizes human effort because IoT devices connect and communicate with one another and perform a variety of tasks without the need for human intervention.
- Patient care can be performed more effectively in real time without the need for a doctor’s visit. It gives them the ability to make choices as well as provide evidence based care.
- Asset tracking, traffic or transportation tracking, inventory control, delivery, surveillance, individual order tracking, and customer management can all be made more cost-effective with the right tracking system.

1.2.7. Disadvantages of IoT

- Hackers may gain access to the system and steal personal information. Since we add so many devices to the internet, there is a risk that our information can be misused.
- They rely heavily on the internet and are unable to function effectively without it.
- With the complexity of systems, there are many ways for them to fail.
- Unskilled workers are at a high risk of losing their jobs, which could lead to unemployment. Smart surveillance cameras, robots, smart ironing systems, smart washing machines, and other facilities are replacing security guards, maids, ironmen, and dry-cleaning services etc.
- It is very difficult to plan, build, manage, and enable a broad technology to IoT framework.
- Deploying IoT devices is very costly and time-consuming.

1.3. THE TECHNOLOGY OF INTERNET

Trigger to Technology

- Technology's great drivers have initially been fundamental needs, such as food and water, warmth, safety, and health.
- Hunting and foraging, fire, building and fortifications, and medicine grew out of these needs.
- Then, because resources for these things are not always distributed where and when one might like, technological advances progressed with enabling and controlling the movement of people, their possessions, livestock, and other resources.

Movement of Information

- Information became the key for the development of language to communicate technology to others.
- Travelers might pass on messages as well as goods and services, and an oral tradition allows this information to pass through time as well as space.
- The invention of writing made this communication ever more important and allowed, to some extent, human lives to be preserved in words by and about writers, from the ancient philosophers and poets to the present day.
- From writing, via the telegraph, radio, and television, to digital information, more and more technology has been about enabling the movement of information or doing interesting things with that information.

Emergence of the Electronic Age

- As technology has progressed, new categories of objects have been created.
- In the electronic age, they have included telephones, radios, televisions, computers, and smartphones.
- As with most new technology, these devices tended to start out very expensive and gradually come down in price.
- Demand drives down prices, and research leads to optimization and miniaturization.
- Ultimately, it becomes not just possible but also feasible to include functionality that would previously have required its own dedicated device inside another one.

Emergence of cheaper wireless Internet connectivity

- Internet Connectivity is also cheaper and more convenient than it used to be.
- Wired Ethernet provides a fairly plug-and-play networking experience, but most home routers today also offer Wi-Fi, which removes the need for running cables everywhere.

Maturity of Online Platforms

- Another factor at play is the maturity of online platforms.
- Whereas early web apps were designed to be used only from a web browser, the much heralded "Web 2.0", as well as bringing us "rich web apps", popularized a style of programming using an Application Programming Interface (API), which allows other programs, rather than just users, to interact with and use the services on offer.
- This provides a ready ecosystem for other websites to "mash up" a number of services into something new, enables mobile phone "Apps", and now makes it easy for connected devices to consume.
- As the online services mature, so too do the tools used to build and scale them.
- Web services frameworks such as Python and Django or Ruby on Rails allow easy prototyping of the online component.
- Similarly, cloud services such as Amazon Web Services mean that such solutions can scale easily with use as they become more popular.

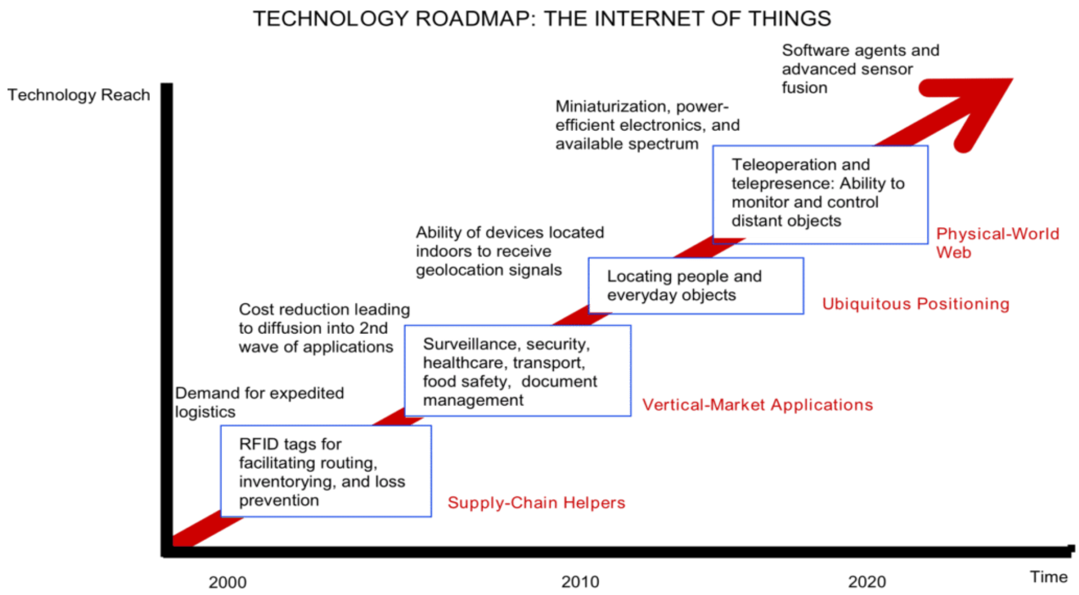

TECHNOLOGY ROADMAP: THE INTERNET OF THINGS
Technology Reach
Software agents and advanced sensor fusion
Miniaturization, power-efficient electronics, and available spectrum
Teleoperation and telepresence: Ability to monitor and control distant objects
Physical-World Web
Ability of devices located indoors to receive geolocation signals
Locating people and everyday objects
Ubiquitous Positioning
Cost reduction leading to diffusion into 2nd wave of applications
Surveillance, security, healthcare, transport, food safety, document management
Vertical-Market Applications
Demand for expedited logistics
RFID tags for facilitating routing, inventorying, and loss prevention
Supply-Chain Helpers
2000
2010
2020
Time

Figure 2: Technology Roadmap

1.4. ENCHANTED OBJECTS FAQ

1. "Any sufficiently advanced technology is indistinguishable from magic." Discuss.

- Technology has evolved to meet our needs and desires.
- The parallel invention of magic serves largely similar goals.
- Enchanted objects are ordinary objects with extraordinary functions and has categorized various objects drawn from fairy tales and fantasy literature in ways that apply as much to technological objects.

Protection

- Example: In story: The magical swords and helmets protected the main characters of fairy tales from their enemies,
- In reality: The development of science and technology throughout history has been driven by the need for military superiority, for the purpose of security.

Health

Health has been a driver for many quests to find an ingredient for a health potion and for research into various branches of medicine, pharmacology and surgery, physiotherapy, and diet.

- Example: In story: Snow White's wicked stepmother asking "Mirror on the wall, who's the fairest of them all?"
- In reality: to the friends settling an argument of fact by looking up articles from Wikipedia on their smartphones.

Human Connection

Human Connection, even when one's loved ones are far away, the postal service, telephones, and social networking help keep us in touch with our family and friends.

- Example: In story: for Effortless Mobility invented flying carpets, and even teleportation.
- In reality: Through technology, we have invented cars and railways, bicycles, and aero planes.

The need for Creative Expression

- Example: In story: by the enchanted paintbrushes and magic flutes
- In reality: from charcoal to paint to computer graphics, or from drums to violins and electronic synthesizers.

- Unlike IOT, the era of enchanted objects is about making the everyday objects in our world smarter, rather than making technology requiring a high cost of ownership.
- The enchanted objects learn on their own, have low or no cost of ownership, and don't require a host of technical people to program or maintain them.
- So, technology has always been associated with magic, and so this will be true almost by default for the Internet of Things.
- A key element of many enchanted objects is that above and beyond their practical enchantment they are given a name and a personality—implying an intelligence greater than strictly necessary to carry out the task for which they are designed.

1.5. WHO IS MAKING THE INTERNET OF THINGS? FAQ

1. List and explain the roles of people making the IOT.

- Many persons are involved and they gave their contribution to develop an IOT platform are as follows:
  - Craftsperson
  - Artist
  - Designer
  - Engineer
  - Hacker
  - Developer

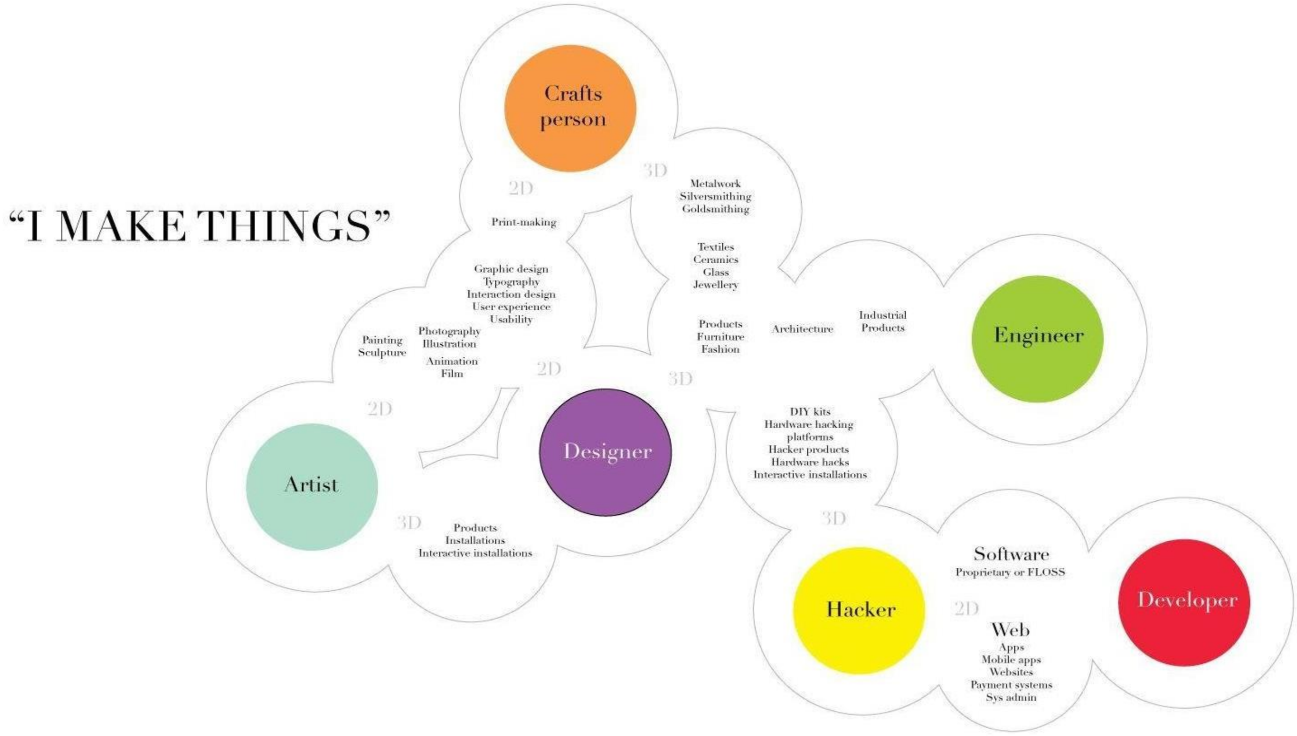


Figure 3: Roles of different people involved in IOT

- Artists may collaborate with the designers on installations or with traditional craftspeople on printmaking.
- Designers and engineers work closely to make industrial products, and hobbyist “hackers” by their nature, are a diverse group encompassing various technical and artistic interests and skills.
- The Internet of Things straddles all these disciplines: a hacker might tinker at the prototype for a Thing; a software developer might write the online component; a designer might turn the ugly prototype into a thing of beauty, possibly invoking the skills of a craftsperson, and an engineer might be required to solve difficult technical challenges, especially in scaling up to production.

2. DESIGN PRINCIPLES FOR CONNECTED DEVICES

2.1. CALM AND AMBIENT TECHNOLOGY FAQ

1) Write a note on Calm and Ambient Technology.
2) Define and Explain Internet of Things and Ubiquitous Computing.
3) What is Calm and Ambient Technology? Explain with an example.
4) Explain Calm and Ambient Technology using example of Live Wire.
5) Define and explain Ubiquitous Computing.

Calm Technology

- Calm technology or calm design is a type of information technology where the interaction between the technology and its user is designed to occur in the user's periphery rather than constantly at the center of attention.
- Information from the technology smoothly shifts to the user's attention when needed but otherwise stays calmly in the user's periphery.
- The use of calm technology is paired with ambient technology as a way to minimize the perceptible invasiveness of computers in everyday life.
- The term Calm technology means a system that doesn’t seek your attention

Examples Live Wire

- Live wire is one of the first IOT devices.
- Live wire also known as Dangling String.
- It is a simple device: an electric motor connected to an eight-foot long piece of plastic string.
- The power for the motor is provided by the data transmissions on the Ethernet network to which it is connected, so it twitches (make a sudden movement) whenever a packet of information is sent across the network.
- Under normal, light network load, the string twitches occasionally.
- If the network is overloaded, the string whirls madly, accompanied by a distinctive noise from the motor’s activity.
- Conversely, if no network activity is occurring, an unusual stillness comes over the string.
- Both extremes of activity therefore alert the nearby human (who is used to the normal behavior) that something is amiss and lets him investigate further.
- The mention of the distinctive sound from the motor when the Live Wire is under heavy load brings up another interesting point.

Split-flap display:

- Split-flap displays have been phased in and out and are replaced by dot-matrix LED displays.
- The newer displays are much easier to update with new destinations.
- Split-flap displays are at airports and railway stations.

Air tunes Wi-Fi speakers:

- Which anyone plays music through.
- Users will often wonder exactly what a particular track is but had no way of finding out who was in charge of the music at that moment and what was playing right now

Ambient Technology

- Ambient Technology is also known as Ubiquitous Computing.
- Ambient Technology is the growing trend of embedding computational capability (generally in the form of microprocessors) into everyday objects to make them effectively communicate and perform useful tasks in a way that minimizes the end user's need to interact with computers as computers.
- In contrast to desktop computing, ubiquitous computing can occur using any device, in any location, and in any format.
- Ambient computing refers to technology that is immersed in your surroundings, ready to help without any prompting.
- Ambient intelligence (AmI) refers to electronic environments that are sensitive and responsive to the presence of people.
- With ubiquitous computing the calm technology is paired.
- Since the devices becomes smaller, more connected and more integrated, the ambient intelligence will change the technology received by the users.
- Until the user interface remains perceivable by the user, the technology disappears into the surrounding.
- Examples of ambient intelligence are biometric systems, Google voice assistant, Alexa etc.

2.2. MAGIC AS METAPHOR FAQ

1. What is the manufactured normalcy field? Explain

- One of the main issues with introducing any new technology or service that is radically different from the norm is getting people to understand and accept it.
- Early adopters are generally happier looking a bit strange or doing things somewhat awkwardly to reap the benefits of the new gadgets.
- However, for the technology/service to catch on, one needs to persuade the majority to take it up.
- In addition to technology becoming capable of a particular action, we often need society to be ready to accept it.
- Manufactured Normalcy field is a term that explains how a new technology becomes adopted.
- For a technology to be adopted, it has to make its way inside the manufactured normalcy field.
- As a result, the successful user-experience designer is the one who presents users with an experience which doesn’t stretch the boundaries of their particular normalcy field too far, even if the underlying technology being employed is a huge leap ahead of the norm.
- For example, the mobile phone was first introduced as a phone that wasn’t tethered to a particular location. Now broadly the same technology is used to provide a portable Internet terminal, which can play movies, carry your entire music collection, and (every now and then) make phone calls. The way that portable Internet terminals made it into our manufactured normalcy field was through the phone metaphor.

2.3. PRIVACY AND KEEPING SECRETS FAQ

1. Discuss the issue of Privacy in the Internet of Things.

- Privacy is a critical concern in the Internet of Things (IoT), as IoT devices collect, store, and transmit large amounts of personal and sensitive information.
- Some of the privacy issues in IoT include:
  - Data collection: Ensuring that only the necessary data is collected and that it is collected in a way that respects individuals' privacy rights.
  - Data storage: Ensuring that the data collected by IoT devices is stored securely and that access to it is strictly controlled.
  - Data sharing: Controlling who has access to the data collected by IoT devices and ensuring that it is not shared without proper authorization.
- To address these privacy challenges, organizations should implement robust privacy policies and procedures, such as data protection, data minimization, and data retention.
- They should also educate users on the privacy implications of using IoT devices and encourage them to take steps to protect their privacy.
- Additionally, organizations should adopt privacy-enhancing technologies, such as encryption and anonymization, to protect the privacy of individuals whose information is collected by IoT devices.
- By prioritizing privacy, organizations can help to ensure that individuals' rights and freedoms are respected, and that sensitive information is protected from unauthorized access or misuse.
- Protecting the privacy of individuals whose personal information is collected and transmitted by IoT devices.

2.3.1. WHOSE DATA IS IT? FAQ

1. "Data available through IOT devices belongs to the public or company which implements the IOT Device." Discuss.

- Many applications like a smart watch that monitors the number of steps taken, a thermostat that can be controlled with the help of an app, or a camera that helps to see who is at the door collect a common thing that is data.
- A lot of this data is passed on to the providers of these services.
- In most cases, it is not clear whose data is being gathered.
- In a public space, this data is being generated by the public, so they should at least have equal rights to be aware of, and also have the access to, that data.
- On private property, you can claim that the members of the public don't have such a right, but perhaps the property owner might assert rights to the data rather than whoever installed/provides the service.

2.4. WEB THINKING FOR CONNECTED DEVICES FAQ

1. “Be Conservative in what you do, be liberal in what you accept from others”. Discuss

- The robustness principle is a design guideline for software that states: "be conservative in what you do, be liberal in what you accept from others".
- This is also referred to as postel law.
- The spirit of Postel's Law is to make different implementations interoperate. There are two parts to the Law and these are briefly explained
- Conservative in sending: Protocol should be careful to send well-formed datagrams.
- Liberal in receiving: Protocol should accept any datagram that it can interpret. In other words, if the semantics are clear then errors in syntax can be overlooked.
- When one thinks about the networked aspect of the IOT, it draws experiences and design guidelines from existing network deployments.
- One should try to get into the mindset of the web and create devices which are of the web rather than those which just exist on the web.
- The Internet grew without centralized control.
- When a protocol was defined, it was implemented by multiple individuals and teams.
- For reliable communication, these different implementations needed to understand one another.
- However, standards are not always unambiguous. Sometimes different interpretations arise.
- In such cases, strict adherence to the standard will result in protocol errors.
- In a distributed system, it would be hard to iron out these differences. If there's tight control, Postel's Law is not needed. But the Internet has many pieces that are loosely joined.
- This is exactly why the Law made sense.
- In early Internet days, implementations were liberal in accepting non-standard inputs provided they could make sense of them and decide how to handle them.
- Without such a liberal approach, the growth of the Internet might have been slower than what it was.
- Without Postel's Law, standardization and their strict implementations would have taken longer.
- Implementations that interwork with one another were more important.
- A similar thing happened with browsers and HTML. The Law made sense for rapid growth of the WWW.

2.4.1. SMALL PIECES LOOSELY JOINED

- The Internet grew without centralized control.
- It is a collection of services and machines following the maxim of many pieces that are loosely joined.
- Each piece should be designed to do one thing well and not rely too much on tight integration with separate components it uses.
- Make the components more generalized and able to serve other systems which require a similar function.
- It should be able to reuse and repurpose the components to build new capabilities.
- Where possible, use existing standards and protocols rather than inventing your own.

2.4.2. FIRST CLASS CITIZENS ON THE INTERNET

- An extension of the concept of loose coupling is to strive to make your devices first-class citizens on the Internet.
- On the Internet, a first-class citizen (also type, object, entity, or value) is an entity which supports all the operations generally available to other entities.
- It means where possible, you should use the same protocols and conventions that the rest of the Internet uses.
- A good rule of thumb for the past 20 years or more has been to expect the IP protocol to penetrate everywhere.
- In the few cases where the existing protocols don't work, such as in extremely low-powered sensors, a better solution is to create new open standards which address the issue.
- When mobile phones were first being connected to the Internet, it was deemed too difficult for them to talk to web servers directly, and a whole suite of new protocols, Wireless Application Protocol (WAP), were developed.

2.4.3. GRACEFUL DEGRADATION

FAQ

1. Explain the following concepts with respect to IOT

a. Affordances

b. Graceful Degradation

- The endpoints have a massively disparate and diverse range of capabilities.
- (End point in IoT, is a physical computing device that performs a function or task as a part of an Internet connected product or service.)
- As a result, building services which can be used by all of them is a nearly impossible task.
- However, a number of design patterns have evolved to mitigate the problem. They are:
- Backwards compatibility
- Graceful Degradation

Backwards Compatibility:

- If you need to come up with a format for some data being transferred between devices, include a way to differentiate between successive versions of the formats—ideally in such a way that older devices can still mostly read newer formats.
- The HTML format does this by stating that any client should ignore any tags (the text inside the <>) that it doesn't understand, so newer versions can add new tags without breaking older parsers.

Graceful Degradation

- Graceful degradation is the practice of creating an endpoint/browser that is both feature-rich and still compatible with older versions of endpoints/browsers or endpoints/browsers that are not compatible.
- This technique involves aiming to provide a fully featured experience if the client is capable of it but then falling back—potentially in a number of levels—to a less feature-rich experience on less capable clients.
- For example, in Gmail, the coder wants to use advanced JavaScript features in modern browsers.
- Well-written apps check that the features are available before using them, but if those features aren't available, the apps might limit themselves to a version using simpler (and more common) JavaScript code.
- And if JavaScript isn't available at all, they fall back to basic HTML forms.
- The same concept applies to end devices.

- When using the same techniques when designing our connected devices, we might also be able to apply that approach to the devices themselves to give a degree of fault tolerance.
- The proliferation of devices and the likelihood that some of them will break in some way means that it is important that their technology continues to add what value it can, as parts cease to function.
- For example, When your early-adopter Internet Fridge can no longer talk to your Wi-Fi because it's only IPv4 and the world has moved to IPv6, you would still be able to use its touchscreen to write messages and view the photos stored in the USB stick stuck in it.
- And if the touchscreen breaks, you should still be able to keep the food inside it cold.

2.5. AFFORDANCES

FAQ

1. Explain the following concepts with respect to IOT

a. Affordances

b. Graceful Degradation

Definition

"Affordances provide strong clues to the operations of things. Plates are for pushing. Knobs are for turning. Slots are for inserting things into. Balls are for throwing or bouncing. When affordances are taken advantage of, the user knows what to do just by looking: no picture, label, or instruction is required. Complex things may require explanation, but simple things should not. When simple things need pictures, labels, or instructions, the design has failed."

- Affordance is a fundamental aspect of interaction design.
- Be it software design or physical object design or even business design, the designers explicitly or implicitly think about how the users and actors of the system behave/perform based on various influencing factors (stimuli).
- Depending upon the specific application of the concept and the context, the path to arriving at the right set of affordances could vary.
- When affordances are done right, the product/service/business process (referred to as P-S-BP, hence forth) is a pleasure to work with. When done poorly, the usability and adoption of the P-S-BP suffers greatly.

3. INTERNET PRINCIPLES

3.1. INTERNET COMMUNICATIONS: AN OVERVIEW FAQ

1. Explain the working of IP.

3.1.1.IP

- The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.
- Data traversing the Internet is divided into smaller pieces, called packets.
- IP information is attached to each packet, and this information helps routers to send packets to the right place.
- Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.
- Once the packets arrive at their destination, they are handled differently depending on which transport protocol is used in combination with IP.
- The most common transport protocols are TCP and UDP.

3.1.2. TCP

- TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite.
- It lies between the Application and Network Layers which are used in providing reliable delivery services
- It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network.
- The main functionality of the TCP is to take the data from the application layer.
- Then it divides the data into several packets, provides numbering to these packets, and finally transmits these packets to the destination.
- The TCP, on the other side, will reassemble the packets and transmit them to the application layer.
- As we know that TCP is a connection-oriented protocol, so the connection will remain established until the communication is not completed between the sender and the receiver.

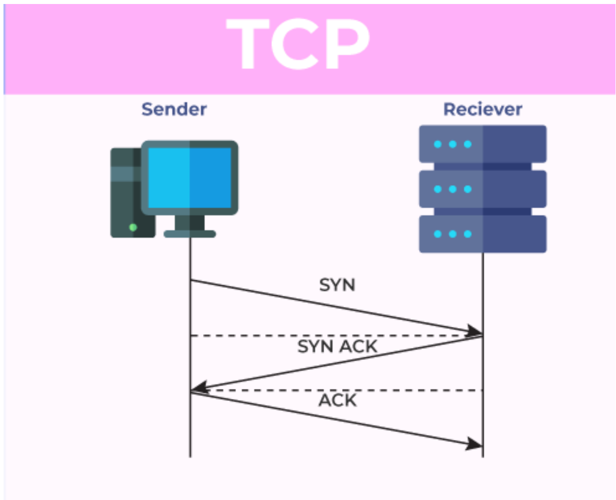


Figure 4: TCP Transmission

3.1.3. UDP

- User Datagram Protocol (UDP) is a Transport Layer protocol.
- UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite.
- Unlike TCP, it is an unreliable and connectionless protocol.
- So, there is no need to establish a connection prior to data transfer.
- The UDP helps to establish low-latency and loss-tolerating connections are established over the network.
- The UDP enables processes to process communication.
- Here, UDP comes into the picture. For real-time services like computer gaming, voice or video communication, live conferences; we need UDP.
- Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets.
- There is no error checking in UDP, so it also saves bandwidth.
- User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

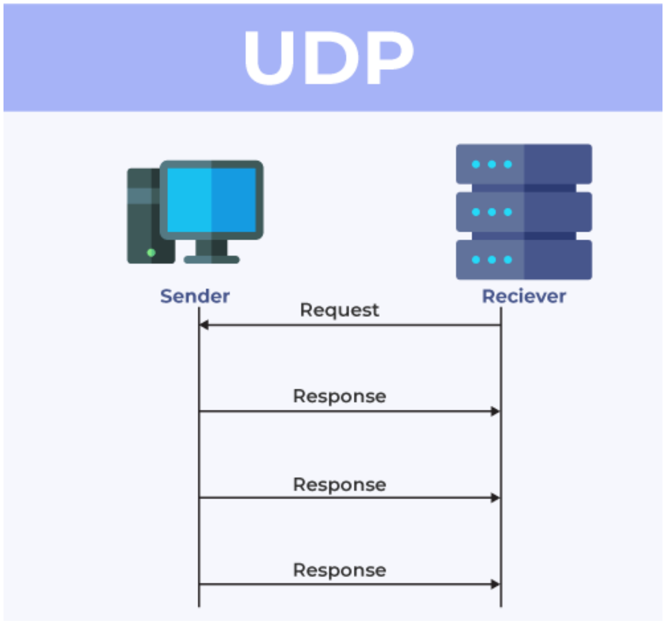


Figure 5: UDP Transmission

3.1.4. TCP/IP SUITE

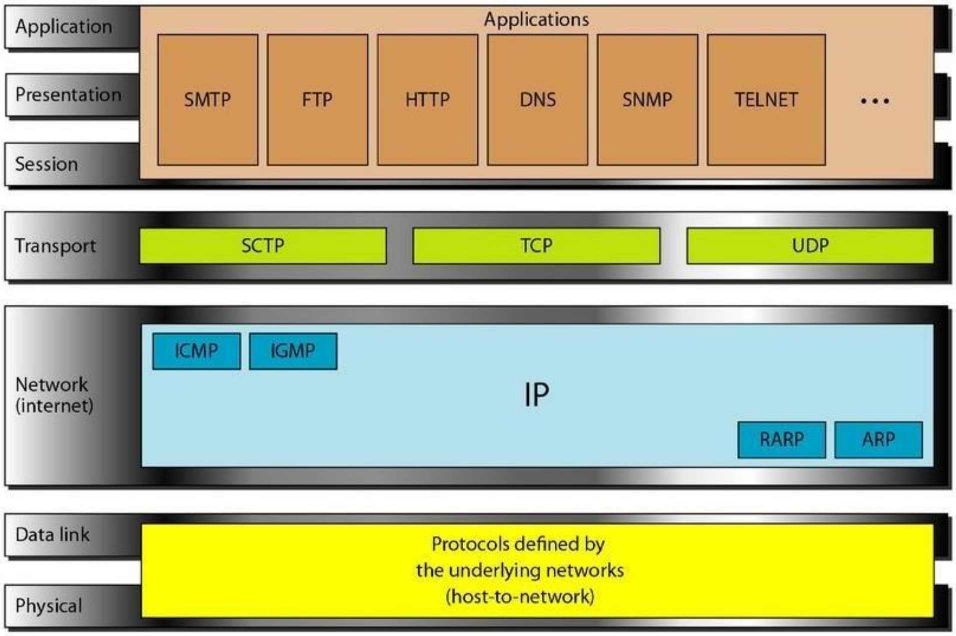


Figure 6: TCP/IP Protocol Suite

- The combination of TCP and IP is so ubiquitous that we often refer simply to “TCP/IP” to describe a whole suite or stack of protocols layered on top of each other, each layer building on the capabilities of the one below.
- The low-level protocols at the link layer manage the transfer of bits of information across a network link.
- This could be by an Ethernet cable, by Wi-Fi, or across a telephone network, or even by short-range radio standards such as IEEE 802.15.4 designed to carry data over the Personal Area Network (PAN), that is to say between devices carried by an individual.
- The Internet layer then sits on top of these various links and abstracts away the gory details in favor of a simple destination address.

- Then TCP, which lives in the transport layer, sits on top of IP and extends it with more sophisticated control of the messages passed.
- Finally, the application layer contains the protocols that deal with fetching web pages, sending emails, and Internet telephony.
- Of these, HTTP is the most ubiquitous for the web, and indeed for communication between Internet of Things devices.

3.2. IP ADDRESS

- An IP address is a unique address that is used to identify computers or nodes on the internet.
- This address is just a string of numbers written in a certain format.
- It is generally expressed in a set of numbers, for example 192.155.12.1.
- Here each number in the set is from 0 to 255 range.
- Or we can say that a full IP address ranges from 0.0.0.0 to 255.255.255.255.
- These IP addresses are assigned by IANA (known as Internet Corporation for Internet Assigned Numbers Authority).

3.2.1.TYPES OF IP ADDRESS

- IP Address is of two types:

3.2.1.1. IPv4:

- Internet Protocol version 4.
- It consists of 4 numbers separated by the dots.
- Each number can be from 0-255 in decimal numbers.
- But computers do not understand decimal numbers, they instead change them to binary numbers which are only 0 and 1.
- Therefore, in binary, this (0-255) range can be written as (00000000 – 11111111).
- Since each number N can be represented by a group of 8-digit binary digits.
- So, a whole IPv4 binary address can be represented by 32-bits of binary digits.
- In IPv4, a unique sequence of bits is assigned to a computer, so a total of (2^32) devices approximately = 4,294,967,296 can be assigned with IPv4.
- IPv4 can be written as:

189.123.123.90

Classes of IPv4 Address:

- There are around 4.3 billion IPv4 addresses and managing all those addresses without any scheme is next to impossible.
- For easier management and assignment, IP addresses are organized in numeric order and divided into the following 5 classes :

IP Class	Address Range	Maximum number of networks
Class A	0-126	126 (27-1)
Class B	128-191	16384
Class C	192-223	2097152
Class D	224-239	Reserve for multitasking

Class E	240-254	Reserved for Research and development

- A loopback address is a distinct reserved IP address range that starts from 127.0.0.0 and ends at 127.255.255.255.
- The loopback addresses are built into the IP domain system, enabling devices to transmit and receive the data packets. The loopback address 127.0.0.1 is generally known as local host.

3.2.1.2. IPv6:

- But, there is a problem with the IPv4 address.
- With IPv4, we can connect only the above number of 4 billion devices uniquely, and apparently, there are much more devices in the world to be connected to the internet.
- So, gradually we are making our way to IPv6 Address which is a 128-bit IP address.
- In human-friendly form, IPv6 is written as a group of 8 hexadecimal numbers separated with colons(:).
- But in the computer-friendly form, it can be written as 128 bits of 0s and 1s.
- Since, a unique sequence of binary digits is given to computers, smartphones, and other devices to be connected to the internet.
- So, via IPv6 a total of (2^128) devices can be assigned with unique addresses which are actually more than enough for upcoming future generations.
- IPv6 can be written as:
- *2011:0bd9:75c5:0000:0000:6b3e:0170:8394*

3.2.1.3. IPv6 and Powering Devices

- We can see that an explosion in the number of Internet of Things devices will almost certainly need IPv6 in the future.
- But we also have to consider the power consumption of all these devices. We know that we can regularly charge and maintain a small handful of devices.
- At any one moment, we might have a laptop, a tablet, a phone, a camera, and a music player plugged in to charge.
- The constant juggling of power sockets, chargers, and cables is feasible but fiddly. The requirements for large numbers of devices, however, are very different.
- The devices should be low power and very reliable, while still being capable of connecting to the Internet.
- Perhaps to accomplish this, these devices will team together in a mesh network.
- This is the vision of 6LoWPAN, an IETF working group proposing solutions for “IPv6 over Low power Wireless Personal Area Networks”, using technologies such as IEEE 802.15.4.

Conclusion on IPv6

- Even though we are getting close to the tipping point, existing IPv4 services will be able to migrate to IPv6 networks with minimal or possibly no rewriting

3.2.2.TYPES OF IP ADDRESS ASSIGNMENT FAQ

1. Differentiate between Static IP Address and Dynamic IP Address.

3.2.2.1. DYNAMIC IP ADDRESS ASSIGNMENT

- Instead, when you connect a laptop, a printer, or even a Twitter-following bubble machine, it can request an IP address from the network itself using the Dynamic Host Configuration Protocol (DHCP).
- When the device tries to connect, instead of checking its internal configuration for its address, it sends a message to the router asking for an address.
- The router assigns it an address.
- It is a temporary "lease" which is selected dynamically according to which addresses are currently available.
- If the router is rebooted, the lease expires, or the device is switched off, some other device may end up with that IP address.
- This means that you can't simply point a DNS entry to a device using DHCP.
- In general, you can rely on the IP address probably being the same for a given work session, but you shouldn't hard-code the IP address anywhere that you might try to use it another time, when it might have changed.

3.2.2.2. STATIC IP ADDRESS ASSIGNMENT

- It was the initial technique of assigning IP addresses to network devices.
- They serve as a permanent internet address.
- These are used by DNS servers.
- The system administrator simply assigns server numbers in order.
- The administrator makes a note of the addresses and updates DNS records and so on to point to these addresses.
- This kind of address static because once assigned it won't change again without human intervention
- Static IP Address provides information such as which device is located on which continent, which country, which city, and which Internet Service Provider provides internet connection to that particular device.
- Once we know who the ISP is, we can trace the location of the device connected to the internet.
- Static IP Addresses provide less security than Dynamic IP Addresses because they are easier to track.

3.2.2.3. DIFFERENCE BETWEEN STATIC IP ADDRESS AND DYNAMIC IP ADDRESS

SR.NO	PARAMETERS	STATIC IP ADDRESS ASSIGNMENT	DYNAMIC IP ADDRESS ASSIGNMENT
1	Definition	It is a permanent numeric address that is manually issued to a network device.	It is a temporary IP address allocated to a system when it connects to a network.
2	Provider	It is provided by an Internet Service	It is provided by DHCP
3	Changes	It doesn't change with time.	It may be changed at any time.
4	Device tracking	Devices may be traced easily.	Devices may be difficult to trace.
5	Cost	It is expensive to utilize and maintain.	It is less expensive to utilize and maintain.
6	Security	It is less secure than the dynamic IP address.	It offers high security.
7	Designation	It is complex to assign and reassign.	It is much easier to assign and reassign.
8	Stability	It is highly stable.	It is less stable.

3.2.3. DNS FAQ

1. Write a note on DNS.
2. What is DNS? How does it work?

- A domain name serves as a distinctive identification for a website.
- It is used in place of an IP address to make it simpler for consumers to visit websites.
- Domain Name System works by executing the database whose work is to store the name of hosts which are available on the Internet.
- The top-level domain server stores address information for top-level domains such as .com and .net, .org, and so on.

Working of DNS

- If the Client sends the request, then the DNS resolver sends a request to DNS Server to fetch the IP Address.
- In case, when it does not contain that particular IP Address with a hostname, it forwards the request to another DNS Server.
- When the IP Address has arrived at the resolver, it completes the request over Internet Protocol.

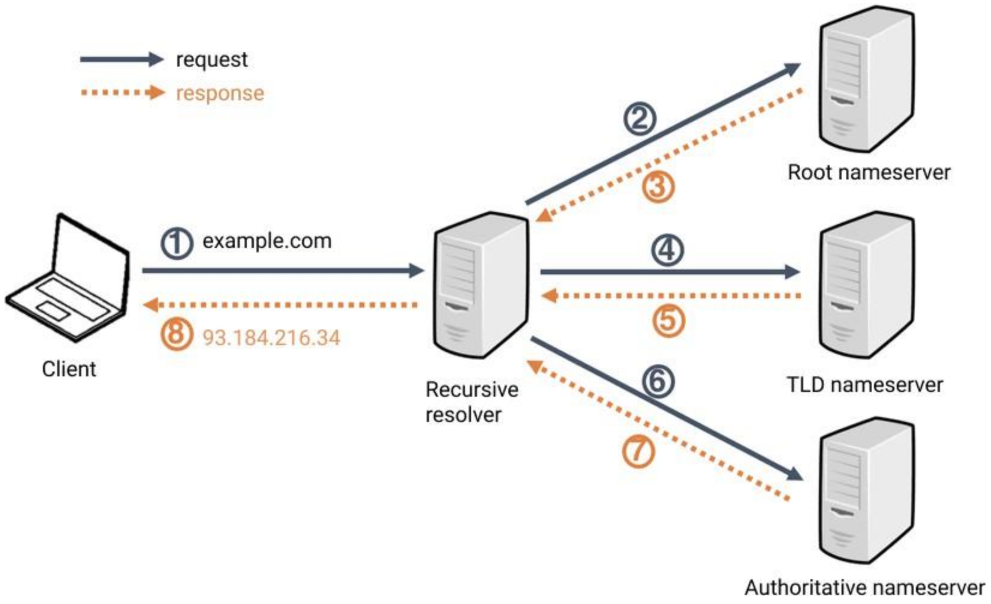


Figure 7: DNS Working

- There are various kinds of DOMAIN:
- **Generic domains:** .com(commercial), .edu(educational), .mil(military), .org(nonprofit organization), .net(similar to commercial) all these are generic domains.
- **Country domain:** .in (India) .us .uk
- **Inverse domain:** if we want to know the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the IP addresses XYZ.org then we have to type *nslookup www.XYZ.org*

3.2.4. MAC ADDRESS FAQ

1. What is MAC Address? Explain

- MAC address is the physical address, which uniquely identifies each device on a given network.
- To make communication between two networked devices, we need two addresses: IP address and MAC address.
- It is assigned to the NIC (Network Interface card) of each device that can be connected to the internet.
- It stands for Media Access Control, and also known as Physical address, hardware address, or BIA (Burned in Address).
- It is globally unique; it means two devices cannot have the same MAC address.
- It is represented in a hexadecimal format on each device, such as 00:0a:95:9d: 67:16.
- It is 12-digit, and 48 bits long, out of which the first *24 bits are used for OUI (Organization Unique Identifier),* and *24 bits are for NIC/vendor-specific.*
- It works on the data link layer of the OSI model.
- It is provided by the device's vendor at the time of manufacturing and embedded in its NIC, which ideally cannot be changed.
- The ARP protocol is used to associate a logical address with a physical or MAC address.

Reason to have both IP and MAC addresses.

- Every mac address is assigned to the NIC of a hardware device that helps to identify a device over a network.
- When we request a page to load on the internet, the request is responded to and sent to our IP address.
- Both MAC and IP addresses are operated on different layers of the internet protocol suite.
- The MAC address works on layer 2 and helps identify the devices within the same broadcast network (such as the router).
- On the other hand, the IP addresses are used on layer 3 and help identify the devices on different networks.
- We have the IP address to identify the device through different networks, we still need a MAC address to find the devices on the same network.

Format of MAC address

- It is 12 digits or 6-byte hexadecimal number, which is represented in colon-hexadecimal notation format. It is divided into six octets, and each octet contains 8 bits.
- The first three octets are used as the OUI or Organizationally Unique Identifier. These MAC prefixes are assigned to each organization or vendor by the IEEE Registration Authority Committee.
- Some example of OUI of known vendors are:
    - CC:46:D6 – Cisco
    - 3C:5A:B4 - Google,
    - Inc. 3C:D9:2B - Hewlett Packard
    - 00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD

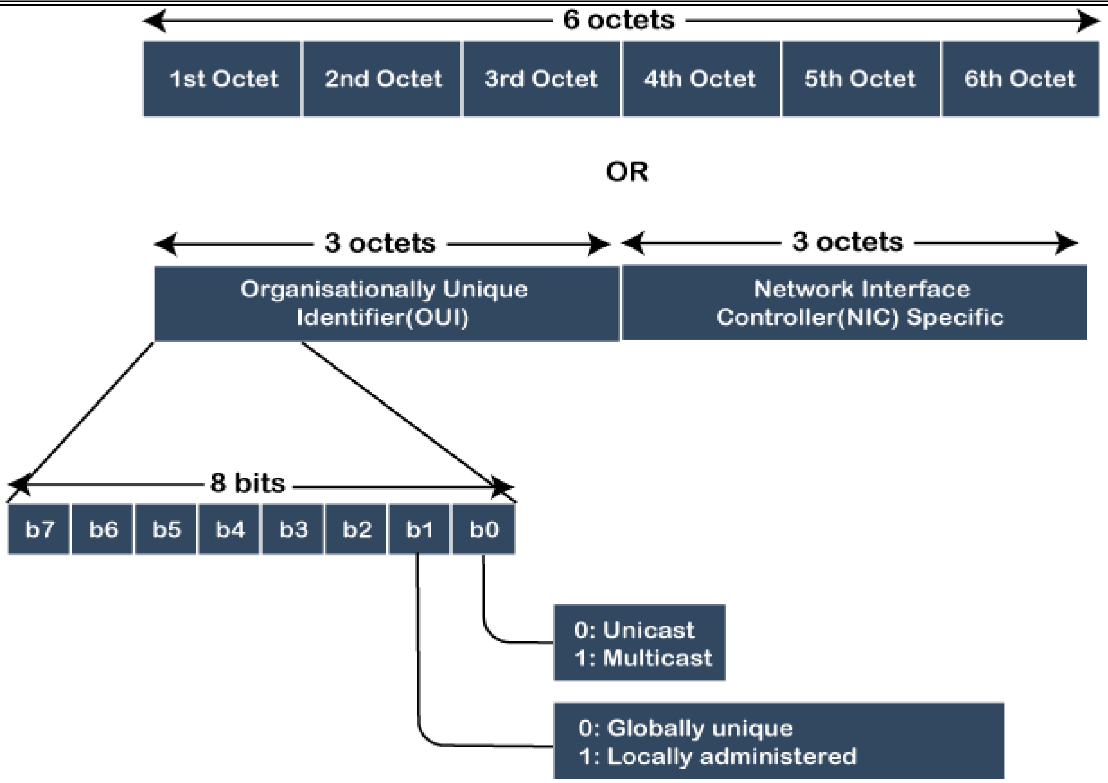


Figure 8: MAC Address Format

- The last three octets are NIC specific and used by the manufacturer to each NIC card. Vendors or manufacturers can use any sequence of digits to the NIC specific digits, but the prefix should be the same as provided by the IEEE.

3.2.4.1. Difference between MAC address and IP address

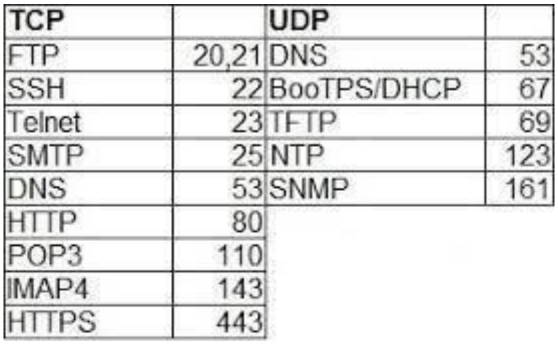
Both the MAC address and IP address are the way to identify the device on the network. Following are some important differences between both:

Parameters	MAC address	IP address
Abbreviation	It stands for Media Access Control.	It stands for Internet Protocol.
Provider	It is the unique address provided by the manufacturer.	It is the logical address provided by the ISP or Internet Service Provider.
Nature of Address	It is the physical address of the device's NIC that is used to identify a device	It is the logical address that identifies a network or device on the internet.
Operating Layer	It operates on the data link layer.	It operates on a network Layer.
Length	It is the 6 -bytes hexadecimal address.	It is of 4 bytes for IPv4 and 8 bytes for IPv6

3.3. TCP AND UDP PORTS FAQ

1. What are TCP and UDP Ports? Explain with examples.

- When information is sent over the Internet to your computer, the computer accepts that information by using TCP or UDP ports**.**
- If it uses the TCP protocol to send and receive the data then it will connect and bind itself to a TCP port.
- If it uses the UDP protocol to send and receive data, it will use a UDP port.
- There can be a total of 65,535 TCP Ports and another 65,535 UDP ports.
- Some common TCP and UDP Ports are:



TCP		UDP	
FTP	20,21	DNS	53
SSH	22	BooTPS/DHCP	67
Telnet	23	TFTP	69
SMTP	25	NTP	123
DNS	53	SNMP	161
HTTP	80		
POP3	110		
IMAP4	143		
HTTPS	443		

3.3.1. AN EXAMPLE: HTTP PORT

- If your browser requests an HTTP page, it usually sends that request to port 80.
- The web server is “listening” to that port and therefore replies to it.
- If you send an HTTP message to a different port, one of several things will happen:
- Nothing is listening to that port, and the machine replies with an “RST” packet (a control sequence resetting the TCP/IP connection) to complain about this.
- Nothing is listening to that port, but the firewall lets the request simply hang instead of replying. The purpose of this (lack of) response is to discourage attackers from trying to find information about the machine by scanning every port.
- The client has decided that trying to send a message to that port is a bad idea and refuses to do it. Google Chrome does this for a fairly arbitrary list of “restricted ports”.
- The message arrives at a port that is expecting something other than an HTTP message.
- The server reads the client’s response, decides that it is garbage, and then terminates the connection (or, worse, does a nonsensical operation based on the message).
- **Ports 0–1023** are “well-known ports”, and only a system process or an administrator can connect to them.
- **Ports 1024–49151** are “registered”, so that common applications can have a usual port number. However, most services are able to bind any port number in this range. The Internet Assigned Numbers Authority (IANA) is responsible for registering the numbers in these ranges.
- **Custom Port Nos:** You see custom port numbers if a machine has more than one web server; for example, in development you might have another server, bound to port 8080: http://www.example.com:8080 Or if you are developing a website locally, you may be able to test it with a built-in test web server which connects to a free port.

3.3.2. OTHER COMMON PORTS

- 80 HTTP
- 8080 HTTP (for testing servers)
- 443 HTTPS
- 22 SSH (Secure Shell)
- 23 Telnet
- 25 SMTP (outbound email)
- 110 POP3 (inbound email)
- 220 IMAP (inbound email)

All of these services are in fact application layer protocols.

3.4. APPLICATION LAYER PROTOCOLS FAQ

1. Define protocol.

Protocol

- A protocol is a set of rules for communication between computers.
- It includes rules about how to initiate the conversation and what format the messages should be in.
- It determines what inputs are understood and what output is transmitted.
- It also specifies how the messages are sent and authenticated and how to handle (and maybe correct) errors caused by transmission.

Application Layer

- The Application layer is the highest layer of the stack.
- This is the layer we most like to interact with while prototyping an Internet of Things project.
- It is responsible for end-to-end communication and error-free delivery of data.
- It shields the upper-layer applications from the complexities of data.
- One of the main application layer protocol is HTTP

3.4.1. HTTP

- HTTP stands for Hypertext Transfer Protocol.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as Hypertext Transfer Protocol because of its efficiency that allows us to use it in a hypertext environment where there are rapid jumps from one document to another document.
- It is a stateless protocol.
- Both the client and server know each other only during the current request.

HTTP Request / Response

Communication between clients and servers is done by requests and responses:

- A client (a browser) sends an HTTP request to the web (URL) with some headers.
- A web server receives the request
- The server runs an application to process the request
- The server returns an HTTP response (output) to the browser
- The client (the browser) receives the response

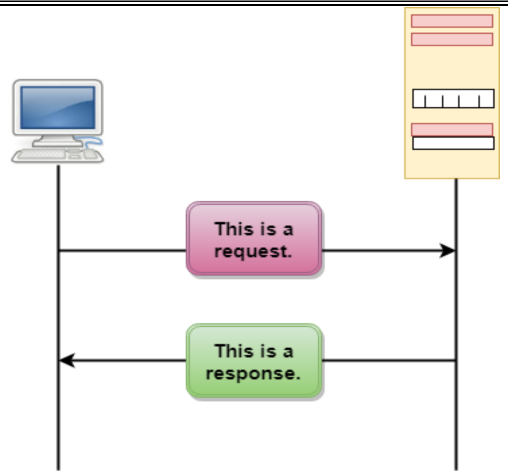


Figure 9: HTTP Transaction

3.4.2. HTTPS: ENCRYPTED HTTP

- HTTPS is an abbreviation of Hypertext Transfer Protocol Secure.
- The HTTPS protocol is a mix-up of plain old HTTP over the Secure Socket Layer (SSL) protocol.
- This protocol is mainly used for providing security to the data sent between a website and the web browser.
- It is widely used on the internet and used for secure communications.
- The data which is transferred in HTTPS is encrypted, i.e., cipher text.
- This protocol uses the 443 port number for communicating the data.
- When that's established, both sides just speak HTTP to each other.
- This protocol operates at the transport layer.

3.4.3. OTHER APPLICATION LAYER PROTOCOLS FAQ

1. Define protocol. Explain the following application layer protocols.

1. HTTPS 2. SMTP 3.FTP 4.POP3 5.IMAP

2. Define protocol. Explain the following application layer protocols.

1. HTTP 2. HTTPS 3.SMTP 4. FTP

- **FTP:**
- FTP stands for File Transfer Protocol.
- This protocol helps to transfer different files from one device to another.
- FTP promotes sharing of files via remote computer devices with reliable, efficient data transfer.
- FTP uses port number 20 for data access and port number 21 for data control.

- **SMTP:**
- SMTP stands for Simple Mail Transfer Protocol.
- It is used to transfer electronic mail from one user to another user.
- SMTP is used by end users to send emails with ease.
- SMTP uses port numbers 25 and 587.
- **POP3**
- POP3 stands for Post Office Protocol 3
- The POP is an Internet standard protocol on the application layer that the local email clients use for retrieving emails from any remote server over the TCP/IP connection.

- POP3 is a very simplified protocol. It can only download the emails on the local computer from the inbox.
- Unidirectional – The changes that you make on a device have zero effect on the content available on the server.
- **IMAP**
- IMAP is an abbreviation for Internet Message Access Protocol.
- The IMAP is a protocol that allows distant users to access their emails directly from the server and read them on any device at any location feasible for them.
- The IMAP protocol is very complex. It allows all the users to view their email folders easily and read them on the mail server itself (from any device they want).
- Whenever you make changes on the device or server, it shows on the other side as well.