Unit 3

Internet

Internet is defined as an Information super Highway, to access information over the web. However, It can be defined in many ways as follows:

1. Internet is a world-wide global system of interconnected computer networks.
2. Internet uses the standard Internet Protocol (TCP/IP).
3. Every computer in internet is identified by a unique IP address.
4. IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.
5. A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.
6. Internet is accessible to every user all over the world.

Evolution

The concept of Internet was originated in 1969 and has undergone several technological & Infrastructural changes as discussed below:

1. The origin of Internet devised from the concept of Advanced Research Project Agency Network (ARPANET).
2. ARPANET was developed by United States Department of Defense.
3. Basic purpose of ARPANET was to provide communication among the various bodies of government.
4. Initially, there were only four nodes, formally called Hosts.
5. In 1972, the ARPANET spread over the globe with 23 nodes located at different countries and thus became known as Internet.
6. By the time, with invention of new technologies such as TCP/IP protocols, DNS, WWW, browsers, scripting languages etc. Internet provided a medium to publish and access information over the web.

Advantages

1. Internet allows us to communicate with the people sitting at remote locations. There are various apps available on the wed that uses Internet as a medium for communication. One can find various social networking sites such as:
    - Facebook
    - Twitter

- Yahoo
- Google+
- Flickr
- Orkut

2. One can surf for any kind of information over the internet. Information regarding various topics such as Technology, Health & Science, Social Studies, Geographical Information, Information Technology, Products etc can be surfed with help of a search engine.
3. Apart from communication and source of information, internet also serves a medium for entertainment. Following are the various modes for entertainment over internet.
    - Online Television
    - Online Games
    - Songs
    - Videos
    - Social Networking Apps
4. Internet allows us to use many services like:
    - Internet Banking
    - Matrimonial Services
    - Online Shopping
    - Online Ticket Booking
    - Online Bill Payment
    - Data Sharing
    - E-mail
5. Internet provides concept of electronic commerce, that allows the business deals to be conducted on electronic systems.

Disadvantage

1. There are always chances to loose personal information such as name, address, credit card number. Therefore, one should be very careful while sharing such information. One should use credit cards only through authenticated sites.
2. Another disadvantage is the Spamming. Spamming corresponds to the unwanted e-mails in bulk. These e-mails serve no purpose and lead to obstruction of entire system.
3. Virus can easily be spread to the computers connected to internet. Such virus attacks may cause your system to crash or your important data may get deleted.

4. Also a biggest threat on internet is pornography. There are many pornographic sites that can be found, letting your children to use internet which indirectly affects the children healthy mental life.
5. There are various websites that do not provide the authenticated information. This leads to misconception among many people.

Intranet

Intranet is defined as private network of computers within an organization with its own server and firewall. Moreover we can define Intranet as:

1. Intranet is system in which multiple PCs are networked to be connected to each other. PCs in intranet are not available to the world outside of the intranet.
2. Usually each company or organization has their own Intranet network and members/employees of that company can access the computers in their intranet.
3. Every computer in internet is identified by a unique IP address.
4. Each computer in Intranet is also identified by a IP Address, which is unique among the computers in that Intranet.

Benefits

1. Communication - Intranet offers easy and cheap communication within an organization. Employees can communicate using chat, e-mail or blogs.
2. Time Saving - Information on Intranet is shared in real time.
3. Collaboration - Information is distributed among the employees as according to requirement and it can be accessed by the authorized users, resulting in enhanced teamwork.
4. Platform Independency - Intranet can connect computers and other devices with different architecture.
5. Cost Effective - Employees can see the data and other documents using browser rather than printing them and distributing duplicate copies among the employees, which certainly decreases the cost.
6. Workforce Productivity - Data is available at every time and can be accessed using company workstation. This helps the employees work faster.
7. Business Management - It is also possible to deploy applications that support business operations.
8. Security - Since information shared on intranet can only be accessed within an organization, therefore there is almost no chance of being theft.

9. Specific Users - Intranet targets only specific users within an organization therefore, once can exactly know whom he is interacting.

10. Immediate Updates - Any changes made to information are reflected immediately to all the users.

Issues

1. Management concern:
   - Loss of control,
   - Hidden complexity,
   - Potential of chaos.
2. Security concern:
   - Unauthorized access,
   - DoS attack,
   - Packet Sniffing
3. Productivity concern:
   - Information overload lowers productivity,
   - Users setup their own web pages,
   - Overabundance of information.

Applications

1. Document publication applications

Document publication applications allow publishing documents such as manuals, software guide, employee profits etc without use of paper.

2. Electronic resources applications

It offers electronic resources such as software applications, templates and tools, to be shared across the network.

3. Interactive Communication applications

Like on internet, we have e-mail and chat like applications for Intranet, hence offering an interactive communication among employees.

4. Support for Internet Applications

Intranet offers an environment to deploy and test applications before placing them on Internet.

Extranet

Extranet refers to network within an organization, using internet to connect to the outsiders in controlled manner. It helps to connect businesses with their customers and suppliers and therefore allows working in a collaborative manner.

Implementation

Extranet is implemented as a Virtual Private Networks (VPN) because it uses internet to connect to corporate organization and there is always a threat to information security. VPN offers a secure network in public infrastructure (Internet).

- The packet is encapsulated at boundary of networks in IPSEC complaint routers.
- It uses an encryption key to encapsulate packets and IP addresses as well.
- The packet is decoded only by the IPSEC complaint routers or servers.
- The message is sent over VPN via VPN Tunnel and this process is known as tunneling.

Issues

1. Hosting - Where the extranet pages will be held i.e. who will host the extranet pages. In this context there are two choices:

- Host it on your own server.
- Host it with an Internet Service Provider (ISP) in the same way as web pages.

But hosting extranet pages on your own server requires high bandwidth internet connection which is very costly.

2. Security - Additional firewall security is required if you host extranet pages on your own server which result in a complex security mechanism and increase work load.

3. Accessing Issues - Information cannot be accessed without internet connection. However, information can be accessed in Intranet without internet connection.

4. Interaction - It decreases the face to face interaction in the business which results in lack of communication among customers, business partners and suppliers.

Benefit

1. Real time market intelligence

2. Improved channel management

3. Access to invoicing information
4. Supply chain integration
5. Sales force enforcement
6. Reduce time to market
7. Online customer care support

IP Address

IP address is a unique logical address assigned to a machine over the network. An IP address exhibits the following properties:

1. IP address is the unique address assigned to each host present on Internet.
2. IP address is 32 bits (4 bytes) long.
3. IP address consists of two components: network component and host component.
4. Each of the 4 bytes is represented by a number from 0 to 255, separated with dots. For example 137.170.4.124

Domain Name System helps to resolve the host name to an address. It uses a hierarchical naming scheme and distributed database of IP addresses and associated names

Internet services

Internet Services allows us to access huge amount of information such as text, graphics, sound and software over the internet.

Communication Services

There are various Communication Services available that offer exchange of information with individuals or groups. The following table gives a brief introduction to these services:

S.N.	Service Description
1	Electronic Mail Used to send electronic message over the internet.
2	Telnet Used to log on to a remote computer that is attached to internet.

3	Newsgroup Offers a forum for people to discuss topics of common interests.
4	Internet Relay Chat (IRC) Allows the people from all over the world to communicate in real time.
5	Mailing Lists Used to organize group of internet users to share common information through e-mail.
6	Internet Telephony (VoIP) Allows the internet users to talk across internet to any PC equipped to receive the call.
7	Instant Messaging Offers real time chat between individuals and group of people. Eg. Yahoo messenger, MSN messenger.

Information Retrieval Services

There exist several Information retrieval services offering easy access to information present on the internet. The following table gives a brief introduction to these services:

S.N.	Service Description
1	File Transfer Protocol (FTP) Enable the users to transfer files.
2	Archie It’s updated database of public FTP sites and their content. It helps to search a file by its name.
3	Gopher Used to search, retrieve, and display documents on remote sites.

4	Very Easy Rodent Oriented Net wide Index to Computer Achieved (VERONICA) VERONICA is gopher based resource. It allows access to the information resource stored on gopher’s servers.

Web Services

Web services allow exchange of information between applications on the web. Using web services, applications can easily interact with each other.

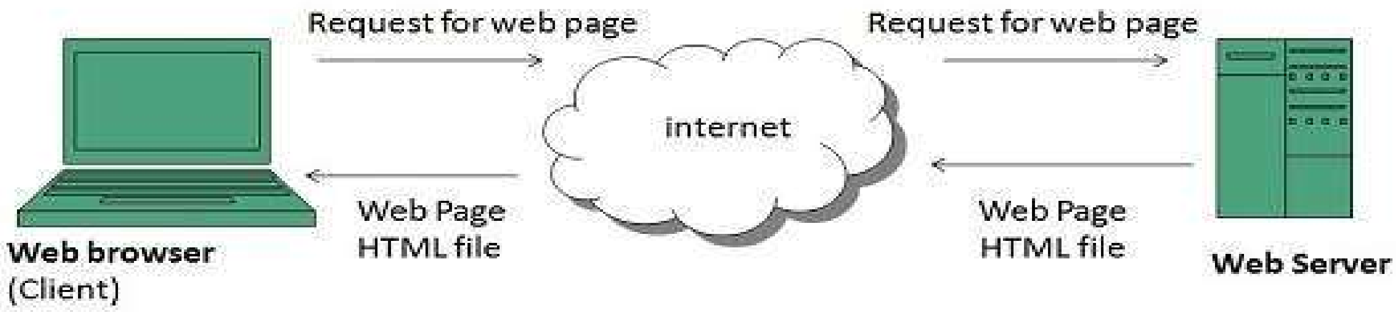
World Wide Web (WWW)

WWW is also known as W3. It offers a way to access documents spread over the several servers over the internet. These documents may contain texts, graphics, audio, video, hyperlinks. The hyperlinks allow the users to navigate between the documents.All the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).

WWW Operation

WWW works on client- server approach. Following steps explains how the web works:

1. User enters the URL of the web page in the address bar of web browser.
2. Then browser requests the Domain Name Server for the IP address corresponding to URL
3. After receiving IP address, browser sends the request for web page to the web server using HTTP protocol which specifies the way the browser and web server communicates.
4. Then web server receives request using HTTP protocol and checks its search for the requested web page. If found server response back to the web browser and close the HTTP connection.
5. Now the web browser receives the web page, it interprets content and display in web browser’s window.



Search Engine

Search Engine refers to a huge database of internet resources such as web pages, newsgroups, programs, images etc. It helps to locate information on World Wide Web.

User can search for any information by passing query in form of keywords or phrase. It then searches for relevant information in its database and return to the user.

Search Engine Components

Generally there are three basic components of a search engine as listed below:

1. Web Crawler
2. Database
3. Search Interfaces

Web crawler

It is also known as spider or bots. It is a software component that traverses the web to gather information.

Database

All the information on the web is stored in database. It consists of huge web resources.

Search Interfaces

This component is an interface between user and the database. It helps the user to search through the database.

Search Engine Working

Web crawler, database and the search interface are the major component of a search engine that actually makes search engine to work. Search engines make use of Boolean expression AND, OR, NOT to restrict and widen the results of a search.

Following are the steps that are performed by the search engine:

1. The search engine looks for the keyword in the index for predefined database instead of going directly to the web to search for the keyword.
2. It then uses software to search for the information in the database. This software component is known as web crawler.
3. Once web crawler finds the pages, the search engine then shows the relevant web pages as a result. These retrieved web pages generally include title of page, size of text portion, first several sentences etc.
4. User can click on any of the search results to open it.

Web Browser

Web Browser is an application software that allows us to view and explore information on the web. User can request for any web page by just entering a URL into address bar.

Web browser can show text, audio, video, animation and more. It is the responsibility of a web browser to interpret text and commands contained in the web page.

Web browser	**Search Engine**
A web browser is a software application used to retrieve data from webpages or HTML files present in servers.	Search Engine is kind of a website where a user can search for information and the results based on the same are displayed on the screen.
A web browser used Graphical Interface to help users experience an interactive online session on the World Wide Web	A search engine has three main components: • Search index • Crawler • Search algorithm
No database of its own. Only comprises a memory to store cache and cookies	It has its own database
Multiple Web Browsers can be installed on a single device	You do not need to install a search engine in your system
Examples of Web Browser are: • Chrome • Firefox • Mosaic • Internet Explorer • Opera	Examples of Search Engine include: • Google • Yahoo • Bing • Ask

Architecture and functioning of internet

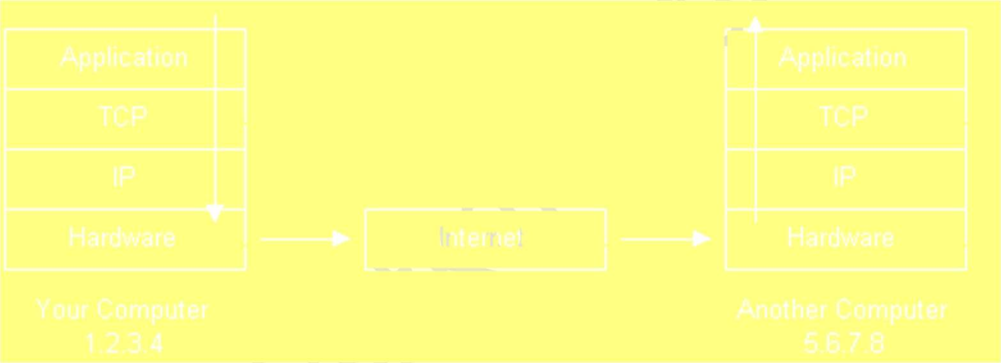
Because the Internet is a global network of computers each computer connected to the Internet **must** have a unique address. Internet addresses are in the form **nnn.nnn.nnn.nnn** where nnn must be a number from 0 - 255. This address is known as an IP address.

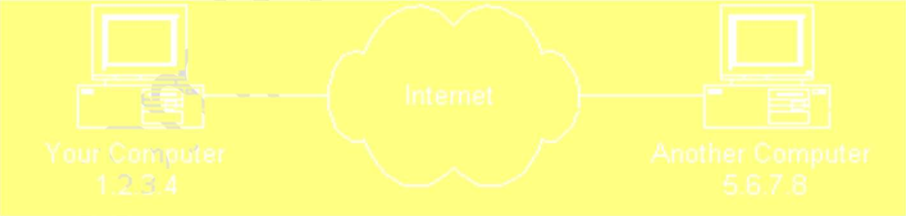
The picture illustrates two computers connected to the Internet; your computer with IP address 1.2.3.4 and another computer with IP address 5.6.7.8. The Internet is represented as an abstract object in-between.

Protocol Stacks and Packets

The message must be translated from alphabetic text into electronic signals, transmitted over the Internet, then translated back into alphabetic text, through the use of a **protocol stack**.

The protocol stack used on the Internet is referred to as the TCP/IP protocol stack because of the two major communication protocols used.





Protocol	Working
Application Protocols Layer	Protocols specific to applications such as WWW, e-mail, FTP, etc.
Transmission Control Protocol Layer	TCP directs packets to a specific application on a computer using a port number (segmentation, add port number and sequence number to packet).
Internet Protocol Layer	IP directs packets to a specific computer using an IP address (logical addressing, add IP address of source and destination).
Hardware Layer	Converts binary packet data to network signals and back. (E.g. Ethernet network card, modem for phone lines, etc.)

If we were to follow the path that the message "Hello computer 5.6.7.8!" took from our computer to the computer with IP address 5.6.7.8, it would happen something like this:

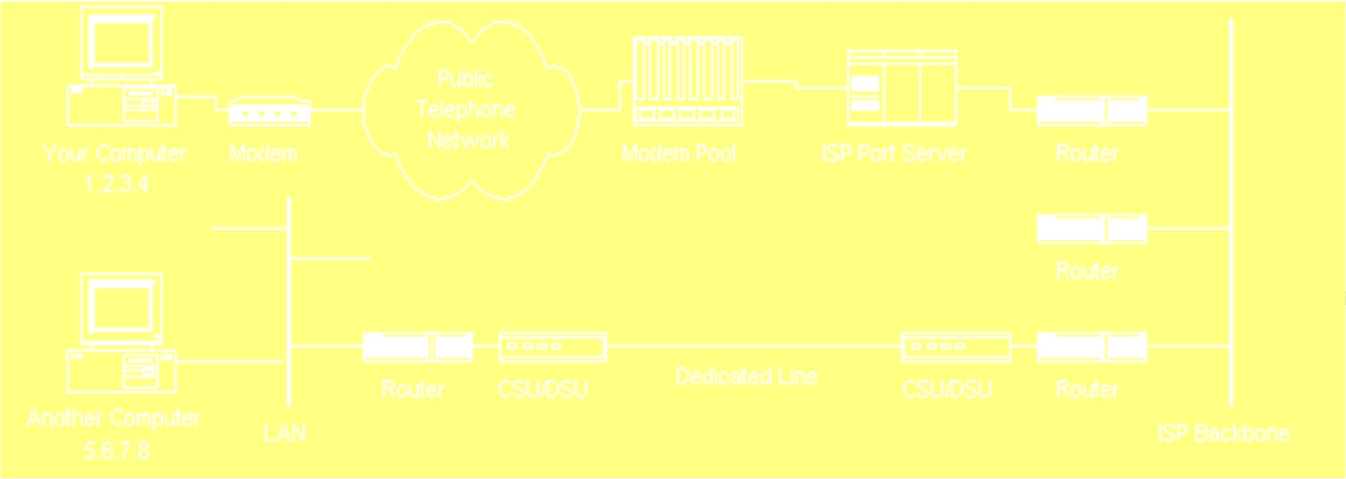
1. The message would start at the top of the protocol stack on our computer and work it's way downward.
2. If the message to be sent is long, each stack layer that the message passes through may break the message up into smaller chunks of data. This is because data sent over the Internet (and most computer networks) are sent in manageable chunks. On the Internet, these chunks of data are known as packets.
3. The packets would go through the Application Layer and continue to the TCP layer. Each packet is assigned a port number.

   Many programs may be using the TCP/IP stack and sending messages, We need to know which program on the destination computer needs to receive the message because it will be listening on a specific port. Port number help to identify the specific application in destination computer.

4. After going through the TCP layer, the packets proceed to the IP layer. This is where each packet receives its destination address, 5.6.7.8.
5. Now that our message packets have a port number and an IP address, they are ready to be sent over the Internet. The hardware layer takes care of turning our packets containing the alphabetic text of our message into electronic signals and transmitting them over the phone line.
6. On the other end of the phone line your ISP has a direct connection to the Internet. The ISPs router examines the destination address in each packet and determines where to send it.
7. Eventually, the packets reach computer 5.6.7.8. Here, the packets start at the bottom of the destination computer's TCP/IP stack and work upwards.
8. As the packets go upwards through the stack, all routing data that the sending computer's stack added (such as IP address and port number) is stripped from the packets.
9. When the data reaches the top of the stack, the packets have been re-assembled into their original form, "Hello computer 5.6.7.8!"

Networking Infrastructure

So now, it is clear that how packets travel from one computer to another over the Internet. But what's in-between? What actually makes up the Internet?



1. The ISP maintains a pool of modems for their dial-in customers known as Modem Pool.
2. Modem Pool is managed by some form of computer which controls data flow from Pool to a backbone or dedicated line router. This setup may be referred to as a port server, as it 'serves' access to the network. Billing and usage information is usually collected here as well.
3. After, packets traverse the phone network and ISP's local equipment, they are routed onto the ISP's backbone or a backbone the ISP buys bandwidth from.
4. From here the packets will usually journey through several routers and over several backbones, dedicated lines, and other networks until they find their destination, the computer with address 5.6.7.8.

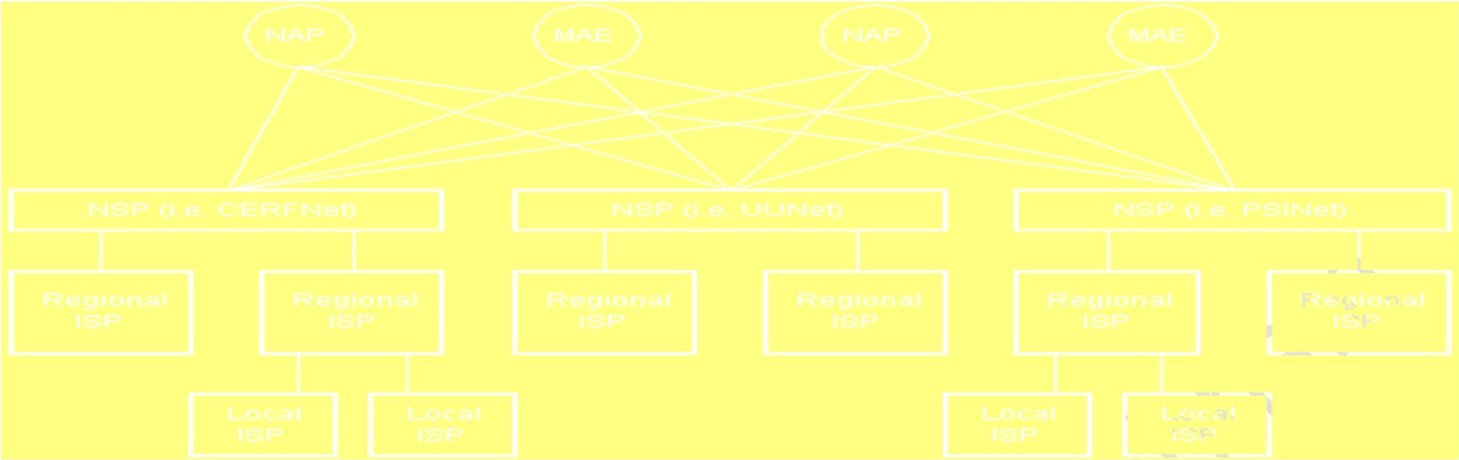
Internet Infrastructure

The Internet backbone is made up of many large networks which interconnect with each other. These large networks are known as **Network Service Providers** or **NSP**s.
Some of the large NSPs are UUNet, CerfNet, IBM, BBN Planet, SprintNet, PSINet, etc.

These networks **peer** with each other to exchange packet traffic.

Each NSP is required to connect to three **Network Access Points** or **NAP**s. At the NAPs, packet traffic may jump from one NSP's backbone to another NSP's backbone.

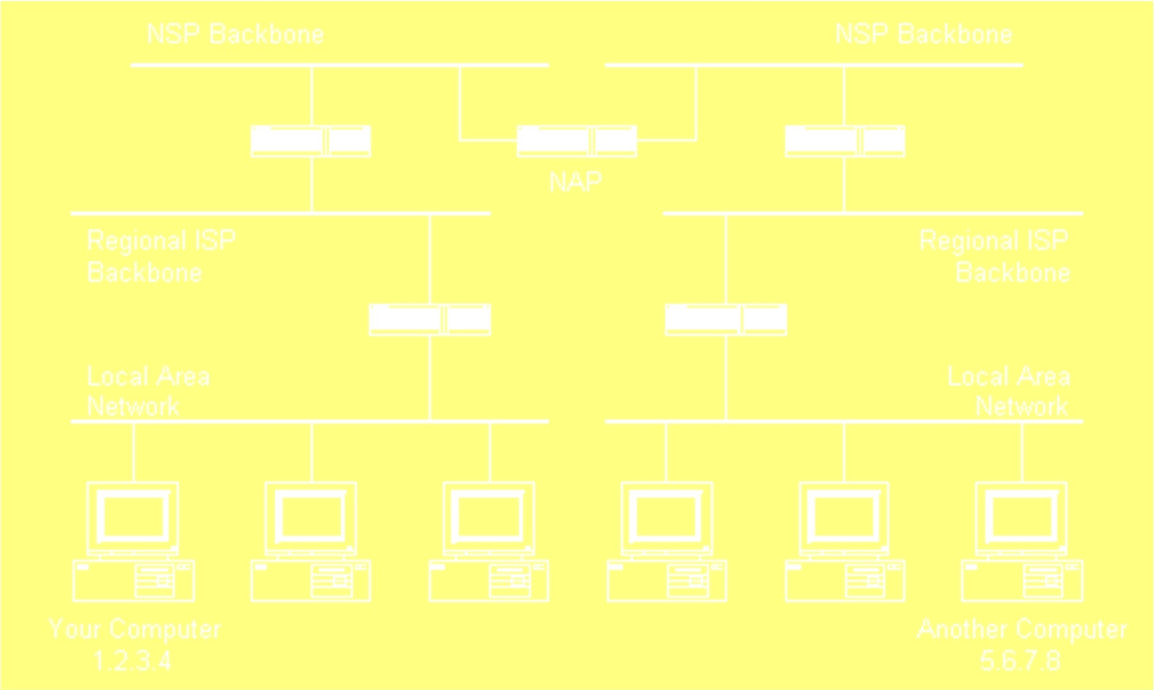
NSPs also interconnect at **Metropolitan Area Exchanges** or **MAE**s. MAEs serve the same purpose as the NAPs but are privately owned. NAPs were the original Internet interconnect points. Both NAPs and MAEs are referred to as Internet Exchange Points or **IX**s.
NSPs also sell bandwidth to smaller networks, such as ISPs and smaller bandwidth providers.



The Internet Routing Hierarchy

Routers are packet switches. A router is usually connected between networks to route packets between them. Each router knows about its sub-networks and which IP addresses they use.

The black boxes connecting the backbones are routers in diagram. The larger NSP backbones at the top are connected at a NAP. Under them are several sub-networks, and under them, more sub-networks. At the bottom are two local area networks with computers attached.



When a packet arrives at a router, the router examines the IP address put there by the IP protocol layer on the originating computer. The router checks its routing table. If the network containing the IP address is found, the packet is sent to that network. If the network containing the IP address is not found, then the router sends the packet on a default route, usually up the backbone hierarchy to the next router. Hopefully the next router will know where to send the packet. If it does not, again the packet is routed upwards until it reaches a NSP backbone.

The routers connected to the NSP backbones hold the largest routing tables and here the packet will be routed to the correct backbone, where it will begin its journey 'downward' through smaller and smaller networks until it finds its destination.

HTTP (Hypertext Transfer Protocol)

HTTP is the protocol that web browsers and web servers use to communicate with each other over the Internet. It is an application level protocol because it sits on top of the TCP layer in the protocol stack and is used by specific applications to talk to one another.

HTTP is a connectionless text based protocol. Clients (web browsers) send requests to web servers for web elements such as web pages and images. After the request is serviced by a server, the connection between client and server across the Internet is disconnected. A new connection must be made for each request.

When we type a URL into a web browser, this is what happens:

1. If the URL contains a domain name, the browser first connects to a domain name server and retrieves the corresponding IP address for the web server.
2. The web browser connects to the web server and sends an HTTP request (via the protocol stack) for the desired web page.
3. The web server receives the request and checks for the desired page. If the page exists, the web server sends it. If the server cannot find the requested page, it will send an HTTP 404 error message.
4. The web browser receives the page back and the connection is closed.
5. The browser then parses through the page and looks for other page elements it needs to complete the web page. These usually include images, applets, etc.
6. For each element needed, the browser makes additional connections and HTTP requests to the server for each element.
7. When the browser has finished loading all images, applets, etc. the page will be completely loaded in the browser window.

Transmission Control Protocol

TCP is responsible for routing application protocols to the correct application on the destination computer. To accomplish this, port numbers are used. Ports can be thought of as separate channels on each computer.

When a packet arrives at a computer and makes its way up the protocol stack, the TCP layer decides which application receives the packet based on a port number.

TCP works like this:

- When the TCP layer receives the application layer protocol data from above, it segments it into manageable 'chunks' and then adds a TCP header with specific TCP information to each 'chunk'. The information contained in the TCP header includes the port number of the application the data needs to be sent to.
- When the TCP layer receives a packet from the IP layer below it, the TCP layer strips the TCP header data from the packet, does some data reconstruction if necessary, and then sends the data to the correct application using the port number taken from the TCP header.

TCP is a connection-oriented, reliable, byte stream service

Connection-oriented means that two applications using TCP must first establish a connection before exchanging data.

TCP is reliable because for each packet received, an acknowledgement is sent to the sender to confirm the delivery. TCP also includes a checksum in its header for error-checking the received data.

Internet Protocol

1. IP is an unreliable, connectionless protocol.
2. IP doesn't care whether a packet gets to its destination or not. Nor does IP know about connections and port numbers.
3. IP's job is too send and route packets to other computers. IP packets are independent entities and may arrive out of order or not at all.
4. It is TCP's job to make sure packets arrive and are in the correct order.

IP receives data and adds its own IP header information to the TCP data.

Email

Email is a service which allows us to send the message in electronic mode over the internet. It offers an efficient, inexpensive and real time mean of distributing information among people.

E-Mail Address

Each user of email is assigned a unique name for his email account. This name is known as E-mail address. Different users can send and receive messages according to the e-mail address.

E-mail is generally of the form username@domainname.

- The username and the domain name are separated by **@ (at)** symbol.

- E-mail addresses are not case sensitive.
- Spaces are not allowed in e-mail address.

E-mail Message Components

E-mail message comprises of different components: E-mail Header, Greeting, Text, and Signature.

1) E-mail Header

The first five lines of an E-mail message is called E-mail header. The header part comprises of following fields:

- From
- Date
- To
- Subject
- CC
- BCC

From

The **From** field indicates the sender's address i.e. who sent the e-mail.

Date

The **Date** field indicates the date when the e-mail was sent.

To

The **To** field indicates the recipient's address i.e. to whom the e-mail is sent.

Subject

The **Subject** field indicates the purpose of e-mail. It should be precise and to the point.

CC

CC stands for Carbon copy. It includes those recipient addresses whom we want to keep informed but not exactly the intended recipient.

BCC

BCC stands for Black Carbon Copy. It is used when we do not want one or more of the recipients to know that someone else was copied on the message.

2) Greeting

Greeting is the opening of the actual message. Eg. Hi Sir or Hi Guys etc.

3) Text

It represents the actual content of the message.

4) Signature

This is the final part of an e-mail message. It includes Name of Sender, Address, and Contact Number.

Advantages

E-mail has proved to be powerful and reliable medium of communication. Here are the benefits of **E-mail:**

1) Reliable - Many of the mail systems notify the sender if e-mail message was undeliverable.
2) Convenience - There is no requirement of stationary and stamps. One does not have to go to post office. But all these things are not required for sending or receiving an mail.
3) Speed - E-mail is very fast. However, the speed also depends upon the underlying network.
4) Inexpensive - The cost of sending e-mail is very low.
5) Printable - It is easy to obtain a hardcopy of an e-mail. Also an electronic copy of an e-mail can also be saved for records.
6) Global - E-mail can be sent and received by a person sitting across the globe.
7) Generality - It is also possible to send graphics, programs and sounds with an e-mail.

Disadvantages

1) Forgery - E-mail doesn't prevent from forgery, that is, someone impersonating the sender, since sender is usually not authenticated in any way.
2) Overload - Convenience of E-mail may result in a flood of mail.
3) Misdirection - It is possible that you may send e-mail to an unintended recipient.
4) Junk - Junk emails are undesirable and inappropriate emails. Junk emails are sometimes referred to as spam.
5) No Response - It may be frustrating when the recipient does not read the e-mail and respond on a regular basis.

E-mail Protocols

E-mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server

SMTP

SMTP stands for Simple Mail Transfer Protocol. It is a standard protocol used for sending e-mail efficiently and reliably over the internet.

Key Points:

1) SMTP is application level protocol.
2) SMTP is connection oriented protocol.
3) SMTP is text based protocol.
4) It handles exchange of messages between e-mail servers over TCP/IP network.
5) Apart from transferring e-mail, SMPT also provides notification regarding incoming mail.
6) When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
7) These SMTP commands specify the sender's and receiver's e-mail address, along with the message to be send.
8) The exchange of commands between servers is carried out without intervention of any user.
9) In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

IMAP

IMAP stands for Internet Message Access Protocol.

Key Points:

1) IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
2) The e-mail is hold and maintained by the remote server.
3) It enables us to take any action such as downloading, delete the mail without reading the mail.It enables us to create, manipulate and delete remote message folders called mail boxes.
4) IMAP enables the users to search the e-mails.
5) It allows concurrent access to multiple mailboxes on multiple mail servers.

POP

POP stands for Post Office Protocol. It is generally used to support a single client.

Key Points

1) POP is an application layer internet standard protocol.
2) Since POP supports offline access to the messages, thus requires less internet usage time.
3) POP does not allow search facility.
4) In order to access the messaged, it is necessary to download them.
5) It allows only one mailbox to be created on server.
6) It is not suitable for accessing non mail data.
7) POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.

E-mail System

E-mail system comprises of the following three components:

1) Mailer - It is also called mail program, mail application or mail client. It allows us to manage, read and compose e-mail.
2) Mail Server - The function of mail server is to receive, store and deliver the email. It is must for mail servers to be running all the time because if it crashes or is down, email can be lost.
3) Mailboxes - Mailbox is generally a folder that contains emails and information about them.

IOT (INTERNET OF THINGS)

The Internet of Things (IoT) describes the network of physical objects—“things”—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

That includes an extraordinary number of objects of all shapes and sizes – from smart microwaves, which automatically cook our food for the right length of time, to self-driving cars, whose complex sensors detect objects in their path, to wearable fitness devices that measure our heart rate and the number of steps we’ve taken a day, then use this information to suggest exercise plans.

How does it work?

Devices and objects with built in sensors are connected to an Internet of Things platform, which integrates data from the different devices and applies analytics to share the most valuable information with applications built to address specific needs.

These powerful IoT platforms can pinpoint exactly what information is useful and what can safely be ignored. This information can be used to detect patterns, make recommendations, and detect possible problems before they occur.

The information picked up by connected devices enables us to make smart decisions about which components to stock up on, based on real-time information, which helps us to save time and money.

What Technologies Have Made IoT Possible?

1) Access to low-cost, low-power sensor technology. Affordable and reliable sensors are making IoT technology possible for more manufacturers.
2) Connectivity: A host of network protocols for the internet has made it easy to connect sensors to the cloud and to other “things” for efficient data transfer.
3) Cloud computing platforms: The increase in the availability of cloud platforms enables both businesses and consumers to access the infrastructure they need to scale up without actually having to manage it all.
4) Machine learning and analytics: With advances in machine learning and analytics, along with access to varied and vast amounts of data stored in the cloud, businesses can gather insights faster and more easily. The emergence of these allied technologies continues to push the boundaries of IoT and the data produced by IoT also feeds these technologies.
5) Conversational artificial intelligence (AI): Advances in neural networks have brought natural-language processing (NLP) to IoT devices (such as digital personal assistants Alexa, Cortana, and Siri) and made them appealing, affordable, and viable for home use.

Sensors

Sensor is a device that is able to detect changes in an environment. By itself, a sensor is useless, but when we use it in an electronic system, it plays a key role. A sensor is able to measure a physical phenomenon (like temperature, pressure, and so on) and transform it into an electric signal.

These three features should be at the base of a good sensor:

1) It should be sensitive to the phenomenon that it measures
2) It should not be sensitive to other physical phenomena
3) It should not modify the measured phenomenon during the measurement process

Properties of sensor:

1) Range: The maximum and minimum values of the phenomenon that the sensor can measure.

2) Sensitivity: The minimum change of the measured parameter that causes a detectable change in output signal.

3) Resolution: The minimum change in the phenomenon that the sensor can detect.

Sensor Classification

1) Passive or Active : Passive sensors do not require an external power source to monitor an environment, while Active sensors require such a source in order to work.

2) Another classification is based on the method used to detect and measure the property (mechanical, chemical, etc.).

3) Analog and Digital : Analog sensors produce an analog, or continuous, signal while digital sensors produce a discrete signal.

Type of Sensors

1) **Temperature Sensor -**A device, used to measure amount of heat energy that allows to detect a physical change in temperature from a particular source and converts the data for a device or user, is known as a Temperature Sensor

2) **Proximity sensor -** A device that detects the presence or absence of a nearby object, or properties of that object, and converts it into signal which can be easily read by user or a simple electronic instrument without getting in contact with them.

.Following are some of the Proximity Sensors sub-categorized:

- Inductive Sensors: Inductive proximity sensors are used for non-contact detection to find out the presence of metallic objects using electromagnetic field or a beam of electromagnetic radiation. It can operate at higher speeds than mechanical switches and also seems more reliable because of its robustness.
- Capacitive Sensors: Capacitive proximity sensors can detect both metallic as well as non-metallic targets. Nearly all other materials are dielectric different from air. It can be used to sense very small objects through a large portion of target. So, generally used in difficult and complicated applications.
- Photoelectric Sensors: Photoelectric sensor is made up of light-sensitive parts and uses a beam of light to detect the presence or absence of an object. It is an ideal alternative of inductive sensors. And used for long distance sensing or to sense non-metal object.

- Ultrasonic Sensors: Ultrasonic sensors are also used to detect the presence or to measure the distance of targets similar to radar or sonar. This makes a reliable solution for harsh and demanding conditions.

3) Pressure sensor

A pressure sensor is a device that senses pressure and converts it into an electric signal. Here, the amount depends upon the level of pressure applied.

There are plenty of devices that rely on liquid or other forms of pressure. These sensors make it possible to create IoT systems that monitor systems and devices that are pressure propelled. With any deviation from standard pressure range, the device notifies the system administrator about any problems that should be fixed.

4) Water quality sensor

Water quality sensors are used to detect the water quality and Ion monitoring primarily in water distribution systems.

Water is practically used everywhere. These sensors play an important role as they monitor the quality of water for different purposes. They are used in a variety of industries.

<u>Following is a list of the most common kind of water sensors in use:</u>

- Chlorine Residual Sensor: It measures chlorine residual in water and most widely used as disinfectant because of its efficiency.
- Total Organic Carbon Sensor: TOC sensor is used to measure organic element in water.
- Turbidity Sensor: Turbidity sensors measure suspended solids in water, typically it is used in river and stream gaging, wastewater and effluent measurement.
- Conductivity Sensor: Conductivity measurements are carried out in industrial processes primarily to obtain information on total ionic concentrations (i.e. dissolved compounds) in water solutions.
- pH Sensor: It is used to measure the pH level in the dissolved water, which indicates how acidic or basic (alkaline) it is.
- Oxygen-Reduction Potential Sensor: The ORP measurement provides insights into the level of oxidation/reduction reactions occurring in the solution.

5) Chemical sensor

Chemical sensors are applied in a number of different industries. Their goal is to indicate changes in liquid or to find out air chemical changes. They play an important role in bigger cities, where it is necessary to track changes and protect the population.

Main use cases of chemical sensors can be found in Industrial environmental monitoring and process control, intentionally or accidentally released harmful chemical detection, explosive and radioactive detection, recycling processes on

6) Gas sensor

Gas sensors are similar to the chemical ones, but are specifically used to monitor changes of the air quality and detect the presence of various gases. Like chemical sensors, they are used in numerous industries such as manufacturing, agriculture and health and used for air quality monitoring, detection of toxic or combustible gas, hazardous gas monitoring in coal mines, oil & gas industries, chemical laboratory research, manufacturing – paints, plastics, rubber, pharmaceutical & petrochemical etc.

Following are some common Gas sensors:

- Carbon dioxide sensor
- Breathalyzer
- Carbon monoxide detector
- Catalytic bead sensor
- Hydrogen sensor
- Air pollution sensor
- Nitrogen oxide sensor
- Oxygen sensor
- Ozone monitor
- Electrochemical gas sensor
- Gas detector
- Hygrometer

7) Smoke sensor

A smoke sensor is a device that senses smoke (airborne particulates & gases), and its level.

They have been in use for a long period of time. However, with the development of IoT, they are now even more effective, as they are plugged into a system that immediately notifies the user about any problem that occurs in different industries.

Smoke sensors are extensively used by manufacturing industry, HVAC, buildings and accommodation infra to detect fire and gas incidences. This serves to protect people working in dangerous environments, as the whole system is much more effective in comparison to the older ones.

Common Type of Smoke Sensors:

Smoke sensors detect the presence of Smoke, Gases and Flame surrounding their field. It can be detected either optically or by the physical process or by the use of both the methods.

- Optical smoke sensor (Photoelectric): Optical smoke sensor used the light scatter principle trigger to occupants.
- Ionization smoke sensor: Ionization smoke sensor works on the principle of ionization, kind of chemistry to detect molecules causing a trigger alarm.

8) IR sensors

An infrared sensor is a sensor which is used to sense certain characteristics of its surroundings by either emitting or detecting infrared radiation. It is also capable of measuring the heat being emitted by the objects.

They are now used in a variety of IoT projects, especially in Healthcare as they make monitoring of blood flow and blood pressure simple. They are even used in a wide array of regular smart devices such as smart watches and smartphones as well.

Other common use includes home appliances & remote control, breath analysis, Infrared vision (i.e. visualize heat leaks in electronics, monitor blood flow, art historians to see under layers of paint), wearable electronics, optical communication, non-contact based temperature measurements, automotive blind-angle detection.

9) Level sensors

A sensor which is used to determine the level or amount of fluids, liquids or other substances that flow in an open or closed system is called Level sensor..

Best use cases of level sensor is, fuel gauging & liquid levels in open or closed containers, sea level monitoring & Tsunami warning, water reservoirs, medical equipment, compressors, hydraulic reservoirs, machine tools, beverage and pharmaceutical processing, high or low-level detection etc.

This helps better streamline their businesses, as sensors collect all the important data at all times. With the use of these sensors, any product manager can precisely see how much liquid is ready to be distributed and whether the manufacturing should be stepped up.

There are two basic level measurement types:

- Point level sensors: Point level sensors usually detect the particular specific level and respond to the user if the sensing object is above or below that level. It is integrated into single device to get an alarm or trigger
- Continuous level Sensor: Continuous level sensors measure liquid or dry material levels within a specified range and provide outputs which continuously indicate the level. The best example of it is fuel level display in the vehicle.

10) Image sensors

Image sensors are instruments which are used to convert optical images into electronic signals for displaying or storing files electronically.

The major use of image sensor is found in digital camera & modules, medical imaging and night vision equipment,thermal imaging devices, radar, sonar, media house, Biometric & IRIS devices.

11) Motion detection sensors

A motion detector is an electronic device which is used to detect the physical movement (motion) in a given area and it transforms motion into an electric signal; motion of any object or motion of human beings

Motion detection plays an important role in the security industry. Businesses utilize these sensors in areas where no movement should be detected at all times, and it is easy to notice anybody's presence with these sensors installed.

These are primarily used for intrusion detection systems, automatics door control, boom barrier, smart camera (i.e motion based capture/video recording),toll plaza, automatic parking systems, automated sinks/toilet flusher,handdryers,energy management systems(i.e. Automated Lighting, AC, Fan, Appliances Control) etc.

Following are key motion sensor types widely used:

- Passive Infrared (PIR): It Detects body heat (infrared energy) and the most widely used motion sensor in home security systems.
- Ultrasonic: Sends out pulses of ultrasonic waves and measures the reflection off a moving object by tracking the speed of sound waves.
- Microwave: Sends out radio wave pulses and measures the reflection off a moving object. They cover a larger area than infrared & ultrasonic sensors, but they are vulnerable to electrical interference and more expensive.

12) Accelerometer sensors

Accelerometer is a transducer that is used to measure the physical or measurable acceleration experienced by an object due to inertial forces and converts the mechanical motion into an electrical output. It is defined as rate of change of velocity with respect to time

These sensors are now present in millions of devices, such as smartphones. Their uses involve detection of vibrations, tilting and acceleration in general. This is great for monitoring our driving fleet, or using a smart pedometer.

Following are few mainly used in IoT projects:

- Hall-effect accelerometers: Hall-effect accelerometers are using Hall principle to measure the acceleration, it measures the voltage variations caused by changes in a magnetic field around them.
- Capacitive accelerometers: Capacitive accelerometers sensing output voltage dependents on the distance between two planar surfaces. Capacitive accelerometers are also less prone to noise and variation with temperature.
- Piezoelectric accelerometers: Piezoelectric sensing principle is working on the piezoelectric effect. Piezo-film based accelerometers are best used to measure vibration, shock, and pressure.

13) Gyroscope sensors

A sensor or device which is used to measure the angular rate or angular velocity is known as Gyro sensors, Angular velocity is simply defined as a measurement of speed of rotation around an axis. It is a device used primarily for navigation and measurement of angular and rotational velocity in 3-axis directions. The most important application is monitoring the orientation of an object.

Their main applications are in car navigation systems, game controllers, cellular & camera devices, consumer electronics, robotics control, drone & RC control helicopter or UAV control, vehicle control/ADAS and many more..

14) Humidity sensors

Humidity is defined as the amount of water vapor in an atmosphere of air or other gases. The most commonly used terms are “Relative Humidity (RH)”.

Their applications and use can be found in Industrial & residential domain for heating, ventilating, and air conditioning systems control.

15) Optical sensors

A sensor which measures the physical quantity of light rays and convert it into electrical signal which can be easily readable by user or an electronic instrument/device is called optical sensor.

Optical sensors are loved by IoT experts, as they are practical for measuring different things simultaneously. The technology behind this sensor allows it to monitor electromagnetic energy, which includes, electricity, light and so on.

Due to this fact, these sensors have found use in healthcare, environment monitoring, energy, aerospace and many more industries. With their presence oil companies, pharmaceutical companies and mining companies are in a much better position to track environmental changes while keeping their employees safe.

Smart cities

A smart city is a city that uses technology to provide services and solve city problems. A smart city does things like improve transportation and accessibility, improve social services, promote sustainability, and give its citizens a voice and using technology to make their citizens’ lives easier.

The main goals of a smart city are to improve policy efficiency, reduce waste and inconvenience, improve social and economic quality, and maximize social involvement.

“Smart” describes to the city’s ability to create well-being for its citizens.

Cities use technology to collect data in real time about all kinds of things, including traffic, air and water quality, and solar radiation. With this information, the government can act immediately to solve any problem.

Some of the best-known applications of smart cities are, installing sensors in the streets that identify things like empty parking spots and traffic jams, estimate how long the next bus will take to arrive, and measure air and water quality. .

The city also uses GPS sensors to improve urgent medical services. Traffic lights detect ambulances and modify their output so that emergency services can move through the city as quickly as possible without creating dangerous situations.

Several major characteristics are used to determine a city's smartness. These characteristics include:

- a technology-based infrastructure;
- environmental initiatives;
- a high functioning public transportation system;
- a confident sense of urban planning and
- Humans to live and work within the city and utilize its resources.

Smart city technology

1. Smart cities use a combination of the internet of things (IoT) devices, software solutions, user interfaces (UI) and communication networks.

2. Data collected and delivered by the IoT sensors and devices is stored in the cloud or on servers.

3. The connection of these devices and use of data analytics (DA) improve both public and private sector efficiency, enabling economic benefits and improving citizen's lives..

4. A firewall security system is also necessary for the protection, monitoring and control of network traffic within a computing system. Firewalls ensure that the data constantly being transmitted within a smart city network is secure by preventing any unauthorized access to the IoT network or city data.

Other smart city technologies include:

- application programming interfaces (APIs)
- artificial intelligence (AI)
- cloud computing
- dashboards
- machine learning (ML)
- machine to machine (M2M)
- mesh network

Features of a smart city.

1) Any area of city management can be incorporated into a smart city initiative.

   A classic example is the smart parking meter that uses an application to help drivers find available parking spaces without prolonged circling of crowded city blocks. The smart meter also enables digital payment, so there's no risk of coming up short of coins for the meter.

2) In the transportation, smart traffic management is used to monitor and analyze traffic flows in order to optimize streetlights and prevent roadways from becoming too congested based on time of day or rush-hour schedules.

   Smart public transit is another aspect of smart cities. Smart transit companies are able to coordinate services and fulfill riders' needs in real time, improving efficiency and rider satisfaction. Ride-sharing and bike-sharing are also common services in a smart city.

3) Energy conservation and efficiency are major focuses of smart cities. Using smart sensors, smart streetlights dim when there aren't cars or pedestrians on the roadways. Smart grid technology can be used to improve operations, maintenance and planning, and to supply power on demand and monitor energy outages.

4) Smart city initiatives also aim to monitor and address environmental concerns such as climate change and air pollution. Waste management and sanitation can also be improved with smart technology.

5) Smart city technology is increasingly being used to improve public safety, from monitoring areas of high crime to improving emergency preparedness with sensors. For

example, smart sensors can be critical components of an early warning system before droughts, floods, landslides or hurricanes.

6) Smart city technologies also bring efficiencies to urban manufacturing and urban farming, including job creation, energy efficiency, space management and fresher goods for consumers.

How a smart city works

Smart cities utilize their web of connected IoT devices and other technologies to achieve their goals of improving the quality of life and achieving economic growth. Successful smart cities follow four steps:

1. Collection - Smart sensors throughout the city gather data in real time.
2. Analysis - Data collected by the smart sensors is assessed in order to draw meaningful insights.
3. Communication - The insights that have been found in the analysis phase are communicated with decision makers through strong communication networks.
4. Action - Cities use the insights pulled from the data to create solutions, optimize operations and asset management and improve the quality of life for residents.