UNIT- 4

Computer Networking: Introduction

Today the world scenario is changing. Data Communication and network have changed the way business and other daily affair works. Now, they rely on computer networks and internetwork. A set of devices often mentioned as nodes connected by media link is called a Network. A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called Communication channels.

Computer network is a telecommunication channel through which we can share our data. It is also called data network. The best example of computer network is Internet. Computer network does not mean a system with control unit and other systems as its slave. It is called a distributed system.

GOALS OF NETWORKING

1. Resource and load sharing
2. Programs do not need to run on a single machine
3. Reduced cost
4. Several machines can share printers, tape drives, etc.
5. High reliability
6. If a machine goes down, another can take over
7. Mail and communication

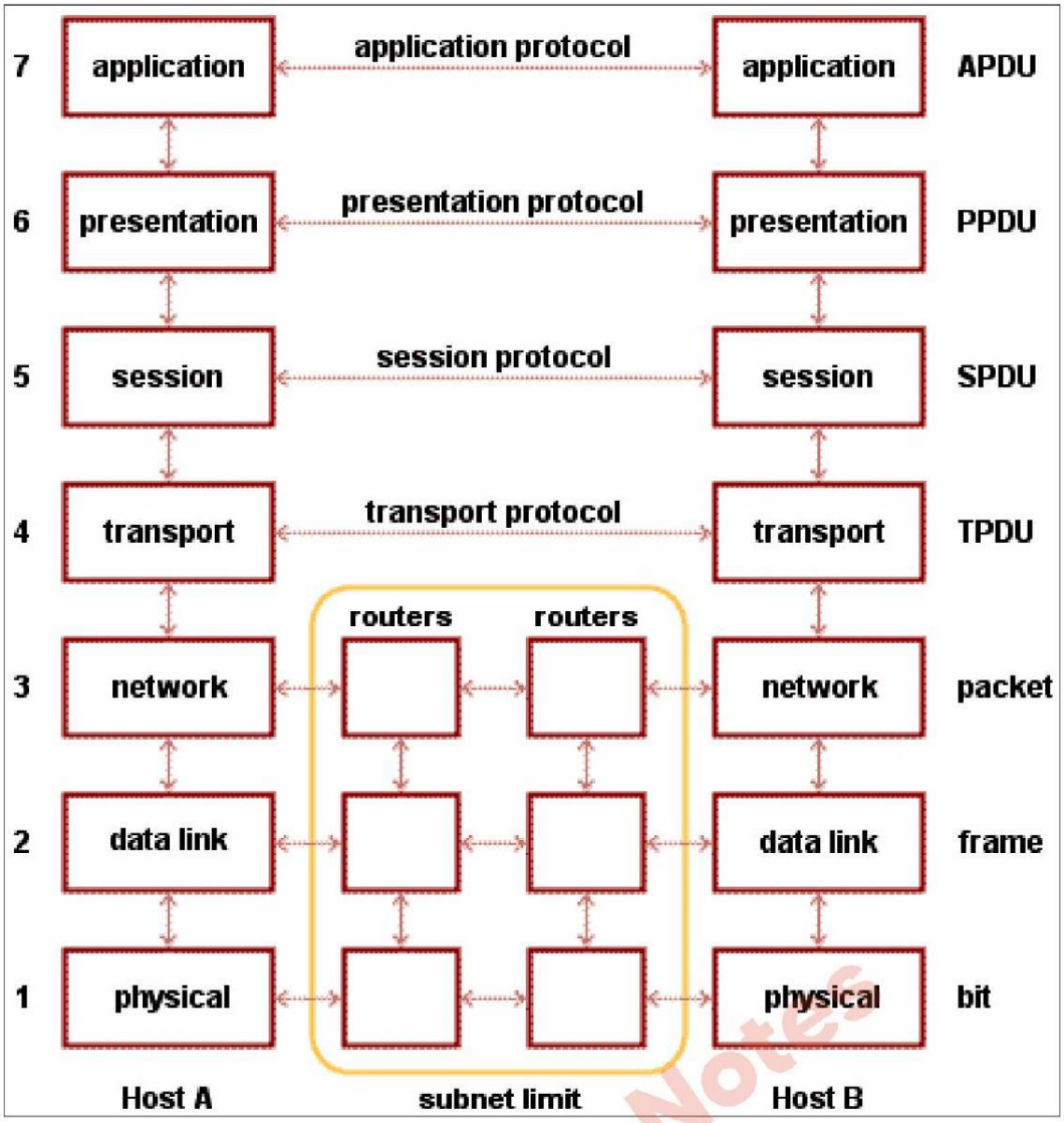
THE OSI REFERENCE MODEL

OSI (Open Systems Interconnection) is reference model for how applications can communicate over a network. A reference model is a conceptual framework for understanding relationships.

Feature of OSI Model:

- Big picture of communication over network is understandable through this OSI model.
- We see how hardware and software work together.
- We can understand new technologies as they are developed.

- Troubleshooting is easier by separate networks.
- Can be used to compare basic functional relationships on different networks.



Functions of Different Layers:

Layer 1: The Physical Layer:

- It is the lowest layer of the OSI Model.
- It activates, maintains and deactivates the physical connection.
- It is responsible for transmission and reception of the unstructured raw data over network.

- Voltages and data rates needed for transmission is defined in the physical layer.
- It converts the digital/analog bits into electrical signal or optical signals.
- Data encoding is also done in this layer.

Layer 2: Data Link Layer:

- It translates logical network address into physical address. Concerned with circuit, message or packet switching.
- Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination.
- Connection services are provided including network layer flow control, network layer error control and packet sequence control.
- Breaks larger packets into small packets.

Layer 3: The Network Layer:

- It translates logical network address into physical address. Concerned with circuit, message or packet switching.
- Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination.
- Connection services are provided including network layer flow control, network layer error control and packet sequence control.
- Breaks larger packets into small packets.

Layer 4: Transport Layer:

- Service Point Addressing: Transport Layer header includes service point address which is port address. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.
- Segmentation and Reassembling: A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission.
- Connection Control: It includes 2 types:

Connectionless Transport Layer: Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.

Connection Oriented Transport Layer: Before delivering packets, connection is made with transport layer at the destination machine.

- Flow Control: In this layer, flow control is performed end to end.
- Error Control: Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error Correction is done through retransmission.

Layer 5: The Session Layer:

- Dialog Control: This layer allows two systems to start communication with each other in half-duplex or full-duplex.
- Synchronization: This layer allows a process to add checkpoints which are considered as synchronization points into stream of data. Example: If a system is sending a file of 800 pages, adding checkpoints after every 50 pages is recommended. This ensures that 50-page unit is successfully received and acknowledged. This is beneficial at the time of crash as if a crash happens at page number 110 ; there is no need to retransmit 1 to100 pages.

Layer 6: The Presentation Layer:

- Translation: Before being transmitted, information in the form of characters and numbers should be changed to bit streams. The presentation layer is responsible for interoperability between encoding methods as different computers use different encoding methods. It translates data between the formats the network requires and the format the computer.
- Encryption: It carries out encryption at the transmitter and decryption at the receiver.
- Compression: It carries out data compression to reduce the bandwidth of the data to be transmitted. The primary role of Data compression is to reduce the number of bits to be Otransmitted. It is important in transmitting multimedia such as audio, video, text etc.

Layer 7: Application Layer:

- It is the topmost layer.
- Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc. are services provided by application layer.

- This layer mainly holds application programs to act upon the received and to be sent data.

Merits of OSI reference model:

- OSI model distinguishes well between the services, interfaces and protocols.
- Protocols of OSI model are very well hidden.
- Protocols can be replaced by new protocols as technology changes.
- Supports connection oriented services as well as connectionless service.

Demerits of OSI reference model:

- Model was devised before the invention of protocols.
- Fitting of protocols is tedious task.
- It is just used as a reference model.

Internetworking

Internetworking started as a way to connect disparate types of computer networking technology. Computer network term is used to describe two or more computers that are linked to each other. When two or more computer networks or computer network segments are connected using devices such as a router then it is called as computer internetworking.

Internetworking is a term used by Cisco. Any interconnection among or between public, private, commercial, industrial, or governmental computer networks may also be defined as an internetwork or Internetworking.

Internetworking in detail

In modern practice, the interconnected computer networks or Internetworking use the Internet Protocol. Two architectural models are commonly used to describe the protocols and methods used in internetworking. The standard reference model for internetworking is Open Systems Interconnection (OSI). Internetworking is implemented in Layer 3 (Network Layer) of this model the most notable example of internetworking is the Internet (capitalized). There are three variants of internetwork or Internetworking, depending on who administers and who participates in them:

- Extranet

- Intranet
- Internet

Extranet: An extranet is a network of internetwork or Internetworking that is limited in scope to a single organization or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities. Technically, an extranet may also be categorized as a MAN, WAN, or other type of network, although, by definition, an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

Intranet: An intranet is a set of interconnected networks or Internetworking, using the Internet Protocol and uses IP-based tools such as web browsers and ftp tools, that is under the control of a single administrative entity. That administrative entity closes the intranet to the rest of the world, and allows only specific users. Most commonly, an intranet is the internal network of a company or other enterprise. A large intranet will typically have its own web server to provide users with browsable information.

Internet: A specific Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and private networks based upon the Advanced Research Projects Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense also home to the World Wide Web (WWW) and referred to as the 'Internet' with a capital 'I' to distinguish it from other generic internetworks. Participants in the Internet, or their service providers, use IP Addresses obtained from address registries
that control assignments.

Different type of networking devices:

Network Hub:

Network Hub is a networking device which is used to connect multiple network hosts. A network hub is also used to do data transfer. The data is transferred in terms of packets on a computer network. So when a host sends a data packet to a network hub, the hub copies the data packet to all of its ports connected to. Like this, all the ports know about the data and the port for whom the packet is intended, claims the packet.
However, because of its working mechanism, a hub is not so secure and safe. Moreover, copying the data packets on all the interfaces or ports makes it slower and more congested which led to the use of network switch.

HUB

Modem

Switch

Network Switch:- Like a hub, a switch also works at the layer of LAN (Local Area Network) but you can say that a switch is more intelligent than a hub. While hub just does the work of data forwarding, a switch does 'filter and forwarding' which is a more intelligent way of dealing with the data packets.
So, when a packet is received at one of the interfaces of the switch, it filters the packet and sends only to the interface of the intended receiver. For this purpose, a switch also maintains a CAM (Content Addressable Memory) table and has its own system configuration and memory. CAM table is also called as forwarding table or forwarding information base (FIB).

Modem:

A modem stands for (Modulator+Demodulator). That means it modulates and demodulates the signal between the digital data of a computer and the analogue signal of a telephone line.

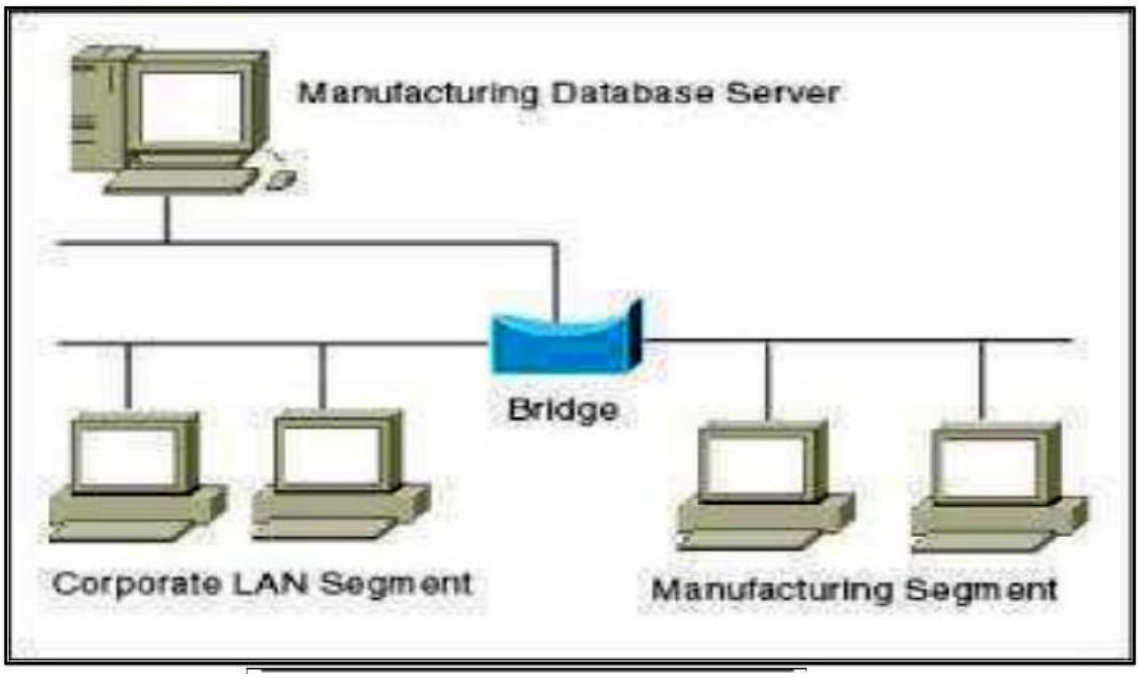
A Modem is somewhat a more interesting network device in our daily life. So, if you have noticed around, you get an internet connection through a wire (there are different types of wires) to your house. This wire is used to carry our internet data outside to the internet world. However, our computer generates binary data or digital

data in forms of 1 s and 0 s and on the other hand, a wire carries an analog signal and that's where a modem comes in.

Network Router:

A router is a network device which is responsible for routing traffic from one to another network. These two networks could be a private company network to a public network. You can think of a router as a traffic police who directs different network traffic to different directions.

1WIFI Router



Bridge:

If a router connects two different types of networks, then a bridge connects two subnetworks as a part of the same network. You can think of two different labs or two different floors connected by a bridge.

Repeater:

A repeater is an electronic device that amplifies the signal it receives. In other terms, you can think of repeater as a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances.
For example, inside a college campus, the hostels might be far away from the main college where the ISP line comes in. If the college authority wants to pull a wire in between the hostels and main campus, they will have to use repeaters if the distance is much because different types of cables have limitations in terms of the distances they can carry the data for.

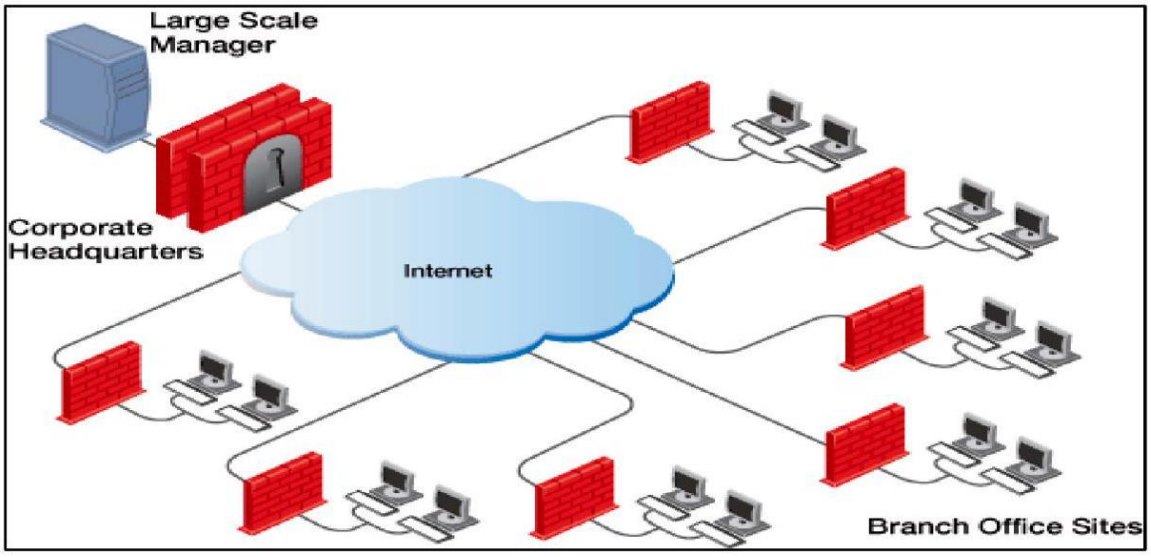
Brouters

Brouters are the combination of both the bridge and routers. They take up the functionality of the both networking devices serving as a bridge when forwarding data between networks, and serving as a router when routing data to individual systems. Brouter functions as a filter that allows some data into the local network

and redirects unknown data to the other network.

Gateways

Gateway is a device which is used to connect multiple networks and passes packets from one packet to the other network. Acting as the 'gateway' between different networking systems or computer programs, a gateway is a device which forms a link between them. It allows the computer programs, either on the same computer or on different computers to share information across the network through protocols. A router is also a gateway, since it interprets data from one network protocol to another.



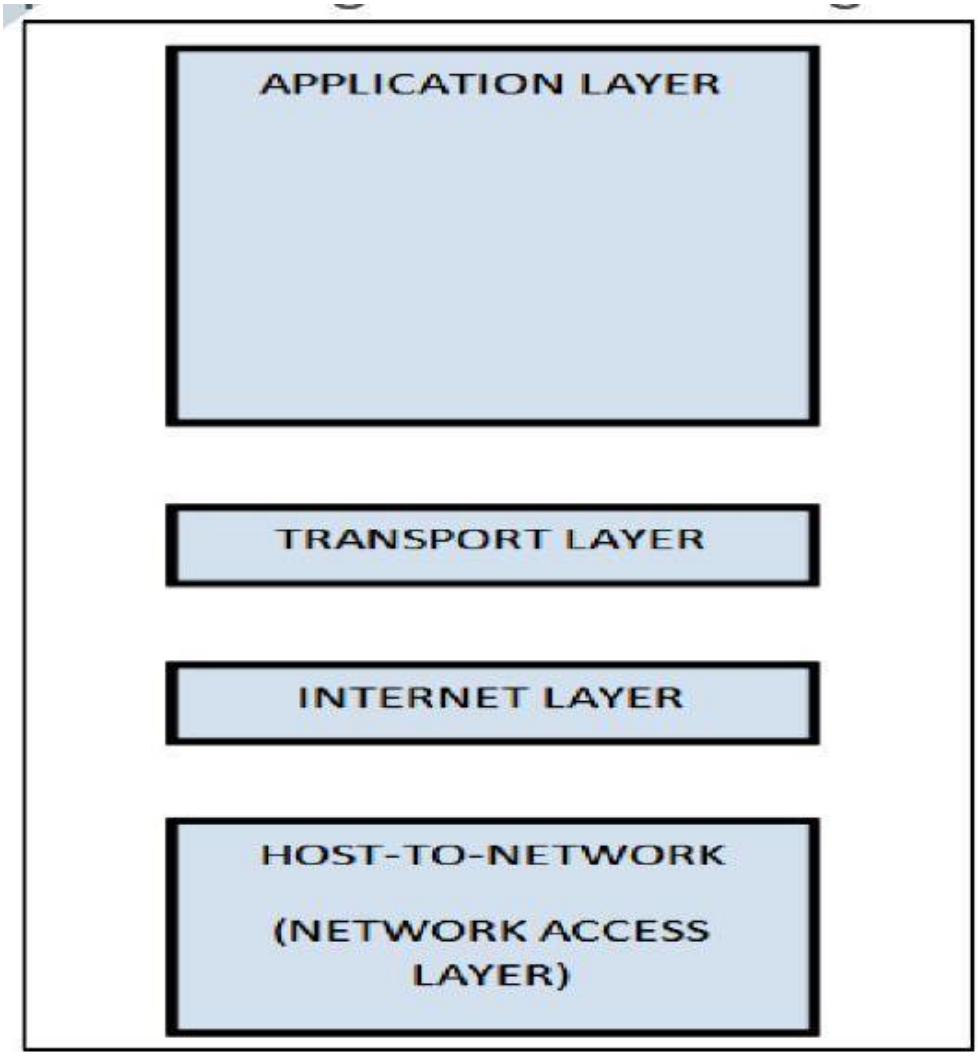
Network card

Network cards also known as Network Interface Cards (NICs) are hardware devices that connect a computer with the network. They are installed on the mother board. They are responsible for developing a physical connection between the network and the computer. Computer data is translated into electrical signals send to the network via Network Interface Cards.

Network Interface Card

The TCP/IP Reference Model

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. These protocols offer simple naming and addressing schemes.



Overview of TCP/IP reference model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defense's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact until the source and destination machines were functioning.
- The overall idea was to allow one application on one computer to talk to (send data packets) another application running on different computer.

Description of different TCP/IP protocols

Layer 1: Host-to-network Layer

- Lowest layer of the all.
- Protocol is used to connect to the host, so that the packets can be sent over it.
- Varies from host to host and network to network.

Layer 2: Internet layer

- Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
- It is the layer which holds the whole architecture together.
- It helps the packet to travel independently to the destination.
- Order in which packets are received is different from the way they are sent.
- IP (Internet Protocol) is used in this layer.

Layer 3: Transport Layer

- It decides if data transmission should be on parallel path or single path.
- Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
- The applications can read and write to the transport layer.
- Transport layer adds header information to the data.
- Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
- Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

- The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.
- TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
- FTP(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
- SMTP(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.

- DNS(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.

Merits of TCP/IP model

- It operated independently.
- It is scalable.
- Client/server architecture.
- Supports a number of routing protocols.
- Can be used to establish a connection between two computers.

Demerits of TCP/IP

- In this, the transport layer does not guarantee delivery of packets.
- The model cannot be used in any other application.
- Replacing protocol is not easy.
- It has not clearly separated its services, interfaces and protocols.

Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model.

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.

5. OSI is a reference model around which the networks are built. Generally, it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers

Internet: -

Internet is a network of computers linking many different types of computers all over the world. It is a network of networks sharing a common mechanism for addressing(identifying) computers, and a common set of communication protocols for communications between two computers on the network.

Applications of Internet

1. Communication

Computer users around the world extensively use the email service on internet to communicate with each other. Pictures, documents and other files are sent as email attachments. Emails can be cc-ed to multiple email addresses

2. Job search

Nowadays, many people search for their jobs online as it is quicker and there is a larger variety of job vacancies present. People can publish resume online for prospective job

3. Online Shopping

The internet has also facilitated the introduction of a new market concept consisting of virtual shops. They provide information about products or services for sale through www servers.

4. Stock market updates

You can sell or buy shares while sitting on computer through internet. Several websites like ndtvprofit.com, moneypore.com, provide information regarding investment

5. Travel

One can use internet to gather information about various tourist place. it can be used for booking Holiday tours, hotels, train, bus, flights and cabs.

6. Research

Research papers are present online which helps in the researcher doing literature review.

7. E-Commerce

E-commerce (electronic commerce or EC) is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the Internet.

8. Social networking

Social networking is the use of internet-based social media programs to make connections with friends, family, classmates, customers and clients.

WWW (World wide Web)

The World Wide Web has been central to the development of the Information Age and is the primary tool billions of people use to interact on the Internet. Web pages

are primarily text documents formatted and annotated with Hypertext Markup Language (HTML). In addition to formatted text, web pages may contain images, video, audio, and software components that are rendered in the user's web browser as coherent pages of multimedia content.
Embedded hyperlinks permit users to navigate between web pages. Multiple web pages with a common theme, a common domain name, or both, make up a website. Website content can largely be provided by the publisher, or interactively where users contribute content or the content depends upon the users or their actions. Websites may be mostly informative, primarily for entertainment, or largely for commercial,
governmental, or non-governmental organizational purposes.

The World Wide Web is a system that makes exchange of data on the Internet easy and efficient. It consists of two basic components:

The Web Server: a computer and software ("server" can refer to either) that stores and distributes data to other computers throughout the Internet that request the information.
The Web Browser: software running on an individual's ("client") computer that request information from the Web server and displays it in a manner of directed in the data file itself.

Introduction to E-Commerce

The term "Electronic commerce" (or e-Commerce) refers to the use of an electronic medium to carry out commercial transactions. Most of the time, it refers to the sale of products via Internet, but the term eCommerce also covers purchasing mechanisms via Internet (for B-To-B).

A client who purchases on the Internet is called a cyber consumer. E-Commerce is not only limited to online sales, but also covers:

- Preparation of estimates online
- Consulting of users
- Provision of an electronic catalog
- Access plan to point of sales
- Real-time management of product availability (stock)
- Online payment

- Delivery tracking
- After-sales service

In certain cases, electronic commerce makes it possible to highly customize products, in particular when the electronic commerce site is linked with the production system of the enterprise (e.g. business cards, customized items such as T-shirts, cups, caps, etc.)

Computer Security Basics

Computer Security is the process of detecting and preventing any unauthorized use of your laptop/computer. It involves the process of safeguarding against trespassers from using your personal or office based computer resources with malicious intent or for their own gains, or even for gaining any access to them accidentally.
"Malware" is short for malicious software and used as a single term to refer to virus, spy ware, worm etc. Malware is designed to cause damage to a standalone computer or a networked pc. So, wherever a malware term is used it means a program which is designed to damage your computer it may be a virus, worm or Trojan.

Worms: -

Worms are malicious programs that make copies of themselves again and again on the local drive, network shares, etc. The only purpose of the worm is to reproduce itself again and again. It doesn't harm any data/file on the computer. Unlike a virus, it does not need to attach itself to an existing program. Worms spread by exploiting vulnerabilities in operating systems

Examples of worm are: - W32.SillyFDC.BBY
Packed.Generic. 236

W32.Troresba

Due to its replication nature it takes a lot of space in the hard drive and consumes more cpu uses which in turn makes the pc too slow also consumes more network bandwidth.

Virus: -

Virus is a program written to enter to your computer and damage/alter your files/data. A virus might corrupt or delete data on your computer. Viruses can also replicate themselves. A computer Virus is more dangerous than a computer worm as it makes changes or deletes your files while worms only replicates itself without making changes to your files/data.

Examples of virus are: - W32.Sfc!mod
ABAP.Rivpas.A
Accept. 3773
Viruses can enter to your computer as an attachment of images, greeting, or audio / video files. Viruses also enters through downloads on the Internet. They can be hidden in a free/trial software's or other files that you download.

Virus is of different types which are as follows.

1. File viruses
2. Macro viruses
3. Master boot record viruses
4. Boot sector viruses
5. Multipartite viruses
6. Polymorphic viruses
7. Stealth viruses

File Virus: -This type of virus normally infects program files such as .exe, .com, .bat. Once this virus stays in memory it tries to infect all programs that load on to memory.

Macro Virus: - These types of virus infect word, excel, PowerPoint, access and other data files. Once infected repairing of these files is very much difficult.

Master boot record files: - MBR viruses are memory-resident viruses and copy itself to the first sector of a storage device which is used for partition tables or OS loading programs. A MBR virus will infect this particular area of Storage device instead of normal files. The easiest way to remove a MBR virus is to clean the MBR area,

Boot sector virus: - Boot sector virus infects the boot sector of a HDD or FDD. These are also memory resident in nature. As soon as the computer starts it gets infected from the boot sector.

Cleaning this type of virus is very difficult.
Multipartite virus: - A hybrid of Boot and Program/file viruses. They infect program files and when the infected program is executed, these viruses infect the boot record. When you boot the computer next time the virus from the boot record loads in memory and then start infecting other program files on disk

Polymorphic viruses: - A virus that can encrypt its code in different ways so that it appears differently in each infection. These viruses are more difficult to detect.

Stealth viruses: - These types of viruses use different kind of techniques to avoid detection. They either redirect the disk head to read another sector instead of the one in which they reside or they may alter the reading of the infected file's size shown in the directory listing. For example, the Whale virus adds 9216 bytes to an infected file; then the virus subtracts the same number of bytes (9216) from the size given in the directory.

Trojans: - A Trojan horse is not a virus. It is a destructive program that looks as a genuine application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans also open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft.

Example: - JS.Debeski.Trojan
Trojan horses are broken down in classification based on how they infect the systems and the damage caused by them. The seven main types of Trojan horses are:

- Remote Access Trojans
  -Data Sending Trojans
- Destructive Trojans
  -Proxy Trojans
- FTP Trojans
- security software disabler Trojans
- denial-of-service attack Trojans

Adware: - Generically adware is a software application in which advertising banners are displayed while any program is running. Adware can automatically get downloaded to your system while browsing any website and can be viewed through

pop-up windows or through a bar that appears on a computer screen automatically. Adware's are used by companies for marketing purpose.

Spywares: - Spyware is a type of program that is installed with or without your permission on your personal computers to collect information about users, their computer or browsing habits tracks each and everything that you do without your knowledge and send it to remote user.

Spam: - Spamming is a method of flooding the Internet with copies of the same message. Most spams are commercial advertisements which are sent as an unwanted email to users. Spams are also known as Electronic junk mails or junk newsgroup postings. These spam mails are very annoying as it keeps coming every day and keeps your mailbox full.

Tracking cookies: - A cookie is a plain text file that is stored on your computer in a cookies folder and it stores data about your browsing session.

Misleading applications: - Misleading applications misguide you about the security status of your computer and shows you that your computer is infected by some malware and you have to download the tool to remove the threat.

The common types of cybercrimes are: -

1.Hacking - An unauthorized user who attempts to or gains access to an information system is known as hacker. Hacking is a cybercrime even if there is no visible damage to the system, because it is an invasion in to the privacy of data.

There are 3 different classes of Hackers.
a) White Hat Hackers - They are those hackers who believe that information sharing is good, and that it is their duty to share their expertise by facilitating access to information. However, there are some white hat hackers who are just "joy riding" on computer systems.
b) Black Hat Hackers - Black hat hackers cause damage after intrusion. They may steal or modify data or insert viruses or worms which damage the system. They are also known as crackers.
c) Grey Hat Hackers - These types of hackers are typically ethical but occasionally they can violate the hacker ethics. They will hack into networks, stand-alone computers and software. Network hackers try to gain unauthorized access to private computer networks just for challenge, curiosity, and distribution of information.

2. Cyber Stalking - Cyber stalking involves use of internet to harass someone. The behavior includes false accusations, threats etc. Normally, majority of cyber stalkers are men and the majority of victims are women.
3. Spamming - Spamming is sending of unsolicited bulk and commercial messages over the internet. Although irritating to most email users, it is not illegal unless it causes damage such as overloading network and disrupting service to subscribers or creates negative impact on consumer attitudes towards Internet Service Provider.
4. Cyber Pornography - With the increasing approach of internet to the people, there is also an increase in the victimization of Women and children for sexual exploitation through internet
5. Cyber Phishing - It is a criminally fraudulent process in which cyber-criminal acquires sensitive information such as username, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.
6. Software Piracy - It is an illegal reproduction and distribution of software for business or personal use. This is considered to be a type of infringement of copy right and a violation of a license agreement. Since the unauthorized user is not a party to the license agreement it is difficult to find out remedies. There are numerous cases of software piracy. Infact according to one report New Delhi's Nehru market is the Asia's largest market where one can easily find pirated software.
7. Money Laundering - Money laundering basically means the moving of illegally acquired cash through financial and other systems so that it appears to be legally acquired. This is possible prior to computer and internet technology and now times electronic transfers have made it easier and more successful.
8. Password Sniffers - These are programs that monitor and record the name and password of network users as they log in, jeopardizing security at a site. Whoever installs the sniffer can impersonate an authorized user and log in to access on restricted documents.
9. Spoofing - Spoofing is the act of disguising one computer to electronically "look" like another compute, in order to gain access to a system that would be normally is restricted.
10. Credit Card Fraud - In U.S.A. half a billion dollars have been lost annually by consumers who have credit cards and calling card numbers. These are stolen from on-line databases. In present world this cybercrime is emerged as a major threat as numerous cases had been filed in almost every major developed and developing country.
13. Web Jacking - The term refers to forceful taking of control of a web site by cracking the password.

11. Cyber terrorism - The use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives is called cyber terrorism. Individuals and groups quite often try to exploit anonymous character of the internet to threaten governments and terrorize the citizens of the country

Cyber defamation is not a specific criminal offense, misdemeanor or tort, but rather defamation or slander conducted via digital media, usually through the Internet.

Penalties for "cyber defamation" vary from country to country, but the fundamental rights covered in the UN Declaration of Human Rights and European Union Fundamental Human Rights.

Stopping or addressing defamation can be difficult. If the person has no serious grudge, then a cease and desist letter may stop the behavior and get the statements removed from the Internet. On the other hand, if the person is acting out of spite, it may be necessary to file a report with the police depending on local law.

Pharming is a cyber-attack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers are sometimes referred to as "poisoned". Pharming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server.

Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet. A firewall can be hardware, software, or both.

Packet filtering: The system examines each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly

effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

Circuit-level gateway implementation: This process applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Acting as a proxy server: A proxy server is a type of gateway that hides the true network address of the computer(s) connecting through it. A proxy server connects to the Internet, makes the requests for pages, connections to servers, etc., and receives the data on behalf of the computer(s) behind it.

Web application firewall: A web application firewall is a hardware appliance, server plug-in, or some other software filter that applies a set of rules to a HTTP conversation. Such rules are generally customized to the application so that many attacks can be identified and blocked.

Computer Ethics & Good Practices: -

Ethics deals with placing a "value" on acts according to whether they are "good" or "bad". Every society has its rules about whether certain acts are ethical or not. These rules have been established because of consensus in society and are often written into laws.

The Ten Commandments of computer ethics have been defined by the Computer Ethics Institute. Here is our interpretation of them:

1. Do not use a computer to harm other people: If it is unethical to harm people by making a bomb, for example, it is equally bad to write a program that handles the timing of the bomb. Or, to put it more simply, if it is bad to steal and destroy other people's books and notebooks, it is equally bad to access and destroy their files.
2. Do not interfere with other people's computer work: Computer viruses are small programs that disrupt other people's computer work by destroying their files, taking huge amounts of computer time or memory, or by simply displaying annoying messages. Generating and consciously spreading computer viruses are unethical.
3. Do not snoop around in other people's files: Reading other people's e-mail messages are as bad as opening and reading their letters: This is invading their privacy. Obtaining other people's non-public files should be judged the

same way as breaking into their rooms and stealing their documents. Text documents on the Internet may be protected by encryption.

4. Do not use a computer to steal: Using a computer to break into the accounts of a company or a bank and transferring money should be judged the same way as robbery. It is illegal and there are strict laws against it.
5. Do not use a computer to bear false witness: The Internet can spread untruth as fast as it can spread the truth. Putting out false "information" to the world is bad. For instance, spreading false rumors about a person or false propaganda about historical events is wrong.
6. Do not use or copy software for which you have not paid: Software is an intellectual product. In that way, it is like a book: Obtaining illegal copies of copyrighted software is as bad as photocopying a copyrighted book. There are laws against both. Information about the copyright owner can be embedded by a process called watermarking into pictures in the digital format.

Introduction to Cyber Law

In a Simple way, we can say that cybercrime is unlawful acts wherein the computer is either a tool or a target or both. Cybercrimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation, and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.
We can categorize Cyber crimes in two ways

- The Computer as a Target: -using a computer to attack other computers. e.g. Hacking, Virus/Worm attacks, DOS attack etc.
- The computer as a weapon: -using a computer to commit real-world crimes. e.g. Cyber Terrorism, IPR violations, Credit card frauds, Pornography etc. Cyberlaw (also referred to as cyberlaw) is a term used to describe the legal issues related to using of communications technology, particularly "cyberspace", i.e. the Internet.

Cyberlaw in India

When the Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all-pervading revolution which could be misused for criminal activities and which required regulation. Today, there

are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage in a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyber laws in India.

Importance of Cyberlaw

Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web, and Cyberspace. Initially, it may seem that Cyber laws is a very technical field and that it does not have any bearing on most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cybercrimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear
of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely because it is in the form of electronic records.

Internet Frauds

Internet fraud is a type of fraud which makes use of the Internet. This type of fraud varies greatly and appears in many forms. It ranges from E-mail spam to online scams. Internet fraud can occur even if partly based on the use of internet services and is mostly or completely based on the use of the internet.

The main types of internet fraud:

- Stolen credit cards

Credit Card fraud across the internet is one of the more common examples of this type of crime. Some people fall prey to this type of scam because they are careless whilst others are duped by clever phishing schemes.

- Emails

Used as intended, email is a great means of communication that can allow messages to be sent to huge numbers of people at virtually no cost. Unfortunately, this means that it is also an ideal medium for scam artists.

- Lotteries

Fake lottery scams will try to persuade you that you've won a huge amount of money in an online draw. People behind this fraud then try to trick you into revealing your personal information as you try to collect your winnings.

- Fake auctions

Buying and selling goods through internet auction sites is an extremely popular pastime for some, and a great means of doing business for others. Unfortunately, scam artists have seen the potential of infiltrating online auction sites. Internet auction fraud is one of the most common rip-offs on the net today.

- Untrustworthy Websites

A slightly newer form of internet fraud is the fake website. Cybercriminals have begun mimicking established websites and then tricking visitors into interacting with them as if they were the real deal.

Good Computer Security Habits

1. Create strong passwords

Passwords are usually the first, and sometimes only, protection against unauthorized access. They are the keys to your online kingdom, so keep these guidelines in mind.
Do not use your name, common phrases or words or acronyms that can be found in the dictionaryincluding foreign languages.

2. Lock your computer screen

You never know who might use your computer when you're not around, so it's important to lock your screen to prevent unauthorized access. In the office, a co-worker, guest or a service provider might view or use your unattended computer. This is an easy way for private information to become public.

3. Secure mobile devices from loss

While mobile devices such as smartphones, tablets, and laptops are valued for their portability, this convenience can become a security risk.
It's easy to lose or misplace these devices, so be sure to:

- Make a list of phone numbers and email addresses to report stolen or lost devices Use a hardware cable lock for your laptop, or store it in a locked drawer.
- Keep smartphones and tablets with you when in public
- Never put devices in your checked baggage when traveling

4. Protect data on mobile devices and removable media

Mobile devices and removable media, such as USB drives, enable us to easily share and transport information but can lead to the loss or misuse of data.

5. Identify URLs before clicking

Simply stated: think before you click. A malicious website that looks legitimate is a common method used by criminals. However, verifying the real destination is easy- just place your cursor over the displayed URL, and the true destination will reveal itself with a small pop-up. Don't click if it looks suspicious.

6. Use public Wi-Fi safely

Public Wi-Fi is riskier than corporate or home Wi-Fi because you can't determine its setup and security features. So, take extra precautions when using it.

- Do not access sensitive personal accounts, such as financial accounts
- Ensure websites use HTTPS and display a lock icon
- Watch out for "shoulder surfing" from people and security cameras
- Never use a public computer, such as one in a hotel lobby, to access personal information
- Use only for general web browsing, e.g., weather forecasts and restaurant reviews.

7. Think before you post to social media

Social media provides a convenient, fun way to stay in touch with friends and family. But be cautious about what you post. Understand both personal and business risks, and take the following precautions:

- Always comply with your company's rules for business conduct
- Ask friends and family to keep your personal information private, including relationships
- Be cautious about participating in games and surveys or clicking on links suggested by others
- Review and update your social media privacy and security settings often.

If you have any queries please visit- https://studywithakash.in/

Gmail – studywithakash311@gmail.com

+918871317984

THANK YOU