

Internet Network

Objectives...

- To learn Basic Concepts in Computer Network
- To study Computer Network Terminologies (Node, LAN, WAN)
- To understand Communication Media
- To learn Types of Network (Peer-to-Peer and Client-Server)

4.0 INTRODUCTION

When two or more separate networks are connected for exchanging data or resources, they become an internetwork (or internet).

An Internetwork is a general term describing multiple networks connected together. The Internet is the largest and most well-known internetwork.

Internet is a world-wide global system of interconnected computer networks. The word 'Internet' is derived from two words namely, interconnection and networks. It is also referred to as 'Net'.

Internet is a global network links thousands of computers at universities, research institutions, government agencies, business and houses throughout the world.

An Internet is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies.

Internet is a worldwide system of computer networks, i.e. a network of networks, which allows the participants (users) to share information.

Computer networks is the one of the fastest growing technological areas in today's modern world. This is because there is an almost unlimited demand for information transfer.

A computer network is an interconnected collection of autonomous computers and computing devices (printer, scanner, router, hub, bridge, modem and so on).

A computer network is an interconnection of computers and computing devices using either wires or radio waves over small or large geographical areas.

4.1 NETWORKS

- A network is the interconnection of a set of devices (like a host (desktop, laptop, workstation, smartphone) and/or connecting devices like router, switch, modem etc.).
- A network is nothing more than two or more computers connected by a cable or by a wireless radio waves connection so that they can exchange information.
- A communication network is a set of devices connected by channels on links and provides a service between users located at various geographical points.
- A network is defined as, "an interconnected collection of autonomous computers". Two computers are said to be interconnected if they are capable of exchanging information.

4.1.1 Computer Networks

- A computer network is an interconnection of computers and computing devices using either wires or radio waves over small or large geographical areas.
- A computer network refers to a collection of two or more computers (nodes) which are connected together to share information and resources.
- A network is the interconnection of a set of computing devices capable of communication.
- A network is a set of devices, (often referred to as nodes) connected by communication media links (See Fig. 4.1).
- A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
- The links connecting the devices are often called communication channels. The term channel refers to a communication path between two communicating devices.

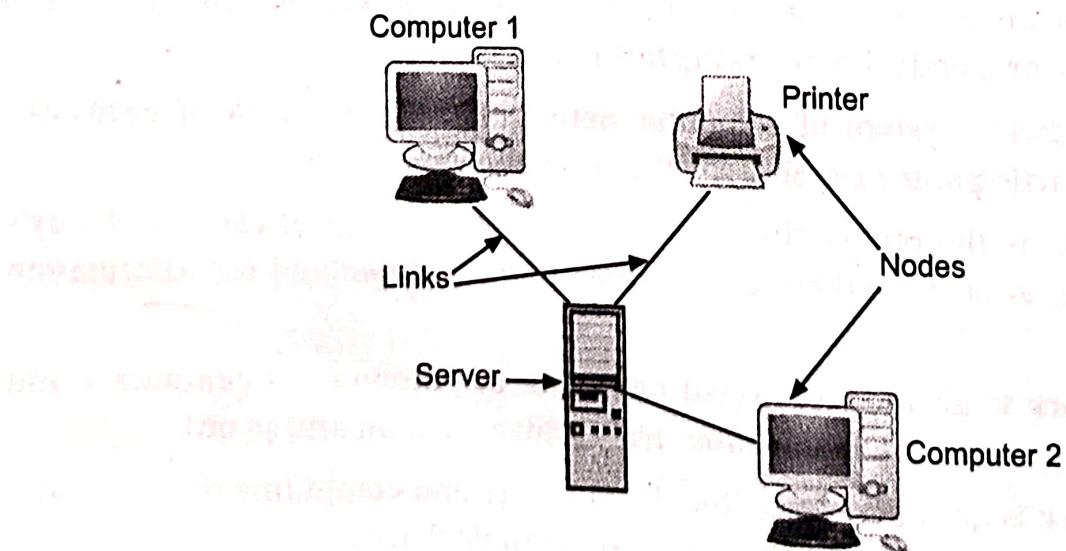


Fig. 4.1: Network Nodes and Links

- Computer network is a set or collection of computing devices that are linked to each other in order to communicate and share their resources with each other.
- In simple words, a computer network is a group of interconnected computing devices. The interconnected computers can share resources, which is called networking.
- Computer network is divided into wired and wireless networks. Fig. 4.2 shows diagrammatic representation of computer networks (wired and wireless).

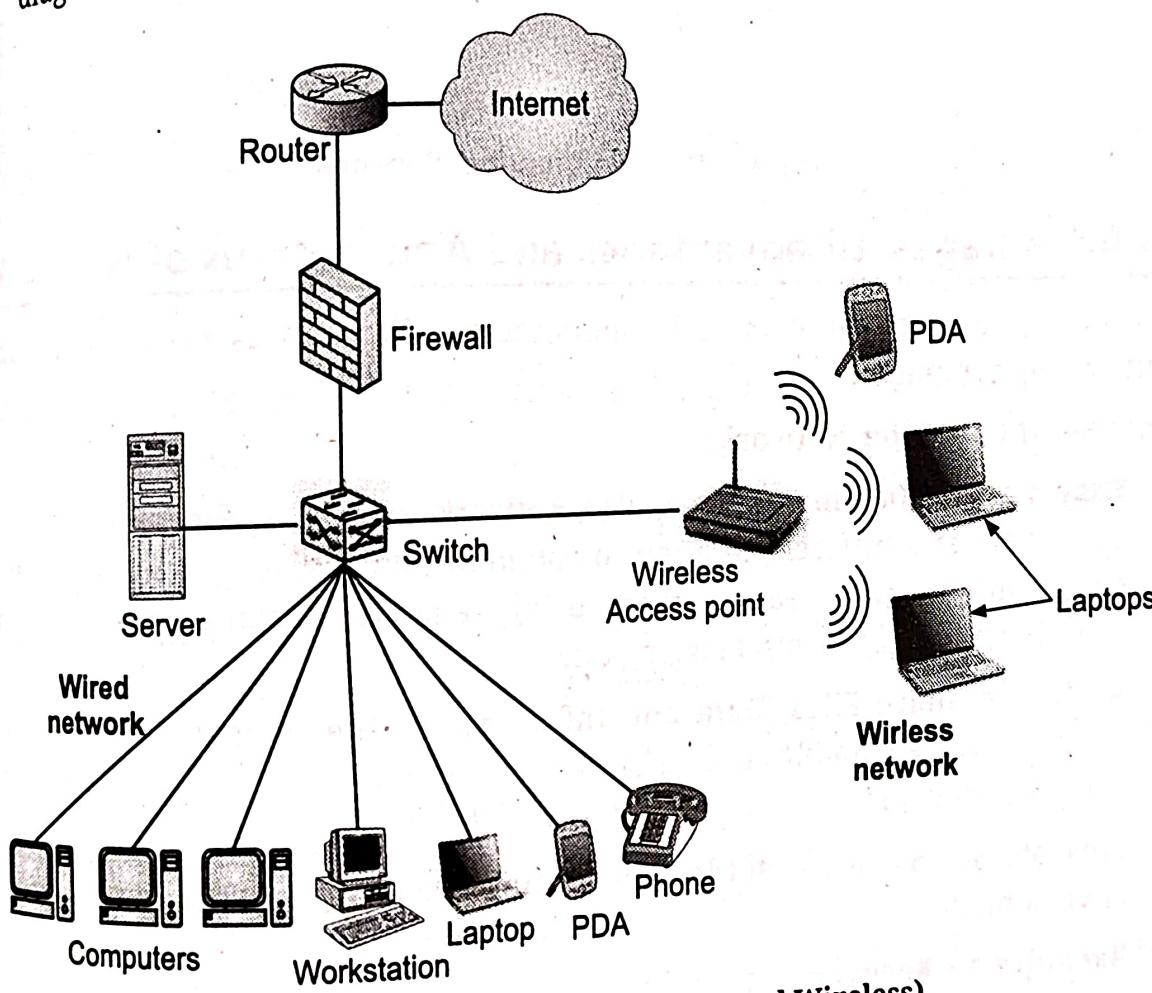


Fig. 4.2: Computer Network (Wired and Wireless)

A **wired network** is simply, a collection of nodes connected by cables like Ethernet, coaxial, fiber optic cable etc. A **wireless network**, which uses high-frequency radio waves to communicate between nodes.

1.1.2 Definition of Computer Network

A computer network can be defined as "an interconnected collection of autonomous computers and computing devices".

OR

A computer network is "an interconnection of computers and computing equipment like printer, scanner etc. using either wires or radio waves (wireless) made to share hardware and software resources".

- Fig. 4.3 shows a typical computer network.

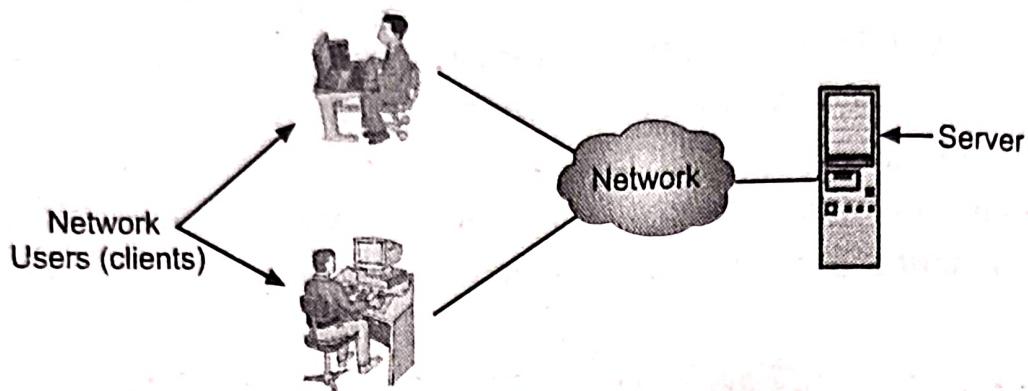


Fig. 4.3: Typical Computer Network

4.1.3 Advantages, Disadvantages and Applications of Network

- The ability to exchange data and communicate efficiently is the main purpose of networking computers.

Advantages of Computer Network:

- Easy Communication:** A computer network allows all the network users or computers at a different location to communicate easily. The network users can communicate with each other using e-mails, instant messaging, video conferencing, chat rooms, blogging etc.
- Ability to Share Files, Data and Information:** The computer network has the ability to share data/files and information to users or computers connected to the computer network.
- Flexible Access:** Access of files from computers throughout the world, and 24×7 environment.
- Backup and Recovery:** Generally, in networking the server is placed in a secure place and the good mechanism is providing for backup of data. If the data is lost accidentally or due to any other reason, then it is possible to restore them from the server.
- Sharing Hardware:** By using networking we can share the hardware resources in an organization and anywhere. For an example, a printer can be shared among the users in a network so that there's no need to have individual printers for each and every computer in the organization. This will significantly reduce the cost of purchasing hardware.
- Instant and Multiple Accesses:** Computer networking enables multiple users to access the same data at the same time from a same or remote location. For example, a World Wide Web (WWW) in which everyone can access a web page from a different location and read the same information at a same time.

7. **Sharing Software:** Users can share software within the network easily. Networkable versions of software are available at considerable savings compared to individually licensed versions of the same software. Therefore, large organizations can reduce the cost of buying software by networking their computers.
8. **Security:** Network security issues consist of prevention from virus attacks and protecting data from unauthorized access. Sensitive files and programs on a network can be password protected. Only authorized users can access resources in a computer network.
9. **Speed:** Sharing and transferring files within networks is very rapid (fast), depending on the type of network. This will save time while maintaining the integrity of files.

Disadvantages of Computer Network:

1. **Expensive to Build:** Building a network is complex and time consuming for large scale organizations.
2. **Virus and Malware:** Viruses can spread on a network easily, because of the inter-connectivity of workstations.
3. **Lack of Robustness:** If the main file server of a computer network breaks down, the entire system becomes down and useless.
4. **Needs an Efficient Handler:** The technical skills and knowledge required to operate and administer a computer network.
5. **High Cost:** The investment for hardware and software can be costly for initial set-up of computer networks.
6. **Security Threats:** Security threats are always problems with computer networks. There are hackers who are trying to steal valuable data/information of large organizations for their own benefit.

Applications of Computer Network:

1. **Marketing and Sales:** Computer networks are used extensively in both marketing and sales organizations. Marketing professionals use them to collect, exchange, and analyze data related to customer needs and product development cycles. Sales application includes teleshopping, which uses order-entry computers or telephones connected to order processing networks, and online-reservation services for hotels, airlines and so on.
2. **Financial Services:** Today's financial services are totally dependent on computer networks. Application includes credit history searches, foreign exchange and

investment services, and electronic fund transfer, which allow users to transfer money without going into a bank (an Automated Teller Machine (ATM) is an example of electronic fund transfer automatic pay-check is another).

3. **Manufacturing:** Computer networks are used in many aspects of manufacturing including the manufacturing process itself. Two of them that use networks to provide essential services are Computer-Aided Design (CAD) and Computer-Assisted Manufacturing (CAM), both of which allow multiple users to work on a project simultaneously.
4. **Directory Services:** Directory services allow lists of files to be stored in a central location to speed worldwide search operations.
5. **Information Services:** A Network information services includes bulletin boards and data banks. A World Wide Web (WWW) site offering technical specification for a new product is an information service.
6. **Electronic Data Interchange (EDI):** EDI allows business information, including documents such as purchase orders and invoices, to be transferred without using paper.
7. **Electronic Mail:** Probably it's the most widely used computer network application.
8. **Teleconferencing:** Teleconferencing allows conferences to occur without the participants being in the same place. Applications include simple text conferencing (where participants communicate through their normal keyboards and monitor) and video conferencing where participants can even see as well as talk to other fellow participants.
9. **E-Commerce:** Computer networks have paved the way for a variety of business and commercial transactions online, popularly called e-commerce. Users and organizations can pool funds, buy or sell items, pay bills, manage bank accounts, pay taxes, transfer funds and handle investments electronically.

4.2 NETWORK TERMINOLOGIES

- Following are the common terminologies are used in networking:
 1. **Node:** A node is the basic building blocks in computer networking. Any device connected to a network, such as a computer, printer, hub or router is called as node.
 2. **Link:** The links are also the basic building blocks in computer networking. A link refers to the transmission media connecting two nodes. Links may be physical, like cable wires or optical fibers, or free space used by wireless networks.
 3. **Host:** A host is a computer or other device that communicates with other hosts on a network. Also known as network hosts, hosts include clients and servers that send or receive data, services and applications.

4. **Network:** A collection of interconnected devices, such as computers, printers and servers, that can communicate with each other.
5. **Protocol:** A protocol is a set of rules and standards that define a language that devices can use to communicate. In networking, the protocol is a set of rules for transmitting data.
6. **Workstation:** It is a high-performance computer system that is basically designed for a single user. A workstation refers to an individual computer, or group of computers, used by a single user to perform work or task.
7. **Internet:** It is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices. It is a network of networks that consists of private, public, academic, business and government networks of local to global scope, linked by a broad array of electronic, wireless and optical networking technologies.
8. **LAN:** LAN stands for Local Area Network. Generally, a LAN network is a combination of two or more connected computers, and a LAN is a type of network that allows the connection of devices within a small geographic area, usually within the same building.
9. **WAN:** WAN stands for Wide Area Network. WAN covers large geographical areas such as states, countries, continents, etc.
10. **Transmission Media:** Transmission media are the channels/paths through which data is transferred from one device to another in a network. The physical path over which the information flows from transmitter to receiver is called the transmission medium/media. The two types of transmission media in networking are guided and unguided transmission media. Guided media is also known as bound media or wired media. Guided transmission media uses a cabling system (coaxial cable, twisted-pair wire, and optical fiber cable) that guides the data signals along a specific path. Unguided media also known as unbounded or wireless media. Unguided media type of communication is often referred to as wireless communication. It uses electromagnetic signals to send data. The signal propagates in the form of electromagnetic waves (like micro waves, radio waves, infrared waves and so on).
11. **World Wide Web (WWW):** The WWW also known as the Web, is a collection of web pages or websites. WWW is the service used on the Internet that allows to retrieval and display of contents such as images, text, audio, video, etc.
12. **Bandwidth:** Network bandwidth can be defined as the maximum capacity of data that can be transmitted over an internet connection at any given amount of time, usually measured in bits per second (bps).
13. **Network Interoperability:** Network Interoperability is the continuous ability to send and receive data among the interconnected networks, providing the quality level expected by the end user without any negative impact to the sending and receiving networks.

14. Network Administrator: A network administrator is an IT expert/professional who manages an organization's network. Network administrators are responsible for maintaining and troubleshooting computer networks to enhance the network's security policies and meet organizational requirements. Some role of network administrators includes:

- A network administrator is responsible for installing, configuring, and maintaining an organization's network infrastructure.
- It includes ensuring that the network is up and running properly and secure from outside threats.
- They must deeply understand network protocols and architecture to effectively manage the network.
- They must be able to troubleshoot network problems and have the skills to resolve them quickly.

15. Network Security: Network security is an essential and critical parameter in the increasingly connected (networked) world. Network security employs various techniques to ensure a network is secure. For example, it uses multiple tools such as firewalls, intrusion detection or prevention systems, and anti-malware software to prevent or detect malicious activity in the network.

Firewalls put up a barrier between our trusted internal network and untrusted outside networks, such as the Internet. They use a set of defined rules to allow or block traffic. Firewalls control incoming and outgoing traffic on networks, with predetermined security rules. A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies or rules.

Email security refers to any processes, products, and services designed to protect our email accounts and email content safe from external threats.

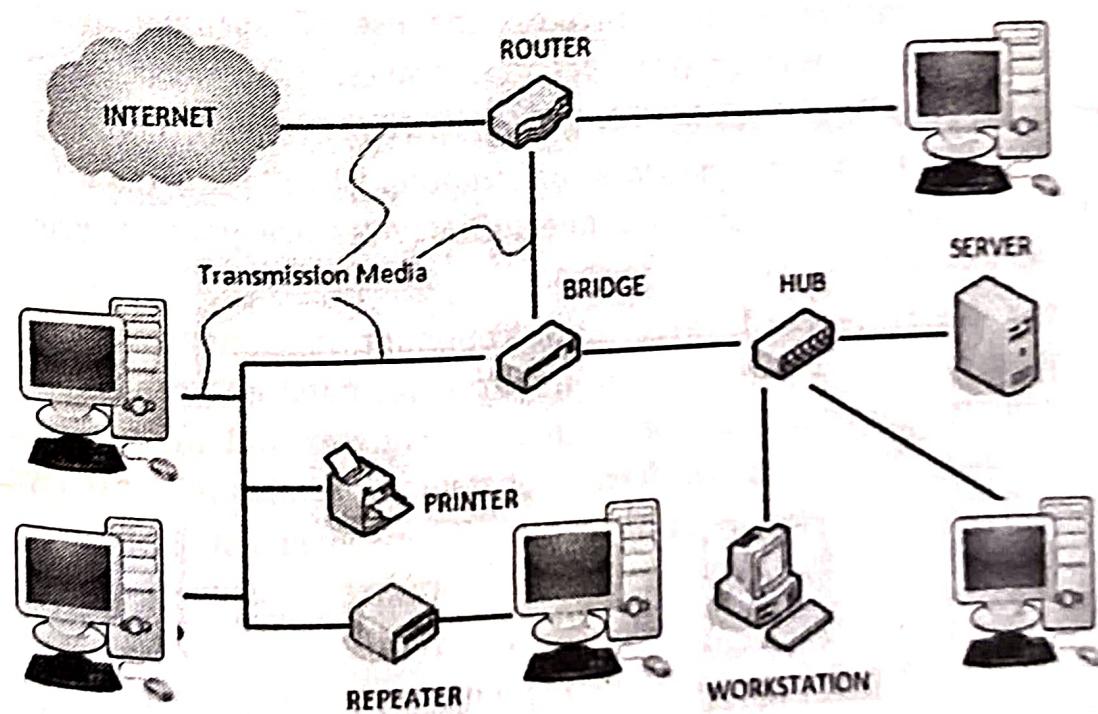
Prevention against Network Attacks:

- **Install Antivirus Softwares:** One of the first lines of defense against malware and other viruses is to install antivirus software on all devices connected to a network. Antivirus software can detect and prevent malicious files from being installed on a system, and it should be updated regularly to include the latest updations.
- **Access Control (Create Strong Passwords):** Access control defines the people or groups and the devices that have access to network applications and systems thereby denying unsanctioned access, and maybe threats. To protecting a network, create strong passwords means the passwords should be at least eight characters long and include a mix of letters, numbers, and symbols. They should also not be easy to guess - for instance, the user's name.

- **Enforce Security Policies:** To reduce risk of attacks on a network is to enforce security policies. Security policies can help ensure that all devices on a network are protected against viruses and malware and that users are using strong passwords. These policies can also restrict access to some network regions and limit user privileges.
- **Use Firewalls:** Firewalls are another essential tool in defending networks against security threats. A firewall can help prevent unauthorized access to a network by blocking incoming traffic from untrusted sources. Additionally, firewalls can be configured to allow only certain types of traffic, such as web traffic or email.
- **Monitor Network Activity:** Finally, it's important to monitor activity on the network. Tracking logs and other data enables suspicious activity to be identified quickly, allowing security personnel to take steps to investigate and mitigate potential threats.

4.3**NETWORK COMPONENTS**

- A network component is a component that is needed to install computer networks that include both physical and software parts.
- Computer networks components comprise both physical parts as well as the software required for installing computer networks.
- The hardware components are the server, client, peer, transmission medium, and connecting devices. The software components are operating system and protocols.
- The Fig. 4.4 shows a network along with its components.

**Fig. 4.4: Network Components**

- The network components in Fig. 4.4 are explained below:
 - Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network.
 - There are many different kinds of servers, and one server can provide several functions. For example, there are file servers, print servers, mail servers, communication servers, database servers, fax servers and web servers, to name a few.
 - Sometimes it is also called host computer, servers are powerful computer that store data or application and connect to resources that are shared by the user of a network.
- 2. **Clients:**
 - Clients are computers that access and use the network and shared network resources.
 - Client computers are basically the customers (users) of the network, as they request and receive services from the servers.
 - These days, it is typical for a client to be a personal computer that the users also use for their own non-network applications.
- 3. **Transmission Media:**
 - Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fiber cable.
 - Wireless transmission medium involves the use of unguided media such as infrared waves, electromagnetic waves, radio waves, microwaves.
- 4. **Network Connecting Devices (Network Hardware Parts):** Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are Routers, Bridges, Hubs, Repeaters, Gateways, Switches and so on.
- 5. **Network Interface Card (NIC):** Each computer in a network has a special expansion card called a NIC which prepares (formats) and sends data, receives data, and controls data flow between the computer and the network. On the transmit side, the NIC passes frames of data on to the physical layer, which transmits the data to the physical link. On the receiver's side, the NIC processes bits received from the physical layer and processes the message based on its contents.
- 6. **Hub:** A hub is a network device that links multiple computers and devices together. Hubs can also be referred to as repeaters or concentrators, and they serve as the center of a LAN.

In a hub, each connected device is on the same subnet and receives all data sent to the hub. The hub then forwards that data out to all other connected devices, creating an efficient system for sharing data between users. Hub networks are a type of computer network that connects multiple devices or nodes in order to share resources, information, and services. A hub network is composed of one or more hubs (central connection points) and all other connected devices. Each device on the network is connected directly to the hub, which acts as a central point for data transmission. Data is sent from one device to another via the hub and can be exchanged between any two devices connected to the hub. There are mainly three types of hub in computer network

- **Passive Hub:** A passive hub is a basic hub that simply provides a physical connection between multiple devices.
 - **Active Hub:** An active hub, also known as a powered hub, is a hub that requires an external power source to operate. It contains active electronic components that amplify and regenerate signals, which allows it to extend the distance over which devices can communicate with each other.
 - **Intelligent Hub:** An intelligent hub is a type of hub that includes additional features such as network management capabilities, error detection, and troubleshooting tools.
7. **Switch:** Switch is like a Hub but built in with advanced features. It uses physical device addresses in each incoming message so that it can deliver the message to the right destination or port. Switches manage the flow of data across a network by transmitting a received network packet only to the one or more devices for which the packet is intended.
 8. **Router:** A router is a networking device that routes data packets between computer networks. A router can connect networked computers to the Internet, so multiple users can share a connection. A router works as a dispatcher. It directs data traffic, choosing the best route for information to travel across the network.
 9. **Modem:** The word Modem stands for "Modulator Demodulator." The main task of this device is to convert analog signals into digital signals. Computer process all data in the form of 0s and 1s, but while browsing the Internet or transmitting data from a sender to a receiver, digital data need to be converted into analog data. The medium carries the signal to the receiver. These modems are connected to the receiver and sender nodes - the modems at the sender end act as modulators that convert digital signals into analog signals. The modem at the receiver ends acts as a demodulator that converts analog signals to digital signals.
 10. **Repeater:** Over the cable, data is transmitted in the form of signals. These signals have a limited range (typically around 100 meters). Signals lose their strength and

become weak once they reach this limit. Original signals must be regenerated in such circumstances. A repeater is an analog device that uses signals from the cables linked. A repeater regenerates and re-transmits the attenuated signal that appears on the cable.

11. **Bridge:** The network devices that can connect more than two LANs to form a single more extensive network are known as bridges. The process of collecting LANs with the help of multiple components is known as bridging the network.
12. **Gateway:** A gateway in networking is a hardware device or software program that serves as a bridge between two different networks, allowing data to flow from one to the other. It acts as a "gate" between networks, and it may be used to connect a local network to the internet or to link a local network to another local network (often of a different type). In simpler terms, a gateway in networking is a network node that acts as an entry point to another network.

Network Software Components:

1. **Network Operating System (NOS):** Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc. The network operating system is a program that runs on computers and servers that allows the computers to communicate over the network.
2. **Protocol Suite:** A protocol is a rule or guideline followed by each computer for data communication. Protocol suite is a set of related protocols that are laid down for computer networks. The two popular protocol suites are OSI Model (Open System Interconnections) and TCP / IP Model.
3. **Local Operating System:** A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer. Examples are MS-DOS, Unix, Linux, Windows 2000, Windows 98, Windows XP etc. The network operating system is the software of the network. It serves a similar purpose that the OS serves in a stand-alone computer.

4.4 TYPES OF NETWORKS

- The two major types of networks are peer-to-peer (P2P) and client-server.
 - In P2P networks, computers with similar capabilities and configurations are referred to peers. The peers in the P2P networks are computer systems that are connected to each other over the Internet. Without the use of a central server files can be shared directly between systems on the network.
 - In client-server networks each computer or process on the network is either a client or a server. The client asks for services (requests) from the server, which the server provides (responses).

4.1 Peer-to-Peer (P2P) Network

A Peer-to-Peer (P2P) network is a decentralized network architecture in which individual devices, called "peers," interact and collaborate directly with each other to share resources, information, or services without the need for a central server.

In a peer-to-peer network, all the computers in the network are connected to one another and share resources such as files, applications, and programs.

In a peer-to-peer network, each computer can function as either a client or a server, enabling it to request or provide services.

In peer-to-peer network each computer is responsible for making its own resources available to other computers on the network.

Fig. 4.5 shows the structure of peer-to-peer network.

Peer-to-peer network is useful for a small network containing less than 8-10 computers on a single LAN.

Advantages of Peer-to-Peer Networks:

1. No dedicated server required.
2. Less expensive and easy to setup.
3. Easy to install and maintain.
4. New clients can be effortlessly added, enhancing the network's flexibility and scalability.
5. Easy setup and lower cost for small network.
6. Due to their decentralized nature, P2P networks can recover from failures more gracefully.
7. Cost effective because no extra investment in server software or hardware is required.

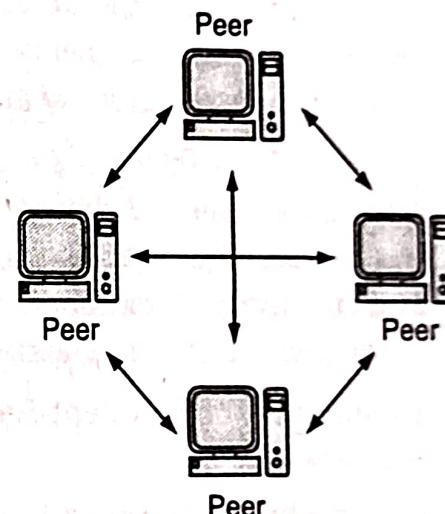


Fig. 4.5: Peer-to-peer (P2P) Network

Disadvantages of Peer-to-Peer Networks:

1. Slow in speed.
2. P2P networks lack central authority, making it challenging to manage and coordinate network activities.
3. Not good for database applications.
4. Less reliable (server is workstation).
5. Limited expandability.
6. Hard to backup.
7. Not very secure because open nature of P2P networks can expose them to security risks, including unauthorized access, data breaches, and malware distribution.

4.4.2 Client-Server Network

- Client-server networks are also called as Server-based network. In this network, a centralized powerful host computer known as server and a user's individual workstation known as client.
- In a server-based network, the server is the central location where users share and access network resources, (See Fig. 4.6).
- This dedicated computer controls the level of access that users have to share resources. Each computer that connects to the network is called a client computer.
- The client requests for services (file sharing, resource sharing etc.) from the server and the server responds by providing that service.
- The servers provide access to resources, while the clients have access to the resources available only on the servers.
- A typical example of client-server architecture is accessing a website (server) from home with the help of a browser (client).
- Advantages of a Client-Server Network:**

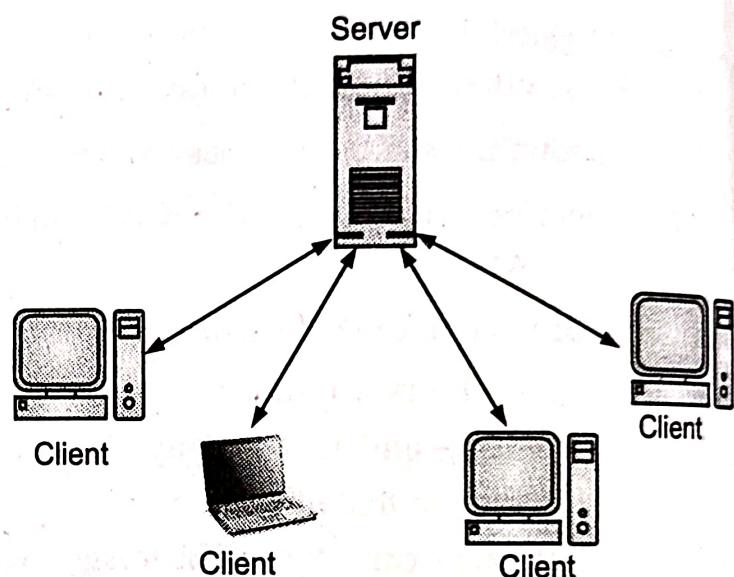


Fig. 4.6: Client-server Architecture

- Scalability:** Any or all elements can be replaced individually as needs increase.
- Flexibility:** New technology can be easily integrated into system.
- Interoperability:** All components (client/network/server) work together.
- Accessibility:** Server can be accessed remotely and across multiple platforms.
- Fast:** Faster than P2P networks.
- Improved Data Sharing:** Data is retained by usual business processes and manipulated on a server is available for designated users (clients) over an authorized access.
- Security:** Servers have better control access and resources to ensure that only authorized clients can access or manipulate data and server updates are administered effectively.
- Centralized Management:** Streamlined server management allows IT teams to update data files centrally, enhancing accessibility for users. Monitoring data from a single server enables the anticipation of potential problems.

9. Seamless Feature Integration: New features can be seamlessly added to a server without disrupting the normal operations of other devices within the network.

Disadvantages of a Client-server Network:

1. **Expensive and High Cost:** Central servers can be expensive to purchase and maintain, contributing to a high overall setup cost for a client-server network.
2. **Maintenance:** Large networks will require a staff to ensure efficient operation.
3. **Dependence:** When server goes down, operations will cease across the network.
4. **Overloaded Servers:** When there are frequent simultaneous client requests, server severely get overloaded, forming traffic congestion.
5. **Impact of Centralized Architecture:** Since it is centralized, if a critical server failed, client requests are not accomplished. Therefore, client-server lacks the robustness of a good network.
6. **Limited Size:** The limit of the number of nodes that can function as both clients and servers on a P2P is between 10 and 25.

Peer-to-peer Network versus Client-server Network:

Sr. No.	Peer-to-Peer (P2P) Network	Client-server Network
1.	In peer-to-peer network each node acts as both a client and server. Every node in a peer-to-peer network has the ability to request and provide service.	In client-server network, the clients request a resource and the server provides/responds that resource.
2.	Low cost.	The cost to set up a client-server network is high.
3.	Decentralized form of networking architecture.	Centralized form of networking architecture.
4.	In peer-to-peer network, peers act as both service providers and service consumers at the same time (data flows within peers).	In a client-server network, the designated clients request for services, and the servers provide them (data flows from server to client).
5.	In a peer-to-peer network, the peers (users) are free to create network share points on their computers. As there is no central security, there is no control over who shares what in the network.	In a client-server network, the server contains central security such as a list of user names and passwords for authenticating the clients.

contd. ...

6.	A peer-to-peer network has no dedicated servers. All the workstations are considered as equal. Any one computer can act as client or server at any instance.	Dedicated server (PDC called As Primary Domain Controller) is required in client-server networks.
7.	In a peer-to-peer network, access to the network is not centrally controlled.	In client-server network, access and security are centrally controlled.
8.	A peer-to-peer architecture can operate on a basic PC operating system, (Windows XP, Windows 98).	A client-server architecture, need a special operating system (SBS 2008).
9.	Are generally simpler and less expensive.	Are generally more complex but give the user more control and more expensive.
10.	Client-Server architecture is more reliable and scalable.	The performance of peer-to-peer networks degrades when the number of peers in the system grows.
11.	Poor performance for large number of users.	Better performance for large number of users.

PRACTICE QUESTIONS

Q.I Multiple Choice Questions:

- Which is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices?
 - Internet
 - Intranet
 - Extranet
 - All of the mentioned
- What is a computer network?
 - An OS used to share information between computers.
 - A collection of interconnected computers and devices that can communicate and share resources.
 - A type of software used to create and share documents and presentations.
 - All of the mentioned
- A computer network spanned inside a building and operated under single administrative system is generally termed as,
 - Wide Area Network (LAN)
 - Metropolitan Area Network (MAN)
 - Local Area Network (LAN)
 - All of the mentioned

4. What is the primary purpose of a firewall in network security?
- Firewalls control incoming and outgoing traffic on networks
 - Speed up Internet connection
 - Monitor user activity
 - All of the mentioned
5. Which is the IT professional/expert responsible for maintaining and troubleshooting computer networks to enhance the network's security policies and meet organizational requirements?
- Database Administrator
 - Network Administrator
 - System Administrator
 - None of the mentioned
6. Which is the connection point among network devices such as routers, printers, or switches that can receive and send data from one endpoint to the other?
- hub
 - NIC
 - modem
 - node
7. Which ensures that any malicious software does not enter the network and jeopardize the security of the data?
- Antivirus Software
 - Anti-malware Software
 - Both (a) and (b)
 - None of the mentioned
8. Which are computers that request and receive service from the servers to access and use the network resources?
- servers
 - clients
 - nodes
 - All of the mentioned
9. Guided transmission media include,
- coaxial cable
 - fiber optic cable
 - twisted-pair cable
 - All of the mentioned
10. In which network individual nodes in the network (called "peers") act as both senders and receivers of resources?
- client-server
 - remote
 - peer-to-peer (P2P)
 - All of the mentioned

Answers

1. (a)	2. (b)	3. (c)	4. (a)	5. (b)	6. (d)	7. (c)	8. (b)	9. (d)	10. (c)
--------	--------	--------	--------	--------	--------	--------	--------	--------	---------

Fill in the Blanks:

1. The _____ is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless and optical networking technologies.

2. A system of interconnected computers and computerized peripherals such as printers is called computer _____.
3. A network of networks is called an _____, (or internet).
4. A _____ is a node that participates in user applications, either as a server, client, or both.
5. A client-server network is a _____ network where one or more devices provide services and resources to other devices, or clients.
6. Security _____ such as firewalls, encryption and user authentication are essential to protect network resources and data.
7. Network _____ is a measure of the data transfer rate or capacity of a given network.
8. Computer networks are vulnerable to security _____ such as unauthorized access, hacking, viruses, and data breaches.
9. _____ are high-configuration computers that manage the resources of the network.
10. The network is used to exchange, store, send, and retrieve data between network devices, also known as network _____.
11. Transmission medium/media is the physical _____ between sender and receiver in a data transmission system.

Answers

1. internet	2. network	3. internetwork	4. host
5. centralized	6. measures	7. bandwidth	8. threats
9. Servers	10. nodes	11. path	

Q.III State True or False:

1. Internet (or internetwork) is a world-wide global system of interconnected computer networks.
2. In P2P network, each and every node can do both request and respond for the services.
3. A network administrator or network admin is responsible to manage, monitor, maintain, secure and service a computer network.
4. Intrusion Detection Systems (IDSs) analyze network traffic for suspicious activities or patterns that may indicate a potential breach.
5. A host is a computer or other device that communicates with other hosts on a network.
6. In a client-server network, the client requests services from the server.

- Fundamentals of Computers**
7. Computer networks are a system of interconnected computers and other devices that allow for the sharing of information and resources.
 8. Firewalls act as a barrier between internal and external networks, monitoring and filtering incoming and outgoing traffic.
 9. Transmission media wireless such as coaxial cable, twisted-pair wire, and optical fiber cable, are carriers used to link computers together in a network.
 10. Security policies can help ensure that all devices on a network are protected against viruses and malware and that users are using strong passwords.
 11. Transmission media may be guided media like coaxial cable, fiber optic cables etc. or maybe unguided media like radio waves, microwaves, infra-red waves etc.
 12. A network node is a connection point in a computer network, which sits at a point in the network where it sends, receives, stores information.

Answers

1. (T)	2. (T)	3. (T)	4. (T)	5. (T)	6. (T)	7. (T)	8. (T)	9. (F)	10. (T)
11. (T)	12. (T)								

Q.IV Answer the following Questions:

(A) Short Answer Questions:

1. Define computer network.
2. Define internetwork.
3. What is the purpose of internetwork?
4. Define the term client and server.
5. Define network security.
6. List types of servers.
7. Define P2P network.
8. What is the purpose of router?
9. What is the function of firewall in network security.
10. What is the purpose of hub?
11. Define the term client.
12. What is NIC?
13. What is the purpose of IDS?
14. Define bandwidth.
15. What is interoperability?

(B) Long Answer Questions:

1. What is internetwork? State its advantages and disadvantages.
2. What is computer network? How it works? Explain diagrammatically.
3. What are nodes and hosts? Compare them, (any four points).
4. What is transmission media? List its types with examples.
5. What is meant by network security? List network security measures.
6. What is firewall? How it works? Explain in detail.
7. What is router? Give its functions.
8. What is bridge? Describe in detail.
9. What is switch? How to use it in network.
10. With the help of diagram describe P2P network. Also, state its advantages and disadvantages.
11. With the help of diagram describe client-server network. Also, state its advantages and disadvantages.
12. Differentiate between P2P network and client-server network.