

**MAA OMWATI DEGREE COLLEGE
HASSANPUR**

NOTES

**SUBJECT: - Computer Networking & Internet
BBA 5th SEMESTER**

Prepared By:-

NARENDER KUMAR

Syllabus Covered as: - M.D University, Rohtak

INDEX

Content

Page No.

1. Introduction to network -	1-10
2. Network Topology	10-12
3. Analog & Digital signals and transmission	12-15
4. Networking devices	16-18
5. OSI model and TCP/IP model	19-24
6. Protocols and their classifications	25-31
7. Flow control and cryptography	32-33
8. Routing	34-35(iii)
9. Overview of Internet, ISP	36(i)-38
10. Newsgroup	39-42
11. Setting window environment for dialup	43-44
12. Search engine	45
13. Audio on Internet	46
14. Intranet & building corporate world wide web	46-48
15. Intranet as business tools, future of Intranet , Security	48-50
16. Fundamental of TCP/IP	51
17. Protocols of communication	52

External Marks: 50
Practical Marks: 50
Time: 3 hrs.

COMPUTER NETWORK AND INTERNET

PAPER CODE: BBA-504

UNIT-I

Introduction to network, advantages and disadvantages of network, network topologies, analog and digital signal, analog and digital transmission

UNIT-II

OSI model and TCP/IP model, protocols and their classification, flow control and cryptography, ranking

UNIT-III

Overview of internet, internet service provider, setting windows environment for dial up networking, search engine, searching web using search engine, audio on internet, newsgroup, subscribing to news groups

UNIT-IV

Intranet concepts and architecture, building corporate world wide web, HTTP protocol, intranet infrastructure, fundamental of TCP/IP, intranet security design, intranet as a business tools, future of intranet, protocols of communication

Lab: HTML and Surfing with Internet

SUGGESTED READINGS:

1. Forouzan , Data Communication & Networking, TMH, N.Delhi.
2. Miller, Data and Network Communication, Vikas Publishing House, New Delhi.
3. Shay, Understanding Data Communication and Networks, Thomson Learning, Vikas Publishing House, New Delhi.
4. Tannenbaum, Computer Networks, PHI, N.Delhi.
5. Uyless Black, Computer Networks, PHI, N.Delhi.

Note:

1. **Instructions for External Examiner:** The question paper shall be divided in two sections. **Section 'A'** shall comprise of five short answer type questions from whole of the syllabus carrying two marks each, which shall be compulsory. Answer to each question should not exceed 50 words normally.
2. **Section 'B'** shall comprise 8 questions (2 questions from each unit). The students will be required to attempt four questions selecting one question from each unit.
3. All questions will carry equal marks.

A computer network, or simply a **network**, is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information.^[1] Where at least one process in one device is able to send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network. Simply, more than one computer interconnected through a communication medium for information interchange is called a computer network.

Networks may be classified according to a wide variety of characteristics, such as the medium used to transport the data, communications protocol used, scale, topology, and organizational scope.

Communications protocols -define the rules and data formats for exchanging information in a computer network, and provide the basis for network programming

Properties

Computer networks:

Facilitate communications

Using a network, people can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing.

Permit sharing of files, data, and other types of information

In a network environment, authorized users may access data and information stored on other computers on the network. The capability of providing access to data and information on shared storage devices is an important feature of many networks.

Share network and computing resources

In a networked environment, each computer on a network may access and use resources provided by devices on the network, such as printing a document on a shared network printer. Distributed computing uses computing resources across a network to accomplish tasks.

May be insecure

A computer network may be used by computer hackers to deploy computer viruses or computer worms on devices connected to the network, or to prevent these devices from normally accessing the network (denial of service).

May interfere with other technologies

Power line communication strongly disturbs certain forms of radio communication, e.g., amateur radio.^[5] It may also interfere with last mile access technologies such as ADSL and VDSL.^[6]

May be difficult to set up

A complex computer network may be difficult to set up. It may also be very costly to set up an effective computer network in a large organization or company.

(N/W-T)

Scale:- Networks are often classified by their physical or organizational extent or their purpose. Usage, trust level, and access rights differ between these types of networks.

* Network Connections: →

There are two types of connection.

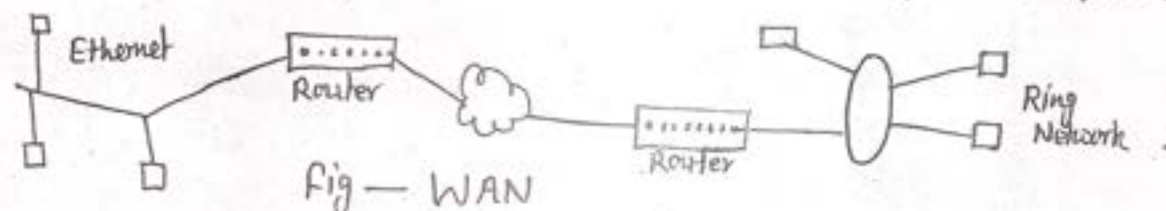
(i) Physical Connection: — The physical connection allow the computers to directly transmit and receive signals from other computers. Physical connections are defined by the medium used to carry the signal, the geometric arrangement of computers i.e. topology of network and method used to share information.

(ii) Logical Connections: — The logical or virtual connections allow the computer applications like word processors, databases to exchange information with other computers.

(N/W-2)

Q. What is WAN ? Explain its types ?

Ans - Wide Area Network connect larger geographic areas such as India or world. A WAN may be defined as data communications networks that covers a relatively broad geographic area to connect LAN's together bet. different cities with the help of transmission facilities provided by common carriers such as telephone companies.



• Types: →

1. Public Network: → These are the networks that are installed and run by the telecommunication authorities and are made available to any orgn. or individual who go in for their subscription.

2. Private Networks: → The basic technique used in all forms of private WAN is to use private circuits to link the locations to be served by the networks.

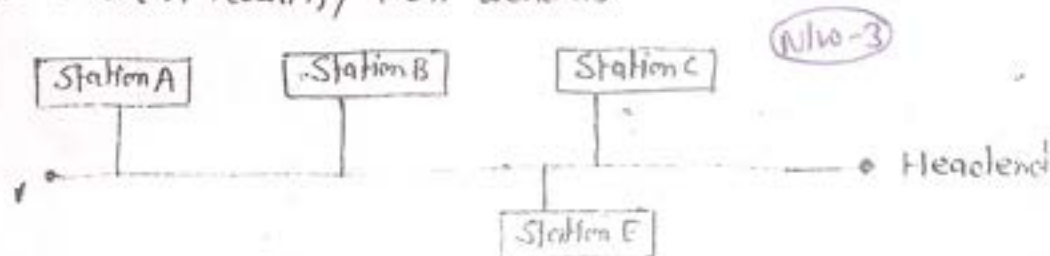
*** Network Topology: →

Topology is physical arrangement for connecting computers. Selection of topology is based on following:-

- 1) Flexible to accommodate.
- 2) Minimum cost of physical media.
- 3) Cable type.

** Types of Topology: →

(1) Bus Topology: → In bus topology, single transmission medium interconnects all the stations. All stations share this medium for transmission to any other station. Every station listen to all the transmission on the bus. Every transmission has source and destination address so that stations can pick the message meant for them & identify their senders.



Bus topology

Q. What is LAN? What are important characteristics of LAN.
Name at least three technologies.

Ans — A LAN is a data communication networks, which connects many computer or workstations and permits exchange of data and info. among them, within localized area, typically confined to a building or a cluster of buildings. The distance between two communication points connection is usually upto 02-05 kilometers.

Characteristics: →

1. Area covered is small.
2. Each device connected in the network can either operate stand-alone or in the network.
3. Data transfer rates are high, usually 1 mbps - 100 mbps
4. Each device connected in the network can communicate with any other device in the network.
5. Cost of setting up network is usually low.

The main LAN technologies are: — Ethernet, Token Ring and ARCNET.

Advantages of LAN: →

1. LAN is a productivity tool.
2. LAN allow for high-speed exchange of essential info. bet. key people in an organisation.
3. LAN allow sharing of expensive resources such as laser printers and high capacity, high speed mass storage devices among no. of users.

Limitation: →

1. This reduces the memory space available for user's programs.
2. The financial cost of LAN is still high.

Q. What is MAN?

Ans — A metropolitan Area Network covers larger geographic areas such as cities or districts. By interconnecting smaller networks within a large geographic area, info. is easily spread throughout the network. Local libraries and government agencies often use a MAN to connect to cities and private industries. The geographical limit of a MAN covers a city.



Fig - MAN

Personal area network

A personal area network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and even video game consoles. A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters.^[11] A wired PAN is usually constructed with USB and Firewire connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.

Local area network

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Current wired LANs are most likely to be based on Ethernet technology, although new standards like ITU-T G.hn also provide a way to create a wired LAN using existing home wires (coaxial cables, phone lines and power lines).^[12]

5

Home area network

A home area network (HAN) is a residential LAN which is used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a cable TV or Digital Subscriber Line (DSL) provider.

Storage area network

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network by other devices.

N/w-5

Campus area network

A campus area network (CAN) is a computer network made up of an interconnection of LANs within a limited geographical area. The networking equipment (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling etc.) are almost entirely owned (by the campus tenant / owner: an enterprise, university, government etc.).

In the case of a university campus-based campus network, the network is likely to link a variety of campus buildings including, for example, academic colleges or departments, the university library, and student residence halls.

Backbone network

A backbone network is part of a computer network infrastructure that interconnects various pieces of network, providing a path for the exchange of information between different LANs or subnetworks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Normally, the backbone's capacity is greater than that of the networks connected to it.

A specific case of a backbone network is the Internet backbone, which is the set of wide-area network connections and core routers that interconnect all networks connected to the Internet.

Metropolitan area network

A Metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.

Wide area network

A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances, using a communications channel that combines many types of media such as telephone lines, cables, and air waves. A WAN often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

Enterprise private network

An enterprise private network is a network built by an enterprise to interconnect various company sites, e.g., production sites, head offices, remote offices, shops, in order to share computer resources.

Virtual private network

N/W-6

A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features. VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point.

Virtual Network

Virtual Network defines data traffic flows between virtual machines within a hypervisor in a virtual computing environment. Virtual Networks may employ virtual security switches, virtual routers, virtual firewalls and other virtual networking devices to direct and secure data traffic.

Internetwork

An internetwork is the connection of multiple computer networks via a common routing technology using routers. The Internet is an aggregation of many connected internetworks spanning the Earth.

Organizational scope

Networks are typically managed by organizations which own them. According to the owner's point of view, networks are seen as intranets or extranets. A special case of network is the Internet, which has no single owner but a distinct status when seen by an organizational entity – that of permitting virtually unlimited global connectivity for a great multitude of purposes.

Intranets and extranets

Intranets and extranets are parts or extensions of a computer network, usually a LAN.

An intranet is a set of networks, using the Internet Protocol and IP-based tools such as web browsers and file transfer applications, that is under the control of a single administrative entity. That administrative entity closes the intranet to all but specific, authorized users. Most commonly, an intranet is the internal network of an organization. A large intranet will typically have at least one web server to provide users with organizational information.

An extranet is a network that is limited in scope to a single organization or entity and also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities—a company's customers may be given access to some part of its intranet—while at the same time the customers may not be considered *trusted* from a security standpoint. Technically, an extranet may also be categorized as a CAN, MAN, WAN, or other type of network, although an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

Internet

N/w-7

The Internet is a global system of interconnected governmental, academic, corporate, public, and private computer networks. It is based on the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the United States Department of Defense. The Internet is also the communications backbone underlying the World Wide Web (WWW).

Advantages of Computer Networks

- **File Sharing:** The major advantage of a computer network is that it allows file sharing and remote file access. A person sitting at one workstation of a network can easily see the files present on the other workstation, provided he is authorized to do so. It saves the time which is wasted in copying a file from one system to another, by using a storage device. In addition to that, many people can access or update the information stored in a database, making it up-to-date and accurate.
- **Resource Sharing:** Resource sharing is also an important benefit of a computer network. For example, if there are four people in a family, each having their own computer, they will require four modems (for the Internet connection) and four printers, if they want to use the resources at the same time. A computer network, on the other hand, provides a cheaper alternative by the provision of resource sharing. In this way, all the four computers can be interconnected, using a network, and just one modem and printer can efficiently provide the services to all four members. The facility of shared folders can also be availed by family members.
- **Increased Storage Capacity:** As there is more than one computer on a network which can easily share files, the issue of storage capacity gets resolved to a great extent. A standalone computer might fall short of storage memory, but when many computers are on a network, memory of different computers can be used in such case. One can also design a storage server on the network in order to have a huge storage capacity.
- **Increased Cost Efficiency:** There are many software available in the market which are costly and take time for installation. Computer networks resolve this issue as the software can be stored or installed on a system or a server and can be used by the different workstations.

Disadvantages of Computer Networks

N/W-8

- **Security Issues:** One of the major drawbacks of computer networks is the security issues involved. If a computer is a standalone, physical access becomes necessary for any kind of data theft. However, if a computer is on a network, a computer hacker can get unauthorized access by using different tools. In case of big organizations, various network security software are used to prevent the theft of any confidential and classified data.
- **Rapid Spread of Computer Viruses:** If any computer system in a network gets affected by computer virus, there is a possible threat of other systems getting affected too. Viruses get spread on a network easily because of the interconnectivity of workstations. Such spread can be dangerous if the computers have important database which can get corrupted by the virus.
- **Expensive Set Up:** The initial set up cost of a computer network can be high depending on the number of computers to be connected. Costly devices like routers, switches, hubs, etc., can add up to the bills of a person trying to install a computer network. He will also have to buy NICs (Network Interface Cards) for each of the workstations, in case they are not inbuilt.
- **Dependency on the Main File Server:** In case the main File Server of a computer network breaks down, the system becomes useless. In case of big networks, the File Server should be a powerful computer, which often makes it expensive.

* Network :→

A computer network is a group of computers, printers and other devices (nodes) that are connected with each other for purpose of communication. Networking can be made through the media of copper wire, fibre optics or radio waves. Network can be small or large, permanent or temporary. A network is a means of transmitting and receiving information — Exchange information — from one or more sources.

Networking refers to the creation of networks that the sharing of information and resources within network. The main goal of a computer network is to allow its users to access and share resources of a network such as hard disk, the expensive laser printer modems, licensed sw etc. irrespective of their physical locations.

* Component of Computer Network :→

- Servers :— These are the computers that provide shared ~~shared~~ resources to network users.
- Clients :— These are computers that access shared networked resources provided by a server.
- Media :— Media are the wires that make physical connections.
- Shared Data :— These are the files provided to clients by server across the network.
- Shared printers and other peripherals :— These are additional resources provided by servers.
- Resources :— Any service or device, such as files, printers or other items made available for use by the member of network.

* Need of Networking :→

Networking has become essential for the following reasons—

- (i) Low cost of transfer of data.
- (ii) To improve communication speed and accuracy.
- (iii) To share computer files.
- (iv) Multimedia transfer.
- (v) To share computer equipments.
- (vi) Instantaneous Availability of Information

* Advantages of Networking :→

(N/w-9)

- (i) Networks allow high speed exchange of essential information bet. key people in an orgⁿ.
- (ii) Networks are productivity tool. In case of a business, a network should be a visible contributor to increased profitability.
- (iii) Networks allow the sharing of expensive resources such as laser printer and high capacity, high speed mass storage devices and of

* Hub — port to port transfer data * Switch — transfer data source to destination, it is intelligent device, it receive the address of dest. (6/11).

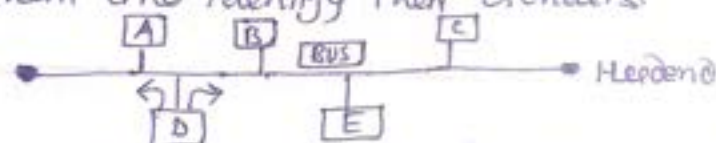
* Disadvantage of Network: →

- (i) Networking commands are so difficult that users feel uncomfortable in learning commands.
- (ii) The financial cost of local area networking is still high in comparison with many other alternatives.
- (iii) Networking software reduces the memory space available for the user's program.

* Network Topology: →

Topology is a term used in networking to describe the geometric arrangement of components that make up the LAN. Local area network topologies can be described using either a physical or logical perspective.

- Bus Topology: — In bus topology, a single transmission medium interconnects all stations. All stations share this medium for transmission to any other station. Every station listens to all the transmissions on the bus. Every transmission to any other station has source and destination addresses so that stations can pick the message meant for them and identify their senders.



If signals are amplified along the bus, the bus becomes unidirectional.

Advantage: —

- (i) The amount of media used is very small.
- (ii) The new station can be added by tapping working bus very easily.
- (iii) The coverage can be increased by extending the bus using repeaters.
- (iv) The stations are connected to the bus using a passive cable.

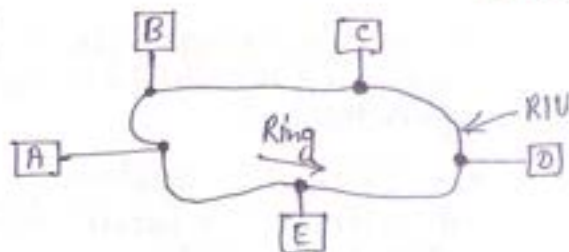
Disadvantage: — N/W-10

- (i) Terminators are required at both ends of backbone cable.
- (ii) The nodes must be intelligent.
- (iii) The fault isolation is difficult, if the entire network shuts down.
- (iv) Can not be used as a stand alone solution in a large building.
- (v) Entire network shuts down if there is a break in the main cable.

(38/11)

• Ring Topology: →

A ring network consists of a number of transmission links joined together in form of a ring through repeaters called Ring Interface Units (RIU). The transmission is usually unidirectional on the ring. Thus, each repeater receives the signal at its input and after regeneration, sends it to the repeater of next station. If the frame belongs to the station, a copy of incoming frame is retained. Each frame contains source and destination addresses.

Ring Topology.Advantage of Ring Topology: →

- (i) Short cable length
- (ii) No wiring closet space required
- (iii) Suitable for optical fibers

Disadvantage of Ring Topology: →

- (i) Node failure cause network failure.
- (ii) Difficult to diagnose faults
- (iii) Network reconfiguration is difficult
- (iv) Topology affect the access protocol.

● STAR Topology: —

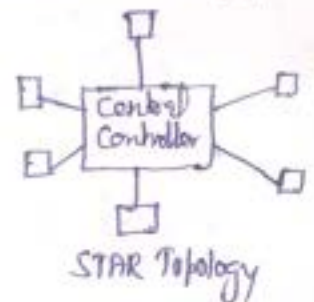
A star network consist of dedicated links from the stations to the central controller. Each interconnection support two-way communication. The central controller acts as a switch to route the frames from source to destination unlike ring or bus topologies where communication is in broadcast mode.

Advantage of Star Network: —

- (i) Ease of service.
- (ii) Simple access protocols.
- (iii) One device per connection
- (iv) ~~Star~~ Centralized control / problem diagnosis.

Disadvantage of Star Network: —

- (i) Long cable length
- (ii) Difficult to expand
- (iii) Central node dependency
- (iv) No sharing of transmission
- (v) Single point of failure.



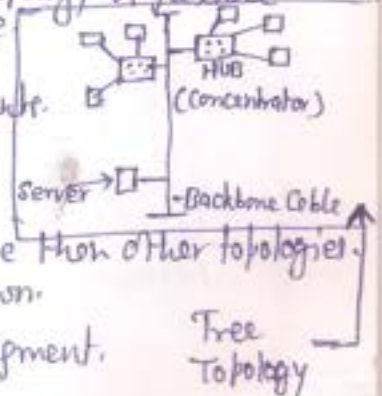
- Tree Topology: → A tree topology combines characteristics of bus topology and star topology. It consist of group of star configured workstations connected to a bus backbone cable. Tree Topology is flexible and allow expansion of an existing network with ease.

Advantage: —

- (i) Point to point wiring is needed for individual segments.
- (ii) Any h/w / s/w vendors have support for it

Disadvantage: —

- (i) Tree topology is more difficult to wire and configure than other topologies.
- (ii) Breakage of backbone line make the entire segment down.
- (iii) The type of cabling used limits the length of each segment.



NW-11

- Mesh Topology :- A network topology featuring a direct path bet. two nodes. All devices are cross-connected so the best path can be chosen at any given moment.

Advantage & Disadvantage :-

- Ease of trouble shooting
- Units affected by media failure
- Difficult installation.
- Difficult reconfiguration.

The Internet is perhaps the most recognisable implementation of mesh topology. There are two types of mesh topologies - full mesh & partial mesh. In full mesh topology, every node has a connection to every other node in the network. A full mesh is very expensive but provides reliability. In partial mesh topology, some nodes are organised in a full mesh but other nodes are connected to only one or two other nodes in the network.

- Hybrid Topology :-

A combination of two or more network topologies is known as Hybrid network. Although the backbone is mostly a mesh network, each local loop is a star network with central office at each hub.

Advantage of Hybrid Network :-

- Ease of Expansion
- Ease of fault diagnosis and isolation.
- Ease of cabling.

Disadvantages of Hybrid Network :-

- Cabling
- Intelligent concentration point required.

* Analog & Digital Signals : →

Data can be analog and digital. Human voice is an example of analog data whereas data stored in computer is an example of digital data. Whenever you speak, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal and then can be converted to a digital signal.

Digital data is stored in the computer's memory in the form of 0's and 1's. It can be converted to a digital signal when it is transformed from one position to another inside or outside the computer.

It can be also modulated in the form of analog signal & then can be sent through a transmission medium to another computer. It is done with a device called modem. Modem is a device that converts digital signals to analog signals & vice-versa. The process of converting digital signal in analog signals is modulation and the process of converting analog signals to digital form is called demodulation. This is why Modem is called Modulator/Demodulator. The speed of a Modem is measured in bits per seconds (bps).

 (Analog)

 (Digital)

* Analog and Digital Transmission :

Data transmission or Digital Communication : — is the physical transfer of data (a digital bit stream) over a point-to-point or point-to-multipoint communication channel. Examples of such channels are copper wires, optical fibers, wireless communication channels, and storage media. The data is often represented as an electro-magnetic signal, such as electrical voltage signal, a radiowave signal, microwave signal, or an infra-red signal.

Analog Transmission : — is a transmission method of conveying voice, data, image, signal or video information using a continuous signal. Digital transmission is always in an exact form of either off or on: there are no in-between states. On the other hand, analog transmission is constantly varying in amplitude (signal strength) and frequency.

* Asynchronous & Synchronous Transmission : →

Data transmission through a medium can be either asynchronous. In asynchronous transmission data is transmitted character by character as one goes on typing on a keyboard. Hence there is an irregular gap bet. characters. It is cheaper to implement.

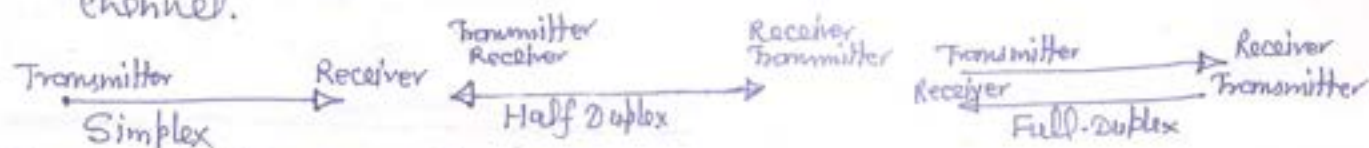
In the synchronous mode, the coded data is transmitted block by block. Each block can contain many characters. Synchronous transmission is well suited for remote communication bet. a computer and related device like card reader and printers.

* Communication Modes : → (N/w-13)

A communication channel is pathway over which information can be conveyed. Information sent through a communication channel has a source from which the information originated and destination to which the information is delivered.

There are mainly three types of mode by which data can be transmitted over communication channel —
(i) Simplex (ii) Half Duplex (iii) Full duplex

- (i) Simplex:— The message source is the transmitter and the destination is the receiver. A channel whose direction of transmission is unchanging is referred to as a simplex channel. For example, a radio station is a simplex channel because it always transmits the signal to its listeners and never allows them to transmit back.
- (ii) Half Duplex:— A half duplex channel is a single physical channel in which the direction may be reversed. Messages may flow in two directions, but never at the same time, in a half-duplex system. In a telephone call, one party speaks while the other listens. After a pause, the other party speaks and the first party listens. Speaking simultaneously results in garbled sound that cannot be understood.
- (iii) Full Duplex:— A full duplex channel allows simultaneous message exchange in both directions. It really consists of two simplex channels, a forward channel and a reverse channel, linking the same points. The transmission rate of the reverse channel may be slower if it is used only for flow control of the forward channel.



* Communication Channel: →

1. Wire Pairs:— Wire pairs are commonly used in local telephone communication and for short distance digital data communication. They are usually made of copper and pair of wires is twisted together. Data transmission speed is normally 9600 bits per second in a distance of 100 mtr.
2. Coaxial Cables:— Co-axial cable is a group of specially wrapped and insulated wires that are able to transfer data at higher rate. They consist of a central copper wire surrounded by an insulation over which copper mesh is placed. They are used for long distance telephone lines and local area network for their noise immunity and faster data transfer.
3. Microwave:— ^{N/A-14} Microwave system uses very high freq. radio signals to transmit data through space. The transmitter and receiver of microwave system should be in line of sight because the radio signal cannot bend. With microwave very long distance transmission is not possible. In order to overcome the problems of line of sight and power amplification of weak signal, repeaters are used at intervals of 25 to 30 km bet. the transmitting and receiving end.
4. Communication Satellite:— The problem of line of sight and repeaters are overcome by using satellites which are the most widely used data transmission media in modern days. A communication satellite is a microwave relay station placed in outer space e.g. INSAT-1B. In comm. sat. microwave signal is transmitted from transmitter on earth to satellite in space. It amplifies weak signals and transmits it back to the receiver. Its transmission rate is 16 Gbps bits per seconds.

* Difference bet. Analog Signals Vs Digital Signal.

Analog

1. Analog signals are more to noise or distortion.
2. Analog signals can not perform high quality data transmission.
3. Analog system can not be upgraded easily
4. The cost of computer components required in analog transmission is relatively high.
5. Analog signals have definite infinite resolution
6. Analog signal can not be sent over long distances
7. Small fluctuations are meaning less analog signals.
8. In analog signals, values taken can be continuous
9. Example: Radio Transmission.

Digital

1. Digital signals are less prone to noise or distortion than analog signals.
2. Digital signals can perform high quality data transmission
3. Digital system can be upgraded relatively easy.
4. The cost of computer components required in digital transmission is very low.
5. Digital signals have low resolution.
6. Digital signals can be sent over long distances.
7. Small fluctuations in digital signals are meaningful.
8. In digital signals, there can only be discrete values.
9. Example: Data transmission of text & integers

* Difference Bet. Digital & Analog Transmission

Digital Transmission

1. Digital transmission uses discrete values.
2. Digital transmission involves more bandwidth (74.5 MHz)
3. Signals-to-Noise ratio is high in digital transmission.
4. Transmitter cost is high in Digital transmission. (N/w-15)
5. Performance over time is excellent in digital transmission
6. Receiver gain adjustment is not required in digital transmission
7. No adjustment are required in their installation.
8. Digital transmission offers a simple means of reconstructing the signal

Analog Transmission

1. Analog transmission uses continuous range of values.
2. Analog transmission involves less bandwidth (4.5 MHz)
3. Signals-to-noise ratio is low to moderate in analog transmission.
4. Transmission cost is moderate in analog transmission.
5. Performance over time is moderate in analog transmission.
6. Receiver gain adjustment is often required in analog transmission
7. Adjustment are often required in their installation.
8. Analog transmission require adjust at receiver end in order to reconstruct the transmitted signal.

* Networking Devices: →

- (i) Repeater: → A repeater is a device that regenerates the weakened data signal to its original strength. It is used to extend the length of a single network. A repeater is used to connect similar networks, such as an Ethernet LAN to another Ethernet LAN. A repeater works upon the physical layer of the OSI model to regenerate the network's signals and send them out on other segments. Repeaters do not translate or filter signals.

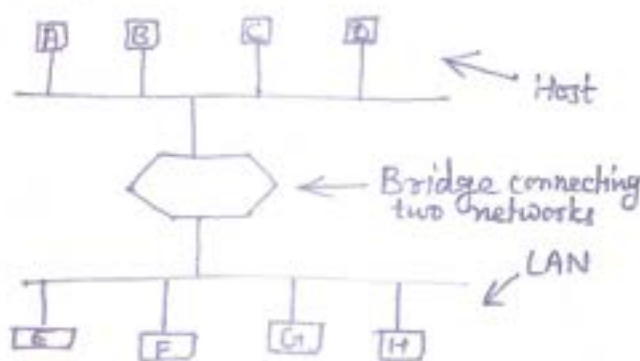
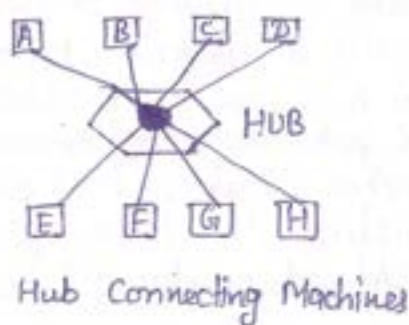
LANs may also require the use of repeaters to boost the transmission signal. This is necessary when the transmission lines run over longer distances; the signal tends to weaken (attenuate) and distort due to 'noise' on the line. A repeater enables a series of cable segments to be treated as a single cable. Repeaters receive signals from one network segment and amplify, retime and retransmit those signals to another network segment.

(ii) HUB : →

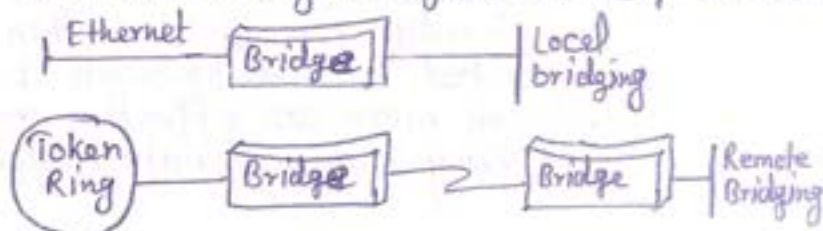
A hub has a no. of input lines that it joins electrically. Frames arriving on any of the lines are sent out on all the others. All lines coming into a hub must operate at same speed. Hubs are designed to hold multiple line cards each with multiple inputs. A hub is a passive network device (physical layer device) that allows network nodes to communicate with each other. The packet received on each port is broadcasted to all connected devices on all ports on the hub. In a hub, the bandwidth is shared bet all connected devices. There are three types of hubs: - Active Hub, Passive Hub, Hybrid Hubs.

- Active Hubs — require electrical power, but are able to regenerate and retransmit network.
- Passive Hubs — Passive hubs simply organise the wiring. They simply take all packets they receive on a single port and re-broadcast them across all ports.
- Intelligent Hubs — Intelligent hubs offer many advantages over active & passive hubs. It is also called hybrid/Advanced hub. Incorporating intelligent hubs into your network infrastructure gives you the ability to manage your network from one central location. If the problem develops with any device on a network connected to an intelligent hub, it can easily identify, diagnose and remedy the problem using mgmt. info. provided by each intelligent hub. (प्राप्त, इलाज करता, to rectify, band)

NW-16



- (ii) Bridges : → Bridges are simple device that connect LANs that use the exact same network architecture. Bridges only pass on message that are for nodes on other LAN's. It does this 'filtering' by maintaining a list of device addresses that are assigned to the network interface cards attached to the network. In that way, bridges can help reduce unnecessary network traffic.



Bridges are either local or remote.

• Local Bridge — provide a direct connection bet. multiple LAN segments in same area.

• Remote bridges — connect multiple LAN segments in different areas, usually over telecommunication lines.

• Advantages of Bridging —

- (i) It handles all protocols.
- (ii) Very less staff needed.
- (iii) It uses automatic path optimisation.
- (iv) It provides more flexibility.
- (v) It provides simpler installation & configuration.

N/W-17

- (iv) Routers : → Routers are the devices provide connectivity bet. LANs and two WAN's over large geographical distances. Router choose best route to send a message, when several possible routes exists in a computer network topology. It does this by maintaining a routing table to identify the path. The routing table contains addresses. These addresses differ from the address used by bridges that look LAN's together. They are called internetwork addresses. Routing is the process of sending message through switches such that they reach their destinations in a efficient way. Advantage : — ① It provides simple administration of network security. ② It may reduce total overhead. ③ It complements bridging in large networks. ④ It is useful for lower speed WAN links. ⑤ It isolates broadcast traffic to individual LAN's.

(v) Gateway: → A gateway make it possible for an application program, running on system, conforming to network architecture to communicate with a application program running on a system conforming to some other network architecture. The function of a gateway is to convert one set of communication protocols to some other set of communication protocols. Protocol conversion may include the following:-
① Message format conversion ② Address translation ③ Protocol Conversion.

(vi) Switches: → Switches can send and receive info. at the same time, so they can send information faster than hub can. Switches costs little more than hubs.

(vii) Brouters: → A brouter has the features of both a bridge and a router. A brouter can act as a router for one protocol and as a bridge for all the others. Brouters can route selected routable protocols, bridge non-routable protocols, Delivers more cost effective and more manageable internetworking than separate bridges and routers.

(viii) NIC: → Network Interface Card is a device that connects your computer to a network. It is also called 'network adapter'. This card is installed in each computer and server on the network which acts as the physical interface or connection bet the computer and network cable.

(n/w-18)

Unit-2

Nlw
Internet
6

* OSI Model : →

ISO (International Standard Orgⁿ) stands for International Orgⁿ for Standardisation. ISO Developed the OSI (Open System Interconnection) reference model to facilitate the open interconnection of computer system. An open interconnection is one that can be supported in a multivendor environment.

The purpose of OSI reference model is to set open communication bet devices without requiring changes to the logic of underlying hardware & software. The OSI Model defines how each layer communicates and work with layers immediately. The layers are separated from each other by boundaries called interfaces. All requests are passed from one layer through the interface, to the next layer.

Layer 7. Application Layer -

It is the highest layer in the OSI Architecture. Protocols of this layer directly serve the end user by providing the distributed information service appropriate to an application, to its management and to system management. Management of OSI comprise those functions required to initiate, maintain, terminate and send data concerning the establishment of connections for data transfer among application processes.

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data-link
1. Physical layer

{ The Seven layers of OSI Reference Model }

Features : -

- i) It defines interface to user processes for communication & data transfer in network.
- ii) It provided standardized services such as file & job transfer.

Layer 6. Presentation Layer - (Nlw-19)

Presentation Layer defines the format used to exchange data among networked computers. It can be considered as network's translator. The presentation layer is responsible for converting protocols, translating the data, encrypting the data, changing or converting the character set and managing data compression to reduce the no. of bits that need to be transmitted.

Layer 5: Session Layer:— Session layer allow two applications on different computers to open, use and close a connection called a session. A session is a highly structured dialog bet. two workstation.

- features:—
- (i) It is responsible for managing dialogues.
 - (ii) It manage the flow of communication during connection bet. two computer system. This flow of communication is known as session.
 - (iii) It determines whether the communication will be unidirectional or bidirectional.
 - (iv) It ensures that one request is completed before a new one is accepted.

Layer 4: Transport Layer:—

The transport layer ensures that packets are delivered error free, in sequence and without losses or duplication. (*A packet is a unit of information transmitted as a whole from one device to another devices on a network, whereas a "frame" is a package of information transmitted on a network as a single unit. Frame is term most often used with Ethernet network. A frame is similar to the packet used in other networks.*)

At the sending computer, this layer repackages data, dividing long messages into several packets and collecting small packets into one package.

At receiving computer, Transport layer open the packets, reassembles the original messages and sends an acknowledgement that message was received. If duplicate packet arrives, this layer recognises the duplication and discards it. It can detect the packets that have been discarded by routers and automatically generate a retransmit request.

(N/w-20) TCP (Transmission Control Protocol & SPX (Sequenced Packet Exchange) are example of Transport Layer Protocols).

Layer 3: Network Layer:—

The network layer provides functional & procedural means to exchange network service data unit bet. two transport entities over a network connection. The main feature of this layer are:—

- (i) It determine how data are transferred bet. network devices.
- (ii) It route packets according to unique network device addresses.
- (iii) It provides flow and congestion control to prevent network resource depletion (नियंत्रण, रोकथाम).

Layer 2: — Data Link Layer: —>

Nilu
ghant
8

The purpose of data link layer is to provide the functional and procedural means to establish maintain and release the data links bet. network entities. The main feature of this layer are:—

- (i) It defines procedures for operating the communication links.
- (ii) It frames packets.
- (iii) It detects and correct packets transmit errors.

Layer 1: — Physical Layer: —>

The Physical layer is also called H/w layer or bottom layer. It provides mechanical, electrical, functional & procedural characteristics to establish, maintain and releases physical connections bet data link entities.

features: —

- (i) It define how the cable is attached to NIC.
- (ii) It also define which transmission technique will be used to send data over the network cable.
- (iii) It defines physical means of sending data over network devices.
- (iv) It interfaces bet. network medium and devices.

© Advantages/Merits/Pros/Benefits of OSI Model: —

- i) If a network conform broadly to agreed standards, users are insulated against some of adverse effects of technological change.
- ii) It promotes modularization of network support software. Each module take the form of layer in the module. (Nilu-21)
- iii) In theory any layer can be replaced by a new layer that provide the same services but in diff. way, without affecting the user's view of the system.

© Disadvantages/Demerits/Cons/Limitation of OSI Model: —

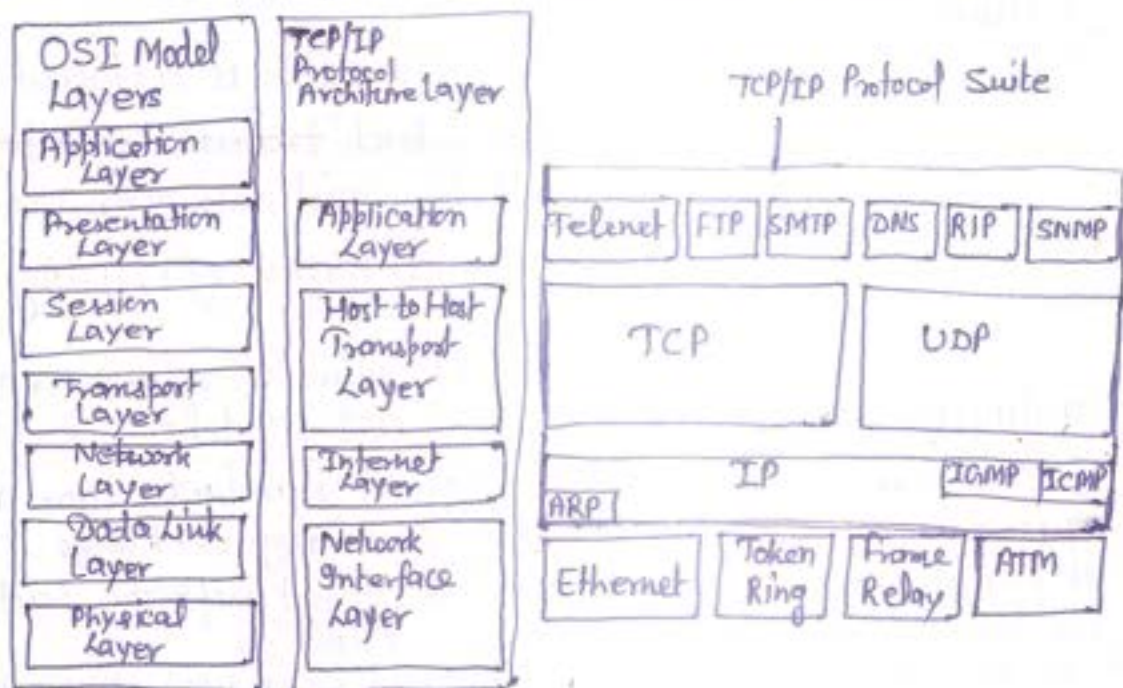
- i) Due to the complexity of system poor performance is obtained.
- ii) Direct substitution of layer is not always possible.

* TCP/IP (Transmission Control Protocol / Internet Protocol):—

The TCP divides the block of information or message or message into packets on the source computer and add special info. — the packet position in the document, error detection code etc. This added information make it sure that these packets at the receiving end are reassembled correctly without any damage to the data. It means that TCP re-assembles the packet in correct sequence on the destination computer.

The IP (Internet Protocol) handles the packets so that each packet is routed or sent to its proper destination.

The TCP/IP was developed in 1969 by the US Department of Defense Advanced Research Projects Agency (DARPA), result of resource sharing experiment called Advanced Research Project Agency Network. The Purpose of TCP/IP was to provide high speed communication network links. Since 1969, ARPANET has grown into a worldwide community of networks known as the Internet.



NW-22

• Layer - 1 Network Interface/Access Layer:—

This layer encompasses the Data Link and physical layers of the OSI Model. It is responsible for placing TCP/IP packets on the network medium and receive the TCP/IP packets from the network medium. TCP/IP was designed to be independent from network access method, frame format and medium. In this way, TCP/IP can be used to connect different network types. This include LAN Technologies such as Ethernet or Token Ring and WAN technologies such as X.25 or Frame Relay.

*

N/w
Internet
10

Layer 2 - Internet Layer :-

The Internet Layer is responsible for addressing, packaging and routing functions. The core protocols of the Internet Layer are IP, ARP, ICMP & RARP. The Internet Layer is analogous to the Network layer of OSI Model.

- (i) The Internet Protocol (IP) is a routable protocol responsible for IP addressing and the fragmentation and reassembly of packets.
- (ii) The Address Resolution Protocol (ARP) is responsible for resolution of the Internet layer address to the Network Interface Layer address, such as a hardware address.
- (iii) The Internet Control Message Protocol (ICMP) is responsible for providing diagnostic functions and reporting error or conditions regarding the delivery of IP packets.
- (iv) The Internet Group Management Protocol (IGMP) is responsible for the management of IP multicast groups.

Layer 3 Transport Layer :-

The Transport Layer (Also known as Host-to-Host Transport) is responsible for providing the Application Layer with session and datagram communication services. The core protocols of the Transport Layer are TCP & UDP.

- ① TCP (Transmission Control Protocol) — TCP provides a one to one, connection-oriented, reliable communication service. TCP is responsible for establishment of a TCP connection, the sequencing and acknowledgement of packets sent and recovery of packets lost during transmission.
- ② UDP (User Datagram Protocol) — UDP provides a one to one or one to many, connectionless, unreliable communication service. UDP is used when the amount of data to be transferred is small, when the overhead of establishing a TCP connection is not desired or when the applications or upper layer protocols provide reliable delivery.

Layer 4 Application Layer :-

The Application Layer provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data. The Process / Application Layer provides protocols for remote access and resource sharing. Applications & protocols such as FTP, Telnet, SMTP, HTTP and many others, all reside and cooperate in this layer and depend on the functionality of the underlying layers.

N/w-23

(11)

© Advantage of TCP/IP —

- (i) TCP/IP can be used to establish connection bet. different types of computer and servers.
- (ii) TCP/IP operates independently of the operating system.
- (iii) A method of gaining access to the Internet.
- (iv) TCP/IP includes support for name and address resolution services, including DNS, DHCP Dynamic Host Configuration Protocol (DHCP) and Windows Internet Name Service (WINS).

© Disadvantage of The TCP/IP —

- (i) TCP/IP is slower than IPX (The NetWare protocol that provides packet forwarding and routing).
- (ii) The overhead of TCP/IP is higher than that of IPX.
- (iii) TCP/IP is intricate to set up and manage.

© Comparison bet. TCP/IP & OSI Model

TCP/IP Reference Model	ISO/OSI Ref. Model
1. TCP/IP is defined after the advent of Internet	1. OSI/ISO is defined before the advent of internet.
2. Service interface and protocols were not clearly distinguished before	Service interface and protocols are clearly distinguished.
3. TCP/IP supports Internet working TCP/IP is loosely layered	Internet working not supported ISO/OSI Model has strict layering
4. TCP/IP is a protocol dependent standard	OSI/ISO is protocol independent standard
5. TCP reliably delivers packets, IP does not reliably deliver packet	All packets are reliably delivered.

N/w-24

⑥ ARP (Address Resolution Protocol) : →

The Address Resolution Protocol is used to translate virtual addresses to physical ones. The network hardware does not understand the usfw-maintained IP address. IP uses ARP to translate the 32-bit IP address to a physical address that matches the addressing scheme of the underlying h/w (Ethernet, the 48-bit ^{Media access control} MAC address).

N/W
Internet
12

There are three general addressing strategies: — i) Table lookup
ii) Translation performed by mathematical function
iii) Message Exchange

TCP/IP can use any of three. ARP employs the third strategy, message exchange. ARP defines a request and a response. A request message is placed in a hardware frame and broadcast to all.

⑦ RARP (Reverse Address Resolution Protocol) : →

A RARP server maintains a database of machine numbers in the form of an ARP table which is created by system administrator. When the RARP server receives a request for an IP number from a node on the network, it responds by checking its routing table for the machine number of the requesting node and sending the appropriate IP number back to the requesting node.

⑧ Simple Mail Transfer Protocol (SMTP) : →

SMTP is simple mail transfer protocol which can send message only in ASCII format. It is used in the TCP/IP based networks. SMTP can not be used mails containing non-ASCII characters, binary file or audio or video data. SMTP works only when both the mail sender and receiver are ready to transact at the same time. If the receiver computer is not connected or available at that moment, then message are stored in temporary server.

N/W-25

It should be noted that two separate protocols are used for sending and receiving e-mail messages. For sending, the SMTP is used whereas for receiving at the other end either POP or IMAP is used at their local server.

⑨ PPP (Point to Point) Protocol : — This protocol is widely used for dialup. Leased connections. Principal parts of PPP are LCP, Authentication and NCP. The LCP is the Link control protocol, which negotiates the link for connection. The Authentication mechanism allows genuine users to access the network resources. The NCP configures and establishes the Network Layer protocol.

Network Control Protocol

There is no third point of contact in bet. a single PPP link. In a dial up PPP, connections are initiated when needed and terminated when the call is completed.

* Broadcasting : → When a single device is transmitting a message to all other devices in a given range of addresses, it is called broadcasting. This broadcast could reach all hosts on the subnet, all subnets or all hosts on all subnets. Broadcast packets have a host portion of address set to all ones. Many existing radio and television broadcasters provide Internet "feeds" of their live audio and video streams. They may also allow time-shift viewing or listening such as Preview, Classic Clips, and Listen Again features. These providers have been joined by a range of pure Internet "broadcasters" who never had on-air licenses. This means that an Internet-connected device, such as a computer or something more specific, can be used to access on-line media in much the same way as ~~was~~ possible only with a television or radio receiver.

These techniques using simple equipment allow anybody, with little censorship or licensing control, to broadcast audio-visual material on a worldwide basis.

* MIME : →

MIME stands for Multipurpose Internet Mail Extension. MIME is a supplementary protocol to SMTP that allows non-ASCII data such as binary files, sound files, video files etc. to be included in the message through SMTP, send it over the Internet. MIME is not a mail protocol and it cannot be used in place of SMTP. Actually MIME converts non-ASCII data on the sender site and delivers them to SMTP client to send over Internet. After this, SMTP server on receiver site receives the ASCII data delivers them to MIME, which converts them into non-ASCII data, i.e. original data. MIME uses Base 64 encoding scheme to convert complex files into ASCII data.

* IMAP : →

Internet Message Access Protocol is a standard protocol for accessing e-mail. IMAP server receives and store mails and the e-mail client can download mails from it. In order to download the mail message, the user has to decide it by viewing only the header part and name of sender. The user can create and manipulate folders (mailbox) on the IMAP server, delete messages or search for certain parts. The downside is that IMAP requires continuous access to mail server while the user is working with his/her mail.

* POP : →

POP stands for Post Office Protocol. In a TCP/IP network SMTP is used to send a mail to the mail-server and POP is used to retrieve a mail from a SMTP mail server. POP is a popular protocol used for receiving e-mail messages. This protocol is often used by ISP's mail server. POP3 server allow access to single inbox in contrast to IMAP servers, which provide access to multiple server-side folders.

POP delivers all the messages stored on the server to the user-email account. It can be configured in such a manner that user can obtain e-mails from his multiple email account into his only software installed on the computer such as Microsoft Outlook or Outlook Express. This facility is available on almost all the Internet based e-mail websites such as Hotmail, Yahoo etc.

Web server, and `ref/mbsys/index.html`: specifies the path of the file—"index.html" stored on Web server's hard disk.

An absolute URL is that which specifies the full path of a resource such as a document whereas a relative URL specifies the path of a resource relative to the current directory.

UNIT-III

Q. 12 Describe in short about WAN.

Ans. Wide Area Network (WAN) refers to a data communication network in which two or more geographically dispersed computers are linked by communication facilities such as telecommunication or microwave relays. One of the most significant aspects of a WAN while comparing with LAN is the involvement of a public telecommunication authority. WAN is usually limited to be used by the larger organisations and government agencies due to high cost involved in building and maintaining them. INTERNET, DECnet, NSFnet, NICnet, etc. are a few examples of WAN. In a WAN, transmission lines are called circuits or channels and they are used along with routers. Transmission lines are used for moving data bits between machines, whereas routers are used to connect two or more transmission lines.

Q. 13 Write a short note on RFC.

Ans. Requests for comments (RFCs) are a series of notes, started in 1969, about the Internet (originally the ARPANET). The notes discuss many aspects of computing and computer communication focusing on:

- Networking protocols
- Procedures
- Programs
- Concepts
- Meeting Notes and
- Opinion

RFCs are numbered sequentially in the order they are accepted. For example, RFC 2026 describes about The Internet Standard Process.

Q. 14 What is FTP and why do you need it?

Ans. FTP (File Transfer Protocol) is a protocol of TCP/IP suite of protocol and a utility/application too that enables the users to upload and download files, that is transfer of files between hosts in a TCP/IP network such as Internet. FTP provides access to directories or folders on remote sites and allows software, data and text files to be transferred between different kinds of computers.

It is basically required for Web publishing, where we need to upload (transfer) files from a local computer to a remote Web server. The FTP protocol is the vehicle of file transfer between hosts, even though www uses HTTP access method.

NIW-27

Q. 15 Describe briefly how do the search engines retrieve the required document on the WEB?

Ans. Search engines are software called spiders, which comb the Internet looking for documents and their Web addresses. The documents and their Web addresses are

(14)

* Differentiate bet. POP & IMAP : →

POP and IMAP, both deal with receiving of e-mails from local server. But, POP just stores and sends the messages whereas IMAP acts totally as a remote file server because it stores messages on the mail server from which user has to connect in order to view the mails. IMAP requires continuous access to mail server whereas POP does not.

* Difference bet. TCP & UDP : →

UDP is a connectionless protocol and is responsible for end-to-end transmission of data. Unlike TCP, however, UDP does not establish a connection. It attempts to send the data and to verify that destination host actually receives the data. UDP is best used to send small amount of data for which guaranteed delivery is not required. While UDP ports are different from TCP ports, therefore, they can use the numbers without interference.

* HTTP & its working for web or Internet : → NW-28

HTTP is a communications protocol for the transfer of information on intranet and WWW. The concept of HTTP is based on Request-Response combination with the client (web-browser), requesting the HTTP server responding to the requests. The server processes the request, generate requests and close connection. Thereafter, the server keeps waiting for other requests.

HTTP is a connectionless text-based protocol. Clients send requests to web server for web element such as web page and images. When the server send response, the connection bet. client and server across the Internet is disconnected. A web server is a computer that has certain amount of space allocated separately and stores a lot of information in the form of HTML files along with other files such as images, sound etc. An HTTP daemon is a program that is designed to wait for a number of incoming HTTP requests and respond them when they arrive.

Introduction to Computer Networks

collected and sent to the search engine's indexing software. The indexing software extracts information from the documents, storing it in a database. The kind of information indexed depends on the particular search engine. Some index every word in a document; others index the document title only.

When a search is required by entering keywords, search engines searches for document in its database. Finally, the search engine assembles a Web page and lists results that are hypertext links, where each hyperlink refers to a URL on the Web. When the user clicks on a link, the browser sends a DNS query for the IP address related to that link (URL). The DNS server returns the IP address for the requested URL (link) and then the browser retrieves that URL and displays page on the user's computer screen.

Q. 16 Write short notes on the following :

- (a) Hypertext (b) Routing of packets on Internet.

Ans.

- (a) **Hypertext:** Hypertext is nonlinear or non-sequential text. There is no single order that determines the sequence in which the text is to be read. That is, the text is organised so that one can easily jump around from topic to topic. Hypertext presents several different options, and the individual readers determine which of them to follow at the time of reading the text. This means that the author of text has set up a number of alternatives for readers to explore rather a single stream of information.
- (b) **Routing Packets on Internet :** Routing of IP packets on Internet is performed by routers and IP software with the help of IP routing table. The IP routing table is maintained by both the host and the routers. The routing table contains a list of IP address of network and IP address of next router along the path to a network. When an IP packet has to be send, the IP routing software consults to the routing table and sends it to the router with it destination IP address, then the router decides the best route for the IP packet to transmit and sends it to next router along the path.

Q. 17 (a) What is World Wide Web? How does the WWW work?

(b) How does the Web browser fetch and display Web pages on the screen?

Ans.

- (a) **World Wide Web** is an architectural framework for accessing millions of documents stored on the millions of computers on Internet all over the world. It is a distributed client-server system in which any user can access the services of a server using a browser. The services provided by the **www** are stored on many locations called Web sites.

As **www** is a client-server system, it has two parts :

- Client side, and
- Server side

In the view of a general user, it can be said that **www** is a linked collection of

* What is telnet? Why it is used? (15)

Telnet is a simple, text based program that allow you to connect to another computer by using internet. If you have been granted the right to connect to that computer by that computer's owner or administrator, Telnet allow you to enter commands used to access programs and services that are on the remote computer, as if you were sitting right in front of it. Telnet can be used for many things, including accessing e-mails, database or files. Telnet works in step-by-step procedure. The commands typed on the client computer is sent to local Internet Server Provider and then from the ISP to the remote Telnet server to which the user has gained access.

Telnet gives direct access to various services on internet. Some of these services are available on a user's machine but many services may be available on the host (Telnet Server). Telnet is useful in such a situation. If one wants to use a program / app developed by other user. Telnet allow access to their host and use their resources. Whenever someone creates a new services on his host with Telnet one can access it.

Telnet is especially used for accessing public services such as universities libraries, bulletin board information, catalogs and database available on machine connected to Internet.

* Internet Protocol (IP)

Internet Layer Protocol : →

(NW-30)

IP is a connectionless, unreliable datagram protocol primarily responsible for addressing and routing packet bet. hosts. Connectionless means that a session is not established before exchanging data. Unreliable means that delivery is not guaranteed. IP will always make a best effort attempt to deliver a packet. An IP packet might be lost, delivered out of sequence, duplicated or delayed. IP does not attempt to recover from these types of errors. The acknowledgement of packets delivered and the recovery of lost packets is the responsibility of a higher-layer protocol, such as TCP.

* ICMP (Internet Control Message Protocol) : →

The ICMP is used by IP and higher-level protocols to send and receive status report about information being transmitted. Routers commonly use ICMP to control the flow or speed of data bet. themselves. Sometimes the flow of data may be too fast for a router. The router then requests other routers to slow down. The two basic categories of ICMP message are reporting errors and sending queries.

A common use of ICMP is 'Pinging' a host. The Ping command (Packet INternet Groper) is a utility that determine whether a specific IP address is accessible.

documents stored on millions of computers on the Internet all over the World. Every document consists of some pages which are called Web pages. A page on the Web may be linked to any page. When the user clicks on a link, the page related to that link is requested by client usually a browser to the server. After this, the server receives that request and processes that page and sends the HTML code (of that page) to the browser (client). But, before receiving the request from client, there is a TCP connection established between client and server. The requests from client and replies from server are managed by a protocol called HTTP (Hypertext Transfer Protocol). When the client (browser) receives the HTML code for the requested page from the server, it (browser) translates and displays the HTML code on the user's computer. When the client (browser) receives the response from the server, the TCP connection is released.

- (b) When a user specifies a URL/Web page to access it either by clicking on a link or by typing in the address bar of a Web browser, the Web browser sends a request to the Web server on which that page is stored. When the server receives a request from a client (browser), it processes the requested page and sends the HTML code of that page to the browser. After this, the browser interprets, formats and displays that page.

Nlw-31

Q. 18 What is a Web server? How does it function?

Ans.

A Web server is a combination of hardware and software that hosts Websites and make them available to clients on Internet. In general, a Web server is a computer that stores Web documents and make them available to rest of the world.

A Web server also refers to the software that provides access to content (executable program) and responds to requests received from clients (Web browsers). Every Web server on Internet has an IP address and a domain name.

Internet Information Server (IIS) for Windows and Apache Web server for UNIX are a few examples of Web server software.

Functioning of a Web Server: WWW is based on client/server architecture, where a client requests to server for services and the server provides those services to the client. In between the process of request and response, a lot of activities are performed, that can be described as follows :

- (i) The client, usually a browser, sends a request for the IP address of the URL that it has detected, to the DNS (Domain Name Server). The URL is specified by the user.
- (ii) The DNS returns the IP address of the URL, i.e., Web server for which client has requested.
- (iii) The client (browser) establishes a TCP connection to the IP address on port 80.
- (iv) The client (browser) sends a GET request for desired content to the Web server.
- (v) The Web server (related to the URL that has been specified by the user) sends HTML code to the client.
- (vi) The TCP connection is released between client (browser) and Web server.

(16)

Q. What do you mean by flow control? Why is it important? Which layer of OSI model is responsible for flow control? How does flow control work?

A. Flow control is the process of managing the rate of data transmission bet. two nodes to prevent a fast sender from over-running a slow receiver.

Flow control is important because it is possible for sending computer to transmit information at a faster rate than the destination computer can receive and process them. This can happen if the receiving computer have a heavy traffic load in comparison to the sending computer or if the receiving computer has less processing power than the sending computer.

The Transport layer in the OSI model provides flow control as well as error handling, and participates in solving problems concerned with the transmission and reception of packets. Transmission Control Protocol and Sequence Packet Exchange (SPX) are examples of Transport layer protocols.

TCP uses sliding window to transmit data stream efficiently and for flow control. A sliding window is used by TCP for transferring data bet. hosts. It regulates how much information can be passed over a TCP connection before receiving host must send an acknowledgement. Each computer has both a send and a receive window that it utilises to buffer data and make the communication process more efficient. A sliding window allows the sending computer to transmit data into a stream without having to wait for each packet to be acknowledged. This allow the receiving machine to receive packet out of order and reorganise them while it waits for more packets. The sending window keep track of data that has been sent and if an acknowledgement is not received within given time, the packets are re-sent.

Q. What is difference bet encryption and decryption? (Nlw-32)

A. Encryption is the process of transforming the plaintext to ciphertext whereas decryption is the process of transforming the ciphertext back to plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algo.

Q. What is key in the context of cryptography? What is the difference bet a key & password?

A. In cryptography, the number (value) needed to encrypt or decrypt something is usually a no. or a short string less than 20 character long. This number is called a key. A key is a ^{password} ~~large~~ ^{secret} word or is simply a series of letters. To encrypt a message, we need an encryption algo., an encryption key and the plaintext. These create the ciphertext. To decrypt a message, we need a decryption algo., a decryption key and ciphertext. In cryptography, the encryption/decryption algo. are public whereas keys are secret.

(17)

Q. What is cryptography? Give some applications of cryptography? Which layer of OSI model is responsible for it?

A. Cryptography refers to the process, art, and science of keeping messages and data secure.

Cryptography is used to enable and ensure confidentiality, data integrity, authentication. Cryptography is used in applications present in technologically advanced societies - security of ATM cards, computer passwords and electronic commerce that depend on cryptography. Presentation layer is concerned with syntax and semantics of information transmitted. Presentation layer is concerned with other aspects of information representation such as data compression which can be used to reduce the size of information that have to be transmitted and cryptography frequently required for privacy and authentication.

Q. What is symmetric key cryptography? Why is it used for encrypting long messages?

A. In symmetric-key cryptography, the same key is used for both encryption & decryption. In this method, the sender uses this key and an encryption algo. to encrypt data and the receiver uses the same key and the corresponding decryption algo. to decrypt the data. Using this technique, the two keys can be created that are mathematically related, but essentially independent from each other. A message encrypted with one of these keys can only be decrypted by other key. In symmetric-key cryptography, the algo. used for decryption is the inverse of the algo. used for encryption.

Symmetric key algo. are efficient. Symmetric key algo. takes less time to encrypt messages while public key algo. takes a longer time to do the same. The reason is that symmetric key is generally smaller. This is why, symmetric key algo. are used to encrypt and decrypt long messages.

Q. What is asymmetric key cryptography?

A. Asymmetric (Public) key encryption uses different keys for encryption and decryption. In public-key cryptography, there are two keys - a private key and public key. The private key is kept by receiver and public key is announced to the public. Since you can keep one key private and make the other public, this is better known as public-key encryption. Asymmetric (public/private) keys are produced in pairs, where one key encrypts, but a mirror key must be used to decrypt the messages and somebody with one key cannot figure out the other key. With asymmetric keys, however hackers can only steal the key to encrypt messages, but cannot use that key to decrypt anything.

* Routing : →

Routing is the act of moving info. across an internet work from a source to a destination. Along the way, at least one intermediate node typically is encountered. Routing is often contrasted with bridging, which might seem to accomplish precisely the same thing to the casual observer. The primary diff. bet. the two is that bridging occurs at Layer 2 (the data link) of OSI Ref. Model, whereas routing occurs at Layer 3 (the network layer).

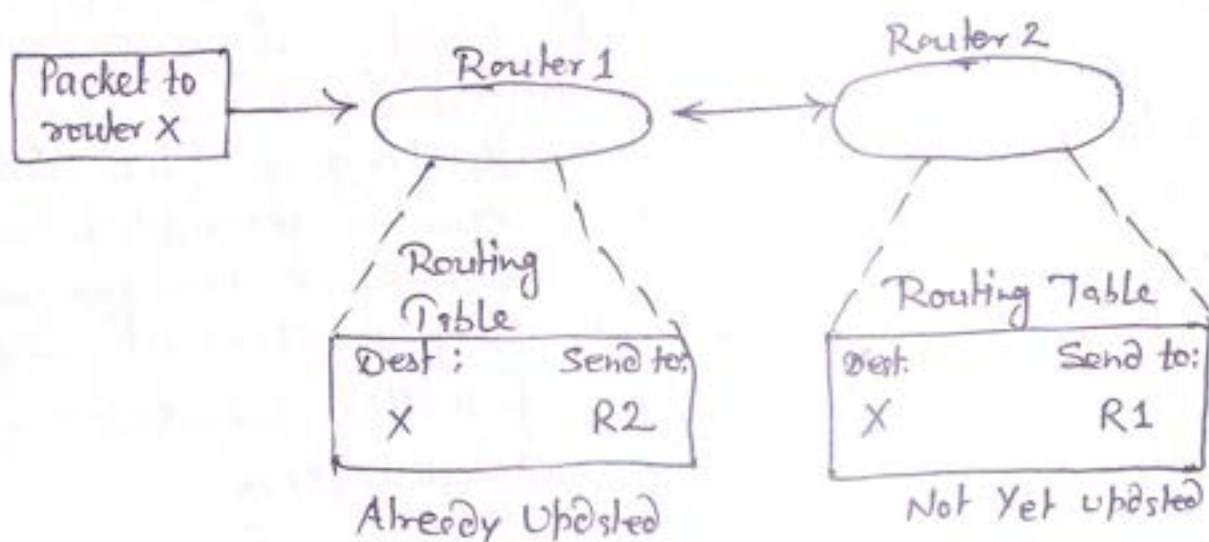
* Routing Components : →

Routing involves two basic activities: - determining optimal routing path & transporting information groups (packets) through an internet work.

(N/w-34)

- Path Determination : → Routing protocols use metrics to evaluate what path will be best for a packet to travel. A metric (मात्रक) is a std. of measurement, such as path bandwidth, that is used by routing algo. to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize & maintain routing tables, which contain route information. Route info. varies depending on the routing algorithm used.

Routing algo. fill routing tables with a variety of information. Destination/next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular router representing the "next hop" on the way to the final destination. When a router receives an incoming packet, it checks the destination address & attempts to associate this address with a next hop. Fig. depicts a sample destination/next hop routing table.



Routing Tables also can contain other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes and these metrics differ depending on the design of the routing algo. used.

N/W - 35

* Routing Algo's : $\rightarrow$ Routing algo can be differentiated based on several key characteristics. First, the particular goal of the algo. designer affect the operation of the resulting routing protocol. Second, various types of routing algorithms exist & each algo has a different impact on network & router resources. Finally, routing algo's use a variety of metrics that affect calculation of optimal routes.

© Design Goals : $\rightarrow$ Routing Algo. often have one or more of following design goals : —

1. Optimally
2. Simplicity & low overhead
3. Robustness & stability
4. Rapid Convergence
5. Flexibility

1. Optimality refers to the capability of routing algo to select the best route, which depend on the metrics & metric weighting used to make calculations
2. Routing algo. also are designed to be as simple as possible. In other words, the routing algo. must differ its functionality efficiently, with a minimum of slw & utilization overhead.
3. Routing Algo. must be robust, which means that they should perform correctly in the face of unusual or unforeseen circumstances, such as n/w failures, high load conditions & incorrect implementations. (N/W-35-i)
4. Routing Algo must converge rapidly. Convergence is the process of agreement, by all routers, on optimal routes.
5. Routing Algo. should also be flexible, which means that they should quickly & accurately adapt to a variety of network circumstances. Assume, for example, a network segment has gone down. As many routing algo become aware of the problem, they will quickly select the next best path for all routes normally using that segment. Routing Algo. can be programmed to adapt to changes in network bandwidth, router queue size and network delay, among other variables.

* Algo. Types : $\rightarrow$

1. Static versus dynamic : $\rightarrow$ Static Routing : $\rightarrow$

Advantage - i) Minimal CPU/Memory overhead

ii) No bandwidth overhead

iii) Granular control on how traffic is routed

Disadvantage - i) Infrastructure changes must be manually adjusted.

ii) No 'dynamic' fault tolerance if a link goes down.

ii) Impractical on large network.

• Advantage of Dynamic Routing

- i) Simpler to configure on large networks.
- ii) Will dynamically choose a diff. route if a link goes down.
- iii) Ability to load balance bet multiple links.

• Disadvantage of Dynamic Routing

- i) Updates are shared bet. routers, thus consuming bandwidth
- ii) Routing protocols put additional load on router CPU/RAM
- iii) The choice of the "best route" is in the hands of the routing protocol and not in the network administrator

2. Single Path versus multipath (NW-35-II)

Some routing protocols support multiple paths to the same destination. Unlike single path, these multipath algorithm permit traffic multiplexing over multiple line. The advantages of multipath algo. is to provide better throughput & reliability. It is generally called Load Sharing.

3. Link State Vs Distance Vector : →

Link-state algo (shortest path first Algo.) flood routing information to all nodes in the internet work. Each router send only the portion of routing table that describe the state of its own links. In link-state Algo. each router builds a picture of the entire network in its routing tables.

Distance vector algo. (Bellman-Ford Algo.) call for each router to send all or some portion of its routing table, but only to its neighbour.

Linkstate Algo send small updates everywhere, while distance vector algo send larger updates only to neighbouring routers. Distance vector algo know only about their neighbours.

* Routing Metrics : →

Routing Algo. have used many diff. metrics to determine the best route. Complex routing algo. can base route selection on multiple metrics, combining them in a single (hybrid) metric. All the following metrics have been used:

1. Path Length: $\rightarrow$ Pathlength is the most common routing metric. Some routing protocols allow network administrators to assign arbitrary cost to each network link. In this case, path length is the sum of cost associated with each link traversed.
2. Reliability: $\rightarrow$
3. Routing Delay: $\rightarrow$ refers to the dependability of each network link.
 $\rightarrow$ refers to the length of time required to move a packet from source to destination through the internet work.
4. Bandwidth: $\rightarrow$ It refers to available traffic capacity of a link.
5. Load: $\rightarrow$ It refers to the degree to which a network resource, such as a router is busy. (N/w-35-III)
6. Communication Cost: $\rightarrow$ It is another important metric, especially because some companies may not care about performance as much as they care about operating expenditures.

Unit-3

(3-1)

* Overview of Internet : →

Internet is a network of networks that links millions of computers around the world. Internet is composed of large number of networks, as it connects many LANs (Local Area Networks) and WANs (Wide Area Networks). For example ARPANET, NSFNET, NASA, BITNET, DECnets etc. are connected to Internet.

In 1969, the ~~Department~~ Department of Defense Advanced Research Projects Agency (ARPA) developed an experimental network called ARPnet to link together four supercomputing centres for military research. From those original four computers, this network converted into Internet, that covers network of millions of computers. (NW-36-1)

In 1984, ARPANET was split into two components: ARPANET, used for research & development & MILNET, used to carry unclassified military traffic. In January 1992, Internet Society (ISOC) was formed with an agreement of providing an institutional home for IETF & Internet standards process. (Internet Research Task Force)

There are millions of computing devices that are connected to this network either permanently or for a short duration. These devices run network applications that communicate through copper wire or fibre optics cables, radio or satellite transmission. The communication is governed by protocols established by an international body - Internet Engineering Task Force.

Internet connectivity is provided by ISP.
These corporations dedicate computers to act as servers — that is they make information available to users of Internet

* Basic Service of Internet : →

- i) File Transfer
- ii) Remote login
- iii) E-mail etc.

* Advantage of Internet : →

- (i) Operates 24 hours.
- (ii) Global Audience
- (iii) Multimedia
- (iv) Communication
- (v) Ocean of Information
- (vi) E-Commerce
- (vii) Provide Technical Support
- (viii) Obtain Customer feedback
- (ix) Product Advertising
- (x) Entertainment etc.

N/W-36-II

* Disadvantage of Internet : →

1. Theft of Personal Information
2. Spamming (sending unwanted mails)
3. Internet Addiction
4. Negative effect on family communication
5. Virus Threat
6. Children using Internet
7. Pornography etc.

(3-3)

* GSP : → GSP (Internet Service Provider) is a company that provides individuals or companies access to Internet & WWW. GSP provides a telephone number, a user name, a password & other connection information so users can connect their computers to the GSP's computers. An GSP typically charges a monthly or hourly connection fee. In the past, most GSP were run by the phone companies. Now-a-days, some individuals & groups with sufficient money & expertise are operating as Internet service providers. (NW-36-3)

The GSP is your only way to access the Internet. There are four classes of GSP: - global, national, regional & local. All regional Internet service providers must route traffic through national Internet service providers. Similarly, all local Internet service providers use a national GSP. National GSP can and There are tiers of service and infrastructure when it comes to moving packets of data around the globe. Depending on what level of service you obtain, you may or may not have to register your Domain.

There are four classes of GSP - global, national, regional, local. Examples of GSP in India - BSNL, VSNL, Sify, Bharti Infotel, Reliance, HCL Infotel, BCN Broad India etc.

* GSP Connection Options : →

A connection to GSP can be established through a modem & telephone line - an ISDN adapter and ISDN line, a cable modem, a digital Subscriber Line or an X.25 network. If you are using a modem, you may want the fastest possible

speed to reduce downloading time while on Internet. ⁽³⁻⁴⁾
A modem of 28.8 kbps or above is recommended. Your
dia-up Internet connection dials the ISP & logs you
onto the system. The actual sequence for logging
on varies based on the requirements of ISP you are
calling and are usually transparent. If you connect
to Internet through DSL or cable modem, your ISP may
offer either an always on connection or require to
log on.

n/w-36-4

Solved Questions

Unit-3

Q.1 What is Internet? What are the basic services provided by Internet? Discuss them in brief?

Ans. Internet is a network of computer networks, which are interconnected with telephone lines and satellites all around the world. Internet is also called simply "Net" is a vast collection of information. Internet connects many LANs and WANs. There are many major networks linked to Internet. Some of these are ARPANET, NSFNET, NASA, BITNET, DECnets etc.

Internet is a public network. It can be accessed and its services can be availed by anyone who gets connected to it. The hyper connectivity feature of World Wide Web makes Internet contents available to the masses.

Following are the basic services/ of Internet:

- **File transfer:** File transfer is a service of Internet and for this it is users FTP protocol and provides FTP utility/tool. On Internet, a user can copy files from his/her computer to a remote computer and vice-versa.
- **Remote login:** Remote login is a service of Internet that facilitates users to logon to a remote computer/site on Internet and use the resources of that computer, as if they are local to him/her. For this, Internet uses Telnet protocol and provides Telnet utility/tool to users.
- **E-mail:** E-mail is the most popular service of Internet, which facilitates users to exchange messages all over the world. For this, it uses different kind of protocols such as SMTP, POP3, IMAP4, MIME etc. Anybody having an e-mail account on any mail-server on the Internet can send and receive mails all around the world on Internet.

NW-36-5

Q.2 What are the basic features of a Web browser?

- Ans. Following are the basic features that a Web browser must possess:
- A Web browser must be able to interpret HTML codes of a Web page.
 - A Web browser should have built in interpreters for interpreting codes, written in scripting language such as VBScript, JavaScript, C++, etc.
 - A Web browser should have the ability to call helper applications to execute (open) files of specific application embedded in a Web page.
 - A Web browser must be able to search websites.
 - A Web browser should be able to send and receive mail-messages.
 - A Web browser must store the Web sites on the local hard disk that have visited a few days or weeks ago. This feature of Web browsers is called History.
 - A Web browser should provide the facility to store the links of favourite Web sites to the user. This feature of a Web browser is called Favourites or Bookmark.
 - A Web browser should have built-in Newsreader program.

* Hosts : →

A host refers to a machine/computer running the user program and TCP/IP protocols. A host may be a server or network to which users can connect and share its resources and utilise as well. Host and local networks are grouped together into domains, which then are grouped together into one or more larger domains. A host name refers to DNS name of device on a network. Host names are used to locate computers on the network. To find another computers, its host name must either appear in the Host file or be known by a DNS server.

* Domains : →

A group of computers that are part of network and share a common directory database is called a domain. A domain is administered as unit with common rules and procedures. Each domain has a unique name. A domain enables the administrator to effectively manage numerous users, resources and devices to keep the administrative tasks relatively simple. A DNS domain is any tree or subtree within the DNS namespace.

* Subdomains : →

A subdomain is a part of domain which may be related to an organisation. On Internet, the computers are arranged in domains under Domain Name System (DNS) hierarchy. DNS is a technology that translates Internet address names into numerical address (IP addresses) so that the address can be found over Internet. For example, if you type www.microsoft.com into web browser, the name is translated into a numerical address and that address is used to connect you to the Microsoft website.

DNS uses a hierarchy to manage its distributed database system of names. The DNS hierarchy is also called name servers that manage portions of a hierarchical namespace. The name servers contain database of Internet's host addresses and the name resolver software translate alphabetic Internet address into numeric IP address. DNS tree has a single node or domain at the top called root domain. Below the root domain are the top-level domains. These domains divide the DNS hierarchy organisationally into following segments.

- .com — Commercial orgn such as IBM (ibm.com)
- .EDU — educational institutions, such as purdue (.purdue.com)
- .MIL — military organisations, such as US Army (army.mil)
- .Gov — Government bodies, such as NASA (nasa.gov)
- .NET — Networking entities such as NSFNET (nsf.net)
- .ORG — for all kinds of orgn.
- .INT — International organisations such as NATO (nato.int)

Additional top level domains organise the domain namespace geographically, for example the top-level domain for India is IN Japan is JP, United Kingdom is UK and France is FR.

Nlw-37

Q. 3 What are the two main purposes for which FTP is used? What are the two different types of FTP services available on Internet? What is the distinguishing factor for these services?

Ans. FTP is used to transfer files from one computer to another on Internet. The two main purposes of FTP are to download and upload applications and other files from the client's computers to servers.

There are two types of FTP services on Internet:

- Anonymous, and ■ Non-anonymous

The anonymous service of FTP is used by those FTP servers that do not require username and password for accessing documents/applications stored on them. The goal of this service is to distribute documents/applications over Internet. This service makes a Web site or some portion of a Web site completely public.

The non-anonymous service of FTP is used by those FTP servers that do require a username and a password for accessing documents/applications stored on them. The goal of this service is to make the documents/application strictly private on the Internet. To avail of anonymous access, a user does not require a username and a password, but for non-anonymous service he/she does require a username and password.

Q. 4 What is the reason for files being compressed when used for downloading on Internet? Which utility is used to decompress these files? What are the two different modes of connections you can open for downloading a file? Give a brief description of each one.

Ans. Files are compressed to reduce their size. Compressed files occupy less space on the secondary storage in comparison to normal ones. On Internet some Websites keep their files compressed. The reason behind compressing files on many Web servers on Internet is to reduce the download time as well as store them in less space on Web servers. In DOS, PKZIP is a utility used to compress files and PKUNZIP utility is used to decompress compressed files. (In Windows WinZip is used to compress and decompress files.) In Unix, Gzip utility is used to compress files and Gunzip is used to decompress compressed files.

The two modes of compression are:

- Lost compression, and ■ Loss-less compression

In Lost Compression some data is lost during the compression process. It is used for compressing picture and graphic files. It is not suitable for data files and text files.

In Lossless Compression data is not lost during the compression of files. Additionally, more than one file can be compressed to form a single small and compressed file.

ASCII mode and Binary mode are the two modes of connections, either of which can be opened for downloading files during FTP session. ASCII mode of connection allows only text files to be transferred between FTP client and FTP server. Binary mode of connection allows binary files such as applications (executable file), picture and graphics files etc. to be transferred between FTP Client and FTP server.

Q. 5

Ans.

Q. 6

Ans.

Q. 7

Ans.

* Web Browsers : →

A Web browser is software used to display Web pages and to navigate Internet. Internet Explorer and Netscape Navigator are popular web browsers. It compiles/runs an HTML document (page) and facilitates you to view Web pages and navigate around World Wide Web. A web browser interprets a Web page written in HTML or translated into HTML by a web server, formats it and displays on the user's computer screen. In early days of WWW, web pages are written in HTML, but now-a-days most web pages are written/developed using Web development languages such as Java, PHP and C++ along with scripting languages such as JavaScript, VB Script and technologies such as ASP.net. A web page written in HTML is directly interpreted by the browser whereas a page written in a Web development language C++ can not be directly interpreted by the browser. In such a case the page is first interpreted by web server and then its equivalent HTML contents are sent to the client/browser. In addition to HTML, the browser can interpret and display information stored in other formats including sound, graphics, Adobe files etc. For this a browsers such as Internet Explorer takes help of helper application.

There are two types of web browsers: - ①. Text only browsers: →

A text only browser can display only text of a web pages. Lynx is a text only Web browser. ② Graphical Web browser: → can display text and multimedia elements such as graphics, images, video, audio and animations of Web pages. Thus they support multimedia aspect of web. Mosaic was the first graphical Web browser.

* Accessing of Web Page by Web Browser: →

① When the address of web page is given to a web browser, it sends a request to web server ② The web server receives the request. The web server processes the requested page and then returns the HTML code for that page to browser, ③ The browser then interprets the HTML code of the requested page sent by web server and displays that web page.

* Usenet : →

Usenet is a large distributed system of message (called articles, posting) involving millions of people all over the world. As so many message are sent everyday they are divided into newsgroup and each newsgroup concentrate on the particular topic - jokes, recipes, mathematics, philosophy, computer, music, movies - all of them on any subject that you can imagine has own group. You can read the newsgroups articles, post replies to articles, Post new articles.

NW-39 Like mailing list you can read articles whenever you want. You can read articles without subscribing to the newsgroup.

* Newsgroup: A service of Internet : →

A Newsgroup is a place where people discuss a subject of common interest. Whether you are curious about what's happening in the news or interested in finding a new recipe for dinner or need help training your dog, there's newsgroup out there for you. People interested in the subject can "subscribe" to the newsgroup. You can find the group by looking or searching through the full list of newsgroup on your system. Subscriber can use a newsreader to read all the articles posted to the newsgroup. People can also post articles to newsgroup. Each article posted to a newsgroup is automatically delivered to entire subscribers. The main difference bet. newsgroup and mailing list is that mailing lists get emailed to certain group of people and message exist only in their mailboxes whereas newsgroup post sent to your news server, which then forwards it to news server around the world.

Introduction to Computer Networks

Q. 5 What is the main purpose of Telnet? What models does Telnet follow? Write in short how does the model operate?

Ans. The main purpose of Telnet is to access and use remote resources on Internet. Remote login and remote access are the services offered by Internet. Internet allows a user to logon to a remote host/server and access the resources of that host (computer) as if they were local to the user.

Telnet follows Client/Server model, wherein a Telnet client requests for resources to a Telnet server and the server authenticates the client and if authenticated, provides the requested resources.

Telnet is a utility and a protocol too of Application Layer of TCP/IP model that enables a user to logon remotely on a remote machine (computer) /site and access/utilise the resources stored on that computer.

When a user logon to remote computer (actually a remote telnet server) using a Telnet client (a program) and types the commands on his/her local computer, those commands are accepted by the local operating system but are not interpreted. Rather, they are sent to the Telnet Client on local operating system. The Telnet Client translates those commands into Network Virtual Characters (NVCs) and then are delivered to the local TCP/IP stack. Further these NVCs travel on Internet and reaches to the TCP/IP stack of remote host/computer (actually Telnet server) where they are delivered to the operating system and then the operating system passes them to the Telnet server.

Q. 6 Write short notes on: (i) Terminal Emulation (ii) Daemons

Ans. ■ **Terminal Emulation:** Terminal Emulation is a mechanism that makes a PC (Personal Computer) acts like a computer terminal. This technique is used to logon to a Telnet server and work with a computer acting as VT100 terminal which is connected via telephone line to the Internet. Terminal Emulators do not allow accessing of graphic and video on World Wide Web. Thus they are suitable to browse only the text portion of Web.

■ **Daemons:** Daemons are system programs that keep running in the background of an operating system as processes. Actually, the term "daemon" comes from Unix and is now applied in all operating systems system programs that run as processes in the background on a computer system. *lpshd* and *crontab* are a few examples of the daemons of Unix. Daemons perform specified tasks and respond when some events occur in the system.

N/W-40

Q. 7 What are the two different types of newsgroups? Explain them briefly.

Ans. There are two types of Newsgroups:

- Moderated Newsgroups, and
- Un-moderated Newsgroups

* Working of Usenet : →

Usenet works on client-server model. Therefore, there are two main components of Usenet — ① News Server ② News reader. The articles posted on newsgroup are distributed over Internet by News Server. The News Server store and forward the articles to the users. A user needs a News Reader program (act as client software) to read these articles. News Reader and news servers communicate by using a protocol called Network News Transfer Protocol (NNTP).

* Hierarchies of Newsgroup : →

The number of newsgroups on the Usenet is so large that they are arranged in hierarchy to make them manageable. Like regular domain names they also have dots separating the different part of their hierarchy. One example of this is the newsgroup ric.art.books. In the hierarchy of Usenet's newsgroups, the major topic comes first; followed by a subtopic. A subtopic can be further subdivided. A Newsgroup can be identified by its name. e.g. Comp is for discussion on computer-related topics.

Sci is for discussion on scientific topics.

Soc is for discussion on social topics.

Ric is for recreation (arts)

Category	what it includes
sci	science (PCM, engineering, medicine)
bionet	biology (the biology network)
comp	Computers (hw, operating system, programming)
biz	business (business news, marketing, advertising)
k12	K-12 education
talk	debate (politics, unusual religions)
misc	miscellaneous (investments, jobs, transportation)
alt	alternative thinking on thousands of topic.
can	Canada (Canadian events, opinions and persons)
uk	United Kingdom.
microsoft	Microsoft's url
news	announcements about newsgroups, analysis of newsgroup.

* Subscribing to Newsgroup : →

You can find out list of newsgroup offered by a website by visiting it. If you enjoy a newsgroup, subscribe to it. The subscription is free. A website does not provide you access to all the newsgroup. Once you get a list of newsgroup offered by website, you can read the message. To participate in newsgroup: —

- ① First you need a news reader program. Both Internet Explorer and Netscape Navigator have built-in-news reader program.
- ② Determine which newsgroup interest you.
- ③ Subscribe to the interested group. e.g. - ① Enter the URL of yahoogroup - <http://groups.yahoo.com> ② The yahoo group page appears. ③ Type a topic in the search box and then click the search button. For example, type computer in the search box and then click search button. The search result page will be displayed. ④ On the search result page select the group, which you want to join. ⑤ Select an article to read it. Read the message and if you want to post a follow up message, click on the hyperlink. Post message at end.

A moderated newsgroup is that in which a human moderator check the incoming messages to ensure whether message is up to the standard for that particular newsgroup or not. If a message meets the standard, the human moderator posts that message to a group; otherwise he/she discards that message.

An un-moderated newsgroup is that in which all the incoming messages are automatically posted and are distributed by Usenet servers to other newsgroups (sites).

(c)

Q. 8 Define the following terms:

- (i) Usenet (ii) IRC (iii) NetMeeting

Ans.

- **Usenet:** Usenet is the World's largest electronic discussion forum connecting a thousand of Usenet servers. Usenet provides a way for messages to be sent among computers across the entire Internet. Actually, Usenet is a Bulletin Board Service of Internet, in which messages/articles are organised into thousands of newsgroups, which cover specific areas of internet.
- **IRC:** IRC stands for Internet Relay Chat. It is a kind of Chatting service of Internet, which is provided by channels live on many IRC servers. IRC is a client/server network, where a user can logon to a chat server using IRC client software such as MIRC. After login-on, a chat server user has to select a channel on which he/she wants to chat. The command/message typed by the user is sent to IRC server by IRC client software.
- **Netmeeting:** Conducting on-line virtual meeting with anyone like videoconferencing is called Netmeeting. The Netmeeting allows transmission of audio, video, graphics and text (data) between the hosts (computers or user). In Netmeeting people talk face to face using video cameras called Web camera connected to computer with Internet facility. In Windows operating system, Netmeeting is the utility which facilitates people to conduct netmeeting on Internet.

Q. 10
Ans.

Q. 9 Write short notes on any three of the following:

- (a) List Server (b) E-mail (c) Internet Explorer

Ans.

- (a) **List Server:** A List Server is an automatic mailing system available on the Internet. A mailing list connects a group of people who are interested in a common topic. When a person sends an e-mail to the mailing list, that e-mail is sent to every person who belong to that mailing list.
In List Server, everyone gets every message that everyone sends to it.
- (b) **E-mail:** Electronic Mail (E-mail) is one of the popular services of Internet. It's a system of Internet for transferring messages among users, who have e-mail IDs on mail servers on Internet. The e-mail system uses SMTP protocol alongwith MIME for sending mails from e-mail clients (users) to mail servers. However, POP3 or IMAP4

Q. 11
Ans.

* Creating a dial-up connection : →

To create a dial up connection, follow these steps : →

1. Click Start, click Control Panel, click Network and Internet Connection and then click Network Connection.
2. Under Network Tasks, click Create a new connection. It will launch the Welcome page of New Connection Wizard.
3. On the Welcome page click Next.
4. On the Network Connection Type selection page select the option, Connect to Internet at my workplace and then click Next.
5. On the Network Connection Page select Dial-up connection and click Next.
6. On the Network Connection Page type the name of your connection to be created in the Company Name box and then click Next.
7. On the Phone Number to Dial page, type the number that your connection and modem will use to dial and then click Next.
8. In the final step, check/select the option Add a shortcut to my desktop. If you want to create a shortcut for the dial-up connection; you are creating to place on the Desktop for easy access. Finally, click on Finish button.

* Configuring a Modem for a Dial-Up connection : →

To configure a modem for a dial-up connection, follow these steps.

1. Click Start, click Control Panel, click Network and Internet Connections and then click Network connection.
2. Click the dial-up connection you want to configure and then under Network Tasks, click Change setting of this connection.
3. On the General tab, under connect using, click the modem you want to configure, and then click configure.
4. Under Hardware Features, select the check box option you want to enable. N/W-43
5. If you want to enable the modem speaker, select the Enable modem-speaker check box.
6. When you have done, click OK and then click Apply.

Introduction to Computer Networks

protocol is used for delivering mails to the mail clients (users). As it is a service of Internet, it also uses TCP and IP for packaging messages into packets and routing them to the destination respectively.

With the help of this service (e-mail) of Internet a person having an e-mail account can send his/her message to anyone in any corner of the world, not only within a few seconds but also with acknowledgment.

- (c) **Internet Explorer:** Internet Explorer (IE) is the Web Browser developed by Microsoft. Its current version is IE (6.0). IE is a graphical Web Browser that enables a user to explore the World Wide Web, send and receive e-mails, participates in newsgroups, etc.

IE (6.0) is able to interpret and display HTML pages, ASP pages written in VBScripts, C#, VB.Net, and JSP pages written in JavaScript.

Internet Explorer invokes helper applications to execute application-specific files embedded in a Web page. For example, it invokes Acrobat Reader to open PDF files embedded in a Web page as links.

Q. 10. Differentiate between private and public FTP servers.

Ans. There are two types of FTP servers on Internet: Anonymous FTP servers and Non-Anonymous FTP servers.

Anonymous FTP servers are public FTP servers because anyone with his/her e-mail address can logon to them. The documents and files on an anonymous FTP server are kept in public directory; so anyone can access and download them on the Internet.

Non-anonymous FTP servers are also known as private FTP servers; because a user requires a user name on a non-anonymous server. The username and password are assigned by the system administrator of the FTP sever to the user. A user having a valid account (a username and a password) can upload and download files to and from a non-anonymous FTP server.

Q. 11 What is URL? How absolute and relative URLs differ?

Ans. URL (Uniform Resource Locator) refers to a unique address of a resource such as a Web document on the Web.

A URL consists of four parts:

- Method ■ Hostname ■ Port, and ■ Path

The first part of URL is written before a colon (:), which specifies the access method. On the Web, it is usually HTTP. But, FTP or Gopher may be specified. The host name is the second part of the URL, written after colon (:) and preceded by two front slashes (//), which is optional and the path specifies the location of resource/document that is stored on the server. For example, in the URL,

<http://www.pcguide.com/ref/mbsys/index.html>

http: is the name of access method **www.pcguide.com** is the host name or name of

N/W-44

* Configuring TCP/IP for Automatic Addressing : →

To configure TCP/IP for automatic addressing, follow these steps:-

1. Click Start, point to setting and then click Network and dial-up connections.
2. Right click the network connection that you want to configure and then click Properties.
3. On the General tab or the Networking tab, click Internet Protocol (TCP/IP) and then click Properties.
4. Click Obtain an IP address automatically and then click OK.

* Connecting to Internet : →

To connect to Internet through Dial-up networking, follow these steps:-

1. Double click on the dial-up connection icon in the Network Connections window. It will launch the Connect connection to dialog box.
2. In the Username box, enter the username, which is provided by the ISP and in the Password box, enter the password of user account. Make sure that modem is ~~connected~~ connected to your PC and switched on as well.
3. Click on Dial button to connect to your ISP. It will launch the connecting connection to -- dialog box. The phone no. you have specified in the New Connection Wizard will be dialed and after a few seconds the connection is made with ISP server. When you PC gets connected to Internet, an icon appears on the notification area of the Taskbar indicating that you are connected to Internet.
4. Now you can launch Internet Explorer to surf the Internet. You can launch Internet Explorer by selecting Internet Explorer from Start menu.

* Search Engine Working : →

A search engine has three major elements. First is the spider, also called the crawler. The spider visit a web page, reads it and then follows links to other pages within the site. This is what it means when someone refers to a site being spidered or crawled. The spider returns to the site on a regular basis, such as every month or two, to look for changes.

Everything the spider finds goes into the second part of search engine, the index. The index, sometimes called catalog, is like a giant book containing a copy of every web page that spider finds. If a web page changes, then this book is updated with new information.

The search engine also is the third part of search engine. This is the program that shifts through the millions of pages recorded in the index to find matches to a search and rank them in order of what it believes is most relevant.

(N/w-45)

Unit - 4

* Audio on Internet : —> Traditional uses of audio on the internet depend on conventional transfer techniques. That is, an audio file must be downloaded from a server, usually via FTP, Gopher or electronic mail, before listening it. Because of this time lapse limitation, audio content providers have used Internet servers mainly as centrally located storage devices that can be accessed worldwide.

Internet telephony, radio broadcasts and tele/videoconferencing are the different form of audio & these different form take place on the internet. The audio functions that work across networks, such as telephony, broadcast audio/video and teleconferencing, are dependent also on sufficient bandwidth for success. The advantage of internet-based telephony & videoconferencing is economic. For the same relatively low price one pays for internet access, bypassing, long-distance phone rates.

① Common Audio File format : —>

- i) AAC (Advanced Audio Coding)
- ii) AIFF (Audio Interchange File Format)
- iii) AVI (Audio/Video Interleaved)
- iv) MIDI (Musical Instrument Digital Interface)
- v) MP3 (MPEG1, Audio Layer 3)
- vi) WMA (Windows Media Audio) etc.

N/W - 46

* Intranet : —> Intranet is an application of internet technology inside an organisation. Internet is a network of network. Extranet is an Internet of Intranet.

Intranet can be defined as an "internal Internet" - network of an office, company, university or college or even a large library that runs on IP protocols. An intranet is a private network that is contained within an enterprise. It may consist of many interlinked LAN and also use leased lines in the Wide Area Network.

The Intranet is a Web-based architecture used for managing internal information. Another definition can be given as Intranet is an organisation's internal information system that uses Internet tools, protocols & technology.

① Characteristics of Intranet : —>

- i) Controlled access ; ii) Shared access to documents
- iii) Centralised scheduling system, iv) Individualisation v) Scalable
- vi) Open vii) Standard-based.

② Advantage & Disadvantage of Intranet : →

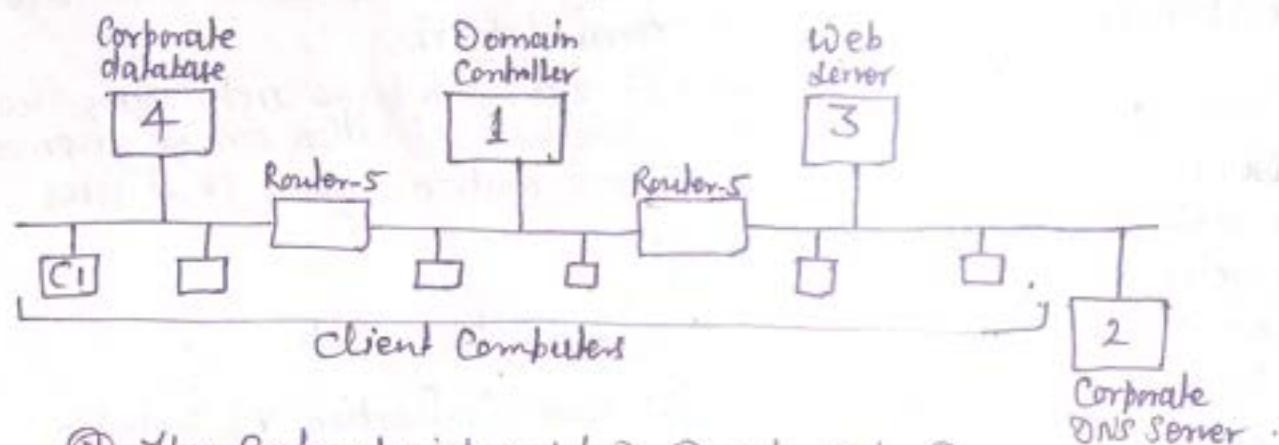
- | | |
|-----------------------------|--|
| i) Replacing Hard Copies | iii) Promoting Employee Self-sufficiency |
| ii) Reducing Content Search | iv) Keeping Knowledge within the Orgn. |
| iv) Easy to use | vi) Cost Affective |
| vii) Communication | viii) Business Operations & Mgt. |

③ Demerits : →

- i) Security features can be inadequate.
- ii) Maintaining content can be time consuming.
- iii) Inadequate system performance management & poor user support
- iv) The aims of the orgn in developing intranet may not align with user needs.

(N/W-47)

* Building Corporate Wide Web : → A corporate Web-app. is a corporate information system that uses World Wide Web technology to provide easy access to a wide variety of corporate information resources for internal & external users on different kinds of platforms in geographically distributed locations. Corporate Web applications serve a specific set of business objectives & provide a presence on World Wide Web. There are two approaches to web application development: top-down & evolutionary. Evolutionary development approach is exploratory & appropriate for learning about technology & the application domain. However the evolutionary development leads to complex applications that are difficult to use & equally difficult to maintain. Top-down development approach organises the complexity of these applications & produces applications that can meet business objectives, be developed by a programming team and be maintained by the people other than developers.



④ The Corporate intranet / World wide Web. ⑤

* Intranet Infrastructure : —>

Q. What are the main issues that must be considered while planning the infrastructure of Intranet.

Ans. While planning the infrastructure for Intranet, the following issues must be taken care of:

- The first issue is to understand exactly what you are being asked to build. Intranet mean different things to different organisations, and even to different people within the same organisation. Before you start to build the unifying piece that bring your Intranet together, you need to know whether you have to develop your Intranet for dashboard, file repository, collaboration or corkboard. Your intranet may be a combination of above. The key is to understand what you want your intranet site to do and what you know it shouldn't do.
- Navigation of Intranet site is one of the most important components of Intranet. This is important because of diverse components of Intranet & varying needs of the users. NLW-48
- Once your site has become functional, you are likely to get hit with a no. of well-meaning comments indicating that the site doesn't look right. This can be caused by difference in the colours & fonts within a site or across multiple sites in Intranet.
- The most critical issues for building Intranet are not technical, or even organisational. Business issues are the primary hurdles to a successful intranet.

* Intranet Architecture : —> Intranet architecture is something bet. mainframes and widely widespread client-server architecture. In Intranet, a client part of system is Internet-browser. In intranet architecture, the client refers to weak. In most cases use of a browser is not enough than by opportunities differ from application of terminal with the system of commands. Weakness of client forces to place logic of the application on a server. Actually, for realisation not only system of submission of the information is required to finish essentially functioning of standard Web-server, but also transforming it in application server. This server also is the heart of all Intranet-architecture.

* Intranet as a business tool : → Intranet is the best communication tool for a company. If it is used properly, it can improve performance, job satisfaction, communication and knowledge transfer bet. the teams. In order to extract full value, your intranet needs to be driven & supported by all teams within a company.

Developing Intranet that increases performance and productivity, support staff on daily basis & boosts your internal communication across the whole orgn is fast becoming a key business strategy. However, many organisations find themselves running Intranet that, after years of uncontrolled growth, could do more for business ~~and~~ and are unclear as to how the intranet can reach its full potential or are unaware of challenges they face if they embark upon a process of change.

* Future of Intranet : → Nlw-49 Nowadays each & every orgn talks about co-ordination, cooperation & collaboration and these all can be achieved through Intranet Technologies. Intranet trends follow closely the latest Internet trends. As Internet technology expands, then it follows that Intranets must necessarily benefit from these advances since the technology is shared.

Many of Web-sites are fueled by Web 2.0 principles. Web 2.0 is all about social media & user-generated content as opposed to static, read-only nature of Web 1.0. It explains the explosion of blogs, the dominance of Wikipedia and popularity of online social networking sites like MySpace, Facebook etc.

Corporate Intranets will take on increasing importance as more & more businesses turn to Web-based applications to manage core business system like SAP & PeopleSoft. Companies are learning that on-demand Web service are cheaper to maintain & easier to use than hosting usw on their own systems. All of these Web based applications can be bundled into corporate Intranet where they can be accessed securely with one network password.

* Intranet Security Design : →

Following are the techniques used for intranet security : —

- ① Encryption : → One technique used in protecting sensitive info. such as password, user ID and human resource files is encryption. "Cryptography refers to processes, art and science of keeping messages & data secure. Cryptography is used to enable and ensure confidentiality, data integrity, authentication. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords & electronic commerce which all depend on cryptography.
- ② Authentication : → Authentication means establishing verification of identity bet. two or more entities. There are three categories of authentication used in Intranet: User-to-Host Authentication, Host to Host Authentication & User-to-user Authentication.
- ③ Firewalls : → A firewall is a combination of h/w & s/w that is built using routers, servers & variety of s/w's. It is installed bet. Internet & the internal network to secure the internal network from intruders & sniffers. It tries to filter harmful traffic bet. & the internal network. It inspects each packets passing through it & decides whether to allow the packet. (N/w-S/W)

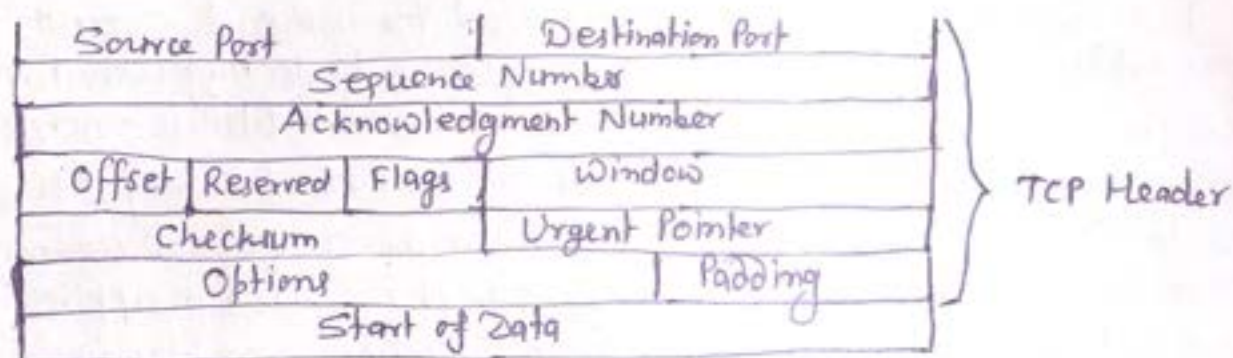
* Fundamental of TCP/IP : →

Transmission Control Protocol/Internet Protocol and its related networking protocol are the fundamental technology that has enabled the growth of global Internet and the current move toward corporate.

① Benefits of Using TCP/IP : →

1. TCP/IP is a routable protocol, which means it can send datagrams over a specific route, thus reducing traffic on other parts of network.
2. TCP/IP has reliable & efficient data-delivery mechanism.
3. TCP/IP is separated from the underlying h/w & will run over Ethernet, Token Ring or X-25 networks & even over dial-up telephone lines.
4. TCP/IP can send data bet. different computer system running completely different operating system, from small PCs all the way to mainframes & everything in between.

① Using the Transmission Control Protocol : →

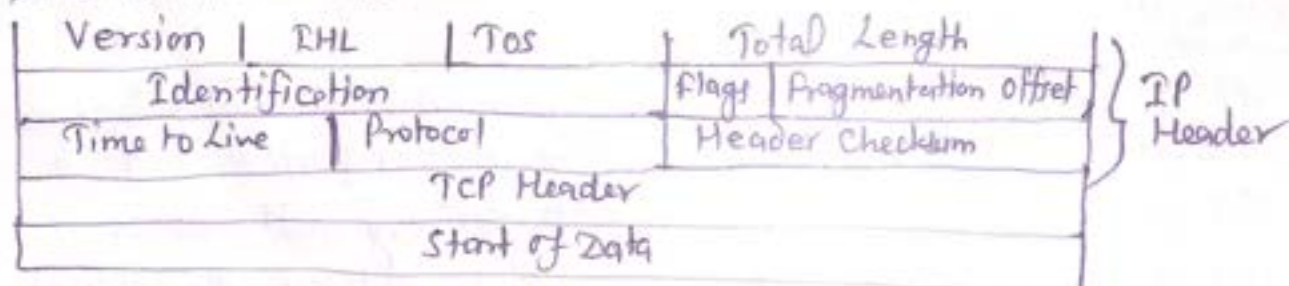


A datagram with its TCP header

In addition to the source & destination port number, the sequence number and the checksum, a TCP header contains the following information:-

- Acknowledgement Number : → Indicates that the data was received successfully.
- Offset : → Specifies the length of header.
- Reserved : → Indicates variables set aside for future use.
- Flags : → Indicates that this packet is the end of data or that the data is urgent. (N/w-51)
- Window : → Provides a way to increase packet size, which improves efficiency in data ~~is urgent~~ transfer.
- Urgent Pointer : → Gives the location of urgent data.
- Options : → Indicates a set of variables reserved for future use.
- Padding : → Ensures that the header ends on a 32-bit boundary.

② Using the Internet Protocol : → The Network layer portion of TCP/IP is called Internet Protocol. This is what actually moves the data from Point A to Point B, a process that is referred to as routing. IP is connectionless.



The main contents of the IP header are the source & destination addresses, the protocol number & checksum.

- TOS : → Indicates the type of service.
- Total Length : → Specifies the total length of datagram.
- Identification : → Provides information that receiving system can use to reassemble fragmented datagrams.
- Flags : → Specifies, using the first flag bit, that datagram should not be fragmented, the second flag bit indicates that datagram is the last of a fragmented packet.
- Fragmentation Offset : → Indicates the original position of data & is used during reassembly.
- Time to Live : → Originally indicated the time in seconds that the datagram could be in transit.
- Protocol : → Identifies the protocol type.
- Header Checksum : → Specifies an error-checking value.
- TCP Header : → Indicate the header added by the TCP part of the protocol suite.

* Protocols of Communication : →

A communication protocol is a set of standard rules for data representation, signaling, authentication & error detection required to send information over a communication channel. Communication protocols follow certain rules so that the system works properly.

The fundamental Internet protocols that led to the success of Internet are 1) TCP/IP, the set of open networking protocols. 2) HTML, the standard document markup language that defines how text, images & sound are presented to a user. 3) HTTP, the hypertext transfer protocol created to deliver HTML documents via the Internet. 4) SMTP, the protocol that enabled basic text-based electronic messaging bet. users. ARP operates at Data Link Layer. IP & ICMP operate at Network Layer & UDP & TCP operate at Transport Layer. All these protocols are examples of communication protocols.

RAM-RAM Q.