ASSIGNMENT-2

DATA COMMUNICATIONS

PUNNYA .S .S

1. What are the different types of networks?

A computer network can be categorized by their size. A computer network is mainly of four types:

- LAN(Local Area Network)

Local Area Network is a group of computers connected to each other in a small area such as building, office. It is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc. It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and Ethernet cables. The data is transferred at an extremely faster rate in Local Area Network. Local Area Network provides higher security.

- PAN(Personal Area Network)

Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters. The devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

- MAN(Metropolitan Area Network)

A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network. Government agencies use MAN to connect to the citizens and private industries. In MAN, various LANs are connected to each other through a telephone exchange line. It has a higher range than Local Area Network

- WAN(Wide Area Network)

A Wide Area Network is a network that extends over a large geographical area such as states or countries. It spans over a large geographical area through a telephone line, fibre optic cable or satellite links. The internet is one of the biggest WAN in the world. A Wide Area Network is widely used in the field of Business, government, and education.

2. Explain the Shielded twisted pair (STP) and Unshielded twisted pair(UTP)

- UTP Cable

Unshielded twisted-pair (UTP) cable is the most prevalent type of telecommunication medium in use today. Its frequency range is suitable for transmitting both data and voice. Therefore, these are most commonly used in telephone systems.

A twisted pair consists of two insulated conductors (usually copper) in a twisted configuration. Color bands are used in plastic insulation for identification. In addition, colors also identify the specific conductors in a cable and to indicate which wires belong in pairs and how they relate to other pairs in a larger bundle.

UTP cableThe two wires are twisted in the twisted pair cable which significantly reduces the noise generated by the external source. The noise here we are talking about is generated when two wires are parallel which causes an increase in voltage level in the wire closest to the source and also uneven load and damaged signal.

- STP Cable

Shielded twisted-pair (STP) cable has an additional braided mesh coating or metal foil that wraps each set of insulated conductors. The metal casing intercepts the penetration of electromagnetic noise. It also can eradicate a phenomenon called crosstalk, which is the unwanted effect of one circuit (or channel) on another circuit (or channel).

STP cableIt occurs when one line (acting as a kind of receiving antenna) picks up some of the signals travelling down another line (acting as a kind of sending antenna). This effect can be experienced during telephone conversations when one can hear other conversations in the background. Shielding each pair of a twisted-pair cable can eliminate most crosstalk.

STP has the similar quality factor and uses the same connectors as UTP, but the shield must be connected to the ground.

3. What is difference between baseband and broadband transmission?

The baseband and broadband are the types of signalling techniques. These terminologies were developed to categorise different types of signals depending on particular kind of signal formats or modulation technique.

The prior difference between baseband transmission and broadband transmission is that in the baseband transmission the whole bandwidth of the cable is utilized by a single signal. Conversely, in the broadband transmission, multiple signals are sent on multiple frequencies simultaneously using a single channel.

- Baseband transmission utilizes digital signalling while broadband transmission uses analog signalling.
- Bus and tree topologies, both work well with the broadband transmission. On the other hand, for the baseband transmission bus topology is suitable.
- Baseband involves manchester and differential manchester encoding. In contrast, broadband does not make use of any digital encoding instead it uses PSK (Phase shift keying) encoding.
- The signals can be travelled in both the direction in baseband transmission whereas in broadband transmission the signals can travel in only one direction.
- In baseband transmission, the signals cover shorter distances because at higher frequencies the attenuation is most pronounced which make a signal to travel short distances without reducing its power. As against, in broadband signals, the signals can be travelled at longer distances.

4. What is the difference between a hub, modem, router and a switch?

- Modem:

Modem stands for "modulating-demodulating". Modems are hardware devices that allow a computer or another device, such as a router or switch, to connect to the Internet. They convert or "modulate" an analog signal from a telephone or cable wire to digital data (1s and 0s) that a computer can recognize. It Simply send traffic from point A to point B without further manipulation.

- Routers:

  Routers are responsible for sending data from one network to another. It works at Layer 3 (Network) of the OSI model, which deals with IP addresses. Typically, routers today will perform the functionality of both a router and a switch - that is, the router will have multiple Ethernet ports that devices can plug into.
- Switches:

  They use the MAC address of a device to send data only to the port the destination device is plugged into. Work at Layer 2 (Data Link) of the OSI model, which deals with MAC addresses.

- Hubs:

  Unlike switches, hubs broadcast data to all ports, which is inefficient. So hubs are basically a multiport repeaters.

5. When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?

Yes, that's because MAC addresses are hard-wired into the NIC circuitry, not the PC. This also means that a PC can have a different MAC address when another one replaced the NIC card. An NIC is the core piece of hardware used for networking connectivity. While traditionally associated with PCs, laptops, and servers, NICs can exist in almost any networked device including printers, telephones, and scanners.

6. When troubleshooting computer network problems, what common hardware-related problems can occur?

A large percentage of a network is made up of hardware. Problems in these areas can range from malfunctioning hard drives, broken NICs and even hardware startups. Incorrectly hardware configuration is also one of those culprits to look into.some other hardwae-related problems include

- Slow Connectivity:

  If there's one thing that frustrates an employee then it's slow connectivity over a network. PCs can grind to a halt and even the simplest task can take an age to complete. It's often caused by large file transfers, so a limit should be put in place on the size that is permitted e.g. no email attachments that total more than 20mb as a standard rule. Sometimes this lag can also be caused by faulty network cards, so it's important to investigate this possibility.
- IP Conflicts:

  Each PC on your network should have a unique IP address such as 209.85.255.255, but sometimes two PCs can be assigned the same IP address. And this can create major connectivity issues for both parties. Sometimes these conflicts will work themselves out, but you can help speed up the process. Restarting the router is the simplest approach as it should assign new IP addresses to every PC on the network.

- Unable to Connect to Local Printer:

  Printers on a network tend to be shared by multiple users, but occasionally an error can arise that leaves people unable to access the printer. This problem is often caused by a sharing issue whereby different security settings between PCs and the printers fail to agree with each other. When this occurs it's recommended that you check firewall settings and that your Windows network adapters have printer sharing enabled.

- Faulty Cables:

  A computer network relies on cables to facilitate its connectivity. And when just one cable fails it can have massive implications for your network. However, it's easy to overlook cables as the source of network issues. People tend to concentrate on software and hardware

troubleshooting first. Nonetheless, investigating the condition of cables in the affected network area is vital. Cables can easily become dislodged or damaged, so sometimes the fix can be as simple as plugging them back in or replacing.

- Weak Wi-Fi Signal:

  If you rely on wireless connections in your organization then you will be well aware of the issues caused a weak signal. This can often be caused by environmental issues such as the presence of a microwave or even the layout of an office. It's important to eliminate these factors to identify the cause of the fault. Alternatively the connection issues could be caused by out-dated firmware, so make sure all updates are installed

7. In a network that contains two servers and twenty workstations, where is the best place to install an Anti-virus program?

An anti-virus program must be installed on all servers and workstations to ensure protection.

That's because individual users can access any workstation and introduce a computer virus when plugging in their removable hard drives or flash drives.

8. Define Static IP and Dynamic IP? Discuss the difference between IPV4 and IPV6.

- Static IP address

A static IP address is simply an address that doesn't change. Once your device is assigned a static IP address, that number typically stays the same until the device is decommissioned or your network architecture changes. Static IP addresses generally are used by servers or other important equipment. Static IP addresses are assigned by Internet Service Providers (ISPs).

- Dynamic Internet Protocol

A dynamic Internet Protocol address (dynamic IP address) is a temporary IP address that is assigned to a computing device or node when it's connected to a network. A dynamic IP address is an automatically configured IP address assigned by a DHCP server to every new network node.

- Difference between IPV4 and IPV6.
  a) IPv4 is 32-Bit IP address whereas IPv6 is a 128-Bit IP address.
  b) IPv4 is a numeric addressing method whereas IPv6 is an alphanumeric addressing method.
  c) IPv4 binary bits are separated by a dot(.) whereas IPv6 binary bits are separated by a colon(:).
  d) IPv4 offers 12 header fields whereas IPv6 offers 8 header fields.
  e) IPv4 supports broadcast whereas IPv6 doesn't support broadcast.
  f) IPv4 has checksum fields while IPv6 doesn't have checksum fields
  g) IPv4 supports VLSM (Virtual Length Subnet Mask) whereas IPv6 doesn't support VLSM.
  h) IPv4 uses ARP (Address Resolution Protocol) to map to MAC address whereas IPv6 uses NDP (Neighbour Discovery Protocol) to map to MAC address.

9. Discuss TCP/IP model in detail.

TCP/IP Model helps you to determine how a specific computer should be connected to the internet and how data should be transmitted between them. It helps you to create a virtual network when multiple computer networks are connected together. The purpose of TCP/IP model is to allow communication over large distances. TCP/IP stands for Transmission Control Protocol/ Internet Protocol. TCP/IP Protocol Stack is specifically designed as a model to offer highly reliable and end-to-end byte stream over an unreliable internetwork.

TCP/IP is a layered server architecture system in which each layer is defined according to a specific function to perform. All these four TCP/IP layers work collaboratively to transmit the data from one layer to another.

- ❖ Application Layer

Application layer interacts with an application program, which is the highest level of OSI model. The application layer is the OSI layer, which is closest to the end-user. It means the OSI application layer allows users to interact with other software application.

- Transport Layer

Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system. It is hosted using single or multiple networks, and also maintains the quality of service functions.It determines how much data should be sent where and at what rate. This layer builds on the message which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence.

- Internet Layer

An internet layer is a second layer of TCP/IP layes of the TCP/IP model. It is also known as a network layer. The main work of this layer is to send the packets from any network, and any computer still they reach the destination irrespective of the route they take.

- Network Interface

This layer is also called a network access layer. It helps you to define details of how data should be sent using the network. It also includes how bits should optically be signalled by hardware device which directly interfaces with a network medium, like coaxial, optical, coaxial, fiber, or twisted-pair cables.

10. What is a Web Browser (Browser)? Give some example of browsers.

A web browser, or simply "browser," is an application used to access and view websites. Common web browsers include Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

The primary function of a web browser is to render HTML, the code used to design or "mark up" webpages. Each time a browser loads

a web page, it processes the HTML, which may include text, links, and references to images and other items, such as cascading style sheets and JavaScript functions. The browser processes these items, then renders them in the browser window.

11. What is a search engine? Give example.

A search engine is a web-based tool that enables users to locate information on the World Wide Web. Popular examples of search engines are Google, Yahoo!, and MSN Search. Search engines utilize automated software applications (referred to as robots, bots, or spiders) that travel along the Web, following links from page to page, site to site. The information gathered by the spiders is used to create a searchable index of the Web.

12. What is the Internet & WWW? What are the uses of internet in our daily life?

The Internet is a vast network that connects computers all over the world. Through the Internet, people can share information and communicate from anywhere with an Internet connection. Internet is referred to as a "network of networks," It supports access to digital information by many applications, including the World Wide Web. The Internet has proved to be a spawning ground for a large and growing number of "e-businesses" that carry out most of their sales and services over the Internet.

The World Wide Web (WWW), commonly known as the Web, is an information system where documents and other web resources are identified by Uniform Resource Locators which may be interlinked by hyperlinks, and are accessible over the Internet. The resources of the Web are transferred via the Hypertext Transfer Protocol (HTTP), may be accessed by users by a software application called a web browser, and are published by a software application called a web server. The World Wide Web is not synonymous with the Internet, which pre-dated the Web in some form by over two decades and upon which technologies the Web is built.

There are many uses of the internet, however, the use of the internet in our daily life depends on individual requirements and goals.

- Uses of the Internet in Education.
- Internet Use to Speed Up Daily Tasks.
- Use of the Internet for Shopping.
- Internet for Research & Development.
- Digital Transactions.
- Money Management

13. What is an Internet Service Provider? Give some example of ISP in India.

Company that provides Internet connections and services to individuals and organizations. In addition to providing access to the Internet, ISPs may also provide software packages (such as browsers), e-mail accounts, and a personal Web site or home page. ISPs can host Web sites for businesses and can also build the Web sites themselves. ISPs are all connected to each other through network access points, public network facilities on the Internet backbone. Examples of ISP are- airtel, BSNL,Idea etc.

14. Discuss the difference between MAC address, IP address and Port address.

- MAC address

A Media Access Control address is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. This use is common in most IEEE 802 networking technologies. Within the Open Systems Interconnection (OSI) network model, MAC addresses are used in the medium access control protocol sublayer of the data link layer. As typically represented, MAC addresses are recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator.

- IP address

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.[1][2] An IP address serves two main functions: host or network interface identification and location addressing. IP Address is either four byte (IPv4) or eight byte (IPv6) address.

- Port address

A port is identified for each transport protocol and address combination by a 16-bit unsigned number, known as the port number. The most common transport protocols that use port numbers are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

SL.No	IP address	MAC address	Port address
1	Internet Protocol address (IP address) used to identify a host in network.	Media Access Control Address (MAC Address) helps in simply identifying the device.	Port number is used to identify processes/services on your system
2	IPv4 is of 32 bits (4 bytes) size and for IPv6 is 128 bits (16 bytes).	MAC Address is a six byte hexadecimal address.	The Port number is 16 bits numbers.
3	IP address is the address of the layer-3 IP protocol.	MAC Address operates in the data link layer.	Port number is the address of the layer-4 protocols.
4	IP address is provided by admin of system or network administrator.	NIC Card's Manufacturer provides the MAC Address.	Port number for application is provided by kernel of Operating System.
5	ipconfig command can be used to find IP address .	ipconfig command can be used	netstat command can be used to find Network Statistics Including Available TCP Ports.

6	IP address identify a host/computer on a computer network.	MAC Address helps in simply identifying the device.	Port numbers are logical interfaces used by communication protocols.

15. How do we view my Internet browser's history?

To view your browsing history in Chrome

In any Chrome window, use the keyboard shortcut Ctrl+H, or navigate to the URL chrome://history . Or, click the Menu button, which is located near the top-right side of the browser window, and choose History, then History again.