“Data Communications.”

Assignment work submitted in partial fulfillment of the requirement for the

Certificate in Computer Application {CCA}

By Longmilan Challam

Email: longmilan26@gmail.com

Phone: 9485182126

CSC ID: 645426570012

DATA COMMMUNICATIONS

1. What are the different types of networks?

Ans. A computer network is a cluster of computers over a shared communication path that works for the purpose of sharing resources from one computer to another, provided by or located on the network nodes.

The different types of computer networks are discussed as follows:

1) Local Area Network (LAN): LAN is the most frequently used network. A LAN is a computer network that connects computers together through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-Fi.

Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.

2) Wireless Local Area Network (WLAN): WLAN is a type of computer network that acts as a local area network but makes use of wireless network technology like Wi-Fi. This network doesn't allow devices to communicate over physical cables like in LAN but allows devices to communicate wirelessly. The most common example of WLAN is Wi-Fi.

3) Wide Area Network (WAN): WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other. The most common example of WAN is the Internet.

4) Personal Area Network (PAN): PAN is the most basic type of computer network. This network is restrained to a single person, that is, communication between the computer devices is centred only to an individual's work space. PAN offers a network range of 10 meters from a person to the device providing communication.
Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.

5) Virtual Private Network (VPN): A VPN is a type of computer network that extends a private network across the internet and lets the user send and receive data as if they were connected to a private network even though they are not. Through a virtual point-to-point connection users can access a private network remotely. VPN protects you from malicious sources by operating as a medium that gives you a protected network connection.

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

Ans.

Shielded Twisted –Pair (STP) Cable: Shielded Twisted –Pair (STP) Cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors. The metal casing prevents the penetration of electromagnetic noise. It also can eliminate the phenomenon called crosstalk. Which is the undesired effect of one circuit (or channel) on another circuit (or channel). It occurs when one line pickup some of signals travelling down another line. This effect can be experienced during telephone conversations when one can hear other conversations in the background. This effect can be experienced during telephone conversations when one can hear other conversations in the background. To eliminate this effect shielding is used for each twisted pair cable. Shielded twisted-pair cable has the same quality consideration and uses the same connectors as unshielded twisted-pair cable, but the shield must be connected to a ground. Materials and manufacturing requirements make STP more expensive than UTP but less Susceptible to noise.

Unshielded Twisted Pair (UTP) Cable: UTP cable is the most general type of telecommunication medium which is mostly used. Although most familiar from its use in telephone system, its frequency range is suitable for transmitting both data and voice. A twisted pair consists or two conductors, generally copper, each with its own coloured plastic insulation. The plastic insulation is colour-banded for identification colours are used both to identify the specific conductors in a cable end to indicate which wires belong in pairs and how they relate to other pairs in a large bundle. A twisted pair consist of two conductors each surrounded by an insulating material. Both Data and voice both are transmitted through UTP because its frequency range is suitable. In UTP grounding cable is not necessary also in UTP much more maintenance are not needed therefore it is cost effective. In Shielded Twisted Pair (STP) much more maintenance are needed therefore it is costlier than Unshielded Twisted Pair (UTP).

3. What is difference between baseband and broadband transmission?

Ans.

Baseband	Broadband
The baseband transmits the digital signal using the physical medium like wires.	The broadband transmits the analog signals using optical fibers and twisted cables as a medium of transmission.
The baseband signalling used Manchester encoding scheme while transmitting the digital signals.	The broadband signalling used Manchester encoding scheme while transmitting the analog signals.
The baseband transmission can transmit the digital signals over a short distance only when compared to broadband transmission. If the digital signals need to be transmitted for a long distance, the attenuation process is required.	The broadband transmission can transmit the analog signals over a long distance compared to baseband transmission, and for transmitting the signals, no need for attenuation technique is required.
The baseband transmission uses the bus topology as the application.	The broadband transmission uses the tree and bus topology as the application.
The baseband transmission can transmit the single data type stream at one glance and can send in bidirectional.	The broadband transmission can transmit multiple data streams at the same time but in one direction only.
The baseband signals used twisted-pair cables, coaxial cables and wires as a medium of transmitting digital signals.	The broadband signals used optical fiber cables, coaxial cables, and radio waves to transmit the analog signals.
The baseband transmission is mostly used for the LAN networks as the baseband signalling can transmit the digital signal for a short distance only. And there is a requirement of repeaters for transmitting the signals.	Broadband transmission is mostly used for telephone networks. The broadband signalling can transmit the analog signals for long-distance without using any external device like a repeater or attenuator.

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

Ans.

Modem: A modem is short for a modulator-demodulator. Its function is to facilitate the transmission of data, by converting an analogue signal to code and decoding digital information. This means that it converts the telephone connection information into digital information for the computer to understand, and converts computer digits into analog waves so that it can be transmitted over telephone lines. It could be seen as the center for information collection from WAN, as it directly connects to the outside world. The modem is connected to your telephone line, and your computer. There it brings in signals from outside your house through your cable outlet; and converts them so your computer understands this information. Moreover, modems provide a connection between the Internet Service Provider (ISP) and your network**.** Modems are necessary for an internet connection. When used alone without a router or switch, it can connect to only one PC using the Ethernet port.

Router: A network router directs the data packets along networks. A router has a minimum of two networks, usually LANs or WANs or a LAN and its ISP. However unlike a modem, it cannot work single standing, however is able to connect to multiple nodes. Routers pass the information provided by the modem and routes it to the devices in the network such as the home computers. The information transferred by a router can be directed to a specific device by its unique number or rather its IP address. As noted before each device in that network is labelled by an IP address that allows other devices to communicate with it.

Switch: A network switch's primary function is to connect network segments on a single network**.** Therefore is quite different from a router and modem; it is used to expand the capability of the router, by providing additional posts. It connects many devices together on the same network; sending data to a device that needs or requests it. A switch is able to improve the performance of a network by increasing network capacity. A switch connects two or more nodes in the same or different network. Unlike the router which labels through IP address, switches use MAC addresses to direct the data to its correct destination. A switch can be used connect multiple Network devices (such as a computer, laptop, printer etc.) to the Home LAN .

Hub: A hub is a device that allows several network devices to connect together to exchange data on a single network however, they have no management component**.** Network hubs are also known as repeaters**.** They are less 'intelligent' than switches. Unlike switches, which forward data to the intended devices, hubs merely send the data packets to all its ports. So as the name repeaters suggests, it only repeats the data from an incoming port to all the other devices; this leads to frequent collisions between packets. This device is one of the more basic networking devices compared to others and thus, can be seen to have a lot of shortcomings. Hubs in the past were used to because they were much cheaper than switches, however nowadays the prices of switches decreased tremendously, making it a better decision.

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

Ans. 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 NIC card was replaced by another one.

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

Ans. 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.

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

Ans. Antivirus software must be installed on the servers and at the endpoint workstations. This software should be centrally managed to keep end users updated constantly and to minimize user meddling with the settings. That's because individual users can access any workstation and introduce a computer virus when plugging in their removable hard drives or flash drives. Good antivirus will also protect email clients.

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

Ans. A static IP address is a 32 bit number assigned to a computer as an address on the internet. This number is in the form of a dotted quad and is typically provided by an internet service provider (ISP). A static IP address is also known as a fixed IP address or dedicated IP address, and is the opposite of a dynamic IP address. A computer with an assigned static IP address uses the same IP address when connecting to the Internet. Routers, phones, tablets, desktops, laptops, and any other device that can use an IP address can be configured to have a static IP address.

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. A dynamic IP address is an IP address that's automatically assigned to each connection, or node, of a network, like your smartphone, desktop PC, or wireless tablet. This automatic assignment of IP addresses is accomplished by what's called a DHCP server.

IPv4	**IPv6**
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end to end, connection integrity is Achievable
It can generate 4.29×10^{9} address space	Address space of IPv6 is quite large it can produce 3.4×10^{38} address space
The Security feature is dependent on application	IPSEC is an inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal

IPv4	IPv6
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by the sender
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available
It has broadcast Message Transmission Scheme	In IPv6 multicast and any cast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has a header of 20-60 bytes.	IPv6 has header of 40 bytes fixed

9. Discuss TCP/IP model in detail.

Ans. TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP is also used as a communications protocol in a private computer network (an intranet or extranet). It was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. 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 requires little central management and is designed to make networks reliable with the ability to recover automatically from the failure of any device on the network. The TCP/IP model is a concise version of the OSI model.

It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

1. Process/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. Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model. Example of the application layer is an application such as file transfer, email, remote login, etc. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD.

The function of the Application Layers are:

- Application-layer helps you to identify communication partners, determining resource availability, and synchronizing communication.
- It allows users to log on to a remote host
- This layer provides various e-mail services
- This application offers distributed database sources and access for global information about various objects and services.

2. Host-to-Host/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. Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or de-segmentation. The transport layer also offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. TCP is the best-known example of the transport layer.

Important functions of Transport Layers:

- It divides the message received from the session layer into segments and numbers them to make a sequence.
- Transport layer makes sure that the message is delivered to the correct process on the destination machine.
- It also makes sure that the entire message arrives without any error else it should be retransmitted.

3. Internet Layer: 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. The Internet layer offers the functional and procedural method for transferring variable length data sequences from one node to another with the help of various networks. Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol. IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol)
Some of the functions of the network layer are:

1. Routing protocols
2. Multicast group management
3. Network-layer address assignment.

4. Network Access/Link Layer: Network Interface Layer is this layer of the four-layer TCP/IP model. 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 devices which directly interfaces with a network medium, like coaxial, optical, coaxial, fiber, or twisted-pair cables. A network layer is a combination of the data line and defined in the article of OSI reference model. This layer defines how the data should be sent physically through the network. This layer is responsible for the transmission of the data between two devices on the same network.

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

Ans. A web browser is a software application that is used to access the World Wide Web (www) or as known by everyone on the Internet. It is an interface between us and the information available on the web. When a user requests some information, the web browser fetches the data from a web server and then displays the webpage on the user’s screen. Web browsers are used primarily for displaying and accessing websites on the internet, as well as other content created using languages such as Hypertext Markup Language (HTML) and Extensible Markup Language (XML). Browsers translate web pages and websites delivered using Hypertext Transfer Protocol (HTTP) into human-readable content. They also have the ability to display other protocols and prefixes, such as secure HTTP (HTTPS), File Transfer Protocol (FTP), email handling (mailto:), and files (file:).

Some of the common browsers are Google, Mozilla Firefox, Safari, internet explorer, Netscape Navigator, etc.

---

11. What is a search engine? Give example.

Ans. A search engine is a software system that is designed to carry out web searches. They search the World Wide Web in a systematic way for particular information specified in a textual web search query. The search results are generally presented in a line of results, often referred to as search engine results pages (SERPs) The information may be a mix of links to web pages, images, videos, infographics, articles, research papers, and other types of files.

Some examples of search engines are Google, Bing, AOL.com, DuckDuckGo, WolframAlpha, Yandex, Internet Archive, Yahoo! Ask.com, Baidu etc.

---

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

Ans. 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. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The internet came in the year 1960 with the creation of the first working model called ARPANET.

World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc. The WWW, along with internet, enables the retrieval and display of text and media to your device.

Some of the most common uses of the internet in our daily life are Search information, News, Communicate and collaboration, File and data transfer, Social networking, Entertainment – relax, watch video, listen to music, Gaming , Business promotion, Earn on the Internet, Shopping (E-commerce), Education, Online services, Blogging etc.

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

Ans. Internet service provider (ISP)**,** can be defined as a 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.

Some of the top ISP in India are:

- BSNL
- MTNL
- Bharti Airtel
- Hathway Cable
- Tata Communications
- You Telecom
- Reliance Communications
- Sify Broadband
- Asianet Communications
- HFCL Infotel

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

Ans. MAC Address:

- MAC Address stands for Media Access Control Address.
- MAC Address is a six byte hexadecimal address.
- A device attached with MAC Address can retrieve by ARP protocol.
- NIC Card's Manufacturer provides the MAC Address.
- MAC Address is used to ensure the physical address of a computer.
- MAC Address helps in simply identifying the device.
- MAC Address of computer cannot be changed with time and environment.
- MAC Address operates in the data link layer.
- MAC Addresses can't be found easily by a third party.
- It is a 48-bit address that contains 6 groups of 2 hexadecimal digits, separated by either hyphens (-) or colons (.). Example: 00:FF:FF:AB:BB:AA or 00-FF-FF-AB-BB-AA
- No classes are used for MAC addressing
- MAC Address sharing is not allowed.

IP Address:

- IP Address stands for Internet Protocol Address.
- IP Address is either a four-byte (IPv4) or an eight-byte (IPv6) address.
- A device attached with IP Address can retrieve by RARP protocol.
- Internet Service Provider provides IP Address.
- IP Address is the logical address of the computer.
- IP Address operates in the network layer
- IP Address identifies the connection of the device on the network.
- IP Address modifies with the time and environment.
- IP Addresses can be found by a third party.
- IPv4 uses 32-bit addresses in dotted notations, whereas IPv6 uses 128-bit addresses in hexadecimal notations. Example: IPv4 192.168.1.1 IPv6 FFFF:F200:3204:0B00
- IPv4 uses A, B, C, D, and E classes for IP addressing.
- In IP address multiple client devices can share the IP address.

Port address:

- Used to identify an application/services on your system

- A port number is a layer-4 address used by some layer-4 protocols e.g. TCP and UDP
- The Port number is 16 bits and assigned by the Network operating system when the application process creates the sockets.
- Port number for application is decided by the Kernel of the OS. This port no. is called port address.
- To find port number used for application, Type “netstat -a” and press “Enter.” A list of all your active TCP/IP connections will populate showing port number used by source and destination hosts.
- After IP delivers the packet to destination , with the help of the port numbers OS directs the data to the correct application
- E.g. – Port number 80 for http traffic , 67 and 68 for DHCP traffic etc

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

Ans. Following steps are given on how to view the Internet Browser history:

Step 1: Open the browser and click on the three dots and then History.

Step 2: Clicking on this will open up your browsing history, with the most recent pages you have visited first. You can scroll down the list.

Step 3**:** From this list you can click on any page displayed to revisit it. Alternatively if you click on the three buttons in the corner you get the options to Open history page or Clear browsing data**.**

Step 4: If you select Open history page you can search the history using a keyword in the Search box, or choose a date range. This is useful if you can remember the name of the site, or approximately when you visited it.