CCA-102: Data Communications

ASSIGNMENT

Q1. What are the different types of networks?
Ans: The different types of networks are

- Local Area Network
- Personal Area Network
- Metropolitan Area Network
- Wide Area Network

Q2. Explain the Shielded twisted pair (STP) and Unshielded twisted pair (UTP).
Ans: **Shielded Twisted Pair (STP):**

Shielded Twisted Pair (STP) is a special kind of cooper telephone and local area network (LAN) wiring used in some business installations. It adds an outer covering or shield that function as a ground to ordinary twisted pair wiring.

Twisted pair is the ordinary copper wire that connects many computer networks to the telephone company. To reduce cross- talk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Each signal on twisted pair requires both wires. Unlike unshielded twisted pair (UTP), shielded twisted pair also encloses these wires in a shield and grounds them to further reduce electromagnetic and radio frequency interference. STP cables are more expensive and harder to install than UTP wiring.

Unshielded Twisted Pair (UTP):

Unshielded Twisted pair cable is a 100ohm copper cable that consist of 2 to 1800 UTP surrounded by an outer jacket. They have no metallic shield. This makes the cable smaller in diameter but unprotected against electrical interference. The twist helps to improve its immunity to electrical noise and EMI.

Unshielded Twisted Pair (UTP) cables are found in many Ethernet networks and telephone systems. For indoor telephone applications, UTP is often grouped into sets of 25 pairs according to a standard 25- pair color code originally developed by AT&T corporation. A typical subset of these colors (white/blue, blue/white, white/orange, orange/white) shows up in most UTP cables. The cables are typically made with copper wires measured at 22 or 24 American Wire Gauge (AWG), with the colored insulation typically made from an insulator such as polyethene or FEP and the total package covered in a polythene jacket.

Q3. What is the difference between baseband and broadband transmission?
Ans: Differences between-

Baseband	Broadband
It refers to a communications channel in which information is carried in digital form.	The signals are modulated as radiofrequency analog waves that use different frequency ranges.
Communications is bi-directional which means the same channel is used to transmit and receive signals.	Communication is unidirectional meaning two different channels are needed in order to send and receive signals.
Every device on a baseband system shares the same channel.	Multiple independent channels can carry analog or digital information through FDM.

Baseband LANs are inexpensive and easier to install and maintain.	Broadband systems are generally more expensive because of the additional hardware involved.
Baseband LANs have a limited distance reach is no more than a couple miles.	Broadband LANs span much longer distance than baseband (up to tens of kilometers).

Q4. What is the difference between hub, modem, router and a switch?

Ans**: 1. 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 repeater suggests, it only repeats the data from an incoming port to all the other devices; this leads to frequent collisions between packets.

2.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.

3. 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.

4. Switch:

- A switch is a network that connect network segments on a single network. It connects many devices together on the same network, sending data to a device that needs or request it. A switch is able to improve the performance of a network by increasing network capacity.

Switch	Router	Modem	Hub
Joins several computers together within one local area network. They cannot join multiple networks, and are incapable of sharing an internet connection.	Joins multiple area networks (LAN & WAN). Serving as "middle man" or intermediate destinations for network traffic. Using the IP, they forward data to specific destinations.	Modems, like routers connect home PCs to the internet.	Connects a network of personal computers together so they can be joined through a central hub.

A home network with a switch must designate one computer as the gateway to the internet. Connects multiple computers together within one local network.	Creates a home network, where all home computers are connected equally to the router, where there is no hierarchy in performance.	Codes and decades data so that it can pass between home and network and internet service provider (ISP). Modem brings in the in the information, while the router distributes it to the devices.	Broadcasts data does not select where the data goes, but rather sends it to every destination. Connects to multiple Ethernet devices, making them act as a single segment.
LAN network	LAN & WAN network		LAN network
Sophistication level is medium	Sophistication level is high	Sophistication level is high	Sophistication level is low

Q5. When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?
Ans: Yes, that is because MAC address are hardwires into the NIC circuity, not the PC. This also means that a PC can have a different MAC address when another one replaced the NIC card.

Q6. When troubleshooting computer network problems, what common hardware- related problems can occur?
Ans: A large percentage of a network is made up of hardware. Problem is these areas can range from malfunctioning hard drives, broken NICs and even hardware startups.

Q7. In a network that contains two servers and twenty workstations, where is the best place to install an Anti- virus program?
Ans: In a network that contains two servers and twenty workstations, the best place to install Anti-virus program is to install in all the computers, system or workstations. If we want to installed only in one system, install in the main server.

Q8. Define Static IP and Dynamic IP? Discuss the difference between IPV4 and IPV6.
Ans**: Static IP Address**: It is an IP Address that a computer or web server has and is identified by the rest of the internet or systems and does not change at all, instead it remains the same.

Dynamic IP Address: It is an IP address that a computer or web server has and id identified by the rest of the internet or system and this IP address does not remain the same, instead it changes over time.

Differences between:

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
Fragmentation performed by sender and forwarding routers	In IPv6 packet flow identification are available and uses the flow label field in the header
In IPv4 packet flow identifications 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. It has broadcast Message Transmission Scheme	In IPv6 checksum field is not available. It has multicast and any cast message transmission scheme is available
In IPv4 has a header of 20- 60 bytes	In IPcv6 has header of 40 fixed

Q9. Discuss TCP/ IP model in detail.
Ans**: TCP/ IP model**:

The TCP/ IP model was developed prior to the OSI model. The TCP/ IP model is not exactly similar to the OSI model. The TCP/ IP model consist of five layers: the application layer, transport layer, network layer, data link layer and physical layer.

The first four layers provide physical standards, network interface, internetworking and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/ IP model by a single layer called the application layer. TCP/ IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionally. Each upper-layer protocol is supported by two or more lower- level protocols.

Application Layer: An application layer is the topmost layer in the TCP/ IP model. It is responsible for handling high- level protocols, issues of representation. This layer allows the user to interact with the application. When one application layer protocol wants to communicate with another application layer, it forward its data to the transport layer. There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system.

Transport Layer: Transport Layer is the second layer of the TCP/IP model. It is end-to-end layer used to deliver messages to a host. It is termed as an end-to-end layer because it provides a point- to -point connection rather than hop-to-hop, between the source host and destination host to deliver the services reliably. The unit of data encapsulation in the Transport Layer is a segment. The standard protocols used by Transport Layer to enhance its functionalities are TCP (Transmission Control Protocol), UDP (User Datagram Protocol), DCCP (Datagram Congestion Control Protocol), etc.

Network Layer: A network layer is the lowest layer of the TCP/IP model. A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model. It defines how the data should be sent physically through the network. This layer is mainly responsible for the transmission of the data between two devices on the same network. The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical address. The protocols used by this layer are Ethernet, token ring, FDDI, X.25, frame relay.
Data Link Layer: The data link layer is a 4_{th} layer from the top and 2_{nd} layer from the bottom. The communication channel that connects the adjacent nodes is known as links and in order to move the datagram from source to the destination, the datagram must be moved across an individual link. The main responsibility of the data link layer is to transfer the datagram across an

individual link. The data link layer protocols are Ethernet, token ring, FDDI and PPP.

Physical Layer: The physical layer is the first and lowest layer; The layer most closely associated with the physical connection between devices. This layer may be implemented by a PHY chip. The physical layer provides an electrical, mechanical and procedural interface to the transmission medium. The shapes and properties of the electrical connectors, the frequencies to broadcast on, the line code to use and similar low-level parameters, are specified by the physical layer. The physical layer defines the means of transmitting a stream of raw bits over a physical data link connecting network nodes. The bit stream may be grouped into code words or symbols and converted to a physical signal that is transmitted over a transmission medium.

Q10. What is Web Browser (Browser)? Give some examples of web browsers.
Ans: A web browser is an application used to access and view websites.

Some examples of browsers include Microsoft Edge, Internet explorer, Google Chrome, Mozilla firefox and apple safari.

Q11. What is a search engine? Give example.
Ans: A **search engine** is a software that is accessed on the internet to assist a user to search its query on the world wide web. It is a web-based tool that enables users to locate information on the world wide web.

Examples of search engine are as follows:

- **Microsoft Bing**
- **Wiki. Com**
- **Yahoo**
- **CC Search**
- **DuckDuckGo**
- **Google**

Q12. What is the Internet & WWW? What are the uses of internet in our daily life?
Ans:
Internet: It is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices.
World Wide Web (WWW): The World Wide Web is the combination of all resources and users on the internet that are using the Hypertext Transfer Protocol (HTTP). "The World Wide Web id the universe of network accessible information, ab embodiment of human knowledge".
Uses of internet in our daily life are as follows:
1. Online booking and orders.
2. Cashless transactions.
3. Online Banking and Trading.
4. Social Networking.
5. Job search.
6. Electronic Mail
7. Education.
8. Research and Development.
9. Communication.
10. Entertainment.
11. Shopping.
12. Utility Bill payment.
13. Business.

Q13: What is an Internet Service Provider? Give some examples of ISP in India.
Ans: An Internet Service Provider is an organization that provide services for accessing using or participation in the Internet.

Examples of ISP in India are: Airtel, BSNL, etc.

Q14. Discuss the difference between MAC address, IP address and Port address.
Ans:

MAC Address

Media Access Control (MAC) refers to the piece of hardware that controls how data is pushed out onto a network. In the OSI reference model for networking, the MAC is a layer 2 -- or data link layer – device, and the MAC address is a layer 2 address. In the current internet era, most devices are connected physically with Ethernet cables or wirelessly with Wi-Fi. Both methods use MAC address to identify a device on the network.
A MAC address consists of 12 hexadecimal digits, usually grouped into six pairs separated by hyphens. MAC address are available from 00-00-00-00-00-00 through FF-FF-FF-FF-FF-FF. The first half of the number is typically used as a manufacturer ID, while the second half is a device identifier. Each MAC address is unique to the network card installed on a device, but the number of devices identifying bits is limited, which means manufacturers do reuse them.

IP Address

IP controls how devices on the internet communicate and defines the behaviour of internet routers. It corresponds to Layer 3, the network layer, of the OSI reference model. The internet was initially built around IP version 4 (IPv4) and is in transition to IPv6. An IP address identifies a device on the global internet, acting as the device's logical address to identify that network connection. An IPv4 address consist of 32 bits, usually written as four decimal numbers, or a dotted quad.
The IP address combines network identification and device identification data. The network prefix is anywhere from eight to 31 bits and the remainder identify the device on the network. Steady, rapid growth in the number of internet-connected devices had led to the looming exhaustion of the IPv4 address list one of Several reasons for the development of IPv6. An address IPv6 consists of 128bits, with the first 64 reserved for network identification and the second 64 dedicated to identifying a device on the network.

Port Address

A Port Address is the logical address of each application or process that uses a network or the internet to communicate. A port number uniquely identifies a network-based application on a computer. Each application/program is allocated a 16-bit integer port number. This number is assigned automatically by the OS, manually by the user or is set as a default for some popular applications.
A port number primarily aids in the transmission of data between a network and an application. Port numbers work in collaboration with networking protocols to achieve this. Port numbers are mainly used in TCP and UDP based networks, with an available range of 65,535 for assignment port numbers. Although an application can change its port number, some commonly used internet/network services are allocated with global port numbers such as Port Number 80 for HTTP, 23 for Telnet and @% for SMTP.

Q15. How do we view my Internet browser's history?
Ans: Steps to view internet browser history are
1. Open the browser and click on the above three dots and then history.
2. After clicking the history resent pages will appear.
3. Scroll down and view or revisit the desire page.