CCA-102: Data Communications

Assignment

Q1. What are the different types of networks?

Ans: There are 11 Types of networks in Use Today they are:

1.Personal Area Network (PAN): The smallest and most basic type of network, a pan is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residence, and are managed by one person or organization from a single device.

2.Local Area Network (LAN): LANs are the most frequently discussed networks, one of the most common, one of the most original and one of the simplest types of networks. LANs connect groups of computers and low-voltage devices together across short distances (within a building in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs.
Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidly and safely transfer data.

3.Wireless Local Area Network (WLAN): Functioning like a LAN, WLANs, make use of wireless technology. Such as Wi-Fi. Typically seen in the same types of applications as LANs, these types of networks don’t

require that devices rely on physical cables to connect to the network.

4.Campus Area Network (CAN): Larger than LANs, but smaller than metropolitan area networks (MANs) these types of networks are typically seen in universities, large K-12 school districts or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.

5.Metropolitan Area Network: These types of networks are larger than LANs but smaller than WANs- and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance are handled by either a single person or company (a local council, a large company, etc.)

6.Wide Area Network (WAN): Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're miles apart.

The internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WANs vast reach, it is typically owned and maintain by multiple administrators or the public.

7.Storage- Area Network (SAN): As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don't rely on a LAN or WAN. Instead, they move storage

resources away from the network and place them into their own high-performance network. SANs can be accessed in the same fashion as a drive attached to a server. Types of storage area networks include converged, virtual and unified SANs.

8.System-Area Network (also known as SAN): This term is fairly new within the past two decades. It is used to explain a relatively local network that is designed to provide high-speed connection in server-to-server applications (cluster environments), storage area networks (called “SANs” as well) and processor-to-processor applications. The computers connected on a SAN operate as a single system at very high speeds.

9.Passive Optical Local Area Network (POLAN): As an alternative to traditional switch- based Ethernet

LANs, POLAN technology can be integrated into structured cabling to overcome concerns about supporting Ethernet protocols and network applications such as PoE (Power over Ethernet). A point-to-multipoint LAN architecture, POLAN uses optical signal from one strand of single mode optical fiber into multiple signals to serve users and devices.

10.Enterprise Private Network (EPN): These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.

11.Virtual Private Network (VPN): By extending a private network across the internet, a VPN lets its user send and receive data as if their devices were connected to the private network – even if they're not. Through a virtual point-to-point connection,

users can access a private network remotely.

Q2. Explain the shielded twisted pair (STP) and Unshielded twisted pair (UTP)

Ans: Shielded twisted pair cables (STP) has the individual pairs of wires wrapped in foil, which are then wrapped again for double protection. Unshielded twisted pair (UTP) has each pair of wires twisted together. Those wires are then wrapped in tubing without any other protection. UTP cables are less expensive, and a more popular type of cabling.

Knowing which cable to use for a specific application depends on the protection needed from power frequency and any electromagnetic interference (EMI). This is where shielded vs unshielded cable becomes important.

Different Types of Shielded Cable:

Shielded twisted pair cabling (STP) reduces electromagnetic and radio frequency interference from other devices and

electronic objects to ensure a steady signal. Cables consist of a bundle of wires divided into four pairs. Each pair is twisted together to reduce crosstalk interference from the other wire pairs in the bundle. There are 3 different shielding configurations, each with their own level of protection:

- **Braided** (90% EMI shielding)
- **Spiral** (98% EMI shielding)
- **Metal-coated Mylar or foil** (100% EMI shielding)

  Shielded cables are useful in any environments where there is a high chance of electronics interference, such as radio stations (telecom cable assemblies) and airports (aerospace cable assemblies). STP cables are also used in security systems to provide protection from power frequency interference, or in box builds where there are multiple

different components operating in close proximity. As well as being protected from external interference, the shielding also keeps noise from existing the cable, minimizing the chance of causing interference in other devices.

Unshielded cable (UTP) does not utilize shielding to reduces interference. UTP cables are designed to limit electromagnetic interference by the way the pairs are twisted inside the cable. UTP cable is most suitable for offices LANs and similar network cabling systems. While offering less protection from interference, unshielded cables are popular because they are

- Versatile
- Inexpensive
- Easy to install
- Lightweight

- Flexible

The main disadvantage of UTP cables is their susceptibility to electromagnetic interference and radio frequency interference. They also have a smaller bandwidth compared to coaxial cables or fiber optic cables.

Q3. What is the difference between baseband and broadband transmission?

Ans: Broadband system use modulation techniques to reduce the effect of noise in the environment. Broadband transmission employs multiple channel unidirectional transmission using combination of phase and amplitude modulation.

Baseband is a digital signal is transmitted on the medium using one of the signal codes like NRZ, RZ Manchester bi phase-M code etc. is called baseband transmission.

These are the following difference between Broadband and Baseband transmission.

Baseband transmission-

1. Digital signaling.
2. Frequency division multiplexing is not possible.
3. Baseband is bi-directional transmission.

4. Short distance signal travelling.
5. Entire band width is for single signal transmission.
6. **Example:** Ethernet is using basebands for LAN.

Broadband transmission-

1. Analog signaling.
2. Transmission of data is unidirectional.
3. Signal travelling distance is long.
4. Frequency division multiplexing possible.
5. Simultaneous transmission of multiple signals over different frequencies.
6. **Example:** Used to transmit cable TV to premises.

S.NO	Baseband Transmission	Broadband Transmission
1.	In baseband transmission, the type of signaling used is digital.	In broadband transmission, the type of signaling used is analog.
2.	Baseband transmission is bidirectional in nature.	Broadband transmission is unidirectional in nature.
3.	Signals can only travel over short distances.	Signals can be travelled over long distances without being attenuated.
4.	It works well with bus topology.	It is used with a bus as well as tree topology.

5.	**In baseband transmission, Manchester and differential Manchester encoding are used.**	**Only PSK encoding is used.**

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

Ans: HUB: A hub is to send out a message from one port to other ports. For example, if there are three computers of A, B, C, the message sent by a hub for computer, A will also come to the other computers. But only computer A will respond and the response will also go out to every other port on the hub. Therefore, all the computers can receive the message and computers themselves need to decide whether to accept the message.

Switch: A switch is able to handle the data and knows the specific addresses to send the message. It can decide which computer is the message intended for and send the message directly to the right computer. The efficiency of switch has been greatly improved, thus providing a faster network speed.

Router: Router is actually a small computer that can be programmed to handle and route

the network traffic. It usually connects at least two networks together, such as two LANs, two WANs or a LAN and its ISP network. Routers can calculate the best route for sending data and communicate with each other by protocols.

Modem: A modulator-demodulator, or simply modem, is a computer hardware device that converts data from a digital format into a format suitable for an analog transmission medium such as telephone or radio. A modem transmits data by modulating one or more carrier wave signals to encode digital information, while the receiver demodulates the signal to recreate the original digital information. The goal is to produce a signal that can be transmitted easily and decoded reliably. Modems can be used with almost any means of transmitting analog signals, from light-emitting diodes to radio.

Q5. 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 hardwired 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.

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. Problems in 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: The best solution is **to install anti-virus on all the computers in the network.**

Q8. Define static IP and Dynamic IP? Discuss the difference between IPV4 and IPV6.

Ans: When a device is assigned a static IP address, **the address does not change.** Most devices use **dynamic IP addresses**, which are assigned by the network when they connect and change over time.

IPV4 is 32-Bit IP address whereas **IPV6** is a 128-Bit IP address. **IPV4** is a numeric addressing method whereas **IPV6** is an alphanumeric addressing method. **IPV4 binary bits are separated a dot (.) whereas IPV6 binary bits are separated by a colon (:).**

Q9. Discuss TCP/IP model in detail.

Ans: TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defense) in the 1960s. It is name after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocols and IP stands for Internet Protocols.

The four-layers in the TCP/IP protocol suite are-

- **Host-to-Network Layer-** It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.
- **Internet Layer-** It defines the protocols for logical transmission of data over the network. The main protocol in this layer is internet protocol (IP) and it is

supported by the protocols ICMP, IGMP, RARP, and ARP.

- **Transport Layer-** It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- **Application Layer-** This is the top most layer and defines the interface of host programs with the transport layer services. This layer include all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

Q10.What is a Web Browser (Browser)? Give some examples of browser.

Ans: A Web Browser, or simply “Browser” is an application used to access and view websites.
The most popular web browsers that are used today are **Mozilla Firefox, Google chrome, Microsoft Internet Explorer, Apple Safari and the Opera browser.** These browsers are free and available for download and use. Web browsers allow users to view resources that are stored on a server.

Q11. What is a search engine? Give example.

Ans: 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.**

Q12. What is the internet & WWW? What are the uses of internet in our daily life?

Ans: The internet is very much useful in our daily routine tasks. For example, it helps us **to see our notifications and emails.** Apart from this, people can use the internet for money transfers, shopping order online food, etc.
A few of the internet's major uses are **e-commerce, e-learning, knowledge sharing, social connectivity, variety of media, file transfer, communication, etc.**
The **World Wide web** or **WWW** or **Web** for short, are the pages you see when you're at a device and you're online. But the internet is the network of connected computers that the web works on, as well as what emails and files travel across.

Q13. What is an Internet Service Provider? Give some examples of ISP in India.

Ans: An Internet Service Provider (ISP) is a company such as AT&T, Verizon, comcast, or spectrum that **provides Internet access to companies, families, and even mobile users**. ISPs use fiber optics, satellite, copper wire, and other forms to provide Internet access to its customers.
The example of some Internet Service Provider are **Hath way, BSNL, Tata teleservices, Verizon, Reliance Jio, ACT Fibernet** and many more working in India as well as worldwide. Internet service provider or ISPs are responsible for providing services for using the Internet.

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

Ans: Both MAC Address and IP Address are used to uniquely define a device on the internet. NIC card's Manufacturer provides the MAC Address, on the other hand, Internet Service Provider provides IP Address.

The main difference between MAC and IP address is that **MAC Address is used to ensure the physical address of the computer.** It uniquely identifies the devices on a network. While IP addresses are used to uniquely identifies the connection of the network with that device takes part in a network.

A Port number 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.

Q15.How do we view my Internet browser's history?

Ans: We can open it by pressing Alt to show the menu bar, **then choosing View -> Sidebar -> History.** Or you can use the keyboard shortcut, ctrl+ H. You can also view your history if you click the hamburger menu button in the top-right hand corner of your window, then click History.