CCA-102:DATA COMMUNICATIONS

ASSIGNMENT-2

6/3/2025
SARANYA R

CCA-102: DATA COMMUNICATIONS
ASSIGNMENT-2

1)WHAT ARE THE DIFFERENT TYPES OF NETWORKS

- ☆ **LAN (Local Area Network):** A LAN connects devices in a limited geographical area, such as a home, office building, or campus.
- ☆ **WAN (Wide Area Network):** A WAN connects devices over a larger geographical area, such as a city or country.
- ☆ **WLAN (Wireless Local Area Networ**k): A WLAN connects devices wirelessly in a limited geographical area.
- ☆ **MAN (Metropolitan Area Network**): A MAN connects devices in a metropolitan area, such as a city or town.
- ☆ **PAN (Personal Area Network**): A PAN connects devices in a very small area, such as a few feet.
- ☆ **SAN (Storage Area Network**): A SAN is a dedicated network for storage devices.
- ☆ **CAN (Campus Area Network):** A CAN connects devices in a university or college campus.
- ☆ **VPN (Virtual Private Network):** A VPN is a secure, encrypted connection over a public network.

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

Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP) cables are both types of twisted-pair wiring used for networking, but they differ in their shielding and how they handle interference. UTP cables are more affordable and easier to install, while STP cables offer better protection against electromagnetic interference (EMI) by adding a shield around the wires.

Unshielded Twisted Pair (UTP):

•**Construction**:

UTP cables consist of pairs of insulated wires twisted together within an outer jacket. There is no additional shield or grounding wire around the twisted pairs.

•**Function:**

The twisting of the wires helps to cancel out some external interference, but UTP is not designed for environments with strong EMI.

•**Advantages:**

UTP is cost-effective, flexible, and easy to install, making it suitable for low-interference areas like homes or small offices.

- • **Disadvantages**

UTP is more susceptible to EMI and crosstalk, which can degrade signal quality in noisy environment

3). What is difference between baseband and broadband transmission?

Baseband transmission uses a digital signal that occupies the entire bandwidth of a channel, while broadband transmission uses an analog signal that allows multiple transmissions to share the bandwidth simultaneously

BASEBAND	BROADBAND
Signal Type: Digital.	Signal Type: Analog, usually modulated.
Bandwidth Usage: The entire bandwidth of the channel is used by a single digital signal.	**Bandwidth Usage:** The channel's bandwidth is divided into multiple frequency channels, allowing multiple transmissions to occur simultaneously.
Examples: Ethernet.	**Examples:** Cable TV.
Key Features: Simple to implement and often used over wires, but doesn't allow for multiple simultaneous transmissions.	**Key Features:** Higher bandwidth utilization, but more complex to implement and usually unidirectional
Advantages: Simpler implementation and can be bidirectional.	**Advantages:** Higher data rates and the ability to transmit multiple signals simultaneously.
Disadvantages: Only one signal can occupy the entire bandwidth at a time, limiting bandwidth utilization.	**Disadvantages:** More complex to implement and typically unidirectional.

4)WHAT IS DIFFERENCE BETWEEN A HUB,MODEM,ROUTERAND A SWITCH?

Understanding Networking Devices: Hub, Modem, Router, and Switch

The question pertains to the differences between four key networking devices: hub, modem, router, and switch. Let's explore each device in detail.

1) **Hub**
   A hub is a basic networking device that connects multiple devices within a Local Area Network (LAN). It operates at the physical layer of the OSI model.
   Receives data from one device.
   Broadcasts the data to all connected devices.

2.Modem

A modem (modulator-demodulator) connects your network to the internet via an Internet Service Provider (ISP).

Modulates digital signals from your devices into analog signals for transmission.

Demodulates incoming analog signals back into digital signals.

3. Router

A router connects multiple networks and routes traffic between them.

Operates at the network layer of the OSI model.

Forwards data packets based on their destination IP addresses.

4. Switch

A switch connects multiple devices within a LAN and forwards data to the intended recipient.

Operates at the data link layer of the OSI model.

Uses MAC addresses to forward data packets.

Key Differences

Hub vs. Switch: Both connect devices within a LAN, but a switch is more intelligent and efficient.

Modem: Connects your network to the internet.

Router: Manages and directs traffic between different networks.

Summary

- ☆ Modem: Internet connection.
- ☆ Router: Traffic management between networks.
- ☆ Switch: Efficient connection within a LAN.
- ☆ Hub: Basic, less efficient connection within a LAN.

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

Yes, the MAC address is transferred when a NIC card is moved from one PC to another. The MAC address is permanently burned into the NIC card's hardware, specifically the ROM or flash memory, by the manufacturer. This means the MAC address stays the same regardless of which computer the NIC is installed in.

Because the MAC address is hard-wired into the NIC circuit, not the personal computer. This also means that a PC can have a different MAC address when another one replaces the NIC card

.

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

When troubleshooting network problems, common hardware issues include problems with **network cables**, network devices like routers or switches, or the computer's network interface card (NIC). Other issues can involve the power supply, CPU overheating, or memory issues.

Network Cables: Damaged, disconnected, or loose network cables can cause connectivity issues or slow speeds.

Network Devices: Misconfigured or faulty routers or switches can lead to connectivity problems or network outages.

Computer's Network Interface Card (NIC): A malfunctioning NIC can prevent a device from connecting to the network.

Power Supply Issues: A failing power supply can prevent a computer from turning on or cause it to shut down unexpectedly.

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

The most effective approach is to install antivirus software on all computers in the network, including both servers and workstations.

This ensures that all devices are protected from threats, whether they originate from external sources or are spread internally within the network. Additionally, you can consider implementing a centrally managed solution for easier deployment and maintenance of the antivirus software across the network.

Why install on all machines?

Comprehensive Protection:

By installing antivirus on all devices, you ensure that each machine is scanned for malicious software, preventing it from becoming infected and spreading the threat to other computers in the network.

Preventing Internal Threats:

If a server becomes infected, it could potentially infect other machines on the network. Similarly, if a workstation becomes infected, it could potentially infect other devices, including the server.

Security Best Practices:

Having antivirus installed on all machines is a standard security practice that helps protect against various types of threats, including malware, viruses, and spyware.

Ease of Management:

Many antivirus vendors offer centralized management solutions, which allows you to deploy, update, and monitor antivirus software on all machines from a single location.

Why not just install on the servers?

Workstations are also at risk:

Workstations are more likely to access external sources and may be more vulnerable to infection. Therefore, it is crucial to protect workstations as well as servers.

Potential for lateral movement:

If a workstation becomes infected, it could potentially infect other machines, including the server, if the network is not properly secured.

Complete network protection:

A complete approach to network security involves protecting all devices, not just the servers.

8). Define Static IP and Dynamic IP? Discuss the difference between IPV4 and IPV6A

Static IP address is a permanent, unchanging IP address assigned to a device.

A dynamic IP address is a temporary address assigned to a device that can change periodically

1. Static IP Addresses:

- *Permanent:* They remain constant and do not change.
- *Manual Configuration:* They are typically assigned manually by a network administrator.
- *Use Cases:* Ideal for devices needing a consistent, publicly accessible address, like servers, routers, and printers.
- *Cost:* Generally more expensive than dynamic IPs.
- *Security:* May be considered slightly less secure due to their fixed nature.

2. Dynamic IP Addresses:

- *Temporary:* They are assigned dynamically and can change.
- *Automatic Assignment:* They are assigned by a DHCP server.
- *Use Cases:* Common for regular internet users who don't need a persistent public address.

- *Cost:* Typically less expensive than static IPs.
- *Security:* May be considered more secure due to their changing nature, making it harder to track

IPv4:	IPv6:
32-bit address: Uses a 32-bit address format.	**128-bit address:** Uses a 128-bit address format.
Limited address space: Has a relatively smaller number of available addresses compared to IPv6.	**Large address space:** Offers a vastly larger number of available addresses.
Dot-decimal notation: Uses a dot-decimal format, like 192.168.1.1.	**Hexadecimal notation:** Uses a hexadecimal format, like 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
Header: Has a more complex header compared to IPv6.	**Simplified header:** Has a simpler header compared to Ipv .

9). Discuss TCP/IP model in detail.

CP/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.

The two main protocols in the IP suite serve specific functions and have numerous differences. The key differences between TCP and IP include the following:

TCP
- It ensures a reliable and orderly delivery of packets across networks.
- TCP is a higher-level smart communications protocol that still uses IP as a way to transport data packets, but it also connects computers, applications, web pages and web servers.
- TCP understands holistically the entire stream of data that these assets require to operate and it ensures the entire volume of data needed is sent the first time.
- TCP defines how applications can create channels of communication across a network.
- It manages how a message is assembled into smaller packets before they're transmitted over the internet and reassembled in the right order at the destination address.

IP

- IP is a low-level internet protocol that facilitates data communications over the internet.
- IP delivers packets of data that consist of a header, which contains routing information, such as the source and destination of the data and the data payload itself.
- It defines how to address and route each packet to ensure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.
- IP is limited by the amount of data it can send. The maximum size of a single IP data packet, which contains both the header and the data, is between 20 and 24 bytes. This means that longer strings of data must be broken into multiple data packets that have to be sent independently and then reorganized into the correct order.

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

A web browser is a software application that allows you to access and view websites on the internet. It displays the content of websites on your screen and enables you to interact with them, such as by clicking links or filling out forms.

Some popular examples of web browsers include Google Chrome, Mozilla Firefox, Apple Safari, Microsoft, and Microsoft Edge.

Examples:

Google Chrome: A popular and widely used browser known for its speed and vast extension library.

Mozilla Firefox: Another popular browser known for its focus on privacy and its ability to be customized with extensions.

Apple Safari: The default browser for Apple devices (Mac, iPhone, iPad), known for its simplicity and integration with Apple's ecosystem.

Microsoft Edge: Microsoft's web browser, which replaced Internet Explorer and is known for its features and integration with the Windows operating system.

11) What is a search engine? Give example.

A search engine is a web-based tool that helps users finds information on the internet. It uses a system of software to index and organize the vast amount of data available online, allowing users to query and receive relevant results based on keywords or phrases.

Examples include Google, Bing, Yahoo!, and DuckDuckGo.

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

he Internet is a global network of interconnected computers and devices that uses standardized protocols for communication and information sharing.

The World Wide Web (WWW) is a specific application that runs on top of the Internet, providing access to information via interconnected webpages, images, and other digital documents.

Uses of the Internet in Daily Life:

Communication: The Internet enables instant and global communication through email, messaging apps, social media, and video conferencing,

Information Access:

The Internet provides access to a vast amount of information on any topic

E-commerce:

Online shopping and banking allow for convenient transactions,

Entertainment:

Streaming services offer access to a wide range of movies, music, and games,

Education and Skill Development:

Online courses, tutorials, and educational resources facilitate learning and skill development,

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

An Internet Service Provider (ISP) is a company that provides individuals and organizations with access to the internet. They offer various internet connection options and services, including broadband, mobile, and fiber optic

Examples of ISPs in India:

Bharti Airtel Limited (Ariel): A major telecom operator providing broadband, fiber optic, and mobile internet services.

Reliance Jio Infocomm Limited (Jio): A prominent player in the Indian telecom market offering broadband, fiber optic and mobile internet services.

Vodafone Idea Ltd. (VI): Another large telecom operator offering mobile internet services.

BSNL (Bharat Sanchar Nigam Limited): A government-owned telecommunications company providing internet services.

Hath way: A well-known broadband service provider.

Excitel Broadband: A provider of fiber-to-the-home (FTTH) internet services.

MTNL Broadband: A provider of FTTH internet services in Delhi and Mumbai.

Tata Communications Limited: A global communications company also providing internet services in India.

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

MAC addresses are physical addresses assigned to network interfaces, ensuring unique identification within a local network. IP addresses are logical addresses used for communication across networks, and port numbers are used within IP communication to identify specific processes or services

MAC Address:

- Purpose: Identifies a device on a local network (LAN). It's a physical address, like a postal address for your house, but within a local network.
- Assigning: Hardwired into the network interface card (NIC) by the manufacturer.
- Uniqueness: Globally unique, ensuring each device on a network has a distinct address.
- Layer: Operates at the data link layer (Layer 2) of the OSI model.
- Fixed: Typically fixed and cannot be changed unless the network interface is replaced.
  IP Address:
- Purpose: Identifies a device on a network (local or across the internet). It's like a postal address for your entire network, allowing communication across the internet.
- Assigning: Assigned by an Internet Service Provider (ISP) or a network administrator.
- Uniqueness: Must be unique within a given network (though different networks can have the same private IP).
- Layer: Operates at the network layer (Layer 3) of the OSI model.
- Dynamic: Can change depending on the network, location, or assignment method.

Port Address:

- Purpose: Identifies a specific process or application on a host device (e.g., a computer) to which incoming data should be directed. It's like identifying which room within a house you should deliver a package to.
- Assigning: Predefined or dynamically assigned.
- Uniqueness: Must be unique within a host.
- Layer: Operates at the application layer (Layer 7) of the OSI model.
- Dynamic: Can be dynamic or static, depending on the application

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

To view your internet browser's history, you'll generally access it through your browser's settings menu. In most browsers, you'll find a "History" option, which will display a list of the websites you've visited.

Google Chrome:

1) Open Chrome: Launch the Chrome browser on your device.
2) Access the Menu: Click the three vertical dots (More) in the top-right corner of the browser window.
3) Select History: Hover your mouse over "History" and choose "History" from the submenu.
4) View History: Your browsing history will be displayed.

Mozilla Firefox:

1) Open Firefox: Launch the Firefox browser.
2) Open the Menu: Click the three horizontal lines (Menu) in the top-right corner of the browser window.
3) Select History: Choose "History" from the menu.
4) View History: Your browsing history will be displayed.

Microsoft Edge:

1) Open Edge: Launch the Edge browser.
2) Open the Menu: Click the three horizontal dots (More actions) in the top-right corner of the browser window.
3) Select History: Choose "History" from the menu.
4) View History: Your browsing history will be displayed.

Safari (macOS):

1) Open Safari: Launch the Safari browser.
2) Select History: Choose "History" from the Safari menu at the top of the screen.

View History: Your browsing history will be displaye