DATA COMMUNICATIONS

CCA

MAY 3, 2025

MONISHA M

CCA-102: DATA COMMUNICATIONS

ASSIGNMENT2

1. What are the different types of networks?

The different types of networks are:

1. LAN (Local Area Network):

- Covers a small area like a home, office, or school.
- High speed and low latency.

2. WAN (Wide Area Network):

- Spans large geographical areas (e.g., between cities or countries).
- The Internet is the largest WAN.

3. MAN (Metropolitan Area Network):

- Covers a city or a large campus.
- Larger than LAN but smaller than WAN.

4. PAN (Personal Area Network):

- Used for personal devices (e.g., between smartphone and laptop via Bluetooth).
- Very limited range (a few meters).

5. WLAN (Wireless LAN):

- A type of LAN that uses wireless communication (Wi-Fi).
- Common in homes and public places.

6. CAN (Campus Area Network):

- Connects multiple LANs within a campus like a university or corporate office

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

- Shielded Twisted Pair (STP) and Unshielded Twisted Pair (UTP) are both types of twisted-pair cabling, but STP has an additional shielding layer for better protection against electromagnetic interference (EMI). UTP is more common for general networking applications, while STP is preferred in environments with high EMI.

3. What is difference between baseband and broadband transmission?

Baseband Transmission:

Digital Signals:

- Baseband uses digital signals, which are discrete pulses representing data.

Single Channel:

- The entire bandwidth of the transmission medium is used by a single signal at a time.

No Modulation:

- Baseband signals are not modulated (shifted in frequency) before transmission.

Example:

Ethernet is a common example of baseband transmission in LANs.

Broadband Transmission:

Analog and Digital Signals:

- Broadband can transmit both digital and analog signals, often using modulated carrier waves.

Multiple Frequencies:

- Different data streams are transmitted on different frequencies (or channels) simultaneously.

Higher Data Rates:

- Broadband allows for higher data transfer rates compared to baseband due to the use of multiple channels.

Example:

Cable TV and some types of internet connections use broadband transmission.

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

- The hub broadcasts all incoming packets to all connected devices without examining destination addresses. A switch forwards packets only to the relevant destination port based on its MAC address table. The router routes packets between different network segments based on destination IP addresses.

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

- other, the MAC address transfers as well. The MAC address is physically burned into the NIC's hardware (ROM) and is tied to the card, not the PC.

Explanation:

- MAC Address is Hardware-Specific:

A MAC (Media Access Control) address is a unique identifier assigned to a specific NIC card. It's like a physical address for a device on a network.

- NIC Hardware:

The MAC address is stored within the NIC's hardware, usually in a Read-Only Memory (ROM) chip.

- Transfer with NIC:

When you move the NIC to another PC, you are physically moving the hardware containing the MAC address, so the MAC address goes along with it.

- No Change in MAC Address:

The MAC address of the NIC will remain the same regardless of which PC it is installed in.

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

When troubleshooting computer network problems, common hardware-related issues that can occur include:

1. Faulty Ethernet cables:

Damaged, broken, or loosely connected cables can disrupt network connectivity

2. Defective Network Interface Card (NIC):

A malfunctioning NIC can prevent a computer from connecting to the network.

3. Switch or Hub Failure:

If a central device like a switch or hub is not working, all connected devices may lose network access.

4. Router or Modem Issues:

Power failure, overheating, or configuration errors in routers/modems can cause network outages.

5. Loose or improperly connected hardware:

Physical disconnections or improperly seated components can interrupt the connection.

6. Overheating devices:

Overheated network hardware can shut down or function erratically.

7. Power supply problems:

Power surges or failures in power adapters or UPS can affect network hardware.

8. Outdated or incompatible hardware:

Older devices may not support modern network standards, causing performance or compatibility issues.

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

In a network with two servers and twenty workstations, the best practice is to install antivirus software on:

- ❖ All Workstations:

Each workstation interacts with users, external devices, and the internet—making them more vulnerable to malware. Antivirus helps protect from user-initiated threats.

- ❖ Both Servers:

Servers store and manage shared data. If infected, they can spread malware to all connected devices. Antivirus is essential for data integrity and network safety.

- ❖ (Optional) Centralized Antivirus Management Server:

In business environments, use a centralized antivirus management system to monitor, update, and control antivirus software across all machines.

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

- static IP address is a permanent, fixed IP address assigned to a device, while a dynamic IP address is a temporary, changing IP address assigned by a DHCP server. IPv4 is an older protocol with 32-bit addresses, while IPv6 is a newer protocol with 128-bit addresses, offering a much larger address space and enhanced security.

Static IP Addresses:

Fixed and Permanent:

Static IP addresses remain the same as long as the device is active and connected to the network.

Manual Configuration:

They are manually configured and assigned to a device.

Used for:

Devices that require a consistent, permanent address, such as servers, routers, or printers.

Benefits:

Reliability: Provides consistent and reliable access to devices.

Accessibility: Ensures devices are always accessible at a known address.

Security: Can be more secure as they don't change, making them easier to track.

Drawbacks:

Cost: Typically, more expensive than dynamic IPs.

Complexity: Requires manual configuration, which can be complex for large networks.

Limited Availability: Limited number of static IPv4 addresses.

Dynamic IP Addresses:

Temporary and Changing:

Dynamic IP addresses are assigned by a DHCP server and change periodically, often every few days or weeks.

Automatic Assignment:

Assigned automatically to a device when it connects to the network.

Used for:

Most home and personal devices, where a consistent address is not required.

Benefits:

Cost-Effective: More cost-effective for ISPs to manage.

Privacy: Changes frequently, making it harder to track and potentially reducing the risk of targeted attacks.

Easy Management: DHCP simplifies IP address assignment and management.

Drawbacks:

Unpredictable: The IP address can change, making it harder to access devices consistently.

Security: Can be exploited by unauthorized servers, potentially leading to network breaches.

IPV4 VS. IPV6:

IPv4:

Address Size: 32-bit address space, resulting in a limited number of available addresses.

Address Format: Dot-decimal notation (e.g., 192.168.1.1).

Limitations: Shortage of available addresses, making it difficult to support the growing number of internet-connected devices.

IPv6:

Address Size: 128-bit address space, offering a vast number of available addresses.

Address Format: Hexadecimal notation (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Benefits:

Scalability: Addresses the shortage of IPv4 addresses.

Security: Incorporates built-in security features like IPsec.

Improved Routing: Enables more efficient and reliable routing.

9. Discuss TCP/IP model in detail.

- The TCP/IP model is a fundamental framework for computer networking. It stands for Transmission Control Protocol/Internet Protocol, which are the core protocols of the Internet. This model defines how data is transmitted over networks, ensuring reliable communication between devices. It consists of four layers: The Link Layer, the Internet Layer, the Transport Layer, and the Application Layer. Each layer has specific functions that help manage different aspects of

network communication, making it essential for understanding and working with modern networks.

- TCP/IP was designed and developed by the Department of Defense (DoD) in the 1970s and is based on standard protocols. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model. In this article, we are going to discuss the TCP/IP model in detail.

- TCP/IP model was developed alongside the creation of the ARPANET, which later became the foundation of the modern internet. It was designed with a focus on the practical aspects of networking at the time. The lower-level hardware details and physical transmission medium were largely abstracted away in favor of higher-level networking protocols.

What Does TCP/IP Do?

- The main work of TCP/IP is to transfer the data of a computer from one device to another. The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end. The TCP/IP model is used in the context of the real-world internet, where a wide range of physical media and network technologies are in use. Rather than specifying a particular Physical Layer, the TCP/IP model allows for flexibility in adapting to different physical implementations.

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

A web browser is a software application used to access, retrieve, and display content from the World Wide Web. It allows users to view websites, interact with online applications, and access various types of multimedia content over the Internet.

Functions of a Web Browser:

- Sends requests to web servers using HTTP/HTTPS protocols.
- Retrieves web content like HTML pages, images, videos, and scripts.
- Renders the content on the user's screen.

- Manages cookies, bookmarks, history, and browser extensions.

Common Features:

- Address bar for entering URLs
- Navigation buttons (Back, Forward, Reload)
- Tabs to open multiple pages
- Download manager
- Private or Incognito mode

Examples of Popular Web Browsers:

- Google Chrome – Developed by Google; widely used for its speed and extension support.
- Mozilla Firefox – Open-source browser known for privacy features.
- Microsoft Edge – Developed by Microsoft; based on Chromium.
- Apple Safari – Default browser for Apple devices.
- Opera – Known for built-in VPN and ad blocker.

11. What is a search engine? Give example.

A search engine is a software system designed to help users find information on the internet. It works by indexing and cataloging content from various sources, then providing users with a list of relevant results based on their search queries. A popular example is Google search.

Elaboration:

Indexing:

Search engines use algorithms to "crawl" the web, visiting and analyzing webpages to create a massive index. This index stores information about the content and structure of each webpage.

Searching:

When a user enters a query, the search engine uses its index to find relevant pages.

Ranking:

The search engine uses complex algorithms to rank the results based on factors like relevance, authority, and user experience. The most relevant and authoritative pages are typically displayed higher in the search results.

Examples:

Besides Google, other popular search engines include Bing, Yahoo!, and DuckDuckGo.

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

What is the Internet?

The Internet is a global network of interconnected computers that communicate with each other using standardized communication protocols (like TCP/IP). It allows devices to share information, access remote systems, and connect users worldwide.

Key Features:

- Worldwide connectivity
- Supports various services (web, email, file sharing, etc.)
- Public and decentralized

What is the WWW (World Wide Web)?

The World Wide Web (WWW) is a system of interlinked hypertext documents and multimedia content, accessible via the Internet using a web browser. It uses the HTTP/HTTPS protocol to transmit data.

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

An Internet Service Provider (ISP) is a company or organization that provides individuals and businesses with access to the Internet and related services such as email, web hosting, and domain registration.

Functions of an ISP:

- Provides internet connectivity via various technologies (broadband, fiber optics, DSL, satellite, etc.)
- Allocates IP addresses
- Offers customer support and technical assistance

- May provide additional services like cybersecurity, cloud storage, or leased lines

Examples of ISPs in India:

- Jiu (Reliance Jiu Info COMM Ltd.)
- Airtel (Bharti Airtel)
- BSNL (Bharat Sanchar Nigam Limited)
- ACT Fibernet
- Hatchway
- spectra
- You Broadband (a subsidiary of Vodafone Idea)

These ISPs offer different internet plans based on speed, data limits, and connection types (fiber, mobile data, etc.).

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

MAC addresses identify devices within a local network, IP addresses identify devices across networks, and port numbers designate specific processes or services on a device.

Here's a more detailed breakdown:

MAC Address:

What it is: A Media Access Control address is a unique identifier assigned to a device's network interface card (NIC) by the manufacturer.

Function: It's used for communication within a local area network (LAN).

Layer: Operates at the data link layer of the OSI model.

Example: Think of it as the physical address of your computer on your local network, similar to a physical address of a house.

Fixed or Dynamic: MAC addresses are typically fixed and don't change.

Scope: Local to a specific network.

Example Use: When you send a file to your local printer, the MAC address of your computer and the printer are used for local communication within the network, according to TechTarget.

IP Address:

What it is: An Internet Protocol address is a logical address that identifies a device on a network, whether it's a local network or the internet.

Function: Used for communication across different networks.

Layer: Operates at the network layer of the OSI model.

Example: Think of it as your device's "global" address, similar to a postal address for mail.

Fixed or Dynamic: IP addresses can be static (fixed) or dynamic (assigned by the network).

Scope: Global, across networks.

Example Use: When you visit a website, your IP address is used to route the data packets from your device to the website server, says Netmaker.

Port Address:

What it is: A port number is a logical identifier that distinguishes between different applications and services running on a device.

Function: Determines which specific application or service on a server should handle the incoming data.

Layer: Operates at the application layer of the OSI model.

Example: Think of it as the specific door you need to enter into a building (the IP address) to reach a particular office (the service).

Fixed or Dynamic: Port numbers can be pre-assigned for common services (e.g., port 80 for web traffic) or dynamically assigned by the operating system.

Scope: Within a single device.

Example Use: When you visit a website, your browser sends data to port 80 or 443 (HTTPS) on the server's IP address,

15. How do we view my Internet browser's

open your browser, navigate to its history section (often found in the menu, settings, or as a dedicated button), and then select the option to view your full history or filter it by date, website, or keywords.

Here's a more detailed explanation for different browsers:

- ❖ Chrome:

1. Open Chrome.
2. Click the "More" button (three dots) in the top right corner.
3. Select "History" from the menu.

4. You can then view your history, search for specific entries, or filter by date.

❖ Firefox:

1. Open Firefox.
2. Click the "Menu" button (three horizontal lines) in the top right corner.
3. Select "Library."
4. Click "History".
5. You can then view your history, search for specific entries, or filter by date, website, or keywords.

❖ Safari:

1. Open Safari.
2. Go to "History" in the menu bar.
3. Select "Show All History".
4. You can then view your history, search for specific entries, or filter by date, website, or keywords.

❖ Edge:

1. Open Edge.
2. Click the "More" button (three dots) in the top right corner.
3. Select "History" from the menu.
4. You can then view your history, search for specific entries, or filter by date, website, or keywords.