Akash Gupta

CCA-102: Data Communications

ASSIGNMENT

1. What are the different types of networks?
2. Explain the Shielded twisted pair (STP) and Unshielded twisted pair(UTP)
3. What is difference between baseband and broadband transmission?
4. What is the difference between a hub, modem, router and a switch?
5. When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?
6. When troubleshooting computer network problems, what common hardware-related problems can occur?
7. In a network that contains two servers and twenty workstations, where is the best place to install an Anti-virus program?
8. Define Static IP and Dynamic IP? Discuss the difference between IPV4 and IPV6.
9. Discuss TCP/IP model in detail.
10. What is a Web Browser (Browser)? Give some example of browsers.
11. What is a search engine? Give example.
12. What is the Internet & WWW? What are the uses of internet in our daily life?
13. What is an Internet Service Provider? Give some example of ISP in India.
14. Discuss the difference between MAC address, IP address and Port address.
15. How do we view my Internet browser's history?

Sharma 14-11-2024

Advance Institute of Computer Education
Bsc
KU
UK

Q1. What are the different types of Networks?

Ans:- There are various types of networks each designed to serve specific purposes and Environment. Here's a concept overview of the main types:

Types of Networks

1. Personal Area Network (PAN)

- Description :- It connects devices within a very limited area, typically within a few meters.

  Uses :- Personal devices like smartphones, tablets, and laptops.

2. Local Area Network (LAN)

- Description :- Connects devices within a limited Geographical area, such as a building or campus.
- Uses :- Office Networks, Home Networks.

3. Wireless Local Area Network (WLAN)

- Description :- A LAN that connects devices wirelessely.
- Uses :- Wi-fi Networks in Homes and bussinesses.

4. Campus Area Network (CAM)

- Description :- It connects multiple LANs within a specific Geographical area like a university campus.

Uses :- University or corporate campus.

5. Metropolitan Area Network (MAN)

- Description :- It connects Networks accross a city or a larger campus.

- Uses :- City - wide wi-fi or Government Networks

6. Wide Area Networks (WAN)

- Description :- It connects devices over large Geographical areas often using leased telecommunication lines.

Uses :- Internet, corporate Networks spanning multiple locating.

7. Storage Area Network (SAN)

- Description :- A Specialized Network designed to provide access to consolidated, block - level data storage.

Uses :- Data centers for high - speed data.

8. Virtual Private Network (VPN)

- Description :- It creates a secure connection over the internet often using Encryption

Uses :- Secure remote access to private Networks.

9. Home Area Network (HAN)

- Description :- It connects devices within a home.

Uses :- Smart Home devices personal computers, and Environment System.

Summary :-

Scale :- Networks vary in size from personal (PAN) to vast (VAN).

Connection type :- They can be wired (LAN, SAN) or wireless (WLAN, VPN)

Purpose :- Each Network type is tailored for specific applications such as personal uses business operations, or data managements.

If you would like more detailed information on any specific type of network, feel free to ask.

Q2. Explain the Shielded twisted pair (STP) and Unshield twisted pair (UTP)

Ans:- Shielded Twisted Pair (STP) and Unshield Twisted Pair (UTP) are both types of twisted pair cables used for networking and telecommunications. They are designed to transmit data over short to medium distances and are commonly used in various application, including computer networks, telephone system, and data transmission.

★ Shielded Twisted Pair (STP)

Definition :- STP cables also consist of twisted pairs of wires, but they include additional shielding around the pairs to protect against electromagnetic interface and crosstalk.

Characteristics :-

- Construction :- In addition to twisted pairs, STP cables have a foil or braided shied that surrounding the pairs, which helps to block interference from external sources.
- Cost :- Generally more expensive than UTP due to the additional materials used for shieding.

- Performance :- STP cables can provide better performance in environments with high levels of electromagnetic interface making them suitable for industrial applications or areas with heavy machinery.

- Applications :- Often used in enviroments where data integrity is critical, such as in data centers, hospitals, and industrial setting.

Limitations :-

Flexibility :- STP cables are typically less flexible and heavier than UTP cables, making installation more challenging in some cases.

Cost Considerations :- The higher cost may not be justified in low-interference environments.

Unshielded Twisted Pair (UTP)

Definition :- UTP cables consist of pairs of wires twisted together without and any additional shielding.

The twisting helps to reduce electromagnetic interface (EMI) and crosstalk between the pairs.

- Characteristics :-

Construction :- Typically made of copper wires twisted into pairs. The twisting helps to cancel out electromagnetic interface.

Cost :- Generally less expensive than STP because they do not include shielding.

Flexibility :- UTP cables are more flexible and easier to install due to their lighter weight and lack of shielding.

Applications :- Commonly used in Ethernet networks, telephone lines and various data communication system.

Limitations :-

Susceptibility to interference :- UTP cables are more susceptible to external interference and crosstalk compared to STP cables, especially in environments with high electromagnetic interference.

Summary :- In summary, the choices between STP and UTP depends on the specific requirements of the installation environment. UTP is suitable for most general-purpose networking needs, while STP is preffered in environments where electromagnetic interference is a concern. Understanding the difference between these two types of twisted pair cables can help in selecting the right one for a given application.

Q3. What is difference between baseband and broadband transmission?

Ans:- Baseband and broadband transmission are two distinct methods of transmitting data over a network. The primary difference lies in the type of signals they use and the way they transmit data.

Baseband transmission utilizes digital signaling and is designed to send a signal at a time, while broadband transmission uses along a analog signaling to transmit multiple data signals simultaneously. Here's a detailed comparison :-

.. Type of Signal :-

Baseband Transmission :-

- Uses digital signals.
- Transmit binary values directly as pulses of different voltage levels.

Broadband Transmission :-

- Uses analog signals.

Employs modulation techniques to mix data into a carrier wave for transmission.

2. Data Transmission :.

Baseband Transmission :-

- Can Only transmit one data stream at a time.
- Supports bidirectional communication, allowing data to be a sent and received simultaneously.

Broadband Transmission :-

- Can transmit multiple data streams simultaneously.
- Typically support unidirectional communication, where data flows in one direction at a time.

. Distance and Signal Strength

- Baseband Transmission :
  - Effective for short distances; signal strength diminishes over longer distances, requiring repeaters to boost the signal.
- Broadband Transmission :-
  - Suitable for long-distance communication; signals can travel further without significant attenuation, using amplifiers to maintain signal strength.

4. Multiplexing Techniques

- Baseband Transmission :-
  - Utilizes Time Division Multiplexing (TDM) to manage multiple signals over a signal channel.
- Broadband Transmission :-
  - Employs Frequency Division Multiplexing (FDM) to divide the channel into sub-channels for simultaneous transmission of multiple signals.

5. Applications

→ Baseband Transmission :-

- Commonly used in Ethernet LAN networks and short-range application

→ Broadband Transmission :-

- Widely used in cable and telephone networks, suitable for services like internet and television.

. What is the Difference between a Hub, modern, Router and a switch?

Ans:- Hubs, moderns routers and switches are Essential networking devices. Each serving dinctinct functions in a network. Here's a detailed comparison of their differences.

→ Hub:-

- Definition:- A Hub is a basic networking device that connects multiple Ethernet devices, allowing them to communicate as part of a single Network Segment.
- Functionally:- It operates at the physical layer of the OSI model. It forwards data packets to all connected devices without filtering.
- Use case:- It is mostly used in small networks or for connecting devices in a star topology. They are largely outdated due to inefficiency.
- Modem

Definition:- A modem (modulator demodulator) converts digital data from a computer into analog signals for transmission over telephone lines and vice versa.

Use case :- Essential for Providing Internet access to Homes and offices.

→ Router

- Definition :- A Router is a device that forwards data packets between Different Networks, directly traffic on the internet.
- Use case :- It is commonly used in homes and Business to connect to the internet and manage local network traffic.

→ Switch

Definition :- A Switch is a networking device that connects devices within a single network and uses MAC addresses to forward data only to the Intended Recipient.

Use case :- It is widely used in local area networks (LANs) to connect computers printers and servers.

Q5. When you move the NIC cards from one PC to another PC, does the MAC addresses gets transferred as well?

Ans :- Yes when you move a Network Interface card (NIC) from one PC to another, the MAC address associated with that NIC is transferred along with it Here are the key points.

NIC and MAC address.

Each NIC has a unique MAC address assigned to it which is used for Network communication at the data link layer.

Physical Transfer

When you physically transfer the NIC from one PC to another the MAC address remains the same because it is hard-coded into the NIC Hardware.

Q6. When troubleshooting computer network problems, what common hardware-related problems can occur?

Ans. Faulty Cables :- Damaged or improperly connected Ethernet cables can lead to connectivity issues. Look for frayed wires, loose connections, or bent pins.

Defective Network Interface Cards (NICs):- A malfunctioning NIC in a computer or device can prevent it from connecting to the network. This can be due to hardware failure or driver issues.

3. Router or switch Failures: Problems with routers or switches, such as power failures firmware issues or hardware malfunctions can distrup network connectivity.

4. Wireless Interface:- In wireless networks, interface from other electronic devices, walls, or even neighboring networks can be cause connectivity problems. Changing the channel or moving the access point can help.

5. Power Supply Issues:- If a network device (like a router, switch or modem) is not receiving adequate power, it may not function properly.

6. Overheating Devices:- Network devices can overheat if not properly ventilated, leading to performance issues or shutdowns.

7. Configuration Errors:- Incorrect setting on routers, switches, or firewall can block traffic. Verifying and resetting configuration may resolve the proplem.

1. 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 with two servers and twenty workstations, the best approach for installing antivirus program involves a combination of server-side and client-side installation to ensure comprehensive protection. Here's breakdown of where to install antivirus software:

1. On Each Server:

- File Server: If one of the servers acts a file server, it should have antivirus software installed to scan files accessed by workstations and to protect against malware that may be introduced through file sharing.

2. On Each workstation:-

Every workstation should have its own antivirus software installed. This is crucial because workstations are often the most vulnerable points in a network, being used by end-users who may inadvertently download malware or visit malicious websites.

3. Centrallized Management :-

Consider using a centrallized antivirus solution that allows for management of antivirus setting and updates from a single console. This makes it easier to ensure that all devices are up-to-date and properly configured.

4. Regular Updates and scans :-

Ensure that both server and workstation antivirus software is configured to receive regular updates and perform scheduled scans to maintain optimal protection against the latest threats.

5. Network Security Measures :-

In addition to antivirus software, consider implementing other security measures such as firewalls, intrusion detection/preventio systems, and regular security audits to provide a layered security approach.

By installing antivirus software on both servers and all workstations you can create a robust defence against malware and other security threats across the entire network.

88. Define Static IP and Dynamic IP? Discuss the difference between IPv4 and IPv6?

Ans:- Definition:-

- Static IP address ✱
- Definition:- A Static IP address is a fixed address assigned to a device that does not change over time. It remains constant and is manually configured.

✱ Usage:- Commonly used for servers network Printers, and device the require, constant access.

✱ Dynamic IP address

- Definition:- A dynamic IP address is assigned by a DHCP server and can change over time. It is allocated from a pool.

✱ Usage:- Typically used for personal devices like laptops and smartphones, where the IP address may change based on the network connection.

Differentiate Between IPv4 and IPv6

- IPv4 (Internet Protocol Version 4)
- Address Format :- 32-bit address, Represented as four decimal numbers.
- Address Space :- Approximately 4.3 billion unique addresses, which have become insufficient due to the internets Expansion.
- Limitations :-
  - Address Exhaution
  - Security features are not mandatory
- IPV6 (Internet Protocol Version 6)
  - Address Format :- 128-bit address Respresented in hexadecimal and separated by calons.
  - Address space :- Vastley larger, allowing for 340 undecillion unique addresses.

Q9. Discuss TCP/IP model in detail.

Ans:- The TCP/IP model, also known as the Internet protocol suite, is a conceptual framework to understand and implement network communications over the internet and similar networks. It

consists of a set of protocols that govern how data is transmitted and received over a network. The model is divided into four layers, each with specific functions and responsibilities.

☆ Layers of the TCP/IP model

1. Application Layer.
2. Transport Layer
3. Internet Layer
4. Link Layer (Network Interface Layer)

Q10:- What is a Web Browser (Browser)? Give some example of browsers.

Ans:- A Web browser is a software application that allows users to access, retrieve, and view content on the World Wide Web. Browser interpret and display HTML documents, enabling users to interact with websites, access multimedia content, and utilizes web applications. They serve as the interface between the user and the internet, handling requests for web pages and presenting the retrived information in a user-friendly format.

Key Functions of a Web Browser:

1. Rendering Web Pages
2. Navigation
3. User Interface
4. Security Features
5. Extension and Plugins
6. Support for Web Standards

★ Examples of Popular Web Browsers:-

1. Google Chrome
2. Mozilla Firefox
3. Microsoft Edge
4. Safari
5. Opera
6. Brave
7. Internet Explorer
8. Tor Browser.

★ Conclusion:-

Web browser are essential tools for accessing the internet, providing users with the ability to view and interact with a vast array of online content. The choice of browser can affect the user experience, performance, and security while browsing the web.

Q. What is a Search Engine? Give Example.

Ans:- A Search engine is a software system designed to search for information on the World Wide Web. It allows users to enter queries (keywords or phrases) and retrives a list of relevant web pages, document, images, videos, and other types of content based on the search terms. Search engines use complex algorithms to index and rank web content, making it easier for users to find the information they are looking for.

☆ Key Functions of a Search Engine :-

1. Crawling
2. Indexing
3. Ranking
4. Displaying Results

☆ Examples of Popular Search Engines:

1. Google
2. Bing
3. Yahoo
4. ~~Brave~~ DuckDuckGo
5. Baidu
6. Yandex
7. Ask.com

Conclusion

Search engines play a crucial role in navigating the vast amount of information available on the internet. They help users find relevant content quickly and efficiently, making them an essential tool for research, learning, and everyday information-seeking.

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

Ans:- The Internet and the world wide web (WWW) are two distinct but interconnected.

→ Internet

- Definition :- The internet is a global Network of interconnected computers that communicate using standarized protocols. It enables data exchange and connectivity between devices worldwide.

→ World Wide Web :-

- Definition :- The WWW is a system of interlinked hytertext documents and multimedia content accessed via the internet. It uses web browser to retrieve and display information.

Uses of the internet in daily life

1. Communication
2. Information Access
3. Entertainment
4. E.-commerce
5. Work and Productivity
6. Education
7. Health and Wellness.

8. What is an internet Service Provider? Give some examples of ISP in india?

Ans:- An Internet Service Provider (ISP) is a company that offers individuals and organizations access to the internet. ISPs provide various services, including broadband, dial-up, and wireless internet connections, as well as additional services like email, web hosting, and domain registration.

★ Examples of ISPs in India

1. Airtel Broadband
2. Jio Fiber
3. Excitel
4. Hathway
5. BSNL (Bharat Sanchar Nigam Limited)

Conclusion

ISPs play a vital role in providing internet access and services to consumers and businesses. In india, the market is competitive, with various providers offering a range of plans and services to meet diverse needs.

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

Ans:- The MAC address, IP address, and Port address are all Essential components of networking, but they serve different purposes and operate at different layers of the networking model. Here's a breakdown of each and their differences

1. Mac Address (Media Access Control Address)

- Definition:- A MAC address is a unique identifier assigned to a network interface controller (NIC) for communication on the physical network segment.
- Format :- Typically expressed in hexadecimal format, a MAC address consists of 48 bits (6 bytes), often represented as six pairs of hexadecimal digit (e.g., '00:1A:2B:3C:4D:5E).

O Layer :- Operates at the Data Link Layer (Layer 2) of the OSI model.

Purpose :- Used for local network communication. MAC addresses are essential for the functioning of Ethernet and wi-fi networks, allowing devices on the same local network to identify and communicate with each other.

- Scope :- MAC addresses are used within a local network and are usually not routable over the internet.

☆ Port Address

Definition :- A port address (or port number) is a numerical label assigned to specific processor or service on a device, allowing multiple services to run on the same IP address.

Format :- Port numbers are 16-bit integers, ranging from 0 to 65535 commonly used port ~~pu~~ numbers include 80 for HTTP, 443 for ~~HPT~~ HTTPS, and 25 for SMTP.

Layer :- Operates at the Transport Layer (Layer 4) of the OSI model.

Purpose :- Used to identify specific application or services on a device.

Scope :- Port addresses are used in conjunction with IP addresses to facillate communicate between applications on different devices.

How do we view my Internet Browser history?

Ans:- Viewing your internet browser history can vary slightly depending on the browser you are using. Below are the steps for some of the most popular web browsers:-

☆ Google Chrome:

1. Open Chrome: Launch the Google Chrome browser.
2. Access History:
   - Click on the three vertical dots (menu) in the upper right corner.
   - Hover over "History" in the dropdown menu, and then click in "History" in the submenu. Alternatively you can press 'ctrl + H (windows/Linux) or command + Y' (Mac) to open the history page directly.
3. View History :- A Library window will open, displaying your browsing history. You can search for specific entries using the search bar.

☆ Microsoft Edge

1. Open Edge: Launch the Microsoft Edge browser.
2. Access History:
   - Click on the three horizontal dots (menu) in the upper right corner.
   - Click on "History". Alternatively, you can press 'ctrl + H' (Windows) or command + Y' (Mac)
3. View History:- A Sidebar will appear showing your browsing history. You can search for specific entries using the search bar.

Safari (Mac)

1. Open Safari :- Launch the Safari browser.

2. Access History :

- Click on "History" in the menu bar at the top of the screen.
- Select "Show All History." Alternatively, you can press 'Command + Y'.

3. View History : A new window will open displaying your browser history. You can search for specific entries using the search bar.