Day 5

Networking fundamentals: -

Introduction to Networking Fundamentals:

Networking fundamentals encompass the basic concepts and principles that form the foundation of computer networking. Here is an overview of key aspects:

1. **Network Topology**:
    - Refers to how nodes and links in a network are arranged.
    - Nodes are devices capable of sending, receiving, storing, or forwarding data.
2. **Communication Protocols**:
    - Networks utilize protocols to send, receive, create, or forward data.
    - Each network node is assigned a unique IP (Internet Protocol) address.
3. **Computer Networking**:
    - Involves connecting computers to facilitate communication and data exchange.
    - Enables seamless interaction between connected devices.
4. **Networking Devices**:
    - Essential components include switches, routers, and wireless access points.
    - Facilitate communication among devices within a network.
5. **Importance of Networking Fundamentals**:
    - Understanding these basics is crucial for effective network management.
    - Helps in establishing reliable and secure communication infrastructures.

By grasping these fundamental concepts, individuals can gain a solid understanding of how networks operate and the principles governing data exchange between devices.

Networking models: -

Networking Models:

Networking models are conceptual frameworks that define the functions and interactions of devices in a network. They provide a structured approach to understanding how data is transmitted, received, and processed across a network. Here are some common networking models:

Introduction to OSI Model and Its Layers:

The OSI (Open Systems Interconnection) model is a conceptual framework that defines how computer systems communicate over a network. It consists of **seven layers**, each responsible for specific functions in the communication process. Here is an overview of the OSI model and its layers:

1. **Physical Layer (Layer 1)**:
    - Deals with the physical connection between devices.

- Transmits raw data bits over a physical medium.

2. **Data Link Layer (Layer 2)**:
    - Provides error detection and correction.
    - Organizes bits into frames for transmission.
3. **Network Layer (Layer 3)**:
    - Handles routing and forwarding of data packets.
    - Manages logical addressing and traffic control.
4. **Transport Layer (Layer 4)**:
    - Ensures reliable data transfer between end systems.
    - Manages flow control and error recovery.
5. **Session Layer (Layer 5)**:
    - Establishes, maintains, and terminates connections between applications.
    - Synchronizes data exchange and manages dialogues.
6. **Presentation Layer (Layer 6)**:
    - Translates data into a format that the application layer can understand.
    - Handles data encryption and decryption.
7. **Application Layer (Layer 7)**:
    - Provides network services directly to user applications.
    - Supports communication between software applications.

Understanding the OSI model and its layers is essential for network professionals to troubleshoot issues, design networks, and ensure efficient communication across different devices and systems.

TCP/IP Model:

The TCP/IP (Transmission Control Protocol/Internet Protocol) model is a networking framework that serves as the foundation of the internet and modern networking. It consists of **four layers** that define how data is transmitted and received between devices. Here is an overview of the TCP/IP model and its layers:

1. **Application Layer**:
    - Responsible for application-level protocols and data exchange.
    - Includes protocols like HTTP, FTP, SMTP, and DNS.
2. **Transport Layer**:
    - Manages end-to-end communication and data flow control.
    - Utilizes protocols like TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

3. **Internet Layer**:
    - Handles addressing, routing, and packet forwarding.
    - Uses IP (Internet Protocol) to facilitate communication between different networks.
4. **Network Interface Layer** (also known as Link Layer or Network Access Layer):
    - Deals with hardware addressing and physical transmission of data.
    - Includes protocols like Ethernet, Wi-Fi (IEEE 802.11), and PPP (Point-to-Point Protocol).

The TCP/IP model is widely adopted due to its scalability, flexibility, and compatibility with diverse networking technologies. It forms the basis for communication on the internet and plays a crucial role in connecting devices across different networks. Understanding the TCP/IP model is essential for network administrators, engineers, and anyone working with computer networks.

IP(Internet protocol): -

IP Overview:

IP (Internet Protocol) is a fundamental communication protocol that enables data packets to be sent across a network. It provides the addressing and routing mechanisms necessary for data transmission over the internet and other networks.

IP Classifications:

IP addresses are classified into different categories based on the size of the network they represent. The classifications are as follows:

1. **Class A:**
    - **Range:** 0.0.0.0 to 127.255.255.255
    - **Netmask:** 255.0.0.0
    - **Example:** 10.0.0.0, 126.0.0.0
    - **Reserved:** 127.x.x.x (loopback)
2. **Class B:**
    - **Range:** 128.0.0.0 to 191.255.255.255
    - **Netmask:** 255.255.0.0
    - **Example:** 172.16.0.0, 191.168.0.0
3. **Class C:**
    - **Range:** 192.0.0.0 to 223.255.255.255
    - **Netmask:** 255.255.255.0
    - **Example:** 192.168.0.0, 200.200.200.0
4. **Class D (Multicast):**
    - **Range:** 224.0.0.0 to 239.255.255.255

- **Used for multicast group addressing**

5. **Class E (Experimental):**
    - **Range:** 240.0.0.0 to 255.255.255.255
    - **Reserved for experimental purposes**

IP Versions:

There are two main versions of IP in use today:

1. **IPv4 (Internet Protocol version 4):**
    - **Address Format:** Consists of 32 bits in four octets (e.g., 192.168.1.1)
    - **Features:** Widely used, but limited address space (4.3 billion addresses)
    - **Example:** 192.168.1.1
2. **IPv6 (Internet Protocol version 6):**
    - **Address Format:** Consists of 128 bits in eight groups of four hexadecimal digits (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334)
    - **Features:** Expanded address space (340 undecillion addresses)
    - **Example:** 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental
Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.		

Understanding IP classifications and versions is crucial for network administrators and IT professionals to effectively manage and configure networks, assign addresses, and ensure seamless communication across the internet and other networks.

Firewall Overview:

A **firewall** is a crucial cybersecurity tool that plays a vital role in monitoring and filtering network traffic to enhance security. It acts as a barrier between a trusted internal network and untrusted

external networks, controlling the flow of data to prevent unauthorized access and potential security threats.

Types of Firewalls:

There are different types of firewalls, each serving specific purposes and offering varying levels of protection. Here are some common types:

1. **Packet Filtering Firewall:**
    - Examines packets of data and filters them based on predefined rules.
2. **Circuit-Level Gateway:**
    - Works at the session layer of the OSI model, monitoring TCP handshakes to determine if a connection is legitimate.
3. **Application-Level Gateway (Proxy Firewall):**
    - Acts as an intermediary for specific applications, inspecting incoming and outgoing traffic at the application layer.
4. **Stateful Inspection Firewall:**
    - Combines packet filtering and inspection of the state of active connections to make more informed decisions on allowing or blocking traffic.
5. **Next-Generation Firewall (NGFW):**
    - Incorporates advanced features like intrusion prevention, deep packet inspection, and application awareness for enhanced security.

Advantages of Firewalls:

- **Enhanced Security:** Protects networks from unauthorized access and cyber threats.
- **Traffic Control:** Monages and filters network traffic efficiently.
- **Policy Enforcement:** Enforces security policies to ensure compliance.
- **Monitoring and Logging:** Tracks and logs network activity for analysis and auditing.