**Assignment 1**

**N+ Assignment**

**By**

**Himanshu Kalambe**

**Guided by**

**Rohit Sir**

**MODULE 1**

1, what is Network ?

Ans: two or multiple devices are connected with each other are it’s called network.

There are three types of network Intranet, extranet, and internet.

2, explain types of LAN MAN and WAN ?

Ans: **LAN** (Local Area Network): It's like a network at your home, school, or office where all your devices (like computers, phones, printers) are connected together. Think of it as your personal network.

**MAN** (Metropolitan Area Network): It's a network that's bigger than your home or office network but smaller than the internet. It connects LANs in a city or a large area. Think of it as the network that connects different neighborhoods or parts of a city.

**WAN** (Wide Area Network): This is a network that connects different LANs over a large area, like connecting networks between cities or countries. It's like the internet, connecting people and devices from all over the world.

3, What is Internet ?

Ans: The Internet is a global network connecting millions of computers, facilitating communication, information sharing, and access to resources.

4, define network topology ?

Ans: Network topologies refer to the physical or logical layout of interconnected devices (such as computers, servers, routers, or switches) and the links between them within a computer network. Common topologies include star, bus, ring, mesh, and hybrid configurations.

5, Define list of cables in use of network—Twisted pair , fiber optics ?

Ans: Twisted Pair Cable: This includes categories such as Cat5e, Cat6, and Cat7, with varying levels of performance and speed.

Coaxial Cable: Used in cable television (CATV) and cable internet connections.

Fiber Optic Cable: Utilizes glass or plastic fibers to transmit data using light pulses, offering high bandwidth and long-distance transmission capabilities.

Ethernet Cable: Refers to cables designed for Ethernet networking, including twisted pair cables and fiber optic cables.

6, Straight cable standard sequence 568 A and 568 B ?

Ans: The standard sequence for straight cables using 568A is: White-Green, Green, White-Orange, Blue, White-Blue, Orange, White-Brown, Brown; for 568B it's: White-Orange, Orange, White-Green, Blue, White-Blue, Green, White-Brown, Brown.

7, What is fiber optics module and fiber connector ?

Ans: A **fiber optics module** is a component used in fiber optic communication systems to transmit and receive optical signals. It typically consists of a transmitter, which converts electrical signals into optical signals for transmission over the fiber optic cable, and a receiver, which converts optical signals back into electrical signals for processing.

A **fiber optic connector** is like a plug that connects two fiber optic cables together so that light signals can travel between them.

8, Explain Switch

Ans A switch is like a traffic controller for your computer network. It's a device that connects multiple devices, like computers, printers, and servers, within a local area network (LAN).

Switch supports unicast multicast and Broadcast.

Switch works on mac Address and create MAC table to store MAC addresses and port no.

First time switch send BPDU packet to all connected devices to collect MAC Addresses.

9, Explain Router

Router is used to connect two or more different network .

Think of a router as a bridge between your home devices (like computers, phones, and tablets) and the internet. It's like a magic box that helps your devices talk to the internet and each other. So, when you want to check your email or watch videos on YouTube, your router makes sure everything gets where it needs to go smoothly

10, Explain MODEM ?

Ans: **(Modulator-Demodulator):** helps your computer talk to the internet. It changes your digital signals into ones that can travel over phone lines, cables, or fiber optics. Then, when data comes back from the internet, it changes those signals back into digital data your computer can use. This lets you do things like browse the web, watch videos, or play games online.

11, Explain DHCP Dynamic host configuration protocol Explain Domain Naming Services What is protocol?

Ans: **DHCP** (Dynamic Host Configuration Protocol) automatically assigns IP addresses to devices on a network, making it easier to connect to the internet without manual configuration.

**DNS** (Domain Name System) translates domain names to IP addresses DNS translates human-readable domain names (like example.com) into IP addresses (like 192.0.2.1), allowing computers to find each other on the internet.

A **protocol** is a set of rules or guidelines governing the exchange of data between devices or systems in a network, ensuring effective communication.

12, What is unicast multicast and broadcast ?

Ans: **Unicast:** Imagine sending a private message to just one person. Unicast is like that - it's a one-to-one communication where data is sent from one sender to one receiver.

**Multicast:** Multicast is like sending a message to a group of friends. It's a one-to-many communication where data is sent from one sender to multiple specific recipients who are interested in receiving it.

**Broadcast:** Broadcast is like making an announcement in a crowded room where everyone hears it. It's a one-to-all communication where data is sent from one sender to all devices in the network, whether they're interested in receiving it or not.

13, What is OSI model?

Ans : The OSI (Open Systems Interconnection) model is like a blueprint that helps computers communicate with each other. It breaks down the communication process into seven layers, each handling a specific aspect of data transmission, from physical connections to application-level interactions.

14, what is port number ?

Ans : A port number is like a door number on a building - it helps data packets find their way to the right application or service running on a computer, enabling communication between different programs over a network

15, Difference between TCP V/S UDP communications What is session development?

Ans: TCP (Transmission Control Protocol):

1. TCP is connection oriented protocol .
2. It ensures that data is delivered reliably and in order.
3. It includes error-checking and retransmission of lost packets.
4. It's a bit slower because of all the checks and confirmations.

UDP (User Datagram Protocol):

1. UDP is connectionless protocol .
2. It's faster because it doesn't include all the extra checks for reliability.
3. It's more like a "best effort" delivery method; there's no guarantee that data will arrive or arrive in order.
4. It's commonly used for real-time applications like video streaming or online gaming, where speed is more important than reliability.

**Session development** is like building a temporary connection between two devices or applications over a network. It involves establishing, managing, and terminating sessions, ensuring smooth communication and data exchange. Think of it as setting up a phone call - you dial the number (establish session), talk (exchange data), and hang up (terminate session) when finished.

16, What is flow control?

Ans: Flow control is like managing traffic on a road - it regulates the flow of data between sender and receiver to prevent overwhelming the receiving device, ensuring smooth and efficient communication over a network.

17, What is the difference between TCP IP model and OSI model?

Ans: The TCP/IP model is like a streamlined version of the OSI model, focusing on four layers instead of seven. It's more commonly used in modern networks and directly integrates with the internet, while the OSI model serves as a conceptual framework for understanding network communication.

18, What is arp broadcast?

ARP (Address Resolution Protocol) broadcast is like calling out to everyone in a room to find out who owns a specific item - it's a message sent by a device to all devices on a local network to discover the MAC address associated with a particular IP address.

19, What is mac-address?

Ans: MAC address is like a unique serial number for a network device - it's a hardware identifier assigned to each device's network interface, allowing it to be identified on a network.

20, What is ip address? Difference between ipv4 address and ipv6 address ?

Ans: An IP address is like a mailing address for your computer - it's a unique identifier assigned to each device connected to a network, allowing them to communicate with each other over the internet.

**IPv4 address** 32 bit is like an older address system with numbers separated by dots (e.g., 192.168.1.1), and it's running out of available addresses due to increasing internet usage.

**IPv6 address** 128 bit is like a newer, more advanced address system with longer combinations of letters and numbers (e.g., 2001:0db8:85a3::8a2e:0370:7334), providing vastly more available addresses to accommodate the growing number of devices connected to the internet.

21, What is a firewall to use for?

Ans: firewall is like a security guard for your computer or network - it monitors and controls incoming and outgoing network traffic based on predetermined security rules, helping to protect against unauthorized access, malware, and other cyber threats.

**Module – 2**

1, What is ping ?

Ans: Ping is like sending a quick message to check if another computer or server is reachable and how long it takes for the message to go and come back, helping to diagnose network connectivity and performance issues.

2, What is traceroute ?

Ans: Traceroute it helps you trace the path that data packets take from your computer to a destination server or website, showing each step along the way and how long it takes to reach each point.

3, What is nslookup?

Ans: NSLookup (Name Server Lookup) is like asking a phone directory - it's a tool used to query DNS (Domain Name System) servers to look up information about domain names, such as their corresponding IP addresses or vice versa.

4, What is NAT?

Ans: NAT, which stands for Network Address Translation, is like a translator for internet traffic. It allows multiple devices in your home or office to share a single public IP address (the one the internet sees) to access the internet. It's like having a receptionist that takes messages for different departments in a big company and sends them out with the company's main phone number. This helps keep your devices safe and saves on the limited number of available public IP addresses.

5, What is PAT?

Ans: PAT stands for Port Address Translation. It's a type of Network Address Translation (NAT) that allows multiple devices in a network to share a single public IP address, but each device is distinguished by the port number it uses. It's like having a single phone number for a company, but each department within the company has its own extension number. PAT helps manage and organize internet traffic from different devices efficiently.

6, What is SOHO network?

Ans: SOHO stands for Small Office/Home Office. A SOHO network refers to the networking environment that supports a small business or a home office setup. These networks are typically smaller in scale compared to enterprise networks but still need to offer reliable connectivity and security.

7, What is PAT?

Ans: PAT (Port Address Translation) allows multiple devices on a local network to share a single public IP address by using different port numbers for each connection. This method is part of network address translation (NAT).

Conserves IP Addresses:

Multiple devices share one public IP address.

Uses Port Numbers:

Differentiates devices by assigning unique port numbers.

Enhances Security:

Hides internal IP addresses from the internet.

8, Different between NAT & PAT?

Ans · Number of Public IPs:

· NAT: Can use multiple public IPs (one-to-one or many-to-many).

PAT: Uses a single public IP for multiple private IPs (many-to-one).

· Translation Method:

· NAT: Translates only IP addresses.

PAT: Translates both IP addresses and port numbers.

· Scalability:

· NAT: Limited by the number of available public IP addresses.

PAT: More scalable as it uses unique ports, allowing many devices to share one public IP.

· Common Usage:

· NAT: Suitable for smaller networks with sufficient public IPs.

PAT: Ideal for larger networks with limited public IPs, such as home networks and small offices.

8, What Is Acl?

Ans:

ACL (Access Control List) Explained

An Access Control List (ACL) is a set of rules used to control network traffic and limit access to network resources. ACLs are essential for network security and management.

Purpose:

Control the flow of traffic into and out of a network.

Filter packets based on specified criteria.

9, What Are Different Types of Acl? What Is Wildcard Mask?

Ans Types:

Standard ACLs: Filter traffic based on source IP addresses.

Extended ACLs: Filter traffic based on multiple criteria such as source and destination IP addresses, port numbers, and protocols.

A wildcard mask is a bit mask used in networking to specify which parts of an IP address should be considered significant when performing access control list (ACL) matching. It is closely related to subnet masks but operates in a reverse manner. Here’s a concise explanation:

To find the wildcard mask for a subnet mask, subtract each octet of the subnet mask from 255. For example, for a subnet mask 255.255.255.0, the wildcard mask would be 0.0.0.255.

10, Explain Circuit switching

Ans Circuit switching is a networking methodology used in traditional telephone networks to establish a dedicated communication path between two devices for the duration of a connection.

Dedicated Path:

When a call is initiated, a dedicated physical circuit or channel is established between the caller and the receiver.

This path remains dedicated and exclusive for the entire duration of the communication session.

11 What is difference between leased line and broadband?

Ans: · Leased Line: Dedicated, reliable, and costly with guaranteed bandwidth, ideal for businesses needing high-performance connectivity.

· Broadband: Shared, more affordable, variable performance, suitable for residential and small business internet access for general usage.

Cable internet, DSL (Digital Subscriber Line), fiber optic broadband are examples of broadband services.

12 What is the difference between cloud and virtualization?

Ans : Virtualization

Virtualization is a technology that allows multiple virtual instances (such as operating systems, applications, or storage devices) to run on a single physical hardware platform.

It abstracts the hardware resources and divides them into multiple virtual environments, each behaving like a standalone physical resource.

· Virtual Machines (VMs): Use software to create multiple virtual instances of operating systems on a single physical server.

· Containers: Lightweight virtualization that shares the host operating system kernel and runs isolated applications.

Cloud

· Cloud computing refers to the delivery of computing services (such as servers, storage, databases, networking, software, and analytics) over the internet ("the cloud").

Users access these services on-demand from a cloud service provider's infrastructure.

· Public Cloud: Services are delivered over the public internet and shared among multiple organizations.

· Private Cloud: Services are hosted on a private network and dedicated to a single organization.

· Hybrid Cloud: Integrates public and private cloud services, allowing data and applications to be shared between them.

13 What are network monitoring tools used

Ans Network monitoring tools are essential for maintaining and optimizing network performance, security, and availability. Here are some commonly used network monitoring tools:

Wireshark:

Type: Packet Analyzer

Purpose: Captures and analyzes network packets in real-time to troubleshoot network issues, analyze protocols, and detect anomalies.

Nagios:

Type: Network Monitoring System (NMS)

Purpose: Monitors network services, hosts, and devices for availability, performance metrics, and alerts administrators of issues.

Zabbix:

Type: Network Monitoring System (NMS)

Purpose: Monitors the performance and availability of network services, servers, and devices, offering extensive customization and alerting capabilities.

PRTG Network Monitor:

Type: Network Monitoring System (NMS)

Purpose: Provides comprehensive monitoring of network devices, bandwidth usage, and server performance with customizable dashboards and alerting.

SolarWinds Network Performance Monitor (NPM):

Type: Network Monitoring System (NMS)

Purpose: Monitors network performance, availability, and traffic patterns, offering deep insights into network health and performance trends.

Splunk:

Type: Data Analytics and Monitoring

Purpose: Collects, indexes, and analyzes log data from network devices, servers, and applications to provide insights into network performance and security incidents.

14 What are the types of network security attacks?

Ans · **Brute Force Attack:**

· Definition: Trying all possible combinations of passwords or keys until the correct one is found.

Examples: Password guessing, cryptographic key cracking.

· **DNS Spoofing/Poisoning:**

Definition: Manipulating DNS (Domain Name System) responses to redirect traffic to malicious websites or servers.

Examples: DNS cache poisoning, DNS hijacking

. **Man-in-the-Middle (MitM)**:

Definition: Intercepting and potentially altering communication between two parties without their knowledge.

Examples: Session hijacking, SSL/TLS interception.

**Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS):**

Definition: Overwhelming a network or service with a flood of illegitimate traffic to disrupt normal operations.

Examples: Ping flood, SYN flood, UDP flood.

**Phishing:**

Definition: Deceptive techniques used to trick users into divulging sensitive information (such as passwords, credit card numbers) or installing malware.

Examples: Email phishing, spear phishing, pharming.

15  Explain core switches .

Ans · Core switches are high-capacity switches that form the backbone of a network.

· They serve as the primary traffic routers within the network, handling large volumes of data traffic between different subnets and network segments.