Name:- Bhavsar Divyansh BirenKumar

Assignment of A+ N+ Assignment

Module 3

]Topic: Local area networking

• Assignment level Basic:

1. What is Network?

Ans: A network is a collection of interconnected devices or nodes that can communicate and share resources. Networks can be physical, such as cables and hardware devices, or they can be wireless, relying on radio waves or infrared signals for communication. The primary purpose of a network is to enable the exchange of information and resources between connected devices. Networks can be classified based on their size, scope, and purpose, ranging from small local area networks (LANs) within a single building to global wide area networks (WANs) that connect geographically dispersed locations.

1. What is Internet & Intranet?

Ans: Internet:

The Internet is a global network of interconnected computers and networks that use standardized communication protocols, such as TCP/IP (Transmission Control Protocol/Internet Protocol), to link billions of devices worldwide. It is a vast network that facilitates the exchange of information, resources, and services. The Internet includes a variety of services like the World Wide Web (WWW), email, file sharing, and more. Users can access the Internet through Internet service providers (ISPs) using various devices like computers, smartphones, and tablets.

Intranet:

An intranet is a private network within an organization that uses Internet technologies and protocols for internal communication and information sharing. It operates similarly to the Internet but is restricted to an organization's internal users. Intranets are used to facilitate collaboration, document sharing, and communication among employees. They often include services such as internal websites, email systems, and file-sharing tools. Intranets help improve organizational efficiency by providing a centralized platform for accessing information and resources within the company. Unlike the Internet, access to an intranet is typically restricted to authorized personnel within the organization.

• Assignment level Intermediate:

1. How many types of Network we used?

Ans: Types of Networks:

There are several types of networks, classified based on their size, scope, and purpose. Here are some common types:

Local Area Network (LAN): A network that is limited to a small geographic area, such as a single building or a campus.

Wide Area Network (WAN): A network that covers a broad area, often spanning across cities, countries, or even continents.

Metropolitan Area Network (MAN): A network that covers a larger geographic area than a LAN but is smaller than a WAN, typically within a city.

Personal Area Network (PAN): A network for personal devices, typically within the reach of an individual person, such as connecting a smartphone to a laptop via Bluetooth.

1. Different between LAN & PAN?

Ans: LAN (Local Area Network):

Scope: Covers a limited geographic area, such as a single building, office, or campus.

Connectivity Range: Typically uses wired (Ethernet) or wireless (Wi-Fi) technologies for device connectivity.

Example: A company's office network connecting computers within the same building.

PAN (Personal Area Network):

Scope: Covers a very small area, usually within the reach of an individual person.

Connectivity Range: Often involves short-range wireless technologies like Bluetooth or infrared.

Example: Connecting a smartphone to a laptop or a tablet using Bluetooth for file sharing or internet connectivity.

• Assignment level advance:

1. Explain LAN?

Ans: A Local Area Network (LAN) is a confined network that spans a limited geographic area, typically within a single building, office, or campus. LANs are characterized by their high data transfer rates, low latency, and private ownership. Devices within a LAN are connected through technologies like Ethernet cables or wireless connections, and LANs play a crucial role in facilitating communication and resource sharing within a localized environment. Examples of LANs include the network within a home, a school's internal network, or the network within an office building. Overall, LANs are essential for enabling efficient connectivity and collaboration among devices in a specific, close-knit location.

2. What are different types of LAN devices?

Ans: Certainly, here are the names of different types of LAN devices:

1. Computers/Workstations

2. Servers

3. Switches

4. Routers

5. Access Points

6. Network Interface Cards (NICs)

7. Hubs

8. Firewalls

9. Print Servers

10. Network Cables and Wiring

Topic: configured Network

• Assignment Level Basic

1. What is configured network?

2. How do we configure network?

• Assignment level Intermediate.

1.How to check the ip address?

Ans:

A configured network refers to a computer network that has been set up and organized according to specific parameters and requirements. This process involves defining and adjusting various settings to establish communication and functionality within the network. Here are three key points about a configured network:

Settings and Parameters: A configured network involves the establishment of settings such as IP addresses, subnet configurations, routing protocols, and security measures. These settings are defined to meet the specific needs and objectives of the network.

Communication Infrastructure: Configuration includes the setup of networking devices like routers, switches, and firewalls to facilitate data transfer between devices within the network. This ensures efficient and secure communication.

Customization for Purpose: The configuration process is tailored to the unique requirements of the network, taking into account factors such as the number of devices, types of devices, security protocols, and performance expectations. This customization ensures that the network functions optimally based on its intended purpose.

2.How to check the ip address through cmd?

Ans: To check the IP address through the Command Prompt (CMD) on Windows:

1. Open CMD: Press the `Windows key + R` to open the Run dialog, type "cmd," and press Enter.

2. Type the command ipconfig and press

3.How can we enter static address in network adapter?

Ans:

To enter a static IP address for a network adapter on Windows, follow these steps:

Open Network Settings:

Right-click on the network icon in the system tray and select "Open Network & Internet settings."

Access Network Adapter Settings:

Click on "Change adapter options" to view a list of network adapters.

Access Adapter Properties:

Right-click on the network adapter for which you want to set a static IP address and choose "Properties."

Select Internet Protocol Version 4 (TCP/IPv4):

In the properties window, locate "Internet Protocol Version 4 (TCP/IPv4)" in the list and select it.

Configure IP Address Settings:

Click on the "Properties" button below the list of protocols. In the properties window, select the option for "Use the following IP address."

Enter IP Address, Subnet Mask, and Default Gateway:

Enter the desired static IP address, subnet mask, and default gateway in the provided fields. You may also need to specify DNS server addresses.

Apply Changes:

Click "OK" to apply the changes and close the properties window.

. Topic: Wireless networking

• Assignment level Basic:

1. What is the difference between WEP and WPA?

Ans: WEP (Wired Equivalent Privacy):

Security Level: Weak

Authentication: Uses a static key for authentication.

Vulnerabilities: Vulnerable to various attacks, and the key can be easily cracked.

Usage: Considered obsolete and insecure; not recommended for use in modern Wi-Fi networks.

WPA (Wi-Fi Protected Access):

Security Level: Stronger than WEP

Authentication: Utilizes stronger encryption methods and dynamic keys through Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES).

Vulnerabilities: More secure than WEP, but older versions (WPA) may still have vulnerabilities. WPA2 and WPA3 are more secure alternatives.

Usage: WPA2 and WPA3 are recommended for securing modern Wi-Fi networks due to improved security features.

1. What is Wireless Network?

Ans:

A wireless network is a type of computer network that enables devices to communicate and exchange data without the need for physical cables or wires. In a wireless network, data is transmitted using radio waves or infrared signals, allowing devices to connect to the network and communicate with each other or access the internet.

• Assignment level Intermediate:

1. What is a wireless network connection?

Ans: A wireless network connection refers to the establishment of communication between devices without the need for physical cables or wires. In a wireless network, data is transmitted through the air using radio waves, infrared signals, or other wireless transmission methods. This allows devices to connect to the network and communicate with each other or access the internet.

1. What are the basic concepts of networking?

Ans: 1. Nodes

2. Communication Channels

3. Protocols

4. IP Addresses

5. Subnetting

6. Routers

7. Switches

8. Firewalls

9. DNS (Domain Name System)

10. LAN (Local Area Network)

11. WAN (Wide Area Network)

12. Topology

13. Bandwidth

14. Latency

• Assignment level advance:

1. What do you need to know about networking?

Ans: Foundational Concepts: Understand basic networking concepts like nodes, communication channels, protocols, IP addresses, subnetting, routers, switches, firewalls, DNS, LAN, WAN, topology, bandwidth, and latency.

Protocols and Models: Familiarize yourself with networking protocols such as TCP/IP, HTTP, DNS, and DHCP. Understand network models like OSI and TCP/IP models and the role of each layer in data transmission.

IP Addressing and Subnetting: Gain proficiency in IP addressing, including IPv4 and IPv6, and learn subnetting techniques to efficiently allocate and manage IP address space.

Security and Troubleshooting: Acquire knowledge of network security principles, including firewalls, encryption, and VPNs. Develop troubleshooting skills to identify and resolve common network issues using diagnostic tools and protocols like ping and traceroute.

1. How do you explain computer networking?

Ans: Computer networking involves connecting and interconnecting devices to share resources and information. It utilizes communication channels, protocols, and network devices to facilitate data transmission between nodes. Key components include nodes (devices), communication channels, and protocols, with the overarching goal of enabling efficient and secure data exchange within a network.

Topic: THE Internet

• Assignment level Basic:

1. What do you mean by the term URL?

Ans: URL stands for Uniform Resource Locator. It is a standardized address used to identify resources on the internet. A URL serves as a web address that specifies the location of a particular resource, such as a webpage, document, image, or file, and also indicates the protocol used to access it.

1. Term which is used to see web pages is called what?

Ans: The term used to refer to a software application or program that allows users to access and view web pages is called a "web browser." Web browsers are designed to interpret and display content written in HTML (Hypertext Markup Language), and they often support additional technologies such as CSS (Cascading Style Sheets), JavaScript, and multimedia elements like images and videos. Examples of popular web browsers include Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, and Opera.

Topic: Virtualization

• Assignment level Basic:

1. What is Virtualization

Ans: Virtualization is a technology that allows multiple operating systems (OS) or instances of an operating system to run on a single physical machine. It involves creating a virtual representation of the computer hardware, including the CPU, memory, storage, and network resources. This virtual environment, often referred to as a virtual machine (VM), operates as if it were a separate physical computer.

1. What is the Difference between Full Virtualization and Para Virtualization?

Ans:

Full virtualization and paravirtualization are two different approaches to implementing virtualization, which is the process of creating a virtual (rather than actual) version of something, such as a virtual machine (VM) that runs an operating system.

• Assignment level Intermediate:

1. What is Hyper-visor?

Ans:

A hypervisor, also known as a Virtual Machine Monitor (VMM), is a software or hardware component that enables the creation and management of virtual machines (VMs). A virtual machine is a software-based emulation of a physical computer that runs an operating system, allowing multiple operating systems to run on a single physical machine.

1. Bare-metal Hypervisor
2. Hosted Hypervisor
3. What are different hypervisors available in Linux?

Ans: 1. KVM (Kernel-based Virtual Machine)

2. Xen

3. VirtualBox

4. QEMU (Quick Emulator)

5. Virt-manager

6. Proxmox Virtual Environment (Proxmox VE)

3. What is Virtualization and what are its types?

Ans: Virtualization:

Virtualization is a technology that involves creating virtual instances of computing resources, abstracting them from the underlying physical hardware. It allows the simulation of multiple independent environments, known as virtual machines (VMs), within a single physical system.

1. Server Virtualization: Creates multiple virtual instances of a physical server, each with its own operating system.

2. Desktop Virtualization: Extends virtualization to desktop computers, enabling multiple desktop environments on a single machine.

3. Network Virtualization: Abstracts and decouples network resources for creating virtual networks independently managed from the physical infrastructure.

- Server Virtualization Examples: VMware ESXi, Microsoft Hyper-V, KVM, Xen.

- Desktop Virtualization Examples: VMware Horizon, Citrix Virtual Apps and Desktops, VirtualBox.

- Network Virtualization Examples: VMware NSX, Cisco ACI.

• Assignment level advance:

1. Name the components that are used in VMware infrastructure What is benefits of Virtualization?

Ans: Components used in VMware Infrastructure:

1. ESXi (vSphere Hypervisor) :

- ESXi is a bare-metal hypervisor that serves as the virtualization host, allowing the creation and execution of virtual machines on physical hardware.

2. vCenter Server :

- vCenter Server is a centralized management platform that enables administrators to manage and monitor multiple ESXi hosts and virtual machines from a single interface.

3. vSphere Client :

- vSphere Client is a web-based interface used for interacting with and managing the virtual infrastructure. It provides a user-friendly platform for various administrative tasks.

4. VMware Tools and vSphere Distributed Switch (VDS) :

- VMware Tools: This set of utilities enhances virtual machine performance, allows guest OS customization, and improves integration between the host and guest operating systems.

- vSphere Distributed Switch (VDS): VDS is a centralized virtual switch that simplifies network configuration and management across multiple ESXi hosts.

Benefits of Virtualization:

1. Resource Utilization and Efficiency:

- Virtualization optimizes resource utilization by running multiple virtual machines on a single physical server, reducing hardware underutilization and improving overall efficiency.

2. Cost Savings :

- Consolidating workloads onto fewer physical servers through virtualization leads to cost savings in terms of reduced hardware expenses, lower energy consumption, and minimized data center footprint.

3. Flexibility and Agility :

- Virtualization provides flexibility in dynamically allocating and reallocating resources, allowing for quick adjustments to changing workloads and business requirements.

4. Isolation, Security, and Additional Features:

- Virtualization enhances security through isolation, containing the impact of vulnerabilities within individual virtual machines. Additionally, features like centralized management, automation, high availability, and disaster recovery contribute to a robust and secure IT infrastructure.