**N+ Assignment**

**Module 5. Network Fundamentals and Building Networks**

1. What is network?

🡪 A network is a collection of computers, servers, mainframes, network devices, and other devices connected to one another for the purpose of sharing data, resources, and services. These connections can be physical, such as cables or wireless signals, or virtual, using software-defined networking technologies.

1. List Common Network Components

🡪 1. Router

2. Switch

3. Hub

4. Modem

5. Firewall

6. NIC

7. Access Point (AP)

8. Cable/Wireless Medium

9. Server

10. Gateway

1. Add and configure loopback adaptor in network and sharing center

🡪 Open Network and Sharing Center -> Change adapter settings -> File -> New Incoming Connection -> Add someone at this computer -> Next -> Through the Internet -> Next -> Check IPv4 -> Properties -> Use the following IP address -> Enter IP and subnet mask -> OK -> Allow access.

1. Explain application of network

🡪 Networks facilitate resource sharing, communication, data transfer, collaboration, and remote access, driving productivity and innovation across various domains.

1. What do you mean by Node?

🡪 A node refers to any device or point in a network where data can be transmitted, received, or processed, such as computers, servers, routers, switches, or printers.

1. practice of simple file folder sharing

🡪1. Creating a folder on a computer or server.

2. Configuring sharing settings to allow access to other users or devices on the network.

3. Granting appropriate permissions (read, write, modify) to users or groups.

4. Accessing the shared folder from other devices on the network by navigating to the network location or using UNC (Universal Naming Convention) paths.

5. Transferring files to and from the shared folder as needed.

1. List types of devices

🡪 1. Computers

2. Servers

3. Printers

4. Routers

5. Switches

6. Hubs

7. Modems

8. Access Points

9. Network Attached Storage

10. Gateways

1. Explain types of router

🡪 1. Home

2. Enterprise

3. Core

4. Edge

5. Wireless

6. Modular

7. Virtual

**Topic: Types of Network**

1. What is Difference between a LAN, MAN, WAN?

🡪 LAN: Small geographical area, limited users, high data transfer rates.

MAN: Larger area (city-scale), connects multiple LANs, moderate data rates.

WAN: Wide area coverage, connects LANs and MANs over long distances, supports many users, lower data rates due to distance.

1. Common Network Components

🡪 Common network components:

1. Router

2. Switch

3. Hub

4. Modem

5. Firewall

6. Network Interface Card

7. Access Point

8. Cable/Wireless Medium

9. Server

10. Gateway

1. Explain Network Backbone

🡪 Network Backbone refers to the primary infrastructure of a network that interconnects various smaller networks or segments within a larger network. It serves as the central pathway for data transmission between different network devices, such as routers, switches, and servers. The backbone typically utilizes high-speed connections, such as fiber optic cables or high-capacity wireless links, to ensure efficient and reliable communication across the network. It forms the core infrastructure that supports the overall functionality and performance of the network, facilitating seamless data exchange and connectivity between different parts of the network.

1. Explain CAN

🡪 CAN (Controller Area Network) is a communication protocol widely used in vehicles and industrial settings for real-time control applications. It enables reliable data exchange between microcontrollers and devices in noisy environments without a host computer.

1. Define Physical Network Topologies

🡪 Physical network topologies refer to the physical layout or arrangement of network devices, cables, and connections within a network. It defines how devices are physically connected to one another and how data flows between them. Common physical network topologies include bus, star, ring, mesh, and hybrid topologies.

1. Network Architecture: Peer-to-Peer

🡪 Network architecture: Peer-to-Peer (P2P) refers to a decentralized network model where all connected devices (peers) have equal privileges and responsibilities. Each device can act as both a client and a server, allowing for direct communication and resource sharing between peers without the need for a central server. P2P networks are commonly used for file sharing, communication, and distributed computing applications.

1. Point-to-multipoint network

🡪 Point-to-multipoint network refers to a communication topology where a single point (or node) can communicate with multiple other points simultaneously, but the other points can only communicate with the single point, not with each other. It's commonly used in scenarios such as broadcasting information from a central node to multiple remote nodes in wireless communication or satellite communication systems.

**Topic: Network Devices**

1. Why we use Network and Devices

🡪 We use networks and devices to facilitate communication, share resources, access information, collaborate, and streamline processes, ultimately enhancing productivity, efficiency, and connectivity in various domains.

1. Explain Switch?

🡪 A switch is a network device that operates at the data link layer (Layer 2) of the OSI model. It connects multiple devices within a local area network (LAN) and forwards data packets between them based on the Media Access Control (MAC) addresses of the devices. Switches improve network performance by reducing collisions and optimizing bandwidth usage compared to hubs, which broadcast data to all connected devices indiscriminately.

1. Define list of cables in use of network

🡪 1. Ethernet cables

2. Fiber optic cables

3. Coaxial cables

4. Twisted pair cables

5. HDMI cables

6. USB cables

1. Explain Define Access point

🡪 An access point (AP) is a networking device that enables wireless devices to connect to a wired network. It acts as a bridge between wired and wireless networks, allowing devices such as laptops, smartphones, and tablets to access network resources and services without requiring a physical connection.

1. Which types of transmission modes in computer network

🡪 Transmission modes in computer networks:

1. Simplex

2. Half-duplex

3. Full-duplex

1. Practice on Remote Desktop connection

🡪 Remote Desktop Connection practice involves connecting to a remote computer over a network or the internet, accessing its desktop interface, and controlling it remotely.

1. Practice on remote assistance

🡪 Remote assistance practice involves connecting to another computer remotely to provide technical support, troubleshoot issues, or perform tasks, typically using remote desktop software or built-in remote assistance tools.

1. Explain Repeater and router

🡪 Repeater: A device that amplifies or regenerates signals to extend the range of a network, typically used in wireless networks to enhance signal strength and coverage.

Router: A networking device that forwards data packets between networks, typically used to connect multiple devices within a local area network (LAN) and route traffic between the LAN and external networks such as the internet.

1. What is multiplexer?

🡪 A multiplexer (MUX) is a device that combines multiple input signals into a single output signal. It selects one of the input signals based on control signals and forwards it to the output.

1. Explain MODEM

🡪 MODEM stands for Modulator-Demodulator. It's a device that modulates digital signals from a computer or terminal into analog signals for transmission over analog communication lines such as telephone lines. At the receiving end, the modem demodulates the analog signals back into digital signals for processing by the receiving device. Modems enable digital devices to communicate over analog networks.

1. Monitor "event viewer"

🡪 Monitoring the "Event Viewer" involves accessing a Windows utility that records and displays system events, errors, and warnings logged by the operating system and applications. It provides insights into system health, performance, and troubleshooting information.

**Topic: Install and configure DHCP, DNS**

1. Explain DHCP Dynamic host configuration protocol

🡪 DHCP (Dynamic Host Configuration Protocol) is a network protocol that automatically assigns IP addresses and other network configuration parameters (such as subnet mask, default gateway, and DNS servers) to devices on a network. It simplifies network administration by dynamically allocating IP addresses to devices when they connect to the network, thereby eliminating the need for manual configuration.

1. Application of DHCP with one example

🡪 Application of DHCP: Automatically assigning IP addresses to devices on a network.

Example: DHCP is used in home routers to assign IP addresses to devices (such as computers, smartphones, and smart TVs) connected to the Wi-Fi network, simplifying the process of setting up and managing network configurations for users.

1. Explain Domain naming Services

🡪 Domain Naming Services (DNS) translates domain names into IP addresses so computers can communicate over networks using human-readable names instead of numerical IP addresses.

1. Application of DNS with one example

🡪 DNS: Translates domain names to IP addresses.

Example: When you visit a website, DNS translates its domain name to the corresponding IP address, allowing your device to connect to the correct server.

**Topic: Network Topologies**

1. What are the 5 network topologies?

🡪 1. Bus Topology

2. Star Topology

3. Ring Topology

4. Mesh Topology

5. Hybrid Topology

1. What is Internet topology?

🡪 Internet topology refers to the structure or layout of interconnected networks that form the global Internet. It's characterized by a decentralized and distributed architecture where various networks, such as ISPs, data centers, and interconnected devices, are linked together through routers and switches.

1. What is protocol

🡪 A protocol is a set of rules and conventions that govern how data is transmitted and received between devices or systems in a network. It defines the format, sequence, and error control procedures for data exchange, ensuring effective communication and interoperability between different entities within a network.

1. What is the most common network topology?

🡪 The most common network topology is the Star Topology.

1. Explain star topology in networking?

🡪 In a star topology, each network device is connected directly to a central hub or switch, forming a star-like structure. All communication between devices passes through the central hub, which manages and controls the data flow. This topology offers simplicity in design, easy troubleshooting, and scalability, making it one of the most popular choices for local area networks.

1. Explain Hybrid topology

🡪 A hybrid topology combines two or more different basic network topologies, such as star, bus, ring, or mesh, into a single network. This approach is often used to leverage the strengths of each individual topology while mitigating their weaknesses. Hybrid topologies are versatile and can be tailored to suit specific network requirements, offering flexibility, redundancy, and scalability.

1. What is physical and logical topology?

🡪 Physical topology refers to the physical layout or arrangement of devices and cables in a network, such as the actual physical connections between nodes.

Logical topology, on the other hand, refers to the way in which data is transmitted between devices in a network, regardless of their physical arrangement. It focuses on how devices communicate and the paths data takes through the network.

1. What are the types of logical topology?

🡪1. Bus

2. Ring

3. Star

4. Mesh

5. Hybrid

**Topic: OSI Model**

1. What is OSI model explain?

🡪 The OSI model is a framework comprising seven layers that standardize communication protocols, from physical transmission to application interaction.

1. List of Application layer protocol

🡪 Some common Application layer protocols include:

1. HTTP

2. FTP

3. SMTP

4. POP3

5. IMAP

6. DNS

7. DHCP

8. SNM

9. SSH

10. Telnet

1. How many types of protocols are there?

🡪 There are numerous types of protocols, but broadly, they can be categorized into three main types:

1. Communication Protocols

2. Network Protocols

3. Application Protocols

1. What is the difference between TCP IP model and OSI model?

🡪 The OSI model consists of seven layers, while the TCP/IP model has four layers.

1. What is TCP IP networking?

🡪 TCP/IP (Transmission Control Protocol/Internet Protocol) networking is a suite of communication protocols used for transmitting data over networks, including the internet. It provides a standardized method for devices to communicate with each other by breaking down data into packets and routing them across interconnected networks. TCP/IP encompasses a range of protocols, including TCP, IP, UDP, ICMP, and others, each serving specific functions in data transmission and network communication.

1. What is a wired Internet connection?

🡪 A wired Internet connection refers to a network connection established using physical cables, such as Ethernet cables, to connect devices directly to a network router or modem. This type of connection offers reliable and consistent data transmission speeds, typically faster than wireless connections, and is commonly used in homes, offices, and data centers.

7. What are the disadvantages of wired networks? 3.How do I configure network

authentication?

🡪Disadvantages of wired networks:

1. Limited mobility

2. Installation complexity

3. Potential cable damage

Configure network authentication:

1. Access network settings

2. Choose authentication method

3. Enter credentials

4. Save settings

8.Practice of Team viewer, Any Desk, Google Hangout, Skype, zoom

🡪Practice of:

- TeamViewer: Remote desktop software used for screen sharing, file transfer, and remote control.

- AnyDesk: Similar to TeamViewer, allows remote desktop access and file sharing.

- Google Hangouts: Communication platform for messaging, voice calls, and video conferencing.

- Skype: Messaging and video chat application for personal and business use.

- Zoom: Video conferencing software for online meetings, webinars, and virtual events.

9.Download google chrome

🡪Download Google Chrome from the official website or app store on your device.

10.configure "date and time" opting in control panel

🡪 Access "Date and Time" settings in the Control Panel or system settings on your device, then adjust the date and time according to your preferences.

**Topic: TCP/IP**

1. What is TCP/IP?

🡪 TCP/IP (Transmission Control Protocol/Internet Protocol) is a suite of communication protocols used for transmitting data over networks, including the internet.

1. What is the full form of TCP/IP?

🡪 The full form of TCP/IP is Transmission Control Protocol/Internet Protocol.

1. List out the types of IP

🡪 The types of IP include:

1. IPv4 (Internet Protocol version 4)

2. IPv6 (Internet Protocol version 6)

1. What is protocol?

🡪 A protocol is a set of rules and conventions that govern how data is transmitted and received between devices or systems in a network.

1. DO a practical to set the tcp/ip in network adapter?

🡪 Right-click on the network adapter, select Properties, choose Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6), and then input the required IP settings.

**Topic: Cables**

1. Types of cables and connectors?

🡪 Types of cables and connectors include:

1. Ethernet cables (RJ45)

2. Coaxial cables (F connectors)

3. Fiber optic cables (LC, SC, ST connectors)

4. USB cables (Type-A, Type-B, USB-C)

5. HDMI cables

6. DisplayPort cables

7. VGA cables

8. DVI cables

1. Explain twisted pair cable and shielded twisted pair cable

🡪 Twisted pair cable: A type of cable consisting of pairs of insulated copper wires twisted together. It is commonly used in Ethernet networks for data transmission.

Shielded twisted pair cable: Similar to twisted pair cable, but with an additional shielding layer to reduce electromagnetic interference (EMI) and crosstalk. It offers better performance in noisy environments.

1. Which of these cables connect computers to monitors?

🡪 The cables that connect computers to monitors include:

1. HDMI cables

2. DisplayPort cables

3. VGA cables

4. DVI cables

1. How do I connect to a shared printer?

🡪 Open "Devices and Printers," select "Add a printer," choose "Add a network, wireless, or Bluetooth printer," then select the shared printer from the list.

1. Which cable that is commonly used to connect a computer to a printer?

🡪 The cable commonly used to connect a computer to a printer is a USB cable.

1. What are the different ports and connectors?

🡪 Different ports and connectors include USB, HDMI, DisplayPort, VGA, Ethernet, Thunderbolt, audio jacks, DVI, FireWire, Serial, Parallel, and PS/2.

1. How do I connect my laptop to my printer without cable?

🡪 You can connect your laptop to your printer without a cable by using a wireless connection. Ensure both your laptop and printer are connected to the same Wi-Fi network, then set up the printer on your laptop as a wireless printer through the printer settings or control panel.

1. Application and brief explanation of fiber optic cable and Coaxial cable

🡪 Fiber optic cable: Transmits data using light signals over long distances, offering high bandwidth and resistance to interference.

Coaxial cable: Utilized for cable TV and internet connections, featuring a central conductor surrounded by insulation and a metallic shield, allowing high-frequency signal transmission with minimal loss.

1. Which of following operates at the 5GHz frequency range?

🡪 Devices operating at the 5GHz frequency range typically include:

- Some models of Wi-Fi routers and access points, particularly those supporting the 802.11a/ac/n Wi-Fi standards.

1. What frequency does 802.11g use?

🡪 802.11g operates at the 2.4GHz frequency range.

1. What standard is compatible with 802.11a?

🡪 802.11a is compatible with the 802.11b standard.

**Topic: TCP/IP concepts - IPv6, IPv4**

1. What is the difference between IPv4 & IPv6? 2.Explain TCP/IP

🡪 1. Difference between IPv4 & IPv6:

- IPv4: 32-bit addresses, around 4.3 billion unique addresses.

- IPv6: 128-bit addresses, significantly more unique addresses.

2. TCP/IP Explanation:

- TCP/IP: Suite of protocols for network communication.

- TCP manages data transmission, while IP handles addressing and routing.

- Structured into four layers: Application, Transport, Internet, and Link.

- Fundamental for internet communication.

1. Explain IPV6 Address with Address structure

🡪 IPv6 Address Structure:

- 128-bit addresses

- Eight groups of four hexadecimal digits separated by colons

- Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

1. Define IPV6 reserve address

🡪 IPv6 reserve addresses are specific addresses set aside for special purposes within the IPv6 address space. These addresses are not meant for normal communication and are reserved for functions such as loopback testing, link-local addressing, multicast addressing, and other network management tasks.

1. Explain Difference between public ip and private ip

🡪 Public IP: Used for direct communication over the internet, unique globally.

Private IP: Used within a private network, not accessible directly from the internet.b

1. Create straight and cross cables and it's testing

🡪 Straight Cable:

- Connects different types of devices.

- Both ends follow the same pinout pattern

Cross Cable:

- Connects similar types of devices.

- One end follows T568A, and the other follows T568B.

Testing:

- Use a cable tester to check continuity and wiring correctness.

- Connect tester to each end of the cable; it should indicate proper wiring.

1. Brief explanation of ip Addresses

🡪 IP Addresses:

- Unique identifiers for devices on a network.

- Used for communication over the internet.

- Two versions: IPv4 (32-bit) and IPv6 (128-bit).

- IPv4 addresses are in decimal format, while IPv6 addresses are in hexadecimal format.

- IPv4 addresses are running out, driving the transition to IPv6.

1. What is the advantage of IPv6 over IPv4?

🡪 IPv6 offers advantages over IPv4:

- Larger address space

- Enhanced security features

- Improved network performance

- Simplified network configuration

- Better support for new technologies

1. Assign multiple IPv4 in single network adapter [lan card]

🡪 Assigning multiple IPv4 addresses to a single network adapter (LAN card) can be achieved through the network adapter settings in the operating system. This process involves accessing the network adapter properties, selecting IPv4 properties, and then adding multiple IP addresses within the same subnet. Each IP address will function independently on the same network adapter, allowing the device to communicate using any of the assigned addresses.

1. Assign simple IPv6 between two system and ping it.

🡪 To assign IPv6 addresses between two systems and ping:

1. Configure IPv6 addresses on each system. Example: `ip address add 2001:db8::1/64 dev eth0` on System 1 and `ip address add 2001:db8::2/64 dev eth0` on System 2.

2. Ensure both systems are on the same subnet.

3. Ping the IPv6 address of the other system. Example: `ping 2001:db8::2` from System 1 and `ping 2001:db8::1` from System 2.

1. Assign and configure simple IPv4 between systems

🡪 Assigning and configuring IPv4 between systems involves:

1. Assigning IP addresses within the same subnet, e.g., 192.168.1.1 for System 1 and 192.168.1.2 for System 2.

2. Ensuring both systems are on the same subnet mask, typically 255.255.255.0 for a local network.

3. Connecting the systems through a network switch or router.

4. Testing connectivity by pinging the IP address of one system from the other. For example, from System 1: `ping 192.168.1.2` and from System 2: `ping 192.168.1.1`.

1. Which is faster IPv4 or IPv6?

🡪 There isn't a significant difference in speed between IPv4 and IPv6. The perceived speed difference, if any, would likely be negligible and influenced more by factors such as network infrastructure, configuration, and efficiency of the devices and protocols involved in communication rather than the IP version itself.

1. What does TCP do?

🡪 TCP ensures reliable and ordered delivery of data packets between devices over a network. It handles error detection, packet sequencing, flow control, and congestion avoidance to guarantee accurate transmission of data.

1. Give security in sharing

🡪 Security in sharing refers to implementing measures to protect shared resources, such as files, folders, or devices, from unauthorized access or misuse. This can include using access controls like passwords, encryption, firewalls, and permissions to ensure that only authorized users can access or modify shared resources.

1. Configure "Map network drive"

🡪 Open File Explorer, select "Map network drive," choose a drive letter, enter the folder path or network address, and click "Finish."

**Topic: IP routing and Routing protocols**

1. What Is Routing?

🡪 Routing is the process of determining the optimal path for data packets to travel from a source to a destination across a network. It involves directing packets based on routing tables, which contain information about available paths, network topology, and other factors. Routing ensures efficient and reliable communication within a network by forwarding packets along the most suitable paths.

1. How Routing Starts Up?

🡪 Routing starts up when a device powers on or connects to a network, initializing its routing software and establishing connections with neighboring devices to exchange routing information.

1. What Is Hybrid Routing Protocol?

🡪 A hybrid routing protocol combines features of both distance-vector and link-state routing protocols. It typically divides the network into areas, using distance-vector within areas and link-state between them. This approach offers a balance between scalability and efficiency, making it suitable for larger networks with complex topologies.

1. What Are the Range of Ad Values?

🡪 The range of Ad values typically varies from 0 to 255, with lower values indicating higher preference for a routing source.

1. What Is an Autonomous System?

🡪 An Autonomous System (AS) is a collection of IP networks and routers under the control of a single organization or entity that operates using a common routing policy. It is identified by a unique number assigned by a regional internet registry (RIR). ASes are used in the Border Gateway Protocol (BGP) to facilitate routing between different networks on the internet.

1. Define Static Routing?

🡪 Static routing is a network routing method in which network administrators manually configure routing tables in routers or devices to define specific paths for data packets to travel between networks. Unlike dynamic routing, static routing does not involve the exchange of routing information between routers, and routes remain fixed unless manually changed.

1. Explain Dynamic Routing?

🡪 Dynamic routing is a network routing method where routers automatically exchange routing information using routing protocols to dynamically update their routing tables. This allows routers to adapt to changes in network topology, such as link failures or new network connections, by recalculating the best paths for data packets to travel between networks.

**Topic: Switching and VLANS**

1. What is VLAN?

🡪 VLAN stands for Virtual Local Area Network, which is a method of segmenting a physical network into multiple logical networks, enhancing security and network management.

1. Which two benefits of creating VLANs?

🡪 Two benefits of creating VLANs are enhanced security and improved network management.

1. What is Dynamic VLAN?

🡪 A Dynamic VLAN is a VLAN assignment method where devices are automatically assigned to VLANs based on certain criteria such as MAC address, username, or device type. This assignment is typically managed by a Dynamic Host Configuration Protocol server or a VLAN Membership Policy Server.

1. What is Static VLAN?

🡪 A Static VLAN is a VLAN configuration where devices are manually assigned to specific VLANs by network administrators. This assignment remains fixed unless manually changed, providing a stable and predictable network configuration.

1. What is VLAN and INTERVLAN?

🡪 VLAN (Virtual Local Area Network) is a method of logically dividing a physical network into multiple separate networks to enhance security and manage traffic more efficiently.

INTERVLAN refers to communication between different VLANs. It involves routing traffic between VLANs to allow devices in different VLANs to communicate with each other.

1. What is trunk port?

🡪 A trunk port is a network port configured to carry traffic for multiple VLANs, facilitating communication between switches.

1. How to configure Trunk port?

🡪 To configure a trunk port, set the port mode to "trunk" and optionally specify allowed VLANs.

1. How to delete VLAN information from Switch?

🡪To delete VLAN information from a switch:

1. Access the switch's configuration interface.

2. Enter the VLAN database mode or VLAN configuration mode.

3. Identify the VLANs you want to delete.

4. Use the appropriate command to remove the VLANs, such as "no vlan [VLAN\_ID]".

5. Repeat the process for each VLAN you want to delete.

6. Save the configuration changes.

7. Verify that the VLAN information has been deleted.