Assignment: Network Fundamentals and Building Networks

**Submitted By :- Purv Patel**

**Section 1: Multiple Choice**

**1. What is the primary function of a router in a computer network?**

**= c) Forwarding data packets between networks**

**2. What is the purpose of DHCP (Dynamic Host Configuration Protocol) in a computer network?**

**= d) Dynamically assigning IP addresses to devices**

**3. Which network device operates at Layer 2 (Data Link Layer) of the OSI model and forwards data packets based on MAC addresses?**

**= b) Switch**

4. Which network topology connects all devices in a linear fashion, with each device connected to a central cable or backbone?

**=** b) Bus

**Section 2: True or False**

5. True or False: A VLAN (Virtual Local Area Network) allows network administrators to logically segment a single physical network into multiple virtual networks, each with its own broadcast domain.

=True.

A VLAN (Virtual Local Area Network) allows network administrators to logically segment a single physical network into multiple virtual networks, each with its own broadcast domain. This segmentation enhances network management, security, and performance by isolating traffic within each VLAN and reducing broadcast traffic.

6. True or False: TCP (Transmission Control Protocol) is a connectionless protocol that provides reliable, ordered, and error-checked delivery of data packet saver a network.

= False.

TCP (Transmission Control Protocol) is not a connectionless protocol; it is a connection-oriented protocol. It provides reliable, ordered, and error-checked delivery of data packets over a network by establishing a connection between the sender and receiver before data transfer begins. Connectionless protocols, like UDP (User Datagram Protocol), do not establish such connections and do not guarantee reliable or ordered delivery of packets.

7. True or False: A firewall is a hardware or software-based security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

= True.

A firewall is a hardware or software-based security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access and protect the network from threats.

**Section 3: Short Answer**

8. Describe the steps involved in setting up a wireless network for a small officer home office (SOHO) environment.

= Steps for Setting Up a Wireless Network for a Small Office or Home Office (SOHO)

1. Plan Your Network

2. Select a Suitable Location

3. Connect the Hardware

4. Access the Configuration Interface

5. Set Up Network Name (SSID)

6. Configure Wireless Security

7. Update Firmware

8. Connect Devices

9. Test the Network

**Section 4: Practical Application**

9. Demonstrate how to configure a router for Internet access using DHCP(Dynamic Host Configuration Protocol).

= Steps to Configure a Router for Internet Access Using DHCP

1. Connect the Hardware

- Power Connection: Plug the router into a power outlet.

- Internet Connection: Connect the router’s WAN (Internet) port to the modem using an Ethernet cable.

- Computer Connection: Connect a computer to one of the router’s LAN (Ethernet) ports using another Ethernet cable (for initial setup).

2. Access the Router’s Configuration Interface

- Open a Web Browser: On the connected computer, open a web browser.

- Enter Router’s IP Address: Type the router’s default IP address (commonly 192.168.0.1 or 192.168.1.1) into the address bar and press Enter.

- Login: Enter the router’s default username and password (found in the router’s manual or on a sticker on the router).

3. Configure Internet Settings Using DHCP

- Navigate to Internet/WAN Settings: Once logged in, find the section label “Internet,” “WAN,” or similar

- Select DHCP (Automatic Configuration): In the Internet/WAN settings, choose the option for DHCP or “Automatic Configuration - DHCP.” This setting tells the router to automatically obtain an IP address and other network settings from your ISP.

4. Save and Apply Settings

- Save Settings: Click on the “Save” or “Apply” button to save the configuration changes.

- Reboot if Necessary: Some routers may require a reboot to apply the new settings. If prompted, reboot the router.

5. Verify Internet Connection

- Check Status: Navigate to the status or overview page of the router’s interface to verify that it has obtained an IP address from the ISP.

- Test Connection: Open a web browser and try accessing a website to confirm the internet connection is working.

6. Configure Wi-Fi Settings (Optional but Recommended)

- Navigate to Wireless Settings: Find the section for wireless settings or Wi-Fi.

- Set SSID: Choose a unique network name (SSID).

- Set Security: Select WPA3 or WPA2 for security and set a strong password.

- Save Settings: Save the wireless configuration settings.

7. Reconnect Devices

- Wi-Fi Devices: For wireless devices, search for the new SSID and enter the Wi-Fi password to connect.

- Wired Devices: Ensure all wired devices are properly connected to the router’s LAN ports.

**Section 5: Essay**

10. Discuss the importance of network documentation in the context of building and managing networks.

= Network documentation is a critical aspect of building and managing networks. It involves creating and maintaining detailed records of network configurations, devices, connections, and processes. Here are the key reasons why network documentation is important:

1. Facilitates Troubleshooting and Maintenance

- Quick Issue Resolution: Detailed documentation allows network administrators to quickly identify and resolve issues by providing a clear understanding of the network’s structure and configuration.

- Reduced Downtime: Faster troubleshooting leads to reduced network downtime, ensuring business continuity and minimizing productivity losses.

2. Supports Network Planning and Upgrades

- Efficient Planning: Documentation provides a comprehensive view of the current network, aiding in capacity planning, network upgrades, and expansions.

- Resource Allocation: Helps in the effective allocation of resources by identifying existing equipment and any additional requirements.

3. Enhances Security

- Security Audits: Detailed records of network devices and configurations help in conducting thorough security audits, identifying vulnerabilities, and implementing necessary security measures.

- Access Management: Documentation includes records of user access levels and changes, which is crucial for maintaining secure access controls and auditing purposes.

4. Aids in Compliance

- Regulatory Compliance: Many industries have regulatory requirements for network documentation to ensure data integrity and security. Proper documentation helps organizations meet these compliance standards.

- Auditable Records: Documentation provides auditable records that demonstrate adherence to industry standards and regulatory requirements.

5. Improves Communication and Collaboration

- Team Coordination: Well-documented networks ensure that all team members have a consistent understanding of the network setup, facilitating better communication and collaboration.

- Knowledge Transfer: Documentation serves as a knowledge base for new team members, making onboarding and training more efficient.

6. Supports Disaster Recovery

- Backup and Recovery: In the event of a network failure or disaster, documentation provides the necessary information to restore network services quickly and accurately.

- Contingency Planning: Helps in creating and maintaining effective disaster recovery and business continuity plans.

7. Simplifies Network Management

- Configuration Management: Keeps track of network configurations and changes, preventing configuration drift and ensuring consistency.

- Inventory Management: Maintains an accurate inventory of all network devices, software, and licenses, which is essential for managing assets and budgeting.