Assignment: module -5 Network Fundamentals and Building Networks

Section 1: Multiple Choice

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

Ans : - c) Forwarding data packets between networks

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

Ans : - 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?

Ans :- b) Switch

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

Ans :- b) Bus

Section 2: True or False

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. Ans :- True

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

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. Ans :- True

Section 3 : Short

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

Ans :- 1. **Choose an Internet Service Provider (ISP):** Subscribe to a reliable ISP.

2. **Select a Wireless Router:** Choose a router that suits your speed and coverage needs.

3. **Connect the Modem to the Router:** Use an Ethernet cable to connect the modem's output to the router's WAN/Internet port.

4. **Power On Devices:** Turn on the modem and router.

5 . **Access Router Settings:** Use a browser to log in to the router (usually at 192.168.0.1 or 192.168.1.1).

6. **Configure Network Name (SSID) and Password:** Set a unique SSID and a strong WPA2/WPA3 password.

7. **Enable Security Features:** Enable firewall, MAC filtering (optional), and firmware updates.

8. **Connect Devices:** Use the SSID and password to connect devices like laptops, phones, printers, etc.

9. **Test the Network:** Ensure internet access is working on all devices.

Section 4: Practical

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

Ans :-

1. **Connect Hardware:**

   - Plug the **modem** into the router's **WAN/Internet port**.

   - Connect your PC/laptop to one of the router's **LAN ports** or connect via **Wi-Fi**.

2. **Access Router Settings:**

   - Open a browser and enter the router's default IP address (e.g., 192.168.0.1 or 192.168.1.1).

   - Log in with the default username and password (often found on the router label).

3. **Enable DHCP for Internet Access:**

   - Go to the **Internet/WAN settings** section.

   - Set the **WAN Connection Type** to **DHCP** (or "Obtain IP Automatically").

   - Save the settings.

4. **Enable Internal DHCP Server (optional):**

   - Navigate to **LAN/DHCP settings**.

   - Ensure **DHCP Server** is enabled to assign IP addresses to connected devices.

   - Set the IP address range if needed.

5. **Reboot and Test:**

   - Restart the router and modem.

   - Check the **Status** page to verify the router obtained a public IP from the ISP.

   - Test internet connectivity on connected devices.

Section 5: Essay

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

Ans :-

Network documentation refers to the detailed records of all components, configurations, connections, and policies within a computer network. It plays a crucial role in both building and managing networks efficiently.

1. Efficient Network Design and Planning

Proper documentation helps network engineers design networks based on current infrastructure, ensuring scalability and future expansion. It provides a clear picture of existing layouts, devices, and IP addressing schemes.

2. Simplified Troubleshooting and Maintenance

In case of network failures or issues, documentation allows administrators to quickly identify problem areas. For example, knowing which switch a specific device is connected to can significantly reduce downtime.

3. Enhanced Security Management

Security policies, firewall rules, access controls, and VLANs should be documented. This helps in regular audits, detecting unauthorized changes, and maintaining a secure network environment.

4. Easier Onboarding and Handover

For new IT staff or external consultants, network documentation acts as a guide, reducing the learning curve. It ensures continuity in case of personnel changes.

5. Compliance and Legal Requirements

Many industries require detailed network documentation for **compliance** with standards like ISO, HIPAA, or GDPR. It helps demonstrate adherence to regulations and supports audits.

6. Inventory and Asset Management

Keeping track of network devices (routers, switches, servers) with their serial numbers, purchase dates, and warranty helps in lifecycle management and budgeting for upgrades.