**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?

-> Forwarding data packets between networks

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

-> 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?

-> Switch

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

-> Bus

**Section 2: True or False**

5. 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

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

-> False

7. 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

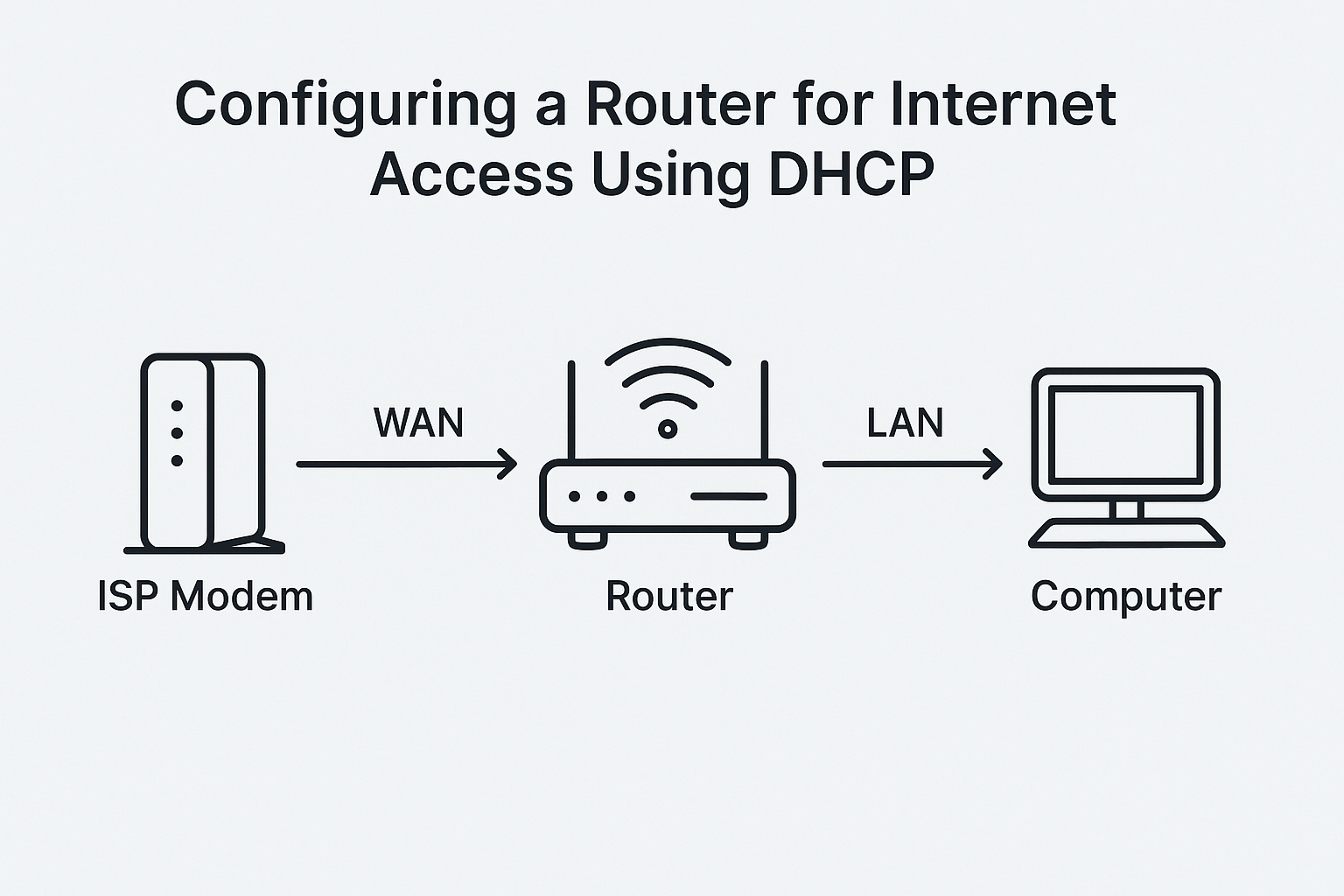
**Section 3: Short Answer**

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

-> In order to configure a wireless network in a SOHO setting:  
Connect the internet modem to the wireless router of your choice.  
Turn on the router and use a web browser to navigate to the configuration page.  
Configure the network name (SSID) and use a strong password to enable WPA2 or WPA3 encryption.  
For security, change the default admin credentials.  
Turn on the firewall and turn off unused functions like remote control.  
Use the SSID and password to connect devices to the Wi-Fi.  
Update the router firmware and check connectivity.  
Save network configurations for later use.

**Section 4: Practical Application**

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

->

* Physical access to the router or access via web interface
* Router powered on and connected to ISP modem (usually via the WAN/Internet port)
* A device (PC/laptop) connected to the router via Ethernet or Wi-Fi

**Step 1: Access the Router's Admin Interface**

1. **Connect to the router** via Wi-Fi or Ethernet.
2. Open a browser and go to the default gateway, commonly:
   * http://192.168.0.1 or http://192.168.1.1
3. Login with default credentials (often on a sticker on the router), or enter your custom username/password.

**Step 2: Set WAN (Internet) Connection Type to DHCP**

Once inside the admin interface:

1. Navigate to the **Network**, **WAN**, or **Internet Settings** tab (depends on router model).
2. Look for **WAN Connection Type** or **Internet Connection Type**.
3. **Select “DHCP” or “Dynamic IP”**.
4. Save the settings.

**Step 3: Verify DHCP Configuration**

1. Go to **Status**, **WAN Status**, or similar section.
2. You should see fields like:
   * **IP Address:** (Public IP assigned by ISP)
   * **Subnet Mask**
   * **Gateway**
   * **DNS Servers**

If these are populated → DHCP is working.

**Step 4: Enable NAT and DHCP Server for LAN (Optional but common)**

To allow internal devices to share the internet connection:

1. Go to **LAN Settings**.
2. Enable **NAT (Network Address Translation)** if not already.
3. Enable **DHCP Server** for LAN:
   * Set a range: 192.168.1.100 to 192.168.1.200
   * Define DNS (can use ISP DNS or public DNS like 8.8.8.8)
   * Set lease time as needed

**Step 5: Save and Reboot**

1. Save all settings.
2. Reboot the router.
3. Test connectivity by browsing from a device on the network.

* IP address from LAN DHCP (192.168.x.x)
* Default Gateway is router’s IP
* DNS servers listed

**Section 5: Essay**

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

-> The Importance of Network Documentation

1. Effective Network Design & Planning

Documentation provides clarity on:

IP addressing schemes

VLANs, subnets

Device role and location

Cabling paths and rack diagrams

Impact: Ensure there are no design conflicts to impede scalability or repeatable deployments.

2. Faster Troubleshooting and Incident Reaction

When bad things happen documentation helps to:

Identify affected areas

Identify dependencies (eg. firewall rules, VLANs)

Access the device configurations quickly

Impact: Drives down time, drives down MTTR (Mean Time to Repair).

3. Enhanced Security Posture Good documentation encompasses:

- Firewall rules

- VPN endpoints

- ACLs

- User access levels

- Overall impact: Easier audits, misconfigurations are easier to identify, improved vulnerability management.

4. Consistency with Maintenance and Updates

Good records help you keep track of things so you avoid:

- Overlapping IP addresses

- Misconfigured routing

- Forgetting devices or unused VLANs

- Overall impact: Increase stability and prevent configuration drift.

5. Streamlined Onboarding & Knowledge Transfer

New members of the team can:

Familiarize with the network topology more quickly

Learn standard operational procedures

Locate devices/services more quickly

Impact: Decreased onboarding time, increased knowledge transfer, reduced knowledge silos.

6. Compliance and Audit Preparedness

Most standards (e.g. ISO 27001, PCI-DSS, NIST) require:

Network architecture diagrams

An inventory of assets

Records of change control

Impact: Aids in meeting legal and regulatory obligations with less stress.

7. Automated Workflows and Integrated Solutions

Structured documentation (e.g., YAML, JSON, or inventory files) is utilized in:

Network automation (Ansible, Nornir)

CMDBs (Configuration Management Databases)

Infrastructure as Code (IaC)

Impact: Aids in improving the efficiency and repeatability of tasks.