

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?

- a) Assigning IP addresses to devices
- b) Providing wireless connectivity to devices
- c) Forwarding data packets between networks**
- d) Managing user authentication and access control

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

- a) Assigning static IP addresses to devices
- b) Resolving domain names to IP addresses
- c) Managing network traffic and congestion
- 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?

- a) Router
- b) Switch**
- c) Hub
- d) Repeater

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

- a) Star
- b) Bus**
- c) Ring
- d) Mesh

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. = **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.=**True**

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**

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

1. Choose the Right Wireless Router

- Select a router that supports the required Wi-Fi standard (e.g., Wi-Fi 5 or Wi-Fi 6).
- Ensure it has good coverage and security features (WPA2/WPA3).

2. Connect the Router to the Internet

- Plug the router into the modem using an Ethernet cable (WAN/Internet port).
- Power on both devices and wait for them to boot up.

3. Access the Router's Configuration Page

- Connect a computer to the router (Wi-Fi or LAN cable).
- Open a browser and enter the router's IP address (192.168.0.1 or 192.168.1.1).
- Log in using the default admin username and password.

4. Change Default Admin Credentials

- Navigate to Administration or System Settings.
- Change the default admin password to prevent unauthorized access.

5. Configure Wireless Settings

- Go to Wireless Settings.
- Set:
 - SSID (Network Name)

- Wi-Fi Band (2.4 GHz / 5 GHz)
- Wi-Fi Mode

Choose a unique and professional network name.

6. Enable Wireless Security

- Enable WPA2-PSK or WPA3-PSK.
- Avoid WEP (insecure).
- Set a strong Wi-Fi password (12–16 characters).

7. Configure DHCP and IP Settings

- Ensure the router's DHCP server is enabled for automatic IP assignment.
- Set a proper IP range (e.g., 192.168.1.2 – 192.168.1.254).
- Configure DNS if needed.

8. Set Up Guest Network (Optional)

- Create a separate SSID for guests.
- Apply WPA2/WPA3 security.
- Keep it isolated from internal devices.

9. Position the Router for Best Coverage

- Place the router centrally.
- Keep it away from walls, metal objects, and interference sources.
- Elevate it for better signal distribution.

10. Connect Devices to the Network

- Use the SSID and Wi-Fi password to connect laptops, phones, printers, and IoT devices.
- Test connectivity and internet speed.

11. Update Firmware

- Check for router firmware updates.
- Install the latest version to improve security and performance.

12. Backup Router Configuration (Optional)

- Save a backup of the configurations for recovery if needed.

Section 4: Practical

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

1. Connect the Router to the Modem

- Plug an Ethernet cable from the modem to the WAN/Internet port of the router.
- Power on both devices.

2. Access the Router Configuration Page

- Connect a computer to the router (via Wi-Fi or LAN cable).
- Open a browser and enter the router's IP address (e.g., 192.168.0.1 or 192.168.1.1).
- Log in using the admin username and password.

3. Navigate to the Internet/WAN Settings

- Go to Internet Settings, WAN Setup, or Network Settings (names vary by router brand).

4. Select “Automatic/Dynamic IP (DHCP)”

- Under WAN Connection Type, choose:
- DHCP / Dynamic IP / Automatic IP
- This tells the router to request an IP address from the ISP automatically.

5. Save the Configuration

- Click Save or Apply.
- The router will now send a DHCP request to the ISP.

6. Verify the Assigned IP Address

- Go to Status or WAN Status page.
- Check if the router received:
 - WAN IP Address
 - Subnet Mask
 - Gateway

- DNS Servers

If values are present, DHCP is working.

7. Configure LAN DHCP (Optional but Recommended)

- Make sure the router's internal DHCP server is enabled to assign IP addresses to local devices.
- Set an IP range such as:
- 192.168.1.2 – 192.168.1.254

8. Test Internet Connectivity

- Connect a computer or phone to the router's Wi-Fi.
- Open a website to confirm internet access.
- If issues occur, reboot the modem and router.

Section 5: Essay

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

1. Helps in Planning and Building the Network

When designing a network, documentation:

- Provides a clear layout of devices, connections, and IP schemes.
- Helps in selecting proper hardware and planning the infrastructure.
- Ensures that the network is built in a structured, organized way.

2. Makes Troubleshooting Faster and Easier

During network issues, documentation:

- Helps technicians quickly identify devices and configurations.
- Reduces guesswork and speeds up fault isolation.
- Minimizes downtime for users and businesses.

3. Improves Maintenance and Upgrades

With proper documentation:

- Administrators know device locations, models, and firmware versions.
- Upgrades, replacements, and patching become easier and safer.

- Misconfigurations are avoided because reference information is available.

4. Enhances Network Security

Documentation helps track:

- User accounts and access rights
- Firewall rules and security policies
- Device configurations and changes

This reduces security risks and prevents unauthorized modifications.

5. Supports Team Collaboration

Network administrators and technicians often work in teams.

Documentation ensures that:

- Everyone understands the network structure
- New employees can quickly learn the setup
- Work continues smoothly even if a technician leaves

6. Essential for Audits and Compliance

Organizations must meet certain standards (ISO, PCI, HIPAA, etc.).

Documentation:

- Proves that the network follows required guidelines
- Helps during internal and external audits

7. Prevents Knowledge Loss

Without documentation, important information may be lost when:

- Employees leave
- Devices are replaced
- Updates are made