# Assignment module 3: Understanding and Maintenance of Network

# 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

#### Ans = c) Forwarding data packets between networks

- 2. What is the purpose of DNS (Domain Name System) in a computer network?
- a) Encrypting data transmissions for security
- b) Assigning IP addresses to devices dynamically
- c) Converting domain names to IP addresses Section
- d) Routing data packets between network segments

#### Ans = c) Converting domain names to IP addresses

3. What type of network topology uses a centralized hub or switch to connect all devices?
a) Star
b) Bus
c) Ring
d) Mesh
Ans = a) Star
4. Which network protocol is commonly used for securely accessing and transferring files over a network?
a) HTTP
b) FTP
c) SMTP
d) POP3
Ans = b) FTP

# Section 2: True or False

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

Ans = True

6. True or False: DHCP (Dynamic Host Configuration Protocol) assigns static IP addresses to network devices automatically.

Ans = False

7. True or False: VLANs (Virtual Local Area Networks) enable network segmentation by dividing a single physical network into multiple logical networks.

Ans = True

# Section 3: Short Answer

8. Explain the difference between a hub and a switch in a computer network.

Ans =

1. Hub = Broadcasts data to all connected devices

Switch = Sends data only to the intended device using MAC address

2.Hub = Dumb device (no traffic filtering or management)

Switch = Dumb device (no traffic filtering or management) 3.hub = Typically operates at 10/100 Mbps Switch = Operates at 10/100/1000 Mbps and beyond 9. Describe the process of troubleshooting network connectivity issues. Ans = process of troubleshooting network connectivity issues are following Step 1: Identify the Problem Ask: Is it one device or multiple? Wired or wireless? Check for error messages or indicators (e.g., "No Internet," red network icon). Step 2: Check Physical Connections

- Ensure Ethernet cables are plugged in.
- Verify the device is connected to Wi-Fi.
- Check LEDs on routers, switches, and NICs for activity.

#### Step 3: Reboot Devices

- Restart the affected device, router, modem, or switch.
- Often resolves minor glitches.

### Step 4: Run Basic Network Commands

### On Windows/macOS/Linux Command Line:

- ping 8.8.8.8 Tests Internet connectivity.
- ping router ip Tests connection to local network.
- ipconfig (Windows) / ifconfig or ip a (Linux/macOS) Check IP configuration.
- tracert or traceroute Trace the path to a remote server.

## Step 5: Check IP Address and DNS Settings

- Ensure device has a **valid IP address** (not 169.x.x.x).
- Try switching to a public **DNS** (e.g., Google DNS: 8.8.8.8).

## Step 6: Test with Another Device

- If other devices work fine, the problem is **isolated to one system**.
- If none work, it may be the router, modem, or ISP.

## Step 7: Check Router/Modem

- Log into the router's admin page to view status.
- Check for firmware updates, DHCP settings, or ISP disconnection.

## Step 8: Contact ISP or Network Admin

• If everything seems correct and still no access, it might be an issue with the **ISP** or a **deeper network configuration** problem.

# Section 4: Practical Application

10. Demonstrate how to configure a wireless router's security settings to enhance network security.

Ans = 1. Access the Router's Admin Interface

- Connect to the router via Wi-Fi or Ethernet.
- Open a web browser and enter the router's IP address (commonly 192.168.0.1 or 192.168.1.1).
- Log in using the admin username and password (often printed on the router or set by the user).
- 2. Change the Wi-Fi Network Name (SSID)
  - Navigate to Wireless Settings or Basic Wireless Setup.
  - Set a custom SSID (Service Set Identifier) that doesn't reveal your name, address, or device type.

Avoid names like "Home WiFi" or "JohnDoe Network".

- 3. Enable Strong Wi-Fi Encryption
  - Under Wireless Security Settings:
    - o Select WPA3 if available. If not, choose WPA2-PSK (AES).
    - o Avoid WEP or WPA, as they are outdated and insecure.
  - Set a strong Wi-Fi password (12+ characters with letters, numbers, and symbols).

# 4. Disable WPS (Wi-Fi Protected Setup)

- WPS is convenient but insecure and vulnerable to brute-force attacks.
- **Disable WPS** in the Wireless or Security section.
- 5. Create a Guest Network (Optional but Recommended)
  - Enable a Guest Network for visitors.
  - Use isolation settings to prevent guests from accessing your main network and devices.
  - Apply a different strong password and security settings.
- 6. Turn Off Remote Management
  - Disable **remote web access** (often called "Remote Management" or "Web Access from WAN").
  - This prevents anyone from logging into your router from outside your local network.
- 7. Keep the Router Firmware Updated

- Go to the Firmware Update or System Tools section.
- Check for updates and apply them to fix security vulnerabilities.

#### 8. Limit DHCP Range (Optional)

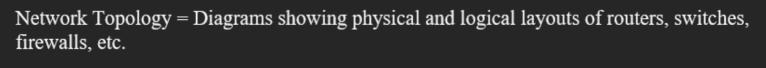
- In LAN settings, reduce the DHCP IP address pool to the number of devices you
  regularly use.
- This can deter unauthorized devices from easily obtaining an IP address.
- Enable MAC Address Filtering (Advanced Users)
  - Only allow specific device MAC addresses to connect.
  - This provides extra security but requires more management and isn't foolproof (MACs can be spoofed).

# Section 5: Essay

11. Discuss the importance of network documentation and provide examples of information that should be documented.

Ans = Network documentation is the process of creating and maintaining detailed records about a computer network's design, components, configurations, and policies. <u>It's</u> critical for network reliability, scalability, troubleshooting, and security.

Examples of Information to Document



- IP Addressing = Static IP assignments, DHCP scopes, subnet ranges, and reserved addresses.
- Device Inventory = List of all hardware (servers, switches, routers, printers), serial numbers, and locations.
- Configuration Settings = Router and switch configurations, firewall rules, VLAN settings, wireless SSIDs, etc
- Login Credentials = Admin usernames/passwords (stored securely), and access control lists (ACLs).
- Cabling Information = Cable types, port numbers, wall jack locations, and labeling schemes.