*Assignment: module -5* Network Fundamentals and Building Network.

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***

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.

ANS: - True

6.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

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.

ANS: - True

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

ANS: - 1**. Plan the Network Layout**

* **Assess Coverage Needs**: Identify areas where wireless coverage is needed.
* **Determine Equipment Needs**: Decide on the number of devices, access points (APs), and type of wireless router required.
* **Choose Network Type**: Decide between a single router setup or a mesh network for larger areas.

**2. Select Suitable Hardware**

* **Wireless Router**: Choose a router that supports the latest Wi-Fi standards (e.g., Wi-Fi 6 for better speed and efficiency).
* **Modem**: Ensure compatibility with your ISP if required separately.
* **Access Points (if needed)**: For extended coverage in larger spaces.
* **Switch (optional)**: For connecting additional wired devices.

**3. Position the Router**

* Place the router in a **central location** to ensure even signal distribution.
* Avoid interference from physical obstructions (walls, metal objects) and devices like microwaves or cordless phones.

**4. Connect and Power On**

* **Connect Modem to Router**: Use an Ethernet cable to connect the modem's output to the router's WAN port.
* **Connect Devices**: Plug in wired devices to LAN ports if needed.
* Power on the modem and router.

**5. Configure the Router**

* **Access Router Settings**: Use a web browser to navigate to the router's IP address (e.g., 192.168.1.1).
* **Log In**: Use the default credentials provided in the router manual (change these later for security).

**6. Set Up the Wireless Network**

* **Name the Network (SSID)**: Create a recognizable but non-identifiable SSID (e.g., avoid "John’s Office").
* **Choose a Security Protocol**: Use **WPA3** or **WPA2** (preferably WPA3 for enhanced security).
* **Set a Strong Password**: Use a complex, unique password for the wireless network.
* **Enable Guest Network** (optional): Isolate guest traffic from the main network.

**7. Optimize Settings**

* **Select a Channel**: Use a less crowded channel to avoid interference (use tools to scan for channel usage if needed).
* **Configure Band Settings**: Use dual-band (2.4 GHz and 5 GHz) or tri-band as appropriate for your devices.
* **Enable QoS (Quality of Service)**: Prioritize critical applications like VoIP or video conferencing.
* **Update Firmware**: Ensure the router is running the latest firmware for security and performance.

**8. Secure the Network**

* **Change Default Admin Credentials**: Replace the default router username and password with unique ones.
* **Enable Firewall**: Use the built-in firewall for added protection.
* **Disable WPS**: Disable Wi-Fi Protected Setup (WPS) if not needed, as it can be a security risk.
* **Enable Network Encryption**: Encrypt traffic within the network using protocols like VPN if necessary.

**9. Test the Network**

* **Connect Devices**: Test connectivity with smartphones, laptops, and other devices.
* **Check Coverage**: Walk through the area to ensure signal strength is consistent.
* **Run Speed Tests**: Verify internet speeds at various locations.

**10. Maintain the Network**

* Regularly update the router firmware.
* Periodically review and update passwords.
* Monitor the network for unusual activity.

By following these steps, you'll ensure a reliable, secure, and efficient wireless network for your SOHO environment.

***Section 4: Practical: -***

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

ANS: - Done in lab

***Section 5: ESSAY: -***

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

ANS: - Network documentation is a critical aspect of building and managing networks, as it provides a clear and organized record of the network’s configuration, components, and operations. Its importance lies in ensuring efficient management, troubleshooting, scalability, and security. Here's a detailed discussion:

**1. Facilitates Network Understanding**

* **Simplifies Complex Systems**: Network documentation serves as a roadmap that details the network's design, components, and connections, making it easier for network administrators to understand how everything is set up.
* **Onboarding New Staff**: New IT personnel can quickly grasp the network’s structure without needing to rely heavily on existing staff for explanations.

**2. Streamlines Troubleshooting**

* **Speeds Up Issue Resolution**: Documentation provides a reference for network configurations, IP addresses, and device locations, enabling faster identification and resolution of issues.
* **Avoids Guesswork**: Instead of manually tracing connections or configurations, administrators can consult the documentation for accurate information.

**3. Supports Scalability**

* **Guides Network Expansion**: With a documented network, administrators can identify available resources, bottlenecks, and optimal areas for expansion.
* **Prevents Redundancy**: Ensures that new additions are compatible with the existing setup and do not duplicate efforts.

**4. Enhances Security**

* **Tracks Access and Permissions**: Documentation includes details about user roles, access control lists (ACLs), and firewall rules, helping to enforce security policies.
* **Identifies Vulnerabilities**: Regularly updated documentation can reveal outdated devices, unpatched systems, or unused ports that need securing.

**5. Ensures Compliance**

* **Regulatory Requirements**: Many industries (e.g., healthcare, finance) require detailed network documentation to comply with standards like HIPAA, GDPR, or PCI DSS.
* **Audit Readiness**: Comprehensive documentation makes it easier to demonstrate compliance during audits.

**6. Improves Disaster Recovery**

* **Accelerates Recovery**: In case of a network failure, documentation provides a reference for restoring configurations and connections quickly.
* **Ensures Redundancy**: Highlights backup systems, failover mechanisms, and disaster recovery plans.

**7. Promotes Efficient Collaboration**

* **Standardizes Communication**: Documentation ensures all team members and stakeholders are on the same page regarding the network’s status and structure.
* **Facilitates Vendor Interaction**: Clear records assist in communicating requirements or issues with external vendors or service providers.

**8. Saves Time and Costs**

* **Reduces Downtime**: Quick access to accurate information minimizes service interruptions.
* **Prevents Unnecessary Expenses**: Avoids redundant purchases or misconfigured setups that could lead to additional costs.

**Components of Effective Network Documentation**

* **Network Topology Diagrams**: Visual representation of the network’s layout.
* **Device Inventory**: List of all hardware, including make, model, and serial numbers.
* **IP Address Management**: Details of assigned and available IP addresses.
* **Configuration Files**: Backup copies of router, switch, and firewall configurations.
* **Access Control Records**: User roles, permissions, and access logs.
* **Change Log**: Record of modifications made to the network.

**Conclusion: -**

Network documentation is not just a best practice but a necessity for maintaining a robust, secure, and efficient network. It ensures operational continuity, supports proactive management, and provides a solid foundation for network growth and adaptation. Neglecting documentation can lead to inefficiencies, increased downtime, and heightened security risks.