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

1. 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

2. 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

3. 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: Setting up a wireless network for a small office or home office involves several key steps to ensure reliable connectivity and security:

- **Planning and Preparation:** First, assess your networking needs by determining the number of devices that will connect, the area that needs coverage, and your internet speed requirements. Choose appropriate equipment including a wireless router or access point that supports current standards like Wi-Fi 6, and ensure your internet service provider (ISP) has activated your connection.
- **Physical Setup:** Connect your modem to the ISP's network connection (cable, DSL, or fiber line). Then connect the wireless router's WAN/Internet port to the modem using an Ethernet cable. Position the router centrally in your space, away from physical obstructions and interference sources like microwaves or cordless phones. Plug in and power on both devices.
- **Initial Router Configuration:** Access the router's web interface by connecting a computer via Ethernet cable or WiFi using the default credentials printed on the router. Log in through a web browser using the router's default IP address (commonly 192.168.1.1 or 192.168.0.1). The setup wizard typically guides you through basic configuration.
- **Network Settings Configuration**: Set up your wireless network by creating a unique SSID (network name) that identifies your network. Configure strong security by selecting WPA3 or WPA2 encryption and creating a complex password. Set up DHCP to automatically assign IP addresses to connected devices, or configure a static IP range if needed for your environment.
- **Security Hardening:** Change the router's default admin username and password to prevent unauthorized access. Disable WPS (Wi-Fi Protected Setup) if not needed, as it can be a security vulnerability. Enable the router's firewall and consider setting up a guest network for visitors to isolate them from your primary network.
- **Testing and Optimization:** Connect various devices wirelessly to verify connectivity and internet access. Test network speed and coverage throughout your space. Adjust the router's position or antenna orientation if needed, and update the router's firmware to the latest version for security patches and performance improvements.
- **Final Documentation:** Record your network configuration details including SSID, passwords, IP address scheme, and any custom settings for future reference and troubleshooting.

Section 4: Practical

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

Ans: Demonstration Steps:

- **Initial Access:** Connect a computer to the router via Ethernet cable. Open a web browser and enter the router's default gateway IP address (typically 192.168.1.1, 192.168.0.1, or 10.0.0.1). Log in using the default credentials found on the router label or manual.
- **WAN Configuration:** Navigate to the WAN or Internet settings section. Select the connection type provided by your ISP (typically DHCP for cable/fiber connections). If using DHCP, the router will automatically obtain an IP address, subnet mask, default gateway, and DNS servers from your ISP. Save the settings and allow the router to establish the connection.
- **DHCP Server Setup:** Access the LAN or DHCP Server settings section. Enable the DHCP server function if not already enabled. Configure the DHCP IP address pool by setting the starting and ending IP addresses (for example, 192.168.1.100 to 192.168.1.200). Set the lease time, which determines how long devices keep their assigned IP addresses (commonly 24 hours).
- **Additional DHCP Settings:** Configure the default gateway (usually the router's IP address) and DNS servers (you can use your ISP's DNS or public DNS like Google's 8.8.8.8 or Cloudflare's 1.1.1.1). Optionally, set up DHCP reservations for devices that need consistent IP addresses like printers or servers.
- **Testing:** Connect client devices wirelessly or via Ethernet. Verify they receive IP addresses automatically by checking their network settings. Test internet connectivity by browsing websites or pinging external addresses. Check the router's DHCP client list to see connected devices and their assigned addresses.

Section 5: Essay

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

Ans: Network documentation is a critical yet often overlooked aspect of building and managing networks. Comprehensive documentation serves as the foundation for effective network administration, troubleshooting, and long-term sustainability.

Operational Efficiency and Troubleshooting: Detailed documentation dramatically reduces troubleshooting time when network issues arise. When problems occur, administrators can quickly reference network diagrams, IP address schemes, and configuration details rather than spending hours rediscovering how the network was built.

Knowledge Preservation and Team Continuity: Networks often outlive the tenure of the people who built them. Without proper documentation, knowledge about network design decisions, custom configurations, and workarounds exists only in individuals' memories. When staff members leave, get promoted, or are unavailable, undocumented networks become mysterious black boxes.

Change Management and Planning: Good documentation enables informed decision-making about network changes and expansions. Before adding new services, devices, or locations, administrators need to understand current IP address allocation, available switch ports, bandwidth utilization, and existing security policies.

Security and Compliance: From a security perspective, documentation helps identify potential vulnerabilities and ensures consistent security policies across the network. Knowing which ports are open, which devices have internet access, and how data flows through the network is essential for threat assessment and incident response.

Cost Management: Proper documentation helps organizations optimize spending by revealing underutilized resources, identifying redundant systems, and planning capacity needs accurately. It prevents unnecessary equipment purchases when existing resources could be reconfigured and helps justify budget requests with concrete data about network requirements.

Essential Documentation Components: Effective network documentation should include physical and logical topology diagrams, IP addressing schemes and DHCP ranges, device inventory with make/model/serial numbers, configuration backups, cable management documentation, security policies and access control lists, disaster recovery procedures, and a change log tracking modifications over time.

In conclusion, network documentation is not merely administrative overhead but an investment that pays dividends through reduced downtime, improved security, easier troubleshooting, and better strategic planning. Treating documentation as an integral part of network management, rather than an afterthought, is the mark of professional network administration and contributes significantly to the overall reliability and maintainability of network infrastructure.