Assignment module 3: Understanding and Maintenance of 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

Answer: 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

d) Routing data packets between network segments

Answer: 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

Answer: 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

Answer: b) FTP

Section 2: True or False

5. A firewall is a hardware or software-based security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Answer: True

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

Answer: False

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

Answer: True

Section 3: Short Answer

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

Answer: A hub is a basic networking device that broadcasts data to all devices connected to it, regardless of the destination. This can lead to network collisions and inefficiency. A switch, on the other hand, is more intelligent—it sends data only to the specific device (based on MAC address) it is intended for, improving performance and reducing unnecessary traffic.

9. Describe the process of troubleshooting network connectivity issues

Answer: Troubleshooting network issues typically involves the following steps:

1. **Check physical connections** (cables, ports, power).
2. **Verify device settings** (IP address, subnet mask, gateway).
3. **Use basic commands** like ping, ipconfig/traceroute to test connectivity.
4. **Restart devices** (computer, router, modem).
5. **Check for IP conflicts** or DHCP issues.
6. **Review firewall and security settings**.
7. **Test with a different device or network** to isolate the issue.
8. **Check for outages or ISP issues** if all else fails.

Section 4: Practical Application

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

Answer: • Go to the **Wireless Settings** or **Wireless Security** section.

- Set the **Security Mode** to **WPA3** (if available) or **WPA2-PSK [AES]**.
- Create a strong **Wi-Fi password** using a mix of letters, numbers, and special characters.
- Turn on the **router's firewall** (usually found under **Security** or **Firewall Settings**).
- Consider setting up **MAC address filtering** to limit which devices can connect.
    - Check for firmware updates in the System Tools or Firmware section.
    - Regularly update to patch vulnerabilities.

Section 5: Essay

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

Answer: **Why Network Documentation Is So Important (and What to Include)**

When it comes to managing a network, documentation might not be the most glamorous task—but it's one of the most important. Think of it like a roadmap for your network. Without it, troubleshooting, upgrading, or even understanding how everything fits together becomes a whole lot harder.

Good documentation helps ensure continuity, especially when team members change. It saves time during emergencies, helps with security audits, and makes training new staff much easier. Basically, it's about keeping everything running smoothly, now and in the future.

What Should Be Documented?

Here are some key things that should always be part of your network documentation:

- **Network Topology Diagrams**
  Visual maps showing how all devices are connected. This gives a quick overview of the whole setup—routers, switches, servers, workstations, etc.
- **IP Addressing Scheme**
  A list or spreadsheet that shows which IP addresses are assigned to which devices. This is essential for tracking down issues or planning expansions.
- **Device Inventory**
  Details about all network hardware—model numbers, serial numbers, firmware versions, and physical locations.
- **Configuration Files**
  Backups of router, switch, and firewall configurations. If a device fails, these files make it way easier to restore service quickly.
- **User Access Levels**
  Who has access to what—and at what level. This includes admin credentials, user roles, and remote access permissions.
- **Change Logs**
  A record of any changes made to the network, including when, why, and by whom. This helps with accountability and troubleshooting.
- **Service Provider Info**
  Contact details for ISPs and other vendors, including account numbers and support procedures.
- **Security Policies**
  Firewall rules, antivirus protocols, VPN settings, and other security measures that protect your network.