**A+ - Understanding and Maintenance of Networks**

**MULTIPLE CHOICE QUE**

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 DNS (Domain Name System) in a computer network?

ANS: C) Converting domain names to IP addresses

3. What type of network topology uses a centralized hub or switch to connect all devices?

ANS: A) STAR

4. Which network protocol is commonly used for securely accessing and transferring files over a network?

ANS: B) FTP

**TRUE OR FALSE**

5. 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

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

**Short Answer**

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

ANS: **Hubs** broadcast data to all devices without filtering, while **switches** direct data to specific devices, thereby enhancing network performance and security.

9. Describe the process of troubleshooting network connectivity issues.

ANS: **1-Identify the Problem,**

**2. Check Physical Connections,**

**3. Test Network Configuration**

**4. Use Command Line Tools,**

**5. Check Network Hardware**

**6. Review Firewall and Security Settings**

**7. Look for ISP Issues**

**8. Update Drivers and Firmware**

**9. Test with Alternate Devices or Cables**

**10. Document Findings and Solutions**

**11. Follow Up**

**Practical Application**

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

ANS: Configuring a wireless router's security settings is crucial for protecting your network from unauthorized access and potential threats. Here’s a step-by-step guide to enhance your wireless network security:

1-Access the router’s admin interface

2-Change default login credentials

3-Update the router firmware

4-Configure wi-fi security setting

5-Disable WPS (wi-fi protected setup)

6-Enable network firewall

7-Create a guest network(optional)

8-Disable SSID broadcasting(optional)

9-Enable MAC address filtering(optional)

10-Regularly monitor and update

**ESSAY**

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

ANS: Network documentation is a critical aspect of managing and maintaining a network infrastructure. It provides a comprehensive overview of the network’s architecture, components, and configurations, which can greatly enhance efficiency, troubleshooting, security, and compliance. Here’s a deeper look at its importance and the types of information that should be documented.

**Importance of Network Documentation**

1. **Facilitates Troubleshooting**: Well-documented networks can be analysed quickly to identify and resolve issues. Documentation helps teams understand the layout and configurations.
2. **Streamlines Onboarding**: New administrators or team members can refer to documentation to understand the network setup and operational procedures without extensive training.
3. **Ensures Consistency**: Documentation assists in maintaining configurations and practices uniformly across the network, reducing the chances of misconfiguration.
4. **Supports Compliance**: Many industries have regulatory requirements. Documentation can help ensure compliance with standards like PCI-DSS, HIPAA, and more.
5. **Aids in Planning and Growth**: Understanding current configurations and specifications helps in effectively planning for future expansions or upgrades to the network.
6. **Provides a Reference for Maintenance**: Regular maintenance tasks such as updates, backups, or patches can be guided by clear documentation.

**Examples of Information to Document**

1. **Network Topology Diagrams**:
   * Visual representations of the network layout, showing devices, connections, and the overall architecture.
2. **Device Inventory**:
   * A list of all network devices (routers, switches, firewalls, servers), including details such as model numbers, serial numbers, locations, and IP addresses.
3. **Configuration Settings**:
   * Detailed configurations for each device, including firewall rules, routing protocols, and VLAN setups.
4. **IP Address Management**:
   * A record of assigned and reserved IP addresses, including subnetting information and DHCP settings.
5. **Network Policies and Procedures**:
   * Documentation of organization-specific policies regarding network access, security standards, and compliance protocols.
6. **Backup Procedures**:
   * Information about backup schedules, methods, and storage locations for network configurations and critical data.
7. **Change Management Logs**:
   * A record of all changes made to the network, including updates to hardware or software, configuration changes, and reasons for the changes.
8. **User Access Controls**:
   * Documentation of who has access to various network segments or resources, along with their permissions and roles.
9. **Maintenance Schedules**:
   * Timelines for regular maintenance tasks, inspections, and updates to ensure the network remains secure and operational.
10. **Incident Response Plan**:
    * A documented process outlining steps to take in response to network incidents or breaches, along with contact information for emergency contacts.