**Assignment: 3**

**Section 1: Multiple Choice**

**1. What is the primary function of a router in a computer network?**

- Forwarding data packets between networks

**2. What is the purpose of DNS (Domain Name System) in a computer network?**

- Converting domain names to IP addresses

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

- Star

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

- FTP

**Section 2: 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.**

- True

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

- False

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

- True

**Section 3: Short Answer**

**8. Explain the difference between a hub and a switch in a**

**computer network.**

* HUB: 1) HUB connects devices to a network.

2) HUB is presented in Physical layer.

3) HUB sends information using bits.

4) It shares bandwidth equally among ports.

5) It cannot avoid switching loops.

6) HUB is best suited for small LANs.

* Switch: 1) Switch connects devices to a network and

manages data packets.

2) It is presented in Data link layer.

3) Switch sends information using data packets.

4) It provides dedicated bandwidth to ports.

5) It uses spanning tree protocol to avoid

switching loops.

6) Switch is preferred for modern networks.

**9. Describe the process of troubleshooting network connectivity issues.**

* Verify the Problem
* Check Physical Connections
* Check IP Address Configuration
* Ping Test
* Verify DNS Settings
* Check for Network Interference
* Examine Firewall/Security Settings
* Check Router/Modem Status
* Check for Network Congestion
* Use Traceroute/Path ping
* Contact ISP or Network Administrator
* Advanced Diagnostics

**Section 4: Practical Application**

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

- To enhance your wireless router's network security, you should change the default router login credentials, update the firmware to the latest version, enable the strongest encryption protocol like WPA3, disable WPS, create a strong network password, hide your network SSID (disable broadcasting), and consider setting up a guest network; additionally, regularly monitor network activity and restrict access to authorized devices using MAC address filtering if possible.

Key steps to configure your wireless router security:

Change default credentials: Modify the username and password used to access your router settings from the factory defaults to a strong, unique combination.

Update firmware: Regularly check for and install the latest firmware updates for your router to patch security vulnerabilities.

Choose strong encryption: Select the most secure encryption protocol available, typically WPA3, to protect data transmitted over your network.

Disable WPS: Turn off Wi-Fi Protected Setup (WPS) as it can be exploited by hackers.

Create a strong password: Set a complex network password with a mix of uppercase and lowercase letters, numbers, and symbols.

Hide your network name (SSID): Disable SSID broadcasting to prevent your network from being easily detected by unauthorized devices.

Guest network: Create a separate guest network for visitors, isolating them from your primary network.

MAC address filtering: If supported by your router, consider filtering devices allowed to connect to your network by their MAC addresses.

Access control: Limit access to specific devices or IP addresses if needed.

Monitor network activity: Regularly check your router logs for suspicious activity.

**Section 5: Essay**

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

Network documentation is critical for the effective management, troubleshooting, and security of an organization's network infrastructure. It serves as a comprehensive record that helps network administrators, IT teams, and even external support personnel understand how the network is structured, how devices are connected, and how configurations are implemented. Proper documentation ensures continuity, reduces downtime, enhances security, and streamlines troubleshooting. Here’s a detailed discussion of why network documentation is important and examples of the information that should be documented.

Importance of Network Documentation

1. Effective Troubleshooting and Maintenance

* When network issues arise, having detailed documentation allows network administrators to quickly identify network components and configurations. Without documentation, troubleshooting can become a time-consuming process, as administrators would have to rely on memory or manual checks.

1. Network Security

* Well-documented network settings and configurations allow for better monitoring and auditing. Documentation helps identify vulnerabilities and misconfigurations that could be exploited by attackers. For example, if certain devices are left unprotected or outdated, it can be spotted in the documentation.

1. Consistency and Standardization

* Network documentation ensures consistency across network management practices. It helps standardize configurations, naming conventions, and setup protocols, making it easier to manage and scale the network.

1. Disaster Recovery and Business Continuity

* In the event of a disaster (e.g., hardware failure, natural disaster), having a documented network allows for quicker recovery and ensures that services are restored faster. Documentation can help rebuild network configurations, restore backup systems, and reduce downtime.

1. Network Planning and Growth

* As an organization’s network grows, it is important to have a record of existing infrastructure and configurations. This helps in planning for future expansions, upgrades, and troubleshooting scalability issues.

1. Compliance and Auditing

* Certain industries have compliance regulations that require network configurations, security policies, and monitoring to be documented. Regular documentation ensures compliance with such regulations (e.g., HIPAA, GDPR, PCI DSS).

1. Staff Training and Knowledge Sharing

* New IT staff or contractors can refer to the network documentation to get up to speed quickly on how the network is structured. It reduces the learning curve and ensures continuity when employees leave or transition roles.