Assignment module 3: Understanding and Maintenance of 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 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) POP3

Section 2: True or False

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

6. DHCP (Dynamic host configuration protocol) assigns static IP addresses to network device automatically.-FALSE

7. 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.

Ans.

Hub: Broadcasts data to all connected devices. Operates at the physical(Layer 1). Simple and inexpensive.

Switch: Forwards data selectively to the specific device it is intended for based on mac addresses. Operates at the data link layer(Layer 2). More efficient and intelligent than a hub.

9. Describe the process of troubleshooting network connectivity issues.

Section 4:

10. Demonstrate how to configure a wireless router’s security setting to enhance network security.

Ans:

Access the Router Settings:

- Connect your computer to the router either via Ethernet cable or wirelessly.
- Open a web browser (e.g., Chrome, Firefox) and enter the router's IP address in the address bar. Common router IPs are

192.168.1.1 or 192.168.0.1. Check your router's manual for the exact IP.

Login to the Router:

- You'll be prompted to enter a username and password. By default, these are often 'admin' for both fields, but it's essential to change these for security reasons. Refer to your router's manual for instructions on changing the login credentials.

Change the Router Admin Username and Password:

- Look for an option like 'Administration', 'Management', or 'System' in the router settings menu.
- Find the fields to change the username and password. Choose a strong password with a mix of letters, numbers, and symbols.

Enable WPA2/WPA3 Encryption:

- Navigate to the 'Wireless' or 'Wireless Settings' section of the router settings.
- Look for the 'Security' options. Select 'WPA2-PSK' or 'WPA3-PSK' (if supported) as the

security mode. Avoid using WEP (Wired Equivalent Privacy) as it's less secure.
- Set a strong passphrase (also known as the Wi-Fi password). Use a mix of uppercase, lowercase letters, numbers, and symbols. The longer, the better.

Change the Default SSID (Network Name):

- While in the wireless settings, locate the 'SSID' or 'Network Name' field.
- Change the default SSID to something unique. Avoid using personal information in the SSID.

Disable SSID Broadcast (Optional):

- Some routers offer an option to disable SSID broadcasting. This prevents the network name from being visible to nearby devices. Note that this may not significantly enhance security but can deter casual users from connecting.

Enable MAC Address Filtering (Optional):

- In the router settings, find 'MAC Address Filtering' under 'Wireless' or 'Security'.

- Enable this feature and add the MAC addresses (unique hardware addresses) of devices you want to allow to connect to the network. This adds an extra layer of security by only allowing specified devices to connect.

Update Router Firmware:

- Check for firmware updates regularly in the router settings. Firmware updates often include security patches and bug fixes that improve the router's security.

Save Settings and Restart the Router:

- After making changes, save the settings. Some routers may require a restart for changes to take effect.

Test the Security Settings:

- Attempt to connect to your wireless network using a device to ensure that the settings are correctly configured.

Section 5:

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

Network documentation is a cornerstone of effective IT management, providing crucial information that supports troubleshooting, enhances security, aids in planning and compliance, facilitates training, ensures business continuity, and enables efficient vendor interactions.

Firstly, network documentation plays a pivotal role in troubleshooting and maintenance. When network issues arise, having detailed documentation readily available allows IT professionals to quickly pinpoint the root cause. For instance, knowing IP addresses, device configurations, and network topology from documentation can expedite troubleshooting processes, minimizing downtime and restoring services promptly. Without accurate documentation, troubleshooting becomes

inefficient and prone to errors, potentially prolonging network disruptions.

Secondly, network security relies heavily on well-documented configurations and policies. Documentation ensures that security measures such as firewall rules, VPN configurations, and access control lists (ACLs) are clearly defined and consistently implemented across the network. This transparency helps in auditing network security practices against compliance standards like HIPAA or GDPR, ensuring that regulatory requirements are met and vulnerabilities are addressed proactively.

Moreover, comprehensive network design and planning hinge on detailed documentation. Networks are dynamic environments that undergo expansions, upgrades, and modifications. Documentation provides insights into existing infrastructure, including network diagrams, equipment inventory, and capacity planning details. Such information is invaluable for making

informed decisions about network improvements, scaling resources, and optimizing performance.

In terms of compliance and auditing, documented policies and procedures are essential for demonstrating adherence to industry regulations. Compliance documentation encompasses not only security measures but also operational procedures, change management records, and disaster recovery plans. These documents serve as evidence of compliance during audits, helping organizations avoid penalties and maintain trust with stakeholders.

Additionally, network documentation supports training and knowledge transfer within IT teams. New staff members benefit from detailed documentation that outlines network architecture, operational guidelines, and troubleshooting procedures. This knowledge transfer ensures continuity of operations and fosters a skilled workforce capable of effectively managing and securing the network environment.

Furthermore, disaster recovery and business continuity planning heavily relies on accurate network documentation. In the event of a network outage or disaster, documented backup configurations, recovery procedures, and critical service dependencies enable swift restoration of network services. This preparedness minimizes downtime, mitigates risks, and safeguards business continuity, essential for maintaining productivity and customer satisfaction.

Lastly, effective vendor and service provider interaction is facilitated by well-maintained documentation. Detailed records of service agreements, vendor contact information, equipment warranties, and procurement details streamline communication and collaboration. This ensures that vendors have accurate information to support troubleshooting, provide maintenance, and deliver timely services, ultimately enhancing operational efficiency and service delivery.

In conclusion, network documentation serves as a cornerstone of efficient IT management, underpinning troubleshooting, security, planning, compliance, training, business continuity, and vendor interactions. Organizations that prioritize thorough documentation practices benefit from enhanced operational resilience, improved security posture, and streamlined IT processes, thereby supporting overall business objectives and ensuring sustainable growth in an increasingly digital landscape.