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

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 Routing data

d) packets between network segments

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

a) Star

b) Bus

c) Ring

d) Mesh

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

a) HTTP

b) FTP

c) SMTP

d) POP3

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.

ANS- TRUE

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

ANS-FALSE

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

ANS-TRUE

Section 3: Short Answer

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

ANS- A hub and a switch are both devices used to connect many computers or devices in a network, but they work in different ways.

- A **hub** is a simple device. When it receives data from one computer, it sends that data to all the computer connected to it, even if only on computer is the actual receiver. This creates unnecessary traffic in the network and makes it slower. A hub does not know which devices the data is meant for; it just broadcast the data to every device.
- A **switch,** on the other hand, is more intelligent. When it receives data, it identifies the correct computer that the data is meant for and sends it only to that device. This makes the networks run faster, safer, and more efficient compared to a hub.
- In short, a hub shares data with all devices, while switch sends data only to the right devices. This is why modern networks prefer using switches.

9. Describe the process of troubleshooting network connectivity issues.

ANS- Troubleshooting networks connectivity issues mean finding and fixing problem in the networks when a computer cannot connect to the internet or other devices.

1. Cheak if the devices are properly connected to the network (cable or wi-fi).
   (we check if the cables are properly connected or if the wi-fi is turned on)
2. Run the ipconfig command to check IP configuration
   (We check the IP address using the ipconfig command to see if the computer is getting the right networks details.)
3. Run ping to test connection with the router or another device
   (We can use the ping command to test if the computer is able to talk to the router or another devices.)
4. Restart the router or network adapter if needed.

(We can try to restart the router or the network adapter.)

5. Update drivers or reset network setting if the problems continue.
   (Sometimes updating the drivers or resetting the networks settings can also fix the issue.)

Section 4: Practical Application

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

ANS- To configure a wireless router's security settings and make the networks more secure, we can follow these steps:

1. First, open a web browser type the router's IP address (for example 192.168.1.1) to log in to the router setting.
2. Enter the admin username and password. It is importance to change the default password to a strong new password so that no one else can access the router.
3. Go to the wireless security section and select WPA2 or WPA3 encryption, because these are more secure than older methods like WEP.
4. Set a stronger Wi-Fi password with a mix of letter, number, and symbols.
5. Turn off WPS (Wi-Fi protected setup) if it is not needed, because it can be a security risk.
6. If required, enable a guest network so visitors can use Wi-Fi without accessing the main network.
7. Save the setting and restart the router so the new security changes take effect.

By doing these steps, the wireless router becomes more secure, and it help to protect the network from unauthorized users and hackers.

Section 5: Essay

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

ANS- Network documentation is the process of recording and maintaining all the important details about a computer networks. It includes diagrams, devices information IP addresses, configurations, and procedures. Proper documentation helps in understanding how the networks is designed, how each device is connected, and how the network operates.

Network documentation is very important for many reasons. First, it helps in troubleshooting problem quickly. When any issue occurs, a well-documented network makes it easier to find where the problem is and fix it helps in network management and maintenance. With proper records, maintenance. With proper records, administrators can easily make changes, upgrade devices, or expand the network without causing errors. Third, it improves security by keeping track of devices, users, and access permissions. It also helps new technicians or team members understand the network structure easily.

Having clear and up-to-date documentation also ensures that the organization can continue working smoothly even if the main network administrator is not available. It reduces confusion and helps maintain consistency in the setup and maintenance of the network.

To make documentation more effective, many companies use network management tools and software that automatically record and update network configurations. These tools help in creating visual network maps, tracking devices performance, and generating reports easily.

Some examples of information that should be included in network documentation are:

- Network topology diagrams showing how devices are connected
- Ip address details and devices names
- Router, switch, and firewall configurations
- User accounts, access levels, and passwords (kept securely)
- Hardware and recovery procedures
- Maintenance logs and update schedules

Thus, network documentation is a key part of managing and protecting a computer network. It improves efficiency, saves time, increases security, and makes it easier for anyone to understand and maintain the network. Without proper documentation, solving problems and managing the network becomes difficult and time-consuming.