MODULE – 3 UNDERSTANDING AND MAINTENANCE OF NETWORKS

1. WHAT IS THE PRIMARY FUNCTION OF A ROUTER IN A COMPUTER NETWORK?

ANS – Forwarding data packets between networks

1. WHAT IS THE PURPOSE OF DNS IN A COMPUTER NETWORK?

ANS - Converting domain names to IP addresses

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

ANS – Star

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

ANS – FTP

Q-2 TRUE AND FALSE

1: 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

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

ANS – FALSE

3:segmentation by dividing a single physical network into multiple logical

networks.

ANS – TRUE

Q – 3 SHORT ANSWER

1:Explain the difference between a hub and a switch in a computer

Network?

ANS – HUB

1. LESS EFFICIENT
2. OPERATES AT LAYER 1
3. LESS SECURE
4. CANNOT MANAGE TRAFFIC INTELLIGENTLY
5. SHARED BANDWIDTH AMONG ALL PORTS

SWITCH

1. MORE EFFICIENT
2. OPERATES AT LAYER 2
3. MORE SECURE
4. MANAGE TRAFFIC INTELLIGENTLY
5. DEDICATED BANDWIDTH PER PORT

2:Describe the process of troubleshooting network connectivity issues?

ANS - Process of Troubleshooting Network Connectivity Issues:-

 Make sure all cables are plugged in and your devices (like modem and router) are turned on.

  See if your computer or phone is connected to the Wi-Fi or network properly.

 Turn off your modem, router, and device. Wait a bit, then turn them back on.

 Make sure your device has a proper IP address. If it’s something weird like 169.x.x.x, your device might not be connecting correctly.

 Use a command like ping 8.8.8.8 (Google’s DNS) to check if your device can reach the internet.

 Try connecting to the internet using a different phone or laptop. If that works, the problem might be your original device.

 If you can’t visit websites but can ping IPs, the issue might be with DNS (the system that turns website names into numbers).

 Sometimes security software can block your connection. Try turning it off briefly to test.

Q-4 PRACTICAL APPLICATION

* Demonstrate how to configure a wireless router's security settings to

enhance network security?

ANS –

 **Log into your router**  
Open your internet browser and type in your router’s address (like 192.168.1.1). Then enter the username and password (check the back of your router if you don’t know).

 **Change the router’s password**  
Don’t use the default admin password! Make it something strong and unique so no one else can mess with your settings.

 **Set Wi-Fi security to WPA2 or WPA3**  
In the wireless settings, pick WPA2 or WPA3 encryption. This scrambles your Wi-Fi signals so others can’t easily snoop on your network.

 **Create a strong Wi-Fi password**  
Make your Wi-Fi password hard to guess. Use a mix of letters, numbers, and symbols — no “123456” or “password.”

 **Turn off WPS**  
WPS is a quick way to connect devices but can be a security risk. It’s best to turn it off.

 **Update your router’s software**  
Check if there’s a firmware update and install it. Updates fix bugs and protect you from hackers.

 **Turn on your router’s firewall**  
This helps block unwanted connections from outsiders.

Q- 5 ESSAY

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

ANS –

**Network Documentation is Important:**

* It helps **track all network components and settings**.
* Makes **troubleshooting faster** when issues happen.
* Simplifies **upgrades and changes** to the network.
* Helps **new team members understand** the network easily.
* Ensures **consistent security and backup practices**

WHAT SHOULD BE DOCUMENTED:

1. It’s important to write down the **IP addresses** assigned to different devices. For example, your router might have an IP address like 192.168.1.1, and a printer might have 192.168.1.20. Knowing these helps in identifying devices and troubleshooting problems.
2. You should also keep track of **device details** such as the model, serial number, and where the device is located. This helps if you need to replace hardware or contact support.
3. Another critical part is to securely save **login information** for your devices and network accounts. This includes usernames and passwords for the router, Wi-Fi, servers, and any other network hardware. It’s important this information is kept safe and only accessible to authorized people.
4. You should document the **configuration settings** of your network devices. For example, your router’s firewall rules, Wi-Fi security settings, and DHCP settings
5. It’s also useful to write down your **network policies**, such as who is allowed to access certain parts of the network, rules about password changes, and how often backups should happen.
6. Finally, keeping track of **software and firmware versions** installed on devices ensures you know when updates are needed, which can fix bugs and improve security.