MODULE - 3

Section 1:

1) c) Forwarding data packets between networks .
2) c) Converting domain names to IP addresses
3) a) Star
4) c) SMTP

Section 2:

5. True

6. False

7. True

Section 3:

9). 1. Identify Problem
2. Check the Basics
- Physical Connections:

○ Cables: Ensure all cables (Ethernet, power) are securely connected and not damaged.
○ Devices: Check for any loose connections or power issues with routers, modems, and other network devices.

- Power Cycle:

○ Restart your modem and router. Unplug them for at least 30 seconds, then power them back on, starting with the modem.

- Device Restart:

○ Restart the device experiencing connectivity issues.

3. Verify Network Settings

- IP Address:

○ Make sure your device has a valid IP address.
○ Check for IP address conflicts (multiple devices with the same IP address).

- DNS Server:

○ Ensure the correct DNS server is configured.
○ Try using a public DNS server like Google Public DNS (8.8.8.8 and 8.8.4.4) if the issue persists.

- Wi-Fi Signal:

○ If using Wi-Fi, check the signal strength.
○ Move closer to the router or consider a Wi-Fi extender.

4. Check Software and Security

- Antivirus/Firewall:

○ Temporarily disable your antivirus and firewall software to see if they are interfering with the connection.
○ Caution: This can increase security risks, so re-enable them as soon as the test is complete.

- Software Updates:

○ Ensure your operating system and network drivers are up to date.
○ Outdated software can sometimes cause compatibility issues.

5. Use Diagnostic Tools

- Network Troubleshooter:

○ Many operating systems have built-in network troubleshooters that can automatically diagnose and fix common problems.

6. Contact Your Internet Service Provider (ISP)

● If the issue persists after trying the above steps, contact your ISP.
● They can help troubleshoot issues with their network infrastructure, such as outages or service interruptions.

● Safety First: Always prioritize your safety when working with electrical equipment.
● Seek Professional Help: If you're not comfortable troubleshooting network issues yourself, consider contacting a qualified IT professional. By following these steps, you can effectively troubleshoot most network connectivity issues. Remember to be patient and methodical in your approach.

Section 4:

10.

1. Access Your Router's Settings

● Find Your Router's IP Address: This is usually found on a sticker on the bottom of your router. Common default addresses include 192.168.1.1 or 192.168.0.1.
● Open a Web Browser: Type the IP address into the address bar and press Enter.
● Enter Login Credentials: You'll need the default username and password. These are usually found on the same sticker as the IP address. If you've changed them, use your custom credentials.

2. Change Default Router Login Credentials

● Locate the Administration Section: This is usually under a tab like "Administration," "Setup," or "Advanced."
● Change Username and Password: Create strong, unique credentials that are difficult to guess. A combination of uppercase and lowercase letters, numbers, and symbols is recommended.

3. Enable Strong Wi-Fi Encryption

● Find Wireless Security Settings: This is typically under a tab like "Wireless," "Wi-Fi," or "Security."
● Select WPA2/WPA3: This is the most secure encryption standard available. If your router doesn't support WPA3, choose WPA2-PSK (AES).
● Create a Strong Wi-Fi Password: Use a long, complex password with a mix of characters. Aim for at least 12 characters.

4. Disable WPS (Wi-Fi Protected Setup)

● Locate WPS Settings: This is usually found in the same section as wireless security settings.
● Disable WPS: This feature can be exploited by hackers. Disabling it adds an extra layer of security.

5. Change Your Network Name (SSID)

● Locate SSID Settings: This is typically found in the same section as wireless security settings.
● Change the Default SSID: Avoid using the default name provided by your router manufacturer. A unique and inconspicuous name can make your network less attractive to attackers.

6. Hide Your SSID (Optional)

● Locate SSID Broadcast Settings: This is usually an option within the SSID settings.
● Disable SSID Broadcast: This makes your network invisible to devices that scan for available networks. However, it doesn't completely hide your network; determined attackers can still find it.

7. Update Your Router's Firmware

● Check for Firmware Updates: This is usually found under an "Administration" or "System" tab.
● Install Updates: Keeping your router's firmware up to date ensures you have the latest security patches and bug fixes.

8. Consider a Guest Network

● Create a Separate Guest Network: This allows you to provide internet access to visitors without giving them access to your main network and its devices.

9. Regularly Review Your Security Settings

● Periodically Check Your Settings: Review your router's security settings regularly to ensure they are still up to date and that no changes have been made without your knowledge.

Section 5: Essay

11.) Faster Troubleshooting: When problems arise, clear documentation can quickly guide technicians to the root cause, minimizing downtime and frustration.
● Improved Efficiency: Well-documented networks allow for faster implementation of changes, upgrades, and expansions.

● Reduced Risk: Documentation reduces the risk of human error, such as misconfigurations or accidental deletions.

● Better Communication: It facilitates clear communication between IT staff, vendors, and other stakeholders.

● Compliance: In many industries, network documentation is essential for regulatory compliance.

Key Information to Document:
● Network Topology: A visual representation (diagram) of the network layout, including all devices (routers, switches, servers, workstations) and their connections.

● Device Inventory:
○ Manufacturer, model, serial number, and location of each device.
○ IP addresses, MAC addresses, and other relevant identifiers.

● Software and Firmware Versions: Keep track of operating systems, drivers, and firmware versions for all devices.
● User Accounts: Document user accounts, permissions, and access rights.

● Network Services: List all network services (e.g., DHCP, DNS, VPN) and their configurations.
● Security Measures: Document security policies, firewalls, intrusion detection systems, and other security measures.

● Backup and Recovery Procedures: Document procedures for backing up and restoring network data and configurations.
● Contact Information: Include contact information for vendors, service providers, and key personnel.

Tools for Network Documentation:

● Spreadsheet Software: Tools like Excel or Google Sheets can be used for basic documentation.
● Dedicated Documentation Software: Specialized tools offer features like version control, collaboration, and automated discovery.
● Network Management Systems (NMS): Some NMS platforms provide built-in documentation features.

.