Section 1: Multiple Choice
1. What is the primary function of a router in a computer network?

Ans. C)forwarding data packets between different networks.

2. What is the purpose of DHCP (Dynamic Host Configuration Protocol) in a computer network?

Ans. D)dynamically assign IP addresses to devices.

3. Which network device operates at Layer 2 (Data Link Layer) of the OSI model and forwards data packets based on MAC addresses?

Ans. B) switch

4. Which network topology connects all devices in a linear fashion, with each device connected to a central cable or backbone

Ans. B) Bus

True or False: A VLAN (Virtual Local Area Network) allows network administrators to logically segment a single physical network into multiple virtual networks, each with its own broadcast domain.

Ans.) TRUE

True or False: TCP (Transmission Control Protocol) is a connectionless protocol that provides reliable, ordered, and error-checked delivery of data packets over a network

Ans.) false

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.

Ans.) true

8. Describe the steps involved in setting up a wireless network for a small office or home office (soho) environment.

Ans.)1. Assess Your Requirements
Determine the number of users and devices that will connect to the wireless network
Estimate the coverage area and identify any potential obstacles or interference sources
Consider the types of devices that will connect (e.g., laptops, smartphones, IoT devices)

2. Choose Reliable Equipment
Select a SOHO wireless router or access point that meets your performance and feature requirements
Ensure compatibility between the router/access point and other network devices
Consider factors like number of Ethernet ports, wireless standards supported (e.g., Wi-Fi 5 or Wi-Fi 6), and security features

3. Configure the Wireless Network
Enable the wireless radio on the router/access point
Set a unique SSID (network name) that doesn't reveal personal information
Choose a strong encryption protocol like WPA2 or WPA3 and set a secure password
Configure wireless settings like frequency band (2.4 GHz or 5 GHz), channel width, and transmit power
Enable any additional security features like MAC address filtering or client isolation

4. Assign IP Addresses
Configure the router's WAN interface with the IP address provided by the internet service provider
Enable DHCP on the router to automatically assign IP addresses to connected devices
Specify the DHCP IP address range and lease time

5. Test and Optimize
Connect test devices to the wireless network and verify internet connectivity
Use wireless network analysis tools to identify potential interference sources and optimize channel selection
Adjust the router's position and antennas to improve wireless coverage and performance

6. Secure and Maintain
Keep the router's firmware up-to-date to address security vulnerabilities and bugs
Monitor network activity and handle any issues or glitches promptly
Regularly review and update wireless security settings and passwords

10. Discuss the importance of network documentation in the context of building and managing networks

Ans.)

The Importance of Network Documentation

Network documentation is crucial for effectively building, managing, and maintaining computer networks. It involves creating and maintaining detailed records of a network's configuration, components, and performance. Here are some key reasons why network documentation is so important:

Improved Troubleshooting and Problem-Solving

When network issues arise, having comprehensive documentation helps IT teams quickly identify the problem area and take appropriate action. Without documentation, troubleshooting becomes a time-consuming guessing game[1][3].

Consistent Operations and Knowledge Sharing

Well-documented network processes and procedures ensure consistency in how issues are resolved and changes are implemented. This prevents errors and enables effective knowledge sharing, especially when onboarding new staff[1][3].

Reduced Risk and Improved Compliance

Up-to-date documentation helps mitigate risks by providing clear guidance on standard operating procedures. It also facilitates compliance with relevant laws, regulations, and industry standards[2][4].

Better Planning for Changes and Expansions

Network documentation provides a clear picture of the current state of the network. This allows administrators to make informed decisions when planning upgrades, expansions, or changes to the infrastructure[2][3].

Faster Disaster Recovery

In the event of a disaster, accurate network documentation can significantly speed up the recovery process by providing the necessary information to restore the network to its pre-disaster state[2][4].

Best Practices for Network Documentation

To ensure network documentation is effective, consider these best practices:

1. **Define the scope of what needs to be documented, such as hardware, software, configurations, and policies[2].**

2. **Use standardized templates to maintain consistency and make information easy to find[2].**

3. **Keep documentation up-to-date by regularly reviewing and updating it as changes occur[1][2].**

4. **Automate documentation where possible using network management tools[2].**

5. **Make documentation easily accessible to all relevant stakeholders[2].**

6. **Use clear and concise language, avoiding technical jargon and acronyms[2].**

7. **Include diagrams and visuals to help stakeholders better understand network configurations[2][4].**

8. **Review and audit documentation periodically to identify areas for improvement.**