### Section 1: Multiple Choice

1. What is the primary function of a router in a computer network?

Answer: c) Forwarding data packets between networks.

* **Explanation:** Think of a router as the traffic cop of the internet. Its main job is to direct your data (in small pieces called packets) from your local network (like your home Wi-Fi) out to the internet and make sure data from the internet finds its way back to your specific device.1

2. What is the purpose of DNS (Domain Name System) in a computer network?

Answer: c) Converting domain names to IP addresses.

* **Explanation:** DNS is like the internet's phonebook.2 It's much easier for us to remember a website name like www.google.com than a string of numbers like 142.250.196.78. DNS does the job of looking up the name and finding the correct number (the IP address) that computers use to communicate.3

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

Answer: a) Star

* **Explanation:** In a star topology, every device on the network has its own dedicated cable connecting it to a central device (a switch or a hub).4 It looks like a star with the hub in the middle and the devices as the points. This is the most common setup used in homes and offices today.

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

Answer: b) FTP

* **Explanation:** FTP stands for **File Transfer Protocol**.5 As its name suggests, its main purpose is to move files from one computer to another over a network. While there are more secure versions of it (like SFTP), FTP is the fundamental protocol listed here for this job.

### Section 2: True or False

5. 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.6

Answer: True.

* **Explanation:** A firewall acts as a security guard for a network.7 It stands between your internal network and the outside internet, inspecting all the data passing through and blocking anything that looks suspicious or doesn't follow the security rules that have been set.8

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

Answer: False.

* **Explanation:** DHCP assigns **dynamic** IP addresses, not static ones.9 "Dynamic" means the addresses are leased for a period of time and can change.10 This is useful because it manages the addresses for you automatically.11 A *static* IP address is one that is set manually and never changes.12

7. True or False: VLANs (Virtual Local Area Networks) enable network segmentation by dividing a single physical network into multiple logical networks.13

Answer: True.

* **Explanation:** VLANs allow a network administrator to take one physical switch and make it act like several separate switches.14 This lets you group certain devices together (like putting all the devices from the Accounting department on one VLAN and Marketing on another), even if they are plugged into the same piece of hardware. This improves security and organization.

### Section 3: Short Answer

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

A hub and a switch both connect devices on a network, but they handle data very differently.15

* A **hub** is a simple, "dumb" device.16 When it receives a piece of data on one of its ports, it doesn't know where it's supposed to go, so it just broadcasts that data out to **every single device** connected to it. This creates a lot of unnecessary traffic and can slow down the network. Think of it like someone shouting in a room—everyone hears it, even if the message is only for one person.
* A **switch** is a "smart" device.17 It learns which device is on which port by remembering their unique MAC addresses. When it receives data, it looks at the destination and sends it **only to the specific device** that is meant to receive it. This is much more efficient and keeps the network fast. It's like a mail carrier delivering a letter directly to the correct mailbox instead of to every house on the street.

9. Describe the process of troubleshooting network connectivity issues.

When you can't connect to the network, you can follow a step-by-step process to find the problem, starting with the simplest solutions first.

1. **Check Physical Connections:** Look at your device and the router. Are the Ethernet cables plugged in securely? Are the Wi-Fi or internet lights on the router lit up and the correct color (usually green or blue)?
2. **Restart Your Device:** The oldest trick in the book often works. Restarting your computer, phone, or tablet can resolve many small software glitches.18
3. **Check Other Devices:** See if other devices in your house can get online. If they can, the problem is likely with your specific device. If nothing can connect, the problem is likely with the router or your internet service.
4. **Restart Your Router and Modem:** Unplug the power from both your modem and your router. Wait about 30 seconds, then plug the modem back in first. Wait for its lights to become stable, then plug the router back in. This process, called a power cycle, fixes a huge number of issues.19
5. **Use Network Tools:** On your computer, you can use a command like ping google.com in the command prompt.20 If you get a reply, you are connected to the internet. You can also use ipconfig (on Windows) to see if your computer has been assigned a valid IP address.21
6. **Contact Your ISP:** If none of the above steps work, the problem may be outside your home. It's time to call your Internet Service Provider (ISP) to see if there is an outage in your area.

### Section 4: Practical Application

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

To make a wireless router more secure, you should log into its settings (usually by typing an address like 192.168.1.1 into a web browser) and make the following changes:

1. **Change the Administrator Password:** Every router comes with a default username and password (like "admin" and "password").22 This is the first thing you should change to a strong, unique password. This prevents anyone from getting into your settings.
2. **Enable WPA3/WPA2 Encryption:** In the wireless security section, make sure you are using the strongest encryption available. **WPA3** is the newest and best, but **WPA2** is also very secure. Avoid older, weaker options like WEP or WPA, as they are easy to crack.23
3. **Create a Strong Wi-Fi Password:** The password you use to connect your devices to the Wi-Fi should be long and complex. Use a mix of uppercase and lowercase letters, numbers, and symbols to make it hard for others to guess.
4. **Change the Network Name (SSID):** Change the default network name from something like "Netgear24" to something unique. Avoid using your family name or address in the SSID, as this gives away personal information.
5. **Keep the Firmware Updated:** Router manufacturers release software updates, called firmware, to fix security problems.24 Check the router’s settings for an "update firmware" option to make sure you have the latest, most secure version.

### Section 5: Essay

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

Network documentation is the practice of keeping detailed records about how a computer network is built, configured, and maintained.25 While it might seem like extra work, it is one of the most critical aspects of managing a network, whether it's for a small business or a large corporation. Its importance lies in its ability to save time, reduce errors, and enhance security.

The most significant benefit of good documentation is **faster troubleshooting**. When a network problem occurs, having a map and detailed records allows a technician to quickly understand how everything is connected and configured, making it much easier to locate the source of the issue. Without it, they are essentially working in the dark, wasting valuable time trying to figure out the basics. Furthermore, documentation is essential for **planning and growth**. When it's time to upgrade the network or add new equipment, having a clear picture of the current setup helps in making informed decisions and ensures that new changes are compatible with the existing infrastructure.

Good documentation also plays a vital role in **security**. By keeping a record of all devices, configurations, and firewall rules, it becomes easier to manage and audit the network's security posture. It helps identify unauthorized devices or unexpected changes that could represent a security breach. Finally, it ensures **consistency and knowledge transfer**. If the primary network administrator leaves the company, the documentation allows a new person to get up to speed quickly, ensuring the network can continue to be managed effectively.26

Examples of essential information to include in network documentation are:

* **A Physical Network Map:** A diagram showing the physical layout of the office, including the location of servers, routers, switches, and wall jacks.27
* **A Logical Network Map:** A diagram that illustrates how data flows, showing IP addresses, subnets, and VLAN configurations.28
* **IP Address Scheme:** A detailed list of all IP addresses used on the network, including which ones are static (assigned permanently to devices like servers) and the range used for dynamic allocation (DHCP).
* **Device Configuration Files:** Backups of the configuration files for key devices like routers, switches, and firewalls.29
* **A Password List:** A securely stored list of login credentials for all network devices.
* **Vendor and Service Information:** Contact details for the internet service provider (ISP) and manufacturers of the network hardware, including account numbers and support contract details.

In summary, network documentation is the blueprint of a network. It's a fundamental practice that provides the clarity and information needed for efficient troubleshooting, strategic planning, and robust security management.