**Assignment Module: 3**

**Section 1: Multiple Choice**

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

**Answer:** Forwarding data packets between networks

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

**Answer:** Converting domain names to IP addresses

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

**Answer:** Star

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

**Answer:** FTP

**Section 2: True or 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**.

**Answer:** TRUE

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

**Answer:** FALSE

**Reason:** DHCP (Dynamic Host Configuration Protocol) automatically assigns dynamic IP addresses to network devices, not static ones. Static IP addresses are manually assigned and remain constant, while dynamic IP addresses are assigned temporarily and can change.

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

**Answer:** TRUE

**Section 3: Short Answer**

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

**Answer:**

|  |  |
| --- | --- |
| HUB | SWITCH |
| Hub is operated on **Physical layer of OSI model.** | While switch is operated on **Data link** layer of OSI model. |
| Hub is a broadcast type transmission. | While switch is a Unicast, multicast and broadcast type transmission. |
| Hub is a half-duplex transmission mode. | While switch is a full duplex transmission mode. |
| Hub has 4/12 ports. | While switch can have 24 to 48 ports. |
| Hacking of systems attached to hub is complex. | Hacking of systems attached to switch is little easy. |
| Speed of original hub 10Mbps and modern internet hub is 100Mbps. | Maximum speed is 10Mbps to 100Mbps. |
| Cheaper as compared to switch. | Expensive as compared to HUB. |

1. **Describe the process of troubleshooting network connectivity issues.**

**Answer:** Network troubleshooting is a repeatable process, which means that you can break it down into clear steps that anyone can follow:

**1. Identify the Problem**

The first step in troubleshooting a network is to identify the problem. As a part of this step, you should do the following:

Gather information about the current state of the network using the network troubleshooting tools that you have available to you. Duplicate the problem on a test piece of hardware or software, if possible. This can help you to confirm where your problem lies. Question users on the network to learn about the errors or difficulties they have encountered. identify the symptoms of the network outage. For example, do they include complete loss of network connection? Slow behavior on the network? Is there a network-wide problem, or are the issues only being experienced by one user? Determine if anything has changed in the network before the issues appeared. Is there a new piece of hardware that’s in use? Has the network taken on new users? Has there been a software update or change somewhere in the network? Define individual problems clearly. Sometimes a network can have multiple problems. This is the time to identify each individual issue so that your solutions to one aren’t bogged down by other unsolved problems.

**2. Develop a Theory**

Once you have finished gathering all the information that you can about the network issue or issues, it’s time to develop a working theory. While you’re producing your theory about the causes of the network issue, don’t be afraid to question the obvious, but remain on the lookout for more serious issues. Sometimes a network outage occurs because someone tripped on a wire or some other simple problem. However, at other times the problems might be related more complicated causes, like a breach in network security.

**3. Test the Theory**

Using the tools at your disposal, it’s time to test your theory. If your theory is that the network router is defective, try replacing it with another router to see if that fixes the issue. At this stage, it’s important to remember that proving your own theories wrong doesn’t mean that you’ve failed. Instead, it means that it’s time to return to step two, develop a new theory, and then find a way to test that one. Sometimes your first theory may be right, but it’s also common to go through several theories before arriving at the true cause of your network’s issues.

**4. Plan of Action**

Once you’ve confirmed your theory about the causes of the network issues, you’re in a position to solve them. Come up with a plan of action to address the problem. Sometimes your plan will include just one step. For example, restart the router. In other cases, your plan will be more complex and take longer, such as when you need to order a new part or roll a piece of software back to a previous version on multiple users’ computers.

**5. Implement the Solution**

Now that you have a plan for fixing the network, it’s time to implement it. There are some solutions that you may be able to do by yourself, while others may require cooperation from other network administrators or users.

**6. Verify System Functionality**

Once you’ve implemented your solution, be sure to test the network. Make sure that the issue in question has been resolved but also be on the lookout for other issues that may have arisen from the changes that you made to the network. As part of your verification process, make sure to consult both the network tools at your disposal as well as individual user accounts of their experiences on the network.

**7. Document the Issue**

If you are a network professional or an enthusiast who is around networks often, then it’s safe to say that this won’t be the last time you encounter this particular issue. Make sure to document each stage of troubleshooting the problem, including the symptoms that appeared on the network, the theory you developed, your strategy for testing the theory and the solution that you came up with to solve the issue. Even if you don’t reference this documentation, it may be helpful to another network engineer at your company in the future and could help to shorten network downtime.

**Section 4: Practical Application**

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

**Answer:** To configure a wireless router's security settings for enhanced network protection, first log into the router's web interface, navigate to the wireless settings, and select the most secure encryption method (WPA3 or WPA2). Next, choose a strong, unique password for your Wi-Fi network. Enable the router's firewall and consider disabling unused features like WPS or UPnP.

Detailed Steps:

1. Access Router Configuration:

Connect to your Wi-Fi network or use an Ethernet cable. Open a web browser and enter the router's IP address (usually 192.168.1.1 or 192.168.0.1) in the address bar. Log in using the default username and password, which can be found on the router's sticker or in the manual.

2. Navigate to Wireless Settings:

Locate the "Wireless," "Wi-Fi," or "Network" section in the router's web interface. Click on "Wireless Settings" or a similar option to access the network configuration.

3. Select Security Protocol:

Choose the most secure encryption method:

WPA3 Personal: Recommended for the latest security features and compatibility.

WPA2 Personal: A strong option, especially if your router doesn't support WPA3.

WPA/WPA2 Mixed: If you have devices that support older WPA/WPA2 encryption but also need to support WPA3. If you are using WPA2, ensure you select AES encryption.

4. Set Wi-Fi Password:

Create a strong, unique password for your Wi-Fi network. Use a combination of uppercase and lowercase letters, numbers, and symbols. A password length of at least 12 characters is recommended.

5. Disable Unused Features:

WPS (Wi-Fi Protected Setup): Disable this feature if you don't need it, as it can be vulnerable to attack.

UPnP (Universal Plug and Play): Disable this feature, as it can expose your network to unauthorized access.

Remote Management: If you don't need to manage your router remotely, disable this feature for added security.

6. Enable Router Firewall: Most routers have a firewall built-in, which should be enabled to block unauthorized access to your network.

7. Save Changes: Click "Save" or "Apply" to save your configuration changes.

8. Reboot Router: Your router may require a reboot to apply the new settings.

**Section 5: Essay**

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

**Answer:**  Network documentation is crucial for understanding, maintaining, and troubleshooting a network infrastructure. It provides a clear roadmap of the network's design, setup, and operation, enabling efficient problem-solving, upgrades, and security management. Examples of information to document include network topology maps, hardware configurations, software versions, server details, backup schedules, and security protocols.

Here's a more detailed look at why network documentation is important and what it should include:

Why Network Documentation Matters:

Efficient Troubleshooting: Documentation helps identify the root cause of problems quickly, reducing downtime and minimizing impact.

Facilitates Upgrades and Changes: A clear understanding of the network allows for smoother upgrades, expansions, and modifications.

Enhances Security: Documentation provides a baseline for security assessments and can help identify vulnerabilities.

Supports Disaster Recovery: Detailed documentation ensures that the network can be restored to its pre-disaster state efficiently.

Improves Knowledge Sharing: Documentation helps onboard new team members and ensures that knowledge is readily available, preventing a single point of failure.

Facilitates Compliance: Documentation helps organizations comply with industry standards and regulations.

Justifies IT Investments: Documentation can demonstrate the value of IT investments by highlighting the benefits of a well-managed network.

Information to Document:

Network Topology Maps: Visual representations of the network infrastructure, including physical and logical layouts, equipment locations, and cabling.

Hardware Configurations: Specific details about each device, such as IP addresses, subnet masks, DNS servers, and firmware versions.

Software Versions: Versions of operating systems, applications, and drivers running on servers and network devices.

Server Details: Operating systems, installed software, user profiles, and directory structures.

Backup Schedules: Regularly scheduled backups, locations, and verification procedures.

Security Protocols: Firewall rules, access control lists, and other security configurations.

Vendor and Contractor Information: Contact details for vendors and contractors, service agreements, and warranties.

Problem Resolutions: Detailed records of past issues, solutions, and results.

Change Management: Logs of network changes, including dates, times, users, and descriptions.