**Assignment 3**

**Peripherals and Power Supply**

Section 1: Multiple Choice

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 (Domain Name System) in a computer network?**

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

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

**Ans:** Star

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

**Ans:** 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**.

**Ans:** TRUE

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

**Ans:** 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.**

**Ans:** TRUE

Section 3: Short Answer

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

**Ans:**

|  |  |
| --- | --- |
| HUB | SWITCH |
| Hub is operated on first layer (**Physical layer) of OSI model.** | While switch is operated on second layer (**Data link** layer) of OSI model. |
| Sends data to all connected devices (broadcast). | Sends data only to the intended recipient (unicast and multicast). |
| Does not learn or use MAC addresses to forward data. | Learns MAC addresses to forward data properly. |
| Hub is a half-duplex transmission mode. | While switch is a full duplex transmission mode. |
| 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| Cheaper as compared to switch at the same time it is outdated. | Expensive as compared to HUB at the same time commonly used technology. |

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

**Ans:** 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**

* Start by gathering basic information:
* What exactly isn't working? (e.g., can't access internet, can't connect to Wi-Fi)
* Is the issue affecting one device or multiple devices?
* When did the issue start?
* What changed recently (new software, hardware, settings)?.

1. **Check Physical Connections**

* Ensure Ethernet cables are securely plugged in.
* Confirm Wi-Fi is turned on (on laptops, phones, routers).
* Check for loose or damaged cables or disconnected routers/switches.

1. **Verify Device Configuration**

* Check the device's IP address (use ipconfig on Windows, ifconfig or ip a on Linux/macOS).
* Ensure it's getting a valid IP address (not 169.254.x.x — that indicates failure to get DHCP).
* Verify correct subnet mask, gateway, and DNS settings.

1. **Test Local and External Network Connectivity**

* Ping the default gateway (e.g., ping 192.168.1.1) to check if the router is reachable.
* Ping another device on the same network to test internal connectivity.
* Ping an external site (e.g., ping 8.8.8.8) to test internet access.
* If that works, test DNS resolution (e.g., ping google.com).
* If DNS fails but IP ping works, the issue is likely with DNS settings.

1. **Restart Networking Equipment**

* Restart the modem, router, and affected device.
* Power cycling can resolve many temporary network issues.

1. **Check Router and ISP Status**

* Log in to the router’s web interface to check status and logs.
* Check your ISP’s service status online or via mobile data.
* Test with another internet source (e.g., mobile hotspot) if possible.

**8. Look for Security or Software Issues**

* Check for firewalls or security software that may be blocking connections.
* Scan for malware or recently installed software that could interfere.
* Check if the device is blocked by MAC address filtering on the router.

**9. Use Diagnostic Tools**

* Use built-in tools:
* Windows: Network Troubleshooter
* macOS: Wireless Diagnostics
* CLI: tracert, nslookup, netstat, arp, nmap
* Tools help trace where the connection breaks down.

**10. Document and Escalate if Needed**

* Record what was tried and the results.
* If unresolved, escalate to:
* Network administrator
* ISP support
* Hardware vendor support (for modems, routers, etc.)

Section 4: Practical Application

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

**Ans:** 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.

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.**

**Ans:**  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: Helps IT staff identify and fix network problems faster by providing clear information about the setup.

Facilitates Upgrades and Changes: A clear understanding of the network allows for smoother upgrades, expansions, and modifications. Makes it easier to add new devices or change settings without causing issues.

Enhances Security: Tracks user access, firewall rules, and device configurations, helping to protect against security threats.

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.

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.