**Assignment**

**Module 3 : Understanding and Maintenance of Networks**

**Section 1: Multiple Choice**

1. What is the primary function of a router in a computer network? a) Assigning IP addresses to devices b) Providing wireless connectivity to devices c) Forwarding data packets between networks d) Managing user authentication and access control

Ans: c) Forwarding data packets between networks

1. What is the purpose of DNS (Domain Name System) in a computer network? a) Encrypting data transmissions for security b) Assigning IP addresses to devices dynamically c) Converting domain names to IP addresses d) Routing data packets between network segments

Ans: c) Converting domain names to IP addresses

1. What type of network topology uses a centralized hub or switch to connect all devices? a) Star b) Bus c) Ring d) Mesh

Ans: a) Star

1. Which network protocol is commonly used for securely accessing and transferring files over a network? a) HTTP b) FTP c) SMTP d) POP3

**Ans**: b) FTP (File Transfer Protocol)

**Section 2: True or False**

1. 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

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

**Ans:** False

DHCP (Dynamic Host Configuration Protocol) assigns dynamic IP addresses to network devices automatically, not static IP addresses.

* Dynamic IP addresses change periodically and are assigned by a DHCP server.
* Static IP addresses are manually configured and remain fixed.

1. True or False: 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.

Certainly! A hub and a switch are both devices used in computer networks to connect multiple devices, but they operate differently:

**Hub**

* **Functionality:** A hub is a basic networking device that connects multiple devices in a network. It broadcasts data to all connected devices, regardless of the intended recipient.
* **Efficiency:** It is less efficient as it doesn't distinguish between devices. All devices share the same bandwidth, which can lead to collisions and slower network performance.
* **Communication:** Operates at the **physical layer** (Layer 1) of the OSI model.
* **Intelligence:** It doesn't filter data or learn device addresses.

**Switch**

* **Functionality:** A switch is a more advanced device. It forwards data only to the intended recipient, using the device's MAC (Media Access Control) address to make decisions.
* **Efficiency:** Much more efficient than a hub because it reduces collisions and improves network speed by managing bandwidth intelligently.
* **Communication:** Operates at the **data link layer** (Layer 2) of the OSI model (some switches also work at Layer 3 for routing).
* **Intelligence:** Switches can learn and store MAC addresses in a table, enabling smarter data forwarding.

1. Describe the process of troubleshooting network connectivity issues.

**Network Connectivity Troubleshooting Process**

Troubleshooting network connectivity involves systematically identifying and resolving issues. Below are the key steps:

1. **Identify the Problem**
   * Gather information:
     + Is it affecting a single device or multiple devices?
     + Is it a wired or wireless connection issue?
     + When did the problem start?
2. **Check Physical Connections**
   * Ensure network cables are securely connected and undamaged.
   * Verify that the router, switch, and modem are powered on and functional.
   * Inspect Ethernet cables for looseness or disconnection (for wired connections).
   * Confirm that Wi-Fi is enabled on the device (for wireless connections).
3. **Verify IP Configuration**
   * Check network settings via the command prompt:
     + **Windows:** ipconfig /all
     + **Linux/Mac:** ipconfig or Ip a
   * Confirm the device has a valid IP address from the DHCP server.
   * For static IPs, ensure they are correctly configured.
4. **Test Network Connectivity**
   * Ping the local router/gateway: ping 192.168.1.1 (or your router's IP).
   * Ping an external website: ping google.com
     + If local ping works but external ping fails, it may indicate an internet issue.
5. **Restart Network Devices**
   * Reboot the computer, router, switch, and modem to refresh connections.
   * Power cycle the modem and router: unplug them for 30 seconds, then plug them back in.
6. **Check DNS Configuration**
   * If websites fail to load but the internet seems to work:
     + Switch to Google DNS: 8.8.8.8 and 8.8.4.4.
7. **Temporarily Disable Firewall/Antivirus**
   * Sometimes, firewalls or security software block connections.
   * Disable them briefly to test the network.
8. **Test with Another Device**
   * If other devices connect successfully, the issue lies with the specific device.
   * If multiple devices fail, the problem likely stems from the router, modem, or network.
9. **Contact the ISP (If Necessary)**
   * For ongoing external connectivity issues, check for an ISP outage.
   * Reach out to your Internet Service Provider for assistance.
10. **Advanced Troubleshooting**
    * Review router logs for potential errors.
    * Update network drivers on the affected computer.
    * Reset the router to factory settings if all else fails.

**Section 4: Practical Application**

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

**How to Secure Your Wireless Router**

1. **Access Your Router**
   * Launch your web browser and navigate to either 192.168.1.1 or 192.168.0.1.
   * Log in using the default credentials found on the router’s label.
2. **Change the Default Administrator Password**
   * Replace the preset password with a strong, unique one to block unauthorized access.
3. **Apply Robust Wi-Fi Encryption (WPA3 or WPA2)**
   * In the Wireless Security Settings, select WPA3-Personal (or WPA2 if WPA3 isn’t supported).
   * Create a secure Wi-Fi password with a minimum of 12 characters.
4. **Conceal Your Wi-Fi Network (Optional)**
   * Disable SSID broadcasting to make your network less visible to outsiders.
5. **Enable MAC Address Filtering**
   * Limit network access by allowing only specific devices identified by their MAC addresses.
6. **Limit the Wi-Fi Signal Range**
   * Adjust the transmit power to keep the wireless signal contained within your home.
7. **Update Router Firmware**
   * Regularly check for and install firmware updates in the System Settings to address security vulnerabilities.
8. **Turn Off WPS**
   * Disable Wi-Fi Protected Setup (WPS) to avoid easy exploitation by hackers.
9. **Activate the Built-In Firewall**
   * Ensure the router’s firewall is enabled to add an extra layer of defense.
10. **Set Up a Guest Network**
    * Create a separate Wi-Fi network for guests to keep your main network secure.
11. **Disable Remote Administration**
    * Turn off any remote access features so that router administration is restricted to local devices.
12. **Monitor Connected Devices Regularly**
    * Regularly review the list of connected devices and remove any unfamiliar entries.

**Section 5: Essay**

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

**The Importance of Network Documentation**

Maintaining thorough network documentation is vital for the smooth operation, troubleshooting, and security of any network infrastructure. It serves as a comprehensive blueprint of your entire network, allowing IT teams to quickly diagnose issues, implement upgrades, and enforce security protocols.

**Why It Matters**

1. **Streamlined Troubleshooting**  
   Detailed records empower teams to identify and resolve network problems efficiently, saving time and resources.
2. **Enhanced Security**  
   By mapping out the network, documentation aids in pinpointing vulnerabilities, reducing the risk of unauthorized access.
3. **Simplified Expansion**  
   An accurate layout of the network makes scaling and integrating new systems or devices much more straightforward.
4. **Reduced Downtime**  
   Quick access to configuration details and system layouts accelerates recovery during outages or cyberattacks.
5. **Standardized IT Processes**  
   Consistent documentation ensures that network setup and maintenance follow a uniform standard, which minimizes errors.
6. **Regulatory Compliance and Auditing**  
   Detailed records support compliance with legal and industry standards, making audits and reviews more manageable.

**Essential Elements to Document**

1. **Network Topology Diagram**
   * A visual map that illustrates how switches, routers, servers, and other devices interconnect.
2. **IP Addressing Scheme**
   * A documented list of assigned IP addresses, subnet masks, and VLAN details.
   * *Example:* Recording that 192.168.1.10 is assigned to a file server.
3. **Device Inventory**
   * An inventory of all network hardware, including routers, switches, and firewalls with details such as model numbers, serial numbers, and firmware versions.
4. **Configuration Settings**
   * Backups and records of configuration settings for network devices, including firewall rules and access control lists (ACLs).
5. **User Access and Permissions**
   * A secured record of which users have administrative or special access to network resources.
6. **ISP and Service Provider Information**
   * Contact details and service parameters for your Internet Service Provider, such as support numbers, service level agreements, and bandwidth specifics.
7. **Backup and Disaster Recovery Plan**
   * Clearly outlined steps and locations for restoring configurations and data in the event of a network failure.
8. **Security Policies**
   * Guidelines detailing firewall configurations, password protocols, and encryption practices.
   * *Example:* A policy requiring password updates every 90 days.
9. **Network Performance Logs**
   * Continuous records of network uptime, latency, and bandwidth usage to track performance and troubleshoot issues over time.
10. **Wi-Fi Settings & SSIDs**
    * A documented list of all wireless network names (SSIDs) paired with their corresponding encryption settings.
    * *Example:* An SSID like "Office WIFI" that uses WPA3 encryption.

By systematically documenting these aspects, an organization not only enhances its ability to maintain and secure its network but also creates a resilient foundation for growth and innovation. This practice streamlines everyday operations and empowers teams to make informed decisions about network upgrades and security strategies.