**Assignment**

**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?**

**Answer:**Forwarding data packets between networks.

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

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

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

**Answer:** Star.

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

**Answer:** FTP

* **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.**

**Answer:** True

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

**Answer:** False

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

**Answer:** True

* **Section 3: Short Answer**

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

**Answer:**

In a computer network, both hubs and switches are devices used to connect multiple devices (like computers, printers, etc.) within a local area network (LAN). However, they operate differently and have distinct functionalities:

**Hub:**

1. **Layer:** Hubs operate at the physical layer (Layer 1) of the OSI model.
2. **Functionality:** A hub is a basic networking device that connects multiple Ethernet devices, making them act as a single network segment. It simply receives data packets from one device and broadcasts them to all other connected devices, regardless of the intended recipient.
3. **Intelligence:** Hubs are considered "dumb" devices because they do not have the capability to filter or manage traffic. They do not analyse the data packets or know where to send them specifically.
4. **Collision Domain:** All devices connected to a hub share the same collision domain, which can lead to data collisions and reduced network efficiency, especially as the number of devices increases.
5. **Speed:** Hubs typically operate at lower speeds (10/100 Mbps) and do not support advanced features like VLANs or Quality of Service (QoS).

**Switch:**

1. **Layer:** Switches operate at the data link layer (Layer 2) of the OSI model, and some switches can also operate at the network layer (Layer 3) for routing purposes.
2. **Functionality**: A switch intelligently receives data packets and forwards them only to the specific device (or port) that is the intended recipient, based on the MAC address of the devices. This reduces unnecessary traffic on the network.
3. **Intelligence**:  Switches are "smart" devices that maintain a MAC address table, allowing them to learn and remember the addresses of devices connected to each port. This enables efficient data transmission.
4. **Collision Domain**: Each port on a switch creates a separate collision domain, which significantly reduces the chances of collisions and improves overall network performance.
5. **Speed**: Switches generally support higher speeds (up to 1 Gbps or more) and can offer advanced features such as VLAN support, QoS, and network management capabilities.

In summary, the main difference between a hub and a switch lies in their functionality and efficiency.

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

**Answer:**

Troubleshooting network connectivity issues involves a systematic approach to identify and resolve problems that prevent devices from communicating effectively over a network. Here’s a step-by-step process to troubleshoot network connectivity issues:

1. **Identify the problem**

* **Gather Information:** Start by asking users about the issue. What symptoms are they experiencing? Is it a complete loss of connectivity, slow performance, or intermittent issues?
* **Determine Scope**: Identify whether the problem is affecting a single device, multiple devices, or the entire network.

1. **Check Physical Connection**

* **Inspect Cables:** Ensure that all network cables are securely connected and undamaged. Look for frayed or broken cables.
* **Check Devices:** Verify that network devices (routers, switches, modems) are powered on and functioning properly. Check for indicator light that show connectivity status.

1. **Verify Network Configuration**

* **IP Addressing**: Check the IP configuration of the affected device. Ensure it has a valid IP address, subnet mask, and default gateway. Use commands like ***ipconfig***(Windows) or ***ifconfig*** (Linux/Mac) to view settings.
* **DHCP Settings**:  If the device is set to obtain an IP address automatically, ensure that the DHCP server is operational and that there are available IP addresses in the pool.

1. **Test Connectivity**

* **Ping Test:** Use the ping command to test connectivity to the local router, other devices on the network, and external addresses (like 8.8.8.8 for Google DNS). This helps identify where the connectivity issue lies.
* **Traceroute:** Use the ***‘tracert’*** (Windows) or ***‘traceroute’*** (Linux/Mac) command to trace the path packets take to reach a destination. This can help identify where packets are being dropped.

1. **Check Network Services**

* **DNS Resolution:** If users can’t access websites, check if DNS is functioning properly. Use the ***‘nslookup’*** command to verify DNS resolution.
* **Firewall Settings**: Ensure that firewalls (both on the device and network level) are not blocking necessary traffic. Temporarily disable firewalls to see if connectivity is restored.

1. **Review Network Devices**

* **Router/Switch Configuration**: Check the configuration of routers and switches for any misconfigurations, such as incorrect VLAN settings or access control lists (ACLs).
* **Logs and Alerts**: Review logs on network devices for any error messages or alerts that could indicate issues.

1. **Check for Interface**

* **Wireless Networks:** If troubleshooting a wireless connection, check for interference from other devices (like microwaves or cordless phones) and ensure the Wi-Fi signal is strong.
* **Network Congestion**: Assess network traffic to determine if congestion is causing slow performance. Tools like network monitoring software can help analyse traffic patterns.

1. **Reboot Devices**

* **Restart Devices**: Sometimes, simply rebooting the affected device, router, or switch can resolve connectivity issues by clearing temporary glitches.

By following this structured approach, you can systematically identify and resolve network connectivity issues, ensuring that users can regain access to network resources efficiently.

* **Section 4: Practical Application**

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

**Answer:** Practical Done in Lab

* **Section 5: Essay**

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

**Answer:**

Network documentation is a critical aspect of network management and administration. It involves creating and maintaining detailed records of a network's configuration, architecture, policies, and procedures. Proper documentation serves several important purposes:

**Importance of Network Documentation**

1. **Operational Efficiency:** Well-documented networks allow IT staff to quickly understand the network's structure and configuration, leading to faster troubleshooting and problem resolution.
2. **Knowledge Transfer:** Documentation serves as a valuable resource for training new staff and ensuring that knowledge is not lost when employees leave or change roles.
3. **Change Management:** Keeping accurate records of network configurations and changes helps in managing updates and modifications, reducing the risk of errors during changes.
4. **Compliance and Auditing:** Many industries have regulatory requirements that mandate proper documentation of network configurations and security measures. Documentation can facilitate audits and compliance checks.
5. **Disaster Recovery:** In the event of a network failure or disaster, documentation provides essential information for restoring services and recovering data.
6. **Security:** Documenting network security policies, configurations, and access controls helps in identifying vulnerabilities and ensuring that security measures are consistently applied.
7. **Planning and Scalability:** Documentation aids in planning for future network expansions or upgrades by providing a clear understanding of the current network setup.

**Examples of Information to Document**

1. **Network Topology Diagrams:**
   * Visual representations of the network layout, including devices (routers, switches, firewalls), connections, and their physical or logical arrangement.
2. **Device Inventory:**

A list of all network devices, including details such as:

* + Device type (router, switch, firewall, etc.)
  + Manufacturer and model
  + Serial numbers
  + IP addresses and MAC addresses
  + Location (physical or logical)

1. **IP Address Management:**

A record of IP address assignments, including:

* + Subnetting information
  + DHCP scope and reservations
  + Static IP assignments
  + Address usage and availability

1. **Configuration Files:**

Backup copies of device configurations, including:

* + Router and switch configurations
  + Firewall rules and policies
  + Access control lists (ACLs)
  + VPN configurations

1. **Network Policies and Procedures:**

Documentation of network policies, including:

* + Security policies (password policies, access controls)
  + Change management procedures
  + Incident response plans
  + Backup and recovery procedures

1. **Network Performance Metrics:**

Records of network performance data, such as:

* + Bandwidth usage
  + Latency measurements
  + Error rates
  + Historical performance trends

1. **User Access and Permissions:**

Documentation of user accounts, roles, and permissions, including:

* + Usernames and roles
  + Access levels to network resources
  + Authentication methods used (e.g., RADIUS, LDAP)

1. **Vendor and Support Information:**

Contact information for vendors and support services, including:

* + Support contracts and service level agreements (SLAs)
  + Warranty information
  + Escalation procedures for technical support

1. **Change Logs:**

Records of changes made to the network, including:

* Date and time of changes
* Description of changes (e.g., device upgrades, configuration changes)
* Personnel involved in the changes
* Impact assessment and rollback procedures

1. **Network Diagrams and Documentation:**

Detailed documentation of network services, such as:

* + DNS records
  + Active Directory structure
  + Application dependencies and configurations

In summary, network documentation is essential for effective network management, security, and compliance. By maintaining comprehensive and up-to-date documentation, organizations can enhance operational efficiency, facilitate troubleshooting, and ensure a robust and secure network environment.