❖ 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?
Ans-1 c) Forwarding data packets between networks.

2.) What is the purpose of DNS (Domain Name System) in a computer network?
Ans-2 c) Converting domain names to IP addresses.

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

4.) Which network protocol is commonly used for securely accessing and transferring files over a network?
Ans-4 b) FTP

★ Section 2: True or False

5.) 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-5 True

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

- DHCP (Dynamic Host Configuration Protocol) assigns dynamic (not static) IP addresses to devices on a network. It automatically allocates IP addresses to devices as they join the network.

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

★ Section 3: Short Answer

8.) Explain the difference between a hub and a switch in a computer network.
Ans-8 In computer networking, hubs and switches are both devices used to connect multiple computers or other network devices together within a network.

1.) Hub:

- ➢ **Function**: A hub is a basic networking device that simply takes data packets from one device and broadcasts them to all other connected devices.
- ➢ **Operation**: Hubs work on a "broadcast" principle. When one device sends data to the hub, the hub sends that data to all devices connected to it, regardless of the intended recipient.
- ➢ **Bandwidth**: Since a hub sends data to every connected device, all devices share the same bandwidth. This can lead to
- ➢ **Layer**: Hubs operate at Layer 1 of the OSI model (Physical Layer). They don't understand anything about the data they are transmitting—just the physical connection.
- ➢ **Efficiency**: Hubs are generally less efficient and less secure because they don't distinguish between different devices.

2.)Switch:

- ➢ **Function**: A switch is a more advanced networking device that connects devices in a network and forwards data only to the specific device (or devices) it is intended for.
- ➢ **Operation**: Switches operate at a data link layer (Layer 2) and use MAC (Media Access Control) addresses to determine the destination of the data packets. When a device sends data, the switch reads the destination MAC address and forwards the data only to the correct device.
- ➢ **Bandwidth**: Unlike hubs, switches allow each device to communicate independently with the switch, meaning there is no shared bandwidth.
- ➢ **Layer**: Switches operate at Layer 2 (Data Link Layer), and some can also operate at Layer 3 (Network Layer) to route traffic between different subnets (these are called Layer 3 switches).
- ➢ **Efficiency**: Switches are more efficient and scalable than hubs, as they reduce network traffic and improve overall performance. Switches also provide better security since the data is not broadcasted to all devices.

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

Ans-9 Troubleshooting network connectivity issues involves systematically identifying and addressing potential problems that prevent devices from communicating over a network.

- ❖ **Process of troubleshooting:**

1.) Understand the Problem.

- ➢ **Clarify Symptoms**: Gather details about the problem. Is it affecting one device or multiple devices? Is it a complete network outage or intermittent connectivity?
- ➢ **Determine the Scope**: Is it an internal network issue (LAN) or external connectivity problem (internet or remote network)?

2.)Check Physical Connections.

- ➢ **Inspect Cables**: Ensure that Ethernet cables, power cords, and other physical connections are securely plugged in.
- ➢ **Check Lights on Network Devices**: Verify the status LEDs on the router, modem, or switch. For instance, a blinking or solid light can indicate different states, such as connection or no signal.

3.) Verify Device Configuration.

- ➢ **IP Configuration**: Ensure that the device is configured to obtain an IP address automatically (via DHCP) or that it has the correct static IP address.
- ➢ **Check Subnet Mask and Gateway**: Verify that the subnet mask and default gateway are correctly configured.
- ➢ **DNS Settings**: Ensure that the DNS server addresses are correct. Incorrect DNS settings can prevent access to websites even if the network is otherwise functional.

4.) Ping the Device.

- ➢ **Ping Local Network**: Ping the local gateway/router (e.g., ping 192.168.1.1). If this fails, the issue is likely within your internal network.

➢ **Ping External Websites**: If you can reach the router but not external sites, the problem might be with your ISP or DNS resolution.

5.) Check Network Interface Status.

➢ **Network Adapter**: Check the network adapter's status (in device settings or Control Panel). Ensure the adapter is enabled and working.

➢ **Restart Adapter**: Disable and then re-enable the network adapter to reset the connection.

6.) Test Other Devices.

➢ **Multiple Devices**: Check if the issue is isolated to one device or affects multiple devices. If others are also affected, the issue is likely at the router or ISP level.

➢ **Swap Cable or Port**: Try using a different Ethernet cable or port on the router/switch to rule out hardware failure.

7.) Review Router and Switch Settings.

➢ **Router Configuration**: Access the router's admin page and ensure it's properly configured for DHCP, NAT, and any necessary security/firewall settings.

➢ **Restart the Router/Modem**: Power cycle the router and modem to refresh the connection, especially if there has been a recent power outage or connectivity disruption.

8.) Test for Interference or Network Congestion.

➢ **Wi-Fi Interference**: If using Wi-Fi, check for interference from other networks, devices, or physical obstructions. Consider switching Wi-Fi channels.

➢ **Network Traffic**: Check for any heavy network usage that could be causing congestion (e.g., large downloads or streaming).

9.) Check for ISP Issues.

➢ **ISP Service Status**: Contact your Internet Service Provider (ISP) to verify if there are any outages or service issues in your area.

- ➢ **Modem and Router Lights**: Ensure that the modem is correctly synced with the ISP and that the appropriate lights are on (e.g., power, internet, and DSL or cable connection).

10.) Advanced Diagnostics.

- ➢ **Traceroute/Pathping**: Use tools like traceroute or pathping to diagnose network hops and pinpoint where the connection fails along the path to the destination.
- ➢ **Firewall/Security Software**: Ensure that firewalls or security software are not blocking connections, either on the router or individual devices.

11.) Document and Verify.

- ➢ **Record the Solution**: Document the steps taken and the solution found. This can be helpful for future reference or recurring issues.
- ➢ **Verify Functionality**: After resolving the issue, test the connectivity thoroughly to ensure everything is working as expected.

★ Section 4: Practical Application

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

Ans- 10 Done

★ Section 5: Essay

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

Ans-11 **Importance of Network Documentation:**

- ➢ Network documentation is vital for the effective and efficient operation of any network infrastructure. It serves as a central record of all network-related information, configurations, and procedures. Proper documentation not only aids in day-to-day management and maintenance but also plays a crucial role in ensuring security, troubleshooting, scalability, and compliance.

- **Important of network documentation:**

1.] Improved Troubleshooting and Faster Issue Resolution:

- ➢ When network issues arise, having detailed documentation allows administrators to quickly identify and address the root cause. Whether it’s a connectivity issue, a misconfiguration, or a device failure, network documentation provides a reference to configurations and network design, facilitating a faster resolution.

2.] Efficient Network Management:

- ➢ Well-documented networks make it easier to track and manage devices, configurations, and services. This helps administrators understand the network's current state, identify changes over time, and make informed decisions about upgrades or optimizations.

3.] Scalability and Growth:

- ➢ As the network expands, documentation is crucial for ensuring the growth process is smooth and does not disrupt the existing infrastructure. Detailed records of IP addressing, subnets, and device configurations ensure new devices or technologies are added efficiently and without conflict.

4.]Security and Compliance:

- ➢ Network documentation supports security efforts by providing records of access controls, firewall settings, and security policies. It is also essential for meeting compliance requirements (e.g., HIPAA, PCI-DSS), as it helps demonstrate how the network is managed and monitored in line with security best practices and regulations.

5.] Disaster Recovery:

- ➢ In the event of a network failure or natural disaster, documentation enables administrators to restore the network configuration and services. Backup configurations, network diagrams, and device inventories ensure that the recovery process is fast and accurate.

6.]Knowledge Transfer and Staff Onboarding:

➢ As new personnel join the IT team or there are staff transitions, network documentation serves as a valuable knowledge resource. It ensures that new administrators understand the network setup, reducing the time it takes for them to become effective in their roles.

7.]Change Management and Auditing:

➢ Network documentation tracks the changes made to the infrastructure, which helps ensure that modifications are implemented properly and in accordance with best practices. It also provides an audit trail, which is essential for diagnosing issues caused by recent changes and for conducting audits.

❖ Examples of Information That Should Be Documented:

1.] Network Topology Diagram.

➔ **Description**: A visual representation of how network devices (routers, switches, firewalls, etc.) are interconnected. It shows the physical and logical layout of the network.

➔ **Example**: A diagram that shows the connection between core routers, distribution switches, access switches, servers, and external connections like the internet or VPN.

2.] IP Addressing Scheme.

➔ **Description**: A record of IP address allocations, including private IP ranges, public IP addresses, subnet masks, and reserved addresses for network devices.

➔ **Example**:

- **192.168.1.0/24** for internal devices
- **10.0.0.0/24** for servers
- **172.16.0.0/24** for guest Wi-Fi

3.] Device Inventory.

- ➔ **Description**: A catalog of all network devices, including routers, switches, firewalls, and access points. The inventory should include device make, model, serial number, firmware version, and location.
- ➔ **Example**: A table listing devices like:
    - **Device Name**: Core Router 1
    - **Model**: Cisco 3900 Series
    - **Serial Number**: 12345ABC
    - **Firmware Version**: IOS 15.2(4)
    - **Location**: Data Center A

4.] Network Configuration Files.

- ➔ **Description**: Configuration details for network devices such as routers, switches, firewalls, and DHCP servers. This includes settings like IP addresses, routing protocols, access control lists (ACLs), and VLAN configurations.
- ➔ **Example**: Configuration files for a router showing routing protocol settings (e.g., OSPF or BGP), interface configurations, and firewall rules.

5.] Security Policies and Access Control.

- ➔ **Description**: Documentation of security measures, such as firewalls, VPN settings, intrusion detection/prevention systems, and ACLs, that protect the network.
- ➔ **Example**: Documentation detailing:
    - Firewall rules specifying allowed ports and services
    - VPN access policies and configurations
    - Access control lists (ACLs) that define what traffic is allowed or blocked

6.] Backup and Recovery Procedures.

- ➔ **Description**: A record of backup schedules, locations, and procedures for restoring network configurations and data.
- ➔ **Example**: A document specifying backup procedures:
    - Backup frequency: Daily at 2:00 AM
    - Storage: Offsite cloud backup for configurations
    - Recovery process: Step-by-step guide to restoring router configurations

7.] Network Services Documentation.

- ➔ **Description**: Details of essential network services such as DNS, DHCP, NTP, and authentication servers, including their configurations and IP addresses.
- ➔ **Example**: A document listing the configurations of the DHCP server:
  - IP Range: 192.168.1.100 to 192.168.1.200
  - DNS Server IP: 8.8.8.8
  - Lease time: 24 hours

8.] Change Management Logs.

- ➔ **Description**: A log of all changes made to the network infrastructure, including hardware updates, configuration changes, and software upgrades.
- ➔ **Example**: A log entry:
  - **Change Description**: Upgraded firewall firmware to v2.3
  - **Date**: January 1, 2025
  - **Reason**: Security patch update
  - **Administrator**: Jane Doe

9.] Service Level Agreements (SLAs).

- ➔ **Description**: Agreements with service providers (e.g., ISPs or cloud services) that define the level of service, uptime guarantees, and support response times.
- ➔ **Example**: An SLA document outlining:
  - 99.9% uptime guarantee for internet connectivity
  - 4-hour response time for critical support issues

10.] Performance Monitoring and Metrics.

- ➔ **Description**: Metrics and monitoring data on network performance, such as bandwidth utilization, latency, packet loss, and uptime..
- ➔ **Example**: A performance report detailing:
  - Average network throughput: 80% of total capacity
  - Latency: 15ms
  - Packet loss: 0.2%