**Name : Chhaya Deep M.**

**Assignment: 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 primary function of a router is to forward data packets between different networks

**2. 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 Routing data**

**d) packets between network segments  
Ans.** c) Converting domain names to IP addresses Routing DNS is responsible for translating domain names into IP addresses allows computers and devices to locate each other on the network.

**3. 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 In a star topology all devices are connected to a central hub or switch.

**4. 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 provide secure methods for accessing and transferring files over a network.

**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**

**Ans.** True because firewall can be either hardware or software-based and is designed to monitor and control network traffic based on predetermined security rules to protect a network.

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

**Ans**. False because DHCP automatically assigns dynamic IP addresses to network devices, not static ones IP addresses can change over time, while static IP addresses are manually assigned and remain constant.

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

**Ans.** True VLANs enable network segmentation by dividing a single physical network into multiple logical networks.

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

**Ans.**

|  |  |
| --- | --- |
| **Hub**   1. Hub is classified as Layer 1 devices per the OSI model 2. Hub are do not recognized MAC address 3. Hub is cheap device 4. Hub are broadcast devices 5. Hub is slower device | **Switch**   1. Switch operate at layer 2 device per the OSI model 2. Switch device is recognized MAC address 3. Switch is expensive device to more than Hub 4. Switch is unicast device 5. Switch is fast device to more than Hub |

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

**Ans.**

1. **Identify the Problem:** Determine the specific issue, such as no internet access, slow connection, or inability to connect to a particular network. Gather information from users or error messages.
2. **Check Physical Connections:** Ensure all cables, devices, and network hardware (like routers and switches) are properly connected and powered on. Look for loose connections, damaged cables, or faulty devices.
3. **Verify Network Configuration:** Check the network settings on affected devices, such as IP addresses, subnet masks, gateways, and DNS settings. Make sure they are correctly configured, and consider resetting or renewing the IP address using DHCP.
4. **Test Connectivity:** Use tools like ping and trace (or traceroute) to test connectivity to local devices, gateways, and external servers. This helps identify whether the issue is local or on a wider network.
5. **Examine Network Devices:** Check the status of routers, switches, firewalls, and other network devices for errors, misconfigurations, or failures. Review their logs for any suspicious activity or errors.
6. **Check for Software Issues:** Verify that there are no software conflicts, outdated drivers, or firewall settings on the devices that could be blocking network traffic. Consider restarting devices to reset connections.
7. **Test with Other Devices:** Determine if the problem is specific to one device or affects multiple devices. If multiple devices are affected, the issue is likely with the network infrastructure.
8. **Check for External Factors:** Investigate if the issue could be related to external factors, like ISP outages or network maintenance. Contact the ISP if necessary.
9. **Apply and Test Fixes:** Implement solutions based on findings (e.g., replacing cables, reconfiguring settings, restarting devices) and test to see if the issue is resolved.

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

**Ans.**

**Step 1: Access the Router's Admin Interface**

**Connect to the Router**: Use a computer or smartphone connected to the router either wired or wirelessly.

**Open a Web Browser:** Enter the router's IP address in the address bar 192.168.1.1 or 192.168.0.1 You can check the router’s label or manual for the default IP address.

**Log In to the Admin Interface:** Enter the router's admin username and password. If you haven't changed these from the default, check the router’s manual or label.

**Step 2: Change the Default Administrator Credentials**

**Find the Administration or Security Section:** Look for an option like "Administration," "System," or "Management."

**Change the Default Username and Password:** Replace the default admin credentials with a strong, unique password to prevent unauthorized access.

**Step 3: Enable WPA3 or WPA2 Security for Wi-Fi**

**Go to the Wireless Security Settings:** Look for "Wireless" or "Wi-Fi Settings" in the router's interface.

**Select the Security Mode:** Choose WPA3 if available or WPA2-PSK as the security protocol. Avoid using older and less secure options like WEP or WPA.

**Set a Strong Password:** Create a strong Wi-Fi password at least 12 characters, including letters, numbers, and symbols.

**Step 4: Disable WPS**

**Locate WPS Settings:** Find the WPS option, usually under the Wireless or Advanced settings.

**Disable WPS:** Turn off WPS to prevent security risks associated with this feature.

**Step 5: Set Up a Guest Network**

**Find the Guest Network Settings:** Look for a section labeled Guest Network or Guest Wi-Fi.

**Enable the Guest Network:** Turn on the guest network and set a separate password. This keeps guests on a different network segment from your main devices, reducing security risks**.**

**Set Access Restrictions:** Limit the guest network's access to your local network and critical devices.

**Step 6: Disable Remote Management**

**Locate Remote Management Settings**: Usually under the Administration or Advanced section.

**Turn Off Remote Management:** This prevents unauthorized access to the router's settings from outside your local network.

**Step 7: Enable Router Firewall**

**Find the Firewall Settings:** Typically located under Security or Advanced settings.

**Turn On the Firewall:** Ensure the firewall is enabled to help block malicious traffic and unauthorized access attempts.

**Step 8: Update the Router's Firmware**

**Check for Firmware Updates:** Find the Firmware Update or Router Update section in the admin interface.

**Update to the Latest Firmware:** Download and install any available updates to patch security vulnerabilities.

**Step 9: Save and Reboot the Router**

**Save Settings:** Click Apply or Save to ensure all changes are updated.

**Reboot the Router:** Restart the router to apply all settings and changes effectively.

**Step 10: Regularly Monitor and Review Security**

**Regularly Check the Router's Settings**: Monitor the router's logs and settings periodically for any suspicious activity.

**Update Passwords and Firmware**: Regularly update your passwords and check for firmware updates to keep the router secure.

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

**Ans.**

**Importance of Network Documentation**

Network documentation is a critical component of managing and maintaining a network infrastructure. It involves creating a detailed record of the network’s design, configuration, and components. Proper documentation helps ensure that a network runs smoothly, can be effectively managed, and is resilient to issues such as downtime, security breaches, and network failures. Here are some reasons why network documentation is important:

1. **Improved Troubleshooting and Problem Resolution:** When network issues arise, well-maintained documentation helps IT professionals quickly identify and resolve problems. It provides a comprehensive view of the network layout, devices, and configurations, reducing the time needed to diagnose and fix issues.
2. **Enhanced Network Security:** Documentation helps maintain security by detailing the configuration of firewalls, access controls, and other security measures. It ensures that all network components adhere to security policies, and helps identify potential vulnerabilities or unauthorized changes.
3. **Streamlined Network Management and Maintenance:** A documented network is easier to manage. It helps IT teams plan and implement changes or upgrades without disrupting operations, as they can clearly understand the existing configuration and dependencies.
4. **Facilitates Knowledge Transfer and Training**: In organizations with multiple IT staff or turnover, documentation ensures that new or less-experienced staff can understand and manage the network effectively. It serves as a guide to help them become familiar with the network's layout, policies, and procedures.
5. **Supports Compliance Requirements:** Many industries are subject to regulatory compliance requirements, such as GDPR, HIPAA, or PCI-DSS, which mandate that organizations maintain proper documentation of their IT and network infrastructure. Proper documentation ensures compliance with these regulations and can help avoid penalties or legal issues.
6. **Improves Planning and Capacity Management:** Network documentation provides a clear picture of current capacity and usage, allowing for better planning for future growth. It enables IT teams to anticipate hardware and software needs, reducing the risk of overloading network resources or experiencing unexpected failures.
7. **Facilitates Disaster Recovery and Business Continuity:** In the event of a disaster or major network outage, having detailed documentation is crucial for restoring services quickly and effectively. It ensures that network administrators know what components are involved, how they are configured, and what steps are needed to recover.

**Information That Should Be Documented**

**Network Topology Diagrams:**

Visual representations of the network layout, including all devices, connections, and their relationships. This should cover both physical topology cabling, device locations and logical topology.

**Inventory of Network Devices:**

A list of all hardware components, including routers, switches, firewalls, servers, access points, and other devices. Each entry should include details such as device names, model numbers,serial numbers, firmware versions, IP addresses, and physical locations.

**Configuration Settings:**

Detailed records of the configuration settings for all network devices. This should include information like IP addressing schemes, VLAN configurations, routing tables, access control lists, firewall rules, and wireless network settings.

**Network Policies and Procedures:**

Documentation of network policies, such as acceptable use policies, security policies, and backup procedures. It should also include any procedures for network management tasks like routine maintenance, monitoring, and software updates.

**Access Controls and Permissions:**

Details of user access controls, including who has access to which parts of the network, how authentication is managed, and what permissions are granted to different user groups. This helps maintain security and track access rights.

**IP Address Management:**

Documentation of the IP address allocation and management plan, including dynamic and static IP addresses, DHCP scope, subnetting, and any reserved IP addresses. This ensures there is no conflict and helps in network planning and expansion.

**Service and Application Information:**

A list of key services and applications running on the network, such as web servers, mail servers, databases, and domain controllers. This should include their configurations,dependencies, and any relevant credentials or access information.

**Network Performance and Monitoring Logs:**

Records of network performance data, monitoring logs, and historical data on network traffic, error rates, and uptime. This helps identify trends, potential issues, and areas for improvement.