**ASSIGNMENT – 3:**

**Understanding and Maintenance Of Networks**

**SECTION 1: MULTIPLE CHOICE**

**1. What is the primary function of a router in a computer network?**

1. **Assigning IP addresses to devices**
2. **Providing wireless connectivity to devices**
3. **Forwarding data packets between networks**
4. **Managing user authentication and access control**

**Answer: (c)** Forwarding data packets between networks

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

1. **Encrypting data transmissions for security**
2. **Assigning IP addresses to devices dynamically**
3. **Converting domain names to IP addresses**
4. **Routing data packets between network segments**

**Answer: (c)** Converting domain names to IP addresses

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

1. **Bus**
2. **Ring**
3. **Mesh**

**Answer: (a)** Star

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

1. **FTP**
2. **SMTP**
3. **POP3**

**Answer: (b)** FTP

**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.**

**Answer:** True

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

**Answer:** False

1. **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

1. **Explain the difference between a Hub and a Switch in a computer network.**
   * **Answer:**

|  |  |
| --- | --- |
| **HUB** | **SWITCH** |
| * Hub is Broadcast Device. * Hub operates at physical layer (Layer 1) of OSI model. * Hub works in half duplex. * Hub does not store any address. | * Switch is Multicast   Device.   * Switch operates at data link layer (Layer 2) of OSI model. * Switch works in full duplex. * Switch store MAC address |

1. **Describe the process of troubleshooting network connectivity issues.**
   * **Answer:**
     + Identify the issue: Observe symptoms, gather information from users, and determine the affected devices. oCheck physical connections: Inspect cables, ports, and devices for damage or loose connections.
     + Basic network commands: Use "ping" to test connectivity, "tracert" to track packet path, and "ipconfig" to view network configuration. oDNS check: Verify if the device can resolve domain names to IP addresses.
     + Device restart: Reboot affected devices like routers and computers.
     + Advanced diagnostics: Utilize tools like "netstat" to analyze network connections and "ifconfig" to check network interface details. oContact ISP: If the issue is beyond local network, contact your internet service provider.

# SECTION 4: PRACTICAL APPLICATION

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

 **Answer: 1**. **Access Your Router's Settings**

* + Open a web browser and type your router's IP address into the address bar. Common addresses are 192.168.1.1 or 192.168.0.1.
  + Enter the username and password. If you haven’t changed them, they are often "admin" and "password".

1. **Change Default Login Credentials**:
   * Navigate to the administration or security settings.
   * Change the default login username and password to something strong and unique.
2. **Update Router Firmware**:
   * Look for a firmware update option in your router’s settings. Often found under “Administration” or “Advanced” sections.
   * Follow the instructions to update the firmware.
3. **Enable WPA3 or WPA2 Encryption**:
   * Go to the wireless security settings.
   * Select WPA3 if available. If not, choose WPA2-PSK (AES) for the encryption method. Avoid using WEP as it’s outdated.
4. **Disable WPS**:
   * Find the WPS settings (usually under wireless settings).
   * Disable WPS to prevent security risks.
5. **Set Up a Guest Network**:
   * Locate the guest network settings.
   * Enable the guest network and set a unique name and password different from your main network.
6. **Disable Remote Management**:
   * Look for remote management settings (under “Administration” or “Advanced”).
   * Disable remote management to prevent access from outside your network.
7. **Change the SSID**:
   * In the wireless settings, change the default SSID (network name) to something unique.
   * Avoid using any personal information in the name.
8. **Enable Router Firewall**:
   * Ensure the router’s built-in firewall is enabled. This option is usually found under security settings.
9. **Limit DHCP Leases and Assign Static IPs**:

* Navigate to DHCP settings.
* Limit the number of IP addresses the DHCP server can assign.
* Assign static IPs to your trusted devices.

1. **Monitor Connected Devices**:

* Regularly check the list of devices connected to your network.
* If you see any unfamiliar devices, disconnect them.

# SECTION 5: ESSAY

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

 **Answer:**  **Troubleshooting**: Well-documented networks make it easier to identify and resolve issues quickly. You’ll know exactly what your network consists of and where potential problems might lie.

 **Security**: Documenting security configurations, access controls, and policies helps ensure that they are consistently applied and audited. It also helps identify any security gaps.

 **Maintenance and Upgrades**: With detailed documentation, upgrading network devices and making changes becomes more manageable. It ensures that you understand the current setup and can plan changes without causing disruptions.

 **Compliance**: Many industries require compliance with specific standards and regulations. Documentation helps demonstrate that your network adheres to these requirements.

 **Knowledge Transfer**: If someone new takes over network management, comprehensive documentation ensures a smooth transition without losing critical knowledge.

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

Network documentation is essential for maintaining a secure, efficient, and manageable network. It provides a clear and organized record of your network's components, configurations, and policies. Here’s why it’s important:

**Importance of Network Documentation**

1. **Troubleshooting**: Well-documented networks make it easier to identify and resolve issues quickly. You’ll know exactly what your network consists of and where potential problems might lie.
2. **Security**: Documenting security configurations, access controls, and policies helps ensure that they are consistently applied and audited. It also helps identify any security gaps.
3. **Maintenance and Upgrades**: With detailed documentation, upgrading network devices and making changes becomes more manageable. It ensures that you understand the current setup and can plan changes without causing disruptions.
4. **Compliance**: Many industries require compliance with specific standards and regulations. Documentation helps demonstrate that your network adheres to these requirements.
5. **Knowledge Transfer**: If someone new takes over network management, comprehensive documentation ensures a smooth transition without losing critical knowledge.

**Examples of Information to Document**

1. **Network Topology**:
   * Diagrams showing how devices are connected.
   * Details of network segments, subnets, and VLANs.
2. **Device Information**:
   * Hardware and software details of routers, switches, firewalls, etc.
   * IP addresses, MAC addresses, serial numbers, and model information.
3. **Configuration Details**:
   * Router and switch configurations.
   * Wireless network settings and security protocols.
   * Firewall rules and settings.
4. **Access and Authentication**:
   * User accounts and access levels.
   * Authentication methods (e.g., WPA2, WPA3, RADIUS, etc.).
   * Password policies and management.
5. **Security Policies**:
   * Details of implemented security measures (encryption, firewalls, intrusion detection systems).
   * Incident response plans and procedures.
   * Backup and disaster recovery plans.
6. **ISP Information**:
   * ISP contact details.
   * Service agreements and bandwidth specifications.
7. **Change Management Logs**:
   * Records of all changes made to the network.
   * Reason for changes, date and time, and person who made the change.