**Assignment module 3 : Understanding and Maintenance of Network**

**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

***Answer: c) Forwarding data packets between 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

d) 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 b) Bus c) Ring d) Mesh

***Answer: a) Star***

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

a) HTTP b) FTP c) SMTP d) POP3

***Answer: b) FTP***

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.

| **Feature** | **Hub** | **Switch** |
| --- | --- | --- |

|  |  |  |
| --- | --- | --- |
| **Function** | Broadcasts data to all devices | Sends data only to the intended device |

|  |  |  |
| --- | --- | --- |
| **Network Layer** | Operates at Layer 1 (Physical) | Operates at Layer 2 (Data Link) or Layer 3 (Network) |

|  |  |  |
| --- | --- | --- |
| **Data Handling** | Sends data to every device on the network | Directs data to specific devices |

|  |  |  |
| --- | --- | --- |
| **Efficiency** | Less efficient, causes network congestion | More efficient, reduces traffic |

|  |  |  |
| --- | --- | --- |
| **Security** | Lower security, all devices see all data | Higher security, data sent only to intended device |

|  |  |  |
| --- | --- | --- |
| **Cost** | Typically cheaper | Slightly more expensive |

9. Describe the process of troubleshooting network connectivity issues.

Here’s Troubleshooting network connectivity issues:

1. **Check Physical Connections**: Ensure cables and devices are properly connected.
2. **Verify Device Status**: Make sure the network adapter is enabled.
3. **Check Network Configuration**: Confirm the device has a valid IP address and is connected to the correct network.
4. **Test Network Access**: Use the ping command to check connectivity.
5. **Restart Devices**: Reboot the router, modem, and computer.
6. **Check for IP Conflicts**: Ensure no two devices share the same IP address.
7. **Disable Firewall/Antivirus**: Temporarily disable them to rule out interference.
8. **Update Drivers/Firmware**: Ensure network drivers and router firmware are up to date.
9. **Check ISP Status**: Verify if there’s an ISP outage.
10. **Contact Support**: If unresolved, seek help from your ISP or network admin.

**Section 4: Practical Application**

1. Demonstrate how to configure a wireless router's security settings to enhance network security.
2. **Log into the Router’s Admin Panel**
   * Open a web browser and enter the router’s IP address.
   * Enter the admin username and password (often found on the router or in the manual).
3. **Change the Default Admin Credentials**
   * Go to the **Administration** or **System** settings and change the default admin username and password to something secure. This prevents unauthorized access to the router.
4. **Enable WPA3 or WPA2 Encryption**
   * Go to the **Wireless Security** section.
   * Set the security mode to **WPA3** (if available) or **WPA2-PSK** (stronger than WEP).
   * Create a strong Wi-Fi password (mix of letters, numbers, and symbols).
5. **Disable WPS (Wi-Fi Protected Setup)**
   * Turn off **WPS** in the wireless settings to prevent an easy backdoor for unauthorized users to access your network.
6. **Enable a Guest Network** (Optional)
   * If you need to allow guest access, create a separate **Guest Network** with a different password. Limit the guest network’s access to your main network resources.
7. **Disable SSID Broadcast (Optional)**
   * To hide your network name, disable **SSID broadcast**. However, this step is optional as it’s not a strong security measure by itself.
8. **Enable MAC Address Filtering** (Optional)
   * Add your devices' **MAC addresses** to the router’s whitelist. This allows only specified devices to connect to your network.
9. **Update Router Firmware**
   * Go to the **Firmware Update** section and check for updates. Install any new firmware to protect against vulnerabilities.
10. **Disable Remote Management**
    * Disable **Remote Management** in the settings to prevent access to your router from outside the local network.
11. **Save Changes and Reboot the Router**

* After making all necessary changes, save the settings and reboot the router.

**Section 5: Essay**

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

Network documentation is important for managing and maintaining a network. It helps keep track of all the devices, settings, and connections in the network, making it easier to fix problems, upgrade the network, and ensure smooth operations.

**Why Network Documentation is Important:**

1. **Easier Troubleshooting**: Helps quickly find and fix network issues.
2. **Better Management**: Keeps track of all devices and settings.
3. **Smooth Upgrades**: Makes it easier to plan changes or add new devices.
4. **Team Continuity**: Ensures new team members understand the network.
5. **Improves Security**: Keeps track of security settings to protect the network.

**What to Document:**

1. **Network Diagram**: A map showing how all devices are connected.
2. **IP Addresses**: A list of devices and their assigned IP addresses.
3. **Device Information**: Details about routers, switches, and other equipment.
4. **Settings**: Router, switch, and firewall configurations.
5. **Cables**: Information on where cables are connected.
6. **User Access**: Records of who can access what in the network.
7. **Security Policies**: Information on firewalls, encryption, and VPNs.

In short, network documentation makes it easier to manage and protect the network.