**Section 4: Practical Application**

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

**Ans:**

**How to Configure a Wireless Router’s Security Settings**

1. **Access the Router’s Admin Interface:**
   * Connect your computer to the router (via Wi-Fi or Ethernet).
   * Open a web browser and enter the router’s IP address (usually something like 192.168.1.1 or 192.168.0.1).
   * Log in with the router’s admin username and password.
2. **Change the Default Admin Password:**
   * Navigate to the **Administration** or **System** settings.
   * Change the default password to a strong, unique password to prevent unauthorized access.
3. **Set a Strong Wi-Fi Password (WPA3 or WPA2):**
   * Go to the **Wireless** or **Wi-Fi Security** settings.
   * Select **WPA3** (if available) or **WPA2-PSK (AES)** encryption for the wireless network. Avoid WEP and WPA as they are outdated and insecure.
   * Create a strong Wi-Fi password (a mix of letters, numbers, and symbols).
4. **Change the Default SSID (Network Name):**
   * Change the default network name (SSID) to something unique but do **not** include personal information. This helps avoid targeting by attackers.
5. **Disable WPS (Wi-Fi Protected Setup):**
   * WPS can be vulnerable to attacks, so it’s safer to disable it in the router settings.
6. **Enable the Router Firewall:**
   * Ensure the built-in firewall is enabled to block unwanted traffic.
7. **Update Router Firmware:**
   * Check for and install any available firmware updates to patch security vulnerabilities.
8. **Optional - Enable MAC Address Filtering:**
   * You can restrict which devices can connect by specifying allowed MAC addresses, though this can be bypassed by skilled attackers.

Section 5: Essay

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

**Ans:**

**The Importance of Network Documentation**

Network documentation is a critical component of effective network management and maintenance. It refers to the systematic recording of detailed information about a network’s design, configuration, hardware, software, policies, and procedures. Proper documentation ensures that network administrators can efficiently manage, troubleshoot, and scale the network, reducing downtime and improving security.

One of the key benefits of network documentation is simplified troubleshooting. When issues arise, having access to up-to-date records about IP addressing schemes, device configurations, and network topology allows technicians to quickly pinpoint problems and implement solutions. Without proper documentation, troubleshooting becomes time-consuming and error-prone.

Network security also benefits significantly from thorough documentation. Knowing exactly what devices are connected, their configurations, and access policies helps administrators identify unauthorized devices or vulnerabilities. It also supports compliance with industry regulations that often require detailed network records.

Another important aspect is network scalability and upgrades. When expanding a network or integrating new technologies, documentation provides a clear blueprint of existing infrastructure, helping to plan changes without disrupting operations.

**Examples of Information That Should Be Documented:**

* **Network Topology:** Diagrams showing how devices are connected physically and logically.
* **IP Addressing:** Details of static and dynamic IP addresses assigned to devices and servers.
* **Device Inventory:** Lists of all network devices (routers, switches, firewalls, servers), including make, model, serial numbers, and locations**.**
* **Configuration Settings**: Backup copies of router, switch, firewall configurations, and wireless settings.
* **Access Controls:** User accounts, passwords (securely stored), permissions, and authentication methods.
* **Policies and Procedures**: Network usage policies, security protocols, and troubleshooting guidelines.
* **Vendor and Support Information**: Contact details for hardware/software vendors and support contracts.
* **Change Logs**: Records of changes made to the network configuration or hardware.

In summary, network documentation is essential for maintaining a reliable, secure, and scalable network. It acts as a reference guide that saves time, prevents mistakes, and ensures continuity, especially during staff changes or emergencies.