Ques 3:

A white paper with black text

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

Ques 4: A screenshot of a computer code

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

To mitigate ARP spoofing attacks, it is important to use various security ways to protect the integrity of the ARP (Address Resolution Protocol) cache and network communication. One effective way is to use **Static ARP entries**, where MAC addresses are manually mapped to IP addresses in network devices, making it impossible for attackers to spoof addresses. Additionally, enabling **Dynamic ARP Inspection (DAI)** on switches can prevent malicious ARP packets from being accepted. Another approach is to implement **port security** on switches, limiting the number of MAC addresses allowed per port, which prevents rogue devices from sending ARP replies. Finally, utilizing **Encrypted Communication** such as HTTPS, SSH, or VPNs can ensure that even if ARP spoofing occurs, attackers cannot intercept or manipulate the sensitive data being transmitte