## **Practice Q&A (Tutorial-Based)**

1. **Can Alice securely use SSH with Bob if she doesn’t know him?**
   * No, because SSH doesn’t use certificates; she must securely acquire Bob’s public key first.
2. **Bob's port 80 is blocked. How can he access his home page via SSH?**
   * Port forwarding: SSH tunnel maps home port to internal port 80.
3. **How is pre\_master\_secret sent in SSL with RSA?**
   * Client encrypts it with server’s public key from the cert.
4. **Advantage of Ephemeral Diffie-Hellman over RSA in SSL?**
   * Provides forward secrecy.
5. **Why doesn’t a server’s cert alone authenticate it?**
   * Cert is public; only proves ID when server signs handshake using private key.
6. **Is SSL or IPSec enough for e-commerce?**
   * SSL encrypts traffic but lacks application-layer signing; not enough for complex payments.
7. **Do all apps running between A and B over TLS hide from hackers?**
   * No, only those using TLS specifically.

## **4. Active Recall Exercises**

### **MCQs**

1. What does ARP spoofing exploit?
   * a) Static routing
   * b) IP fragmentation
   * c) MAC-IP mapping vulnerabilities ✅
   * d) TCP SYN floods
2. Which Wi-Fi protocol introduced AES encryption?
   * a) WEP
   * b) WPA
   * c) WPA2 ✅
   * d) WPA3

### **Fill in the Blanks**

1. WEP uses the \_\_\_\_\_\_\_\_\_\_ stream cipher.
   * **RC4**
2. The protocol used to discover neighboring devices on LAN is \_\_\_\_\_\_\_\_\_\_.
   * **LLDP**
3. In 802.1X, the access point acts as the \_\_\_\_\_\_\_\_\_\_.
   * **Authenticator**

### **Short Answers**

1. What is the role of EAP in 802.1X?
   * Provides extensible methods for client authentication and key generation.
2. How does WPA3 ensure forward secrecy?
   * It uses ephemeral Diffie-Hellman so session keys are unrelated to long-term keys.
3. Why are wireless networks more vulnerable than wired?
   * Lack of physical barriers and data broadcast make interception easier.