5.2.4 Spoofing Facts

Spoofing is used to hide the true source of packets or redirect traffic to another location. Spoofing attacks:

- Use modified source and/or destination addresses in packets
- Can include site spoofing, which tricks users into revealing information

Common methods of spoofing are listed in the table below:

Attack	Description
IP Spoofing	IP spoofing changes the IP address information within a packet. It can be used to: ▪ Hide the origin of the attack by spoofing the source address. ▪ Amplify attacks by sending a message to a broadcast address and then redirecting responses to a victim who is overwhelmed with responses.
MAC Spoofing	MAC spoofing is when an attacking device spoofs the MAC address of a valid host currently in the MAC address table of the switch. The switch then forwards frames destined for that valid host to the attacking device. This can be used to bypass: ▪ A wireless access point with MAC filtering on a wireless network ▪ Router access control lists (ACLs) ▪ 802.1x port-based security
ARP Spoofing	ARP spoofing (also known as ARP *poisoning*) uses spoofed ARP messages to associate a different MAC address with an IP address. ARP spoofing can be used to perform a man-in-the-middle attack as follows: 1. When an ARP request is sent by a client for the MAC address of a device, such as the default gateway router, the attacker's system responds to the ARP request with the MAC address of the attacker's system. 2. The client receives the spoofed ARP response and uses that MAC address when communicating with the destination host. For example, packets sent to the default gateway are sent instead to the attacker. 3. The attacker receives all traffic sent to the destination host. The attacker can then forward these packets on to the correct destination using its own MAC address as the source address. ARP spoofing can also be used to perform Denial of Service (DoS) attacks by redirecting communications to fake or non-existent MAC addresses.

Countermeasures for preventing spoofing are as follows:

- Implement firewall and router filters to prevent spoofed packets from crossing into or out of your private secured network. Filters will drop any packet suspected of being spoofed.
- Use certificates to prove identity.
- Use reverse DNS lookup to verify the source email address.
- Use encrypted communication protocols, such as IPsec.
- Use ingress and egress filters to examine packets and identify spoofed packets. Ingress filters examine packets coming into the network, while egress filters examine packets going out of the network. Any packet suspected of being spoofed on its way into or out of your network will be dropped.