The MAC Layer and Attacks

N2.1. What is the promiscuous mode for?

N2.2. How can MAC addresses be used for tracking users?

N2.3. Why is the loopback interface called "loopback"?

N2.4. What is the similarity and difference between the loopback and dummy interfaces?

N2.5. Why do we need the ARP protocol?

N2.6. A computer with the IP address `10.8.8.5/24` tries to ping `10.8.8.8`. An ARP request will be sent out first. What are the values of the following fields in the Ethernet header: (1) destination MAC and (2) source MAC?

N2.7. A computer with the IP address `10.8.8.5/24` tries to ping `10.8.8.8`. An ARP request will be sent out first. What are the values of the following fields in the ARP message: (1) sender's MAC, (2) sender's IP, (3) target MAC, and (4) target IP?

N2.8. A computer is on the `10.8.8.0/24` network with the default router set to `10.8.8.1`. It tries to ping `93.184.216.34`. Before the ping packet is sent out, an ARP request will be sent out. What is the value of the target IP address field of the ARP message?

N2.9. A computer with the IP address `10.8.8.5/24` tries to ping `10.8.8.100`, which does not exist on the LAN. If another machine on the same LAN tries to sniff the ping packet, will it be able to get the ping packet?

N2.10. A computer with the IP address `10.8.8.5/24` tries to ping `1.2.3.4`, which does not exist on the Internet. If another machine on the `10.8.8.0/24` network tries to sniff the ping packet, will it be able to get the ping packet?

N2.11. Please write a code snippet to spoof an ARP request message, with the goal of poisoning the ARP cache of the machine `10.8.8.5`. Your attack machine is on the same LAN.

N2.12. Please write a code snippet to spoof an ARP reply message, with the goal of poisoning the ARP cache of the machine `10.8.8.5`. Your attack machine is on the same LAN.

N2.13. Please write a code snippet to spoof an ARP gratuitous message, with the goal of poisoning the ARP cache of the machine `10.8.8.5`. Your attack machine is on the same LAN.

N2.14. Can we launch an ARP cache poisoning attack from a remote computer? Please explain.

N2.15. A news report says that company XYZ's network was attacked by outsiders, who apparently sent a lot of spoofed ARP requests/responses from remote machines to the company's network, trying to launch ARP cache poisoning attacks. Please comment on whether this is a fake news or not.

N2.16. In an MITM attack, the attacker M tries to intercept the communication between A and B that are on the same LAN. Please describe what M needs to do, so it can modify the packets from A to B.

N2.17. In the MITM attack described in the book, the attacker M uses the ARP cache poisoning attack to redirect the A-to-B packets to M. (1) If the IP forwarding on the attacker machine M is turned off, what will happen to the packets? (2) If the IP forwarding on M is turned on, what will happen to the packets? (3) If the attacker wants to modify the packet, should the attacker turn on or off the IP forwarding.

N2.18. In the MITM attack described in the book, the attacker M uses the ARP cache poisoning attack to redirect the A-to-B packets to M. How does the attacker get this packet?

N2.19. In the MITM attack code, the attacker tries to modify the packets from A to B. After intercepting such a packet, the attacker makes a copy of the packet, and then does the following. Why does the attacker have to delete the IP and TCP checksums?

```
newpkt = IP(bytes(pkt[IP]))
del(newpkt.chksum)
del(newpkt[TCP].chksum)
```

N2.20. In the MITM attack described in the book, when the attack code sniffs the packet from A to B, it uses A's Ethernet address in the filter. Can we use A's IP address in the filter? Why or why not?

N2.21. Machines A, B, and M are on the same LAN, and their IP addresses and MAC addresses are listed below.

```
A's IP:  10.9.0.5
B's IP:  10.9.0.6
M's IP:  10.9.0.9

A's MAC address: aa:bb:cc:dd:ee:05
B's MAC address: aa:bb:cc:dd:ee:06
M's MAC address: aa:bb:cc:dd:ee:09
```

The attacker on M wants to use the ARP cache poisoning to launch the MITM (Man-In-The-Middle) attack against A and B, i.e., intercepting the communication between A and B. To achieve this goal, the attacker wants to use the following program to send spoofed ARP requests. Please complete the code.

```
# Constructing spoofed ARP request to Host A
ether1 = Ether(dst = _____________________________)
arp1 = ARP(op=1)
arp1.psrc  = ________________________   # An IP address
arp1.hwsrc = ________________________   # An Ethernet address
arp1.pdst  = ________________________   # An IP address
sendp(________________________)

# Constructing spoofed ARP request to Host B
ether2 = Ether(dst = _____________________________)
arp2 = ARP(op=1)
```

```
arp2.psrc  = _____________________
arp2.hwsrc = _____________________
arp2.pdst  = _____________________
sendp(_____________________)
```