In this second practical exercise, I will perform a man-in-the-middle (**MITM**) attack.

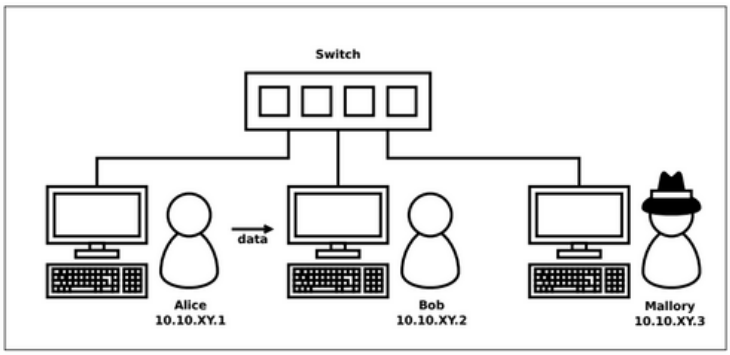


Figure 1: Sketch of the network scenario with ARP.

I will play **Mallory's role** in this experiment: Since I joined **Group 10**, I got permission to access **Mallory's PC (Log in Key: *msw0j0zvl6*)**.

I aim to establish myself as the man in the middle of the communication between Alice and Bob by applying an **ARP spoofing attack**.

After accessing **Mallory's PC**, I can see (***ifconfig -a***) a list of network interfaces available on Mallory's machine but I'm allowed to access the interface **eth10** only.

By Commanding on terminal: ***ifconfig eth10***, I can see Mallory's MAC Address:

c0:00:00:00:00:10

To check the **ARP table** at Mallory's PC of network interface eth10 , I command "***arp -i eth10***": Here I got the following IP addresses and MAC addresses. Now, I can distinguish which Hardware address is belong to Alice and Bob.

```
user10@mallory:~$ arp -i eth10
Address                  HWtype  HWaddress           Flags Mask
10.10.10.2               ether   b0:00:00:00:00:10   C
10.10.10.1               ether   a0:00:00:00:00:10   C
user10@mallory:~$
```

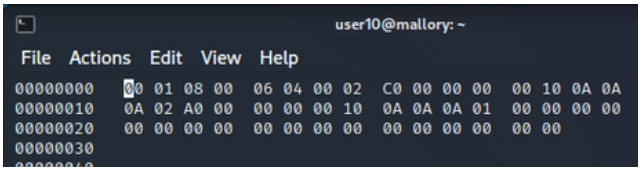
☞ At first, I **listened/analyzed network traffic** to the interface **eth10** by using the command: "***sudo tcpdump -i eth10 -Xn***"

I captured the same packet **repeatedly** from **Alice** (**ARP, Request who-has 10.10.10.2 tell 10.10.10.1**) where she asked for the MAC address to Bob.

```
user10@mallory:~$ sudo tcpdump -i eth10 -Xn
[sudo] password for user10:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth10, link-type EN10MB (Ethernet), capture size 262144 bytes
18:46:46.225554 ARP, Request who-has 10.10.10.2 tell 10.10.10.1, length 46
        0x0000:  0001 0800 0604 0001 a000 0000 0010 0a0a  ................
        0x0010:  0a01 0000 0000 0000 0a0a 0a02 0000 0000  ................
        0x0020:  0000 0000 0000 0000 0000 0000 0000       ..............
18:47:22.954302 ARP, Request who-has 10.10.10.2 tell 10.10.10.1, length 46
        0x0000:  0001 0800 0604 0001 a000 0000 0010 0a0a  ................
        0x0010:  0a01 0000 0000 0000 0a0a 0a02 0000 0000  ................
        0x0020:  0000 0000 0000 0000 0000 0000 0000       ..............
18:47:59.788819 ARP, Request who-has 10.10.10.2 tell 10.10.10.1, length 46
        0x0000:  0001 0800 0604 0001 a000 0000 0010 0a0a  ................
        0x0010:  0a01 0000 0000 0000 0a0a 0a02 0000 0000  ................
        0x0020:  0000 0000 0000 0000 0000 0000 0000       ..............
```

☞ In order to play the man-in-the-middle, I will send an ARP reply to Alice as Bob. I will use Bob's IP address but with Mallory's MAC Address so that Alice's ARP Cash will store Mallory's MAC address as Bob's MAC address along with Bob's IP Address.

For doing, that I will create a fake ARP reply hexfile (payload).



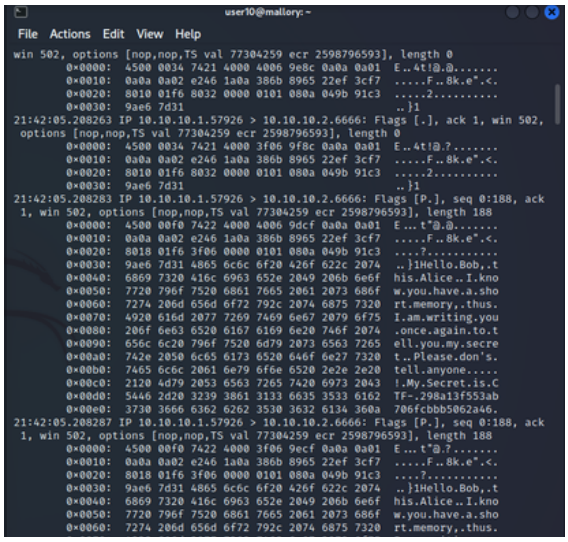
☞ The given **RAW_Packet.c** program will generate an ethernet frame of the form: dst addr | src addr | payloadproto | payload; and sends exactly one ethernet frame to the target.

☞ Sending the packet by using command: ***sudo raw_packet eth10 Alice's_MAC_Address 0x0806 payload_file_name***

*[Here **0x0806** as Payload protocol. Ethernet Frame Type- For an ARP request/reply, this field is 0x0806.]*

☞ Now by **listening to network traffic** to the interface **eth10** by using the command: "***sudo tcpdump -i eth10 -Xn***"
I captured the packet where **Alice** shares her **secret** to Bob.

And of course, this package is being redirected to Bob as Mallory's PC doesn't think the message is for her due to the IP Address 10.10.10.2. That's why it redirects to Bob.



Bonus Part

This time we assume Alice and Bob run an **intrusion detection system** capable to detect **modified ARP replies**,

I am not quite sure whether an **intrusion detection system** can detect **modified ARP requests or not.**
If not, then I can send a **modified ARP request** to Alice. Acting as Bob but using Mallory's MAC address.

I did send a modified ARP request to Alice and I got the same key from Alice but I do not know whether the intrusion detection system detect it or not.