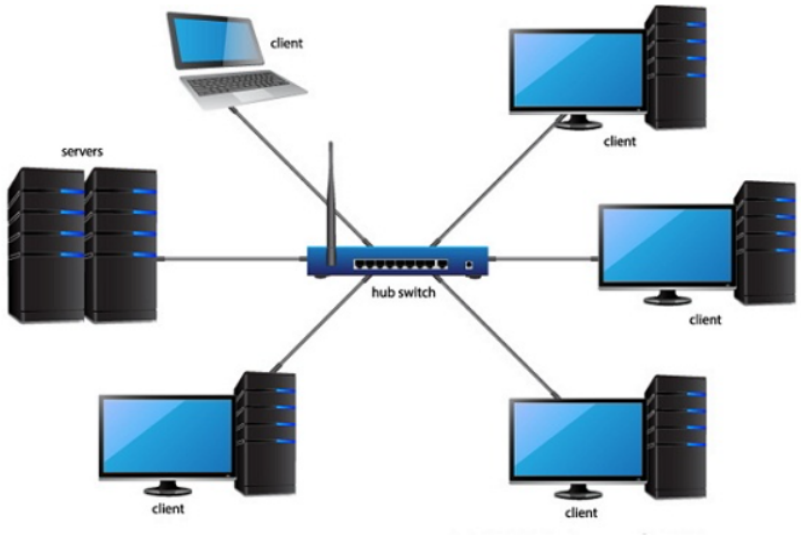
Vježba 1: ARP Spoofing

Općenito o LAN mreži i ARP cache-u

ARP Spoofing je oblik MITM (Man In The Middle) napada gdje napadač presluškuje komunikaciju između dva uređaja tj. riječ je o pasivnom napadu. Napad se događa na **LAN** mreži tj. lokalnoj računalnoj mreži gdje se komunikacija odvija **TCP/IP** protokolom.

Primjer **LAN** mreže:



ARP (Address Resolution Protocol) je komunikacijski protokol tj. procedura kojom se mapira lokalna mreža na način da se svakom uređaju s fiksnom **MAC** adresom pridodaje **IP** adresa.

Gateway je hardverski dio mreže koji omogućuje prijenos podataka između uređaja na mreži i on traži od ARP programa da pronađe **MAC** adresu koja pripada **IP** adresi.

Na **ARP cache** memoriji nalazi se lista svih **IP** adresa pridruženih **MAC** adresama.

Primjer **ARP cachea**:

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.8.129 --- 0x7
  Internet Address      Physical Address      Type
  192.168.8.1           a4-9b-4f-1b-d0-8f     dynamic
  192.168.8.105         70-54-b4-11-af-da     dynamic
  192.168.8.133         70-77-81-37-34-77     dynamic
  192.168.8.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.56.1 --- 0x14
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

ARP Spoofing

Pomoću programa Docker kreirali smo kontenjere koji se spajaju na LAN mrežu i pomoću čega ćemo izvršiti ARP Spoofing. **Kontenjeri** su softverske jedinice slične virtualnim mašinama, koje se lagano kreiraju i brišu, te ne zauzimaju puno memorije.

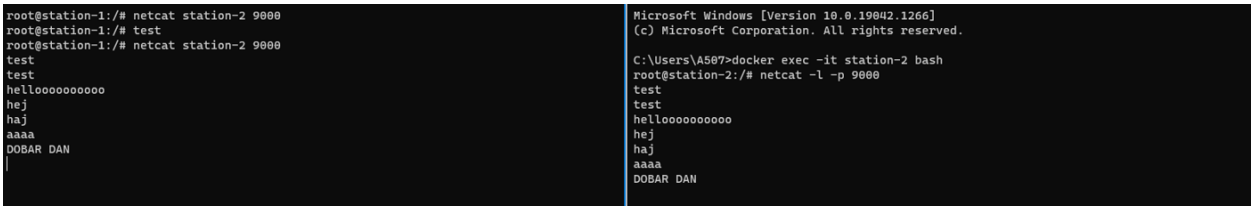
Kreiranje kontenjera:

```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/SRP/mkusacic/SRP-2021-22/arp-spoofing$ $ ./start.sh
$: command not found
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/SRP/mkusacic/SRP-2021-22/arp-spoofing$ ./start.sh
No running containers to stop.
Removing existing containers, networks, images ...
Error: No such container: station-1
Error: No such container: station-2
Error: No such container: evil-station
srp-lab
Untagged: srp/arp:latest
Deleted: sha256:3e40599dbd82e2cb9cf2c6893ef1d0f060574822581feaef808e25503aec6b83
Building a new image srp/arp ...
[+] Building 2.6s (7/7) FINISHED
 => [internal] load build definition from Dockerfile
 => => transferring dockerfile: 318B
 => [internal] load .dockerignore
 => => transferring context: 2B
```

Kreirali smo 3 kontenjera, tj. 3 uređaja na mreži:

- **station-1**
- **station-2**
- **evil-station**

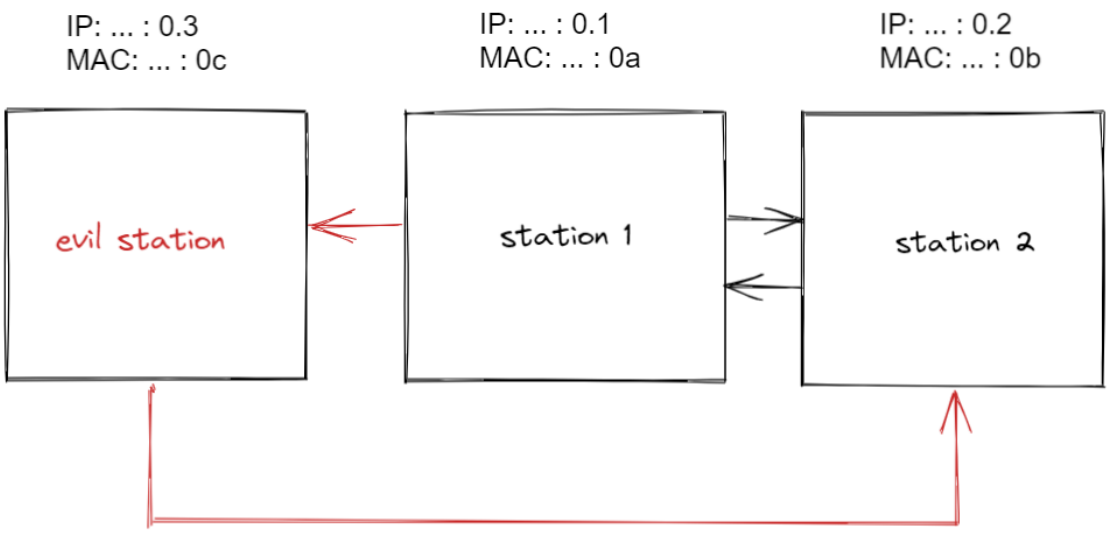
Komunikacija između **station-1** i **station-2**.



evil-station je napadač koji vrši ARP Spoofing.

Pokušava presluškivati komunikaciju između uređaja **station-1** i **station-2.**
To radi na način da se komunikacija izvršava preko njega tj. **evil-station** se predstavlja kao **station-2.**

Pri uspostavi komunikacije **station-1** i **station-2,** station-1 traži MAC adresu na IP adresi (0.2)
tj. traži **ARP request** pri kojem želi da IP adresa (0.2) pošalje svoju MAC adresu. Taj **ARP request** primaju svi uređaji na mreži. U tom trenutku evil-station (napadač) šalje **lažni ARP reply** pri kojem tvrdi da je MAC adresa uređaja s IP adresom (0.2) zapravo njegova MAC adresa (0c).
Dok s druge strane pri slanju podataka stationu-2 tvrdi da je IP adresa evil-stationa zapravo IP adresa stationa-1 (0.1).
Rezultatno, komunikacija između stationa-1 i stationa-2 se odvija preko evil-stationa.



Poruka uhvaćena ARP Spoofingom.

```
(c) Microsoft Corporation. All rights reserved.

C:\Users\A507>docker exec -it evil-station bash
root@evil-station:/# tcpdump -X host station-1 and not arp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:07:45.483708 IP station-1.srp-lab.32996 > station-2.srp-lab.9000: Flags [P.], seq
2236921316:2236921326, ack 1535444426, win 502, options [nop,nop,TS val 755786501 ecr
 3781670189], length 10
        0x0000:  4500 003e 11e1 4000 4006 d0af ac12 0002  E..>..@.@.......
        0x0010:  ac12 0003 80e4 2328 8554 b5e4 5b85 05ca  ......#(.T..[...
        0x0020:  8018 01f6 585a 0000 0101 080a 2d0c 6305  ....XZ......-.c.
        0x0030:  e167 b52d 444f 4241 5220 4441 4e0a       .g.-DOBAR.DAN.
15:07:45.483750 IP station-1.srp-lab.32996 > station-2.srp-lab.9000: Flags [P.], seq
0:10, ack 1, win 502, options [nop,nop,TS val 755786501 ecr 3781670189], length 10
        0x0000:  4500 003e 11e1 4000 3f06 d1af ac12 0002  E..>..@.?.......
        0x0010:  ac12 0003 80e4 2328 8554 b5e4 5b85 05ca  ......#(.T..[...
        0x0020:  8018 01f6 585a 0000 0101 080a 2d0c 6305  ....XZ......-.c.
        0x0030:  e167 b52d 444f 4241 5220 4441 4e0a       .g.-DOBAR.DAN.
```