Lab 1: Man-in-the-middle attack (ARP spoofing)

U prvoj laboratorijskoj vježbi izveli smo *man in the middle* (*MitM*) i *denial of service* (*DoS*) napade na računala koja su spojena na LAN. Napade smo izveli iskorištavanjem ranjivosti ARP protokola.

Korištenjem Dockera napravili smo 3 virtualizirana računala te smo ih povezali u virtualnu mrežu. To su:

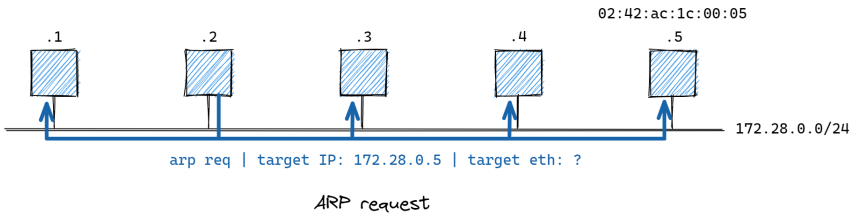
- `evil-station` - računalo kojim ćemo prisluškivati promet između klijenta i servera (napadač)
- `station-1` - računalo koje će se ponašati kao klijent (žrtva)
- `station-2` - računalo koje će se ponašati kao server (žrtva)

Spojili smo se u shell `station-1` računala i saznali njegovu IP i MAC adresu koristeći naredbu `ipconfig`. Nakon toga smo koristili naredbu `ping` da bismo saznali nalazi li se `station-2` računalo na istoj mreži. Kada smo to utvrdili uspostavili smo vezu klijent-server između ta dva računala koristeći naredbu `netcat`. Promet između ovih računala se može odvijati u oba smjera.

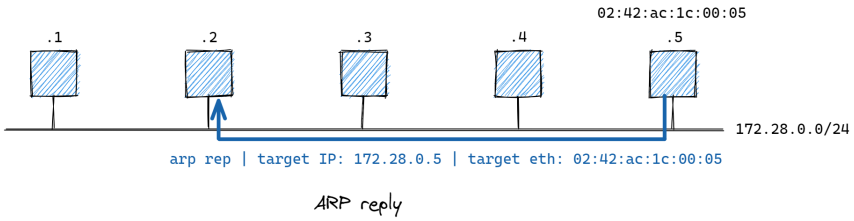
Kako bi presreli promet između `station-1` i `station-2` računala (žrtve) trebali smo ubaciti napadača (`evil-station`) u kanal kojim komuniciraju. To smo napravili na način da se `evil-station` predstavio `station-1` računalu kao `station-2`.

Za to smo koristili naredbe `arpspoof` i `tcpdump`. Sada je `station-1` slao promet `evil-stationu`, a on ga je dalje prosljeđivao `stationu 2`. Tako smo narušili i povjerljivost podataka (confidentiality). Time smo završili `MitM` napad.

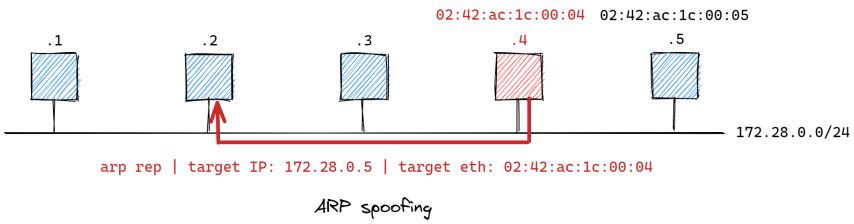
Na kraju smo prekinuli prosljeđivanje prometa `evil-stationa` prema `stationu-2` čime smo napravili *Dos* napad te smo na taj način narušili i dostupnost (avaliability). Time nismo onemogućili razmjenu podataka od `stationa-2` prema `stationu-1`.



ARP request



ARP reply



ARP spoofing