LV 2

OSNOVNA ANALIZA MREŽNOG PROMETA

MARKO SIKIRIĆ i NIKO SKELIN

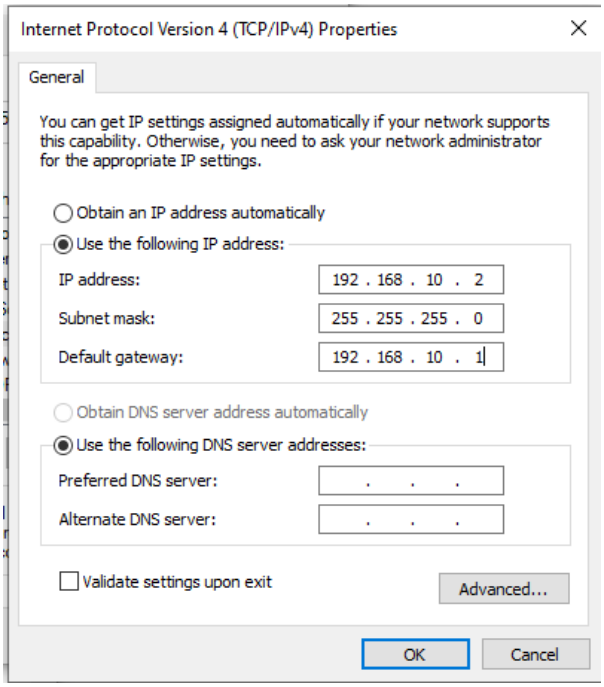
PRIPREMA ZA VJEŽBU

1. **Što je i čemu služi protokol ARP?**
   Adressing Resolution Protocol se koristi za otkrivanje MAC adrese uz priloženu IP adresu
2. **Što je i čemu služi protokol ICMP?**
   Internet Control Message Protocol - koriste ga mrežni uređaji za slanje poruka o pogreškama, i operativnih informacija.
3. **Što znaš o naredbi ping?**
   Naredba ping se koristi za testiranje povezanosti uređaja u mreži. Šalje par paketa za provjeru povezanosti te uz njih prikazuje nekoliko podataka poput TTL, veličine...

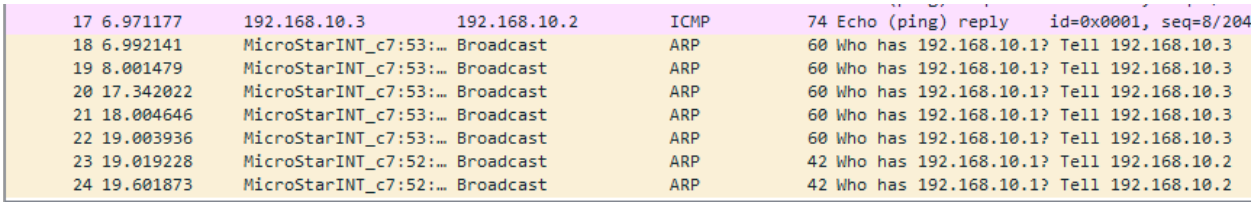
IZVOĐENJE VJEŽBE

- **Pokrenuti program za praćenje protokola Wireshark**
- **Odabrati mrežnu karticu na kojoj će se pratiti promet podataka**
- **Pokrenuti praćenje prometa na mrežnoj kartici**

1. **zadatak Povezati dva susjedna računala odgovarajućim kabelom te uspostaviti P2P spoj. Topologija: PC1 PC2 2**
   Povezali smo računala.
2. **zadatak Konfigurirati računala za rad u mreži, pri čemu koristiti adresnu shemu prema tablici:**



3. **zadatak Pokrenuti program Wireshark. Pričekati da se prikaže prvih dvadesetak redaka, a onda zaustaviti hvatanje (Capture – Stop).**



17	6.971177	192.168.10.3	192.168.10.2	ICMP	74 Echo (ping) reply id=0x0001, seq=8/204
18	6.992141	MicroStarINT_c7:53:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.3
19	8.001479	MicroStarINT_c7:53:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.3
20	17.342022	MicroStarINT_c7:53:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.3
21	18.004646	MicroStarINT_c7:53:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.3
22	19.003936	MicroStarINT_c7:53:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.3
23	19.019228	MicroStarINT_c7:52:…	Broadcast	ARP	42 Who has 192.168.10.1? Tell 192.168.10.2
24	19.601873	MicroStarINT_c7:52:…	Broadcast	ARP	42 Who has 192.168.10.1? Tell 192.168.10.2

a) Koliko je točno okvira Wireshark „uhvatio“? Uhvatio je 24 okvira.

b) Koje su oznake protokola na tim okvirima?

ARP, ICMP.

c) Koristeći dostupne informacije sa predavanja/Interneta opiši kratko funkcije tih protokola.

ARP - se koristi za otkrivanje MAC adrese uz priloženu IP adresu, ICMP - koriste ga mrežni uređaji za slanje poruka o pogreškama, i operativnih informacija.

d) Analiziraj okvir koji u sebi nosi:

ARP paket (protokol) request te ispiši:

- polazišnu MAC adresu

04:7c:16:c7:52:c0

- odredišnu MAC adresu

04:7c:16:c7:53:29

- polazišnu IP adresu

192.168.10.2

- odredišnu IP adresu

192.168.10.3

ARP paket (protokol) – reply te ispiši:

- polazišnu MAC adresu

04:7c:16:c7:53:29

- odredišnu MAC adresu

04:7c:16:c7:52:c0

- Kolika je veličina svake od ovih adresa?

48 bita

- polazišnu IP adresu

192.168.10.3

- odredišnu IP adresu

192.168.10.2

e) Kako glasi odredišna MAC adresa prvog Ethernet okvira kod ARP protokola i zašto?

Glasi ff: ff: ff: ff: ff: ff, jer je to broadcast MAC adresa.

4. zadatak U istom spoju računala pomoću Wiresharka analiziraj ICMP promet korištenjem naredbe ping sa jednog računala na drugo.

a) Koliko je ICMP echo i reply paketa? 4 ICMP echo i reply paketa

b) Koji protokol pokreće naredba ping? Pokreće protokol ICMP.

c) Sastavni dio kojeg protokola je ICMP protokol? Sastavni je dio IP-a.

d) U koji okvir je enkapsuliran IP paket?

Izaberi jedan redak koji se odnosi na protokol ICMP, ispiši njegov sadržaj te odgovori na slijedeća pitanja:

e) Koja je polazišna IP adresa?

192.168.10.3

f) Koja je odredišna IP adresa?

192.168.10.2

g) Koja je MAC adresa polazišnog uređaja?

04:7c:16:c7:53:29

h) Koja je MAC adresa odredišnog uređaja?

04:7c:16:c7:52:c0

i) Koja je oznaka vrste podataka u Ethernet okviru?

j) Koja je veličina IP adrese, a koja MAC adrese u okvirima/paketima?

Veličina IP adrese je 32 bita, a veličina MAC adrese je 48 bita.

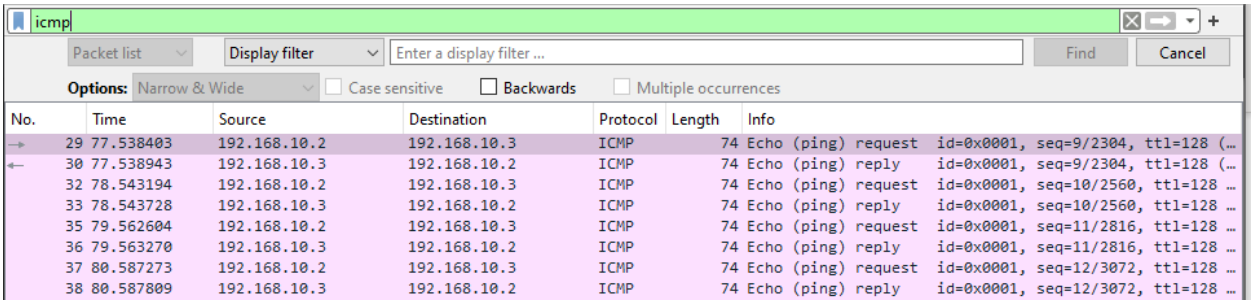
k) Koja je veličina IP paketa kod ICMP protokola?

74 bajta.

l) Koja je veličina podataka u IP paketu kod ICMP protokola?

32 bajta.

m) Postavi filter da se prati samo ICMP protokol.



No.	Time	Source	Destination	Protocol	Length	Info
29	77.538403	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (…
30	77.538943	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=128 (…
32	78.543194	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 …
33	78.543728	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=128 …
35	79.562604	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 …
36	79.563270	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=128 …
37	80.587273	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 …
38	80.587809	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=128 …

5. Zadatak Računala ponovno spojiti u školsku mrežu i provjeriti mrežne postavke. Učitati tri web stranice po želji i pratiti promet na vezi pomoću alata Wireshark.