OSNOVNA ANALIZA MREŽNOG PROMETA

Patrik Dalip i Gabrijela Grgić, 3.C

PRIPREMA ZA VJEŽBU

1. Što je i čemu služi protokol ARP?

Addressing Resolution Protocol je protokol koji mapira odgovarajuće IP adrese s MAC adresom na lokalnim mrežama.

2. Što je i čemu služi protokol ICMP?

Internet Control Message Protocol je protokol za slanje dijagnostičkih kontrolnih poruka između uređaja u mreži.

3. Što znaš o naredbi ping?

Naredba ping koristi se za provjeru mrežne povezanosti između dva uređaja. Rezultat pinga uključuje broj poslanih i primljenih paketa, vrijeme odziva i postotak izgubljenih paketa.

IZVOĐENJE VJEŽBE

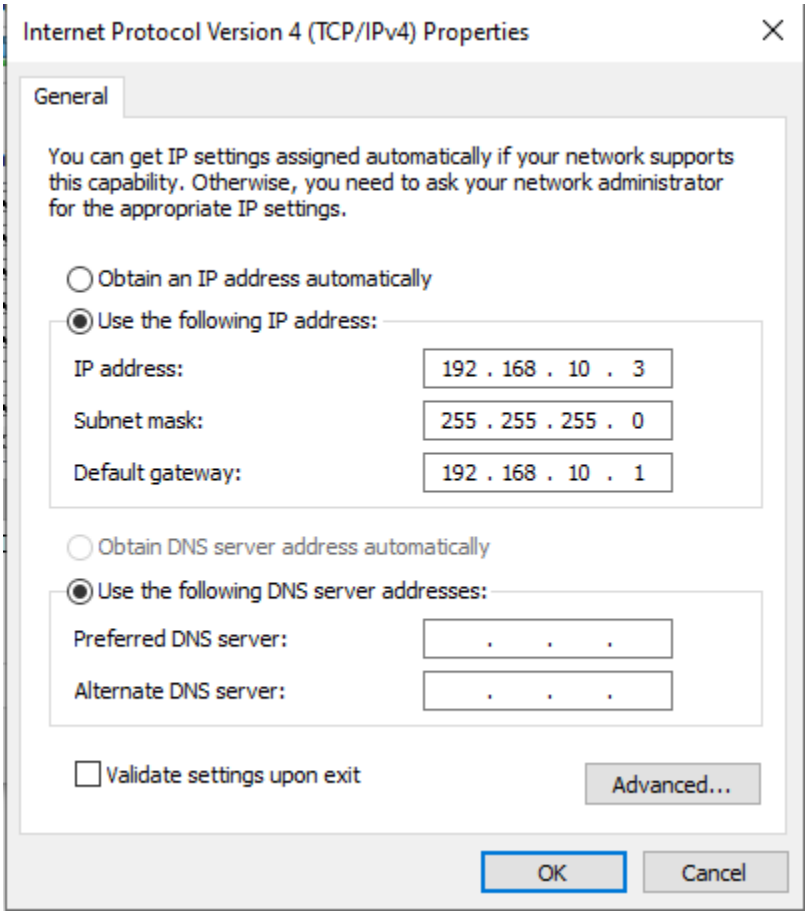
1. Povezati dva susjedna računala odgovarajućim kabelom te uspostaviti P2P spoj.

Jesmo.

2.

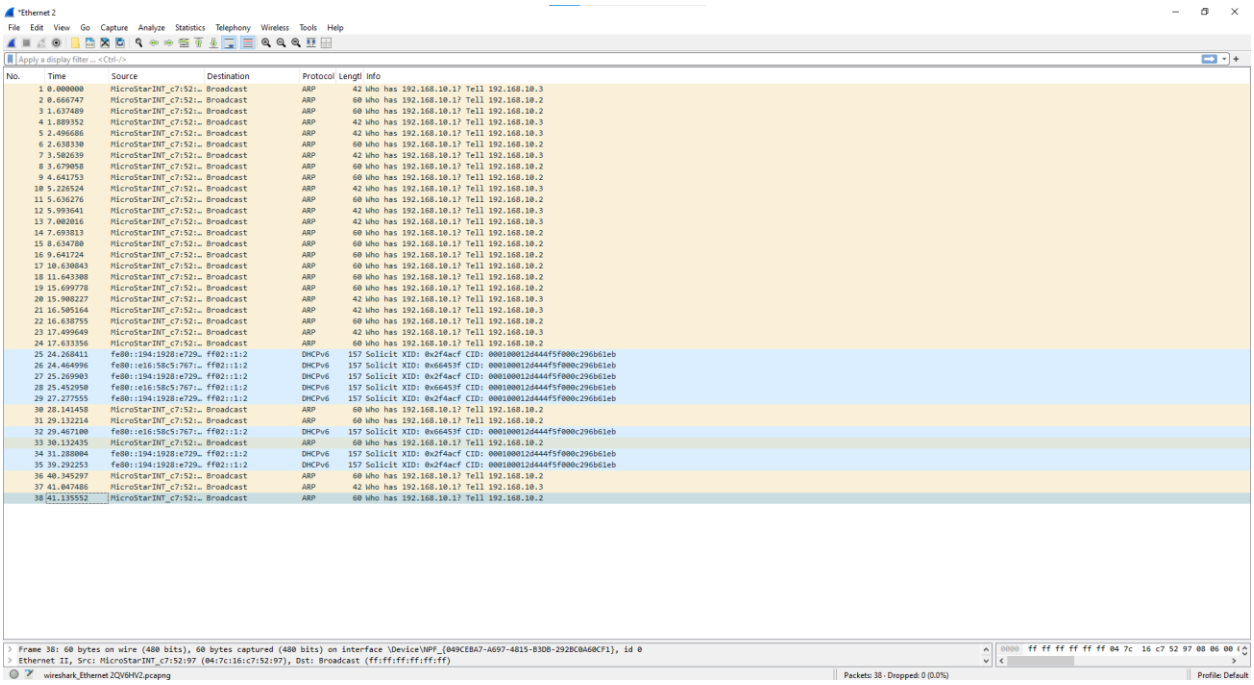
Konfigurirati računala za rad u mreži, pri čemu koristiti adresnu shemu prema tablici:

Oznaka na shemi	PC1	PC2
Naziv radne stanice	WSx	WSy
IP adresa	192.168.10.2	192.168.10.3
Subnet maska	255.255.255.0	255.255.255.0
Default Gateway	192.168.10.1	192.168.10.1



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

a) Koliko je točno okvira Wireshark „uhvatio“?



Uhvatio je 38 frameova.

b) Koje su oznake protokola na tim okvirima?

DHCP i ARP.

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

DHCP: automatski dodjeljuje IP adrese računalima.

ARP: Addressing Resolution Protocol je protokol koji mapira odgovarajuće IP adrese s MAC adresom na lokalnim mrežama.

d) Analiziraj okvir koji u sebi nosi:

ARP paket (protokol) request te ispiši:

Polazišnu MAC adresu: 03:7c:16:c7:52:97

Odredišnu MAC adresu: 00:00:00:00:00:00

Polazišnu IP adresu: 192.168.10.3

Odredišnu IP adresu: 192.168.10.1

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: MicroStarINT_c7:52:d7 (04:7c:16:c7:52:d7)
    Sender IP address: 192.168.10.3
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.10.1
```

ARP paket (protokol) – reply te ispiši:

- polazišnu MAC adresu: 04:7c:16:c7:52:d7

- odredišnu MAC adresu: 04:7c:16:c7:52:97

- Kolika je veličina svake od ovih adresa? 6 bajta(48 bita)

- polazišnu IP adresu: 192.168.10.3

- odredišnu IP adresu: 192.168.10.2

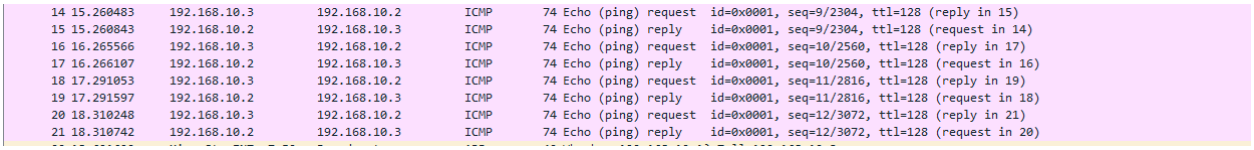
```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: MicroStarINT_c7:52:d7 (04:7c:16:c7:52:d7)
    Sender IP address: 192.168.10.3
    Target MAC address: MicroStarINT_c7:52:97 (04:7c:16:c7:52:97)
    Target IP address: 192.168.10.2
```

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

ff:ff:ff:ff:ff:ff zato što se prvo treba poslati boradcast poruka da bi se povezale IP i MAC adrese.

4. 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? 8



14	15.260483	192.168.10.3	192.168.10.2	ICMP	74 Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 15)
15	15.260843	192.168.10.2	192.168.10.3	ICMP	74 Echo (ping) reply id=0x0001, seq=9/2304, ttl=128 (request in 14)
16	16.265566	192.168.10.3	192.168.10.2	ICMP	74 Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 17)
17	16.266107	192.168.10.2	192.168.10.3	ICMP	74 Echo (ping) reply id=0x0001, seq=10/2560, ttl=128 (request in 16)
18	17.291053	192.168.10.3	192.168.10.2	ICMP	74 Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 19)
19	17.291597	192.168.10.2	192.168.10.3	ICMP	74 Echo (ping) reply id=0x0001, seq=11/2816, ttl=128 (request in 18)
20	18.310248	192.168.10.3	192.168.10.2	ICMP	74 Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 21)
21	18.310742	192.168.10.2	192.168.10.3	ICMP	74 Echo (ping) reply id=0x0001, seq=12/3072, ttl=128 (request in 20)

b) Koji protokol pokreće naredba ping?

ICMP.

c) Sastavni dio kojeg protokola je ICMP protokol?

IP protokola.

d) U koji okvir je enkapsuliran IP paket?

U ethernet okvir.

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:c7:52:d7

h) Koja je MAC adresa odredišnog uređaja?

04:7c:16:c7:52:97

i) Koja je oznaka vrste podataka u Ethernet okviru?

IPv4.

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

IP: 4 bajta.

MAC: 6 bajta.

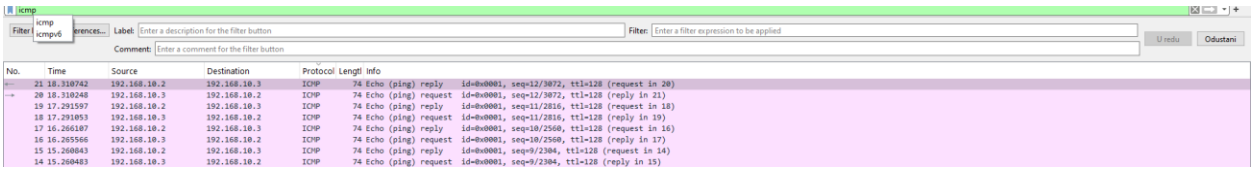
k) Koja je veličina IP paketa kod ICMP protokola?

60 bitova.

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

40 bitova.

m) Postavi filter da se prati samo ICMP protokol.



n) Koliko je ICMP echo i reply paketa?

8.

o) Koji protokol pokreće naredba ping?

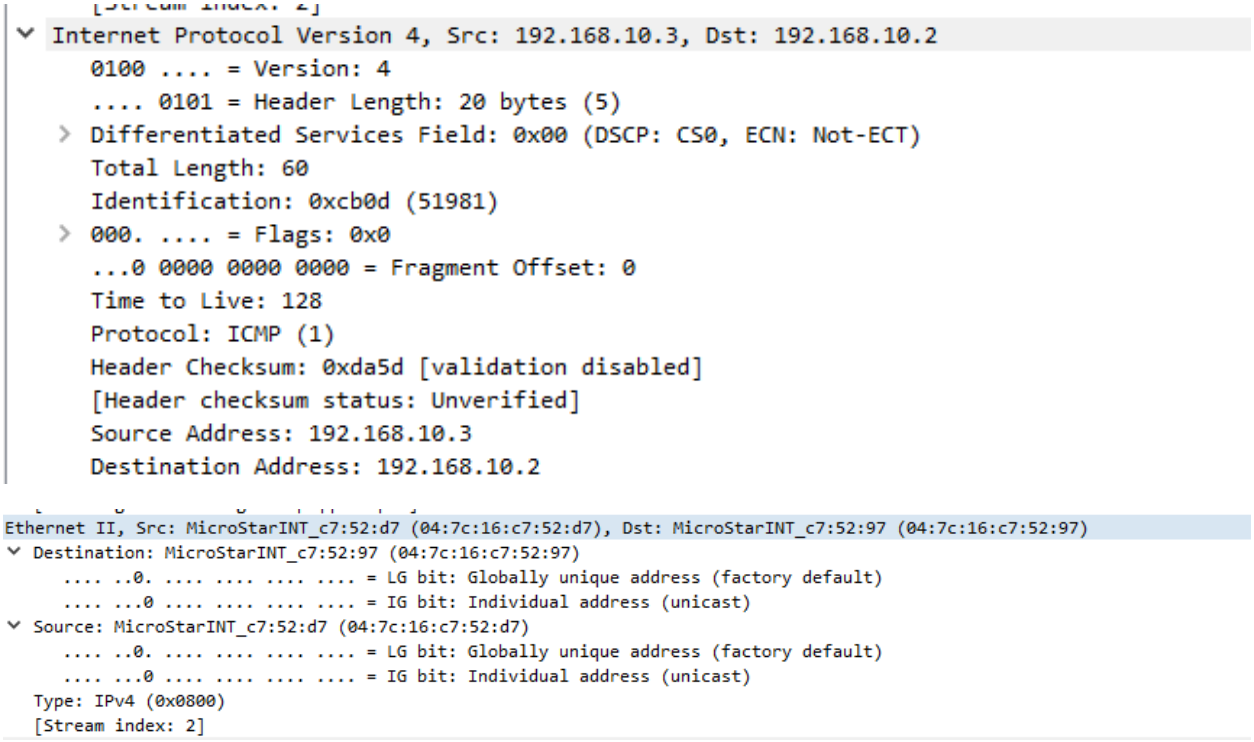
ICMP.

p) Sastavni dio kojeg protokola je protokol ICMP?

IP protokola.

q) U koji okvir je enkapsuliran IP paket?

Ethernet frame.



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

Jesmo.