Vježba 2: Osnovna analiza mrežnog prometa

Vid Pokrajac & Ante Prgin, 3.C

Pripreme za vježbu

Što je i čemu služi protokol ARP?

Address resolution protocol, on povezuje MAC I IP adrese.

Što je i čemu služi protokol ICMP?

Internet control message protocol koji je ugrađen u svaki IP modul, prijavljuje greške.

Što znaš o naredbi ping?

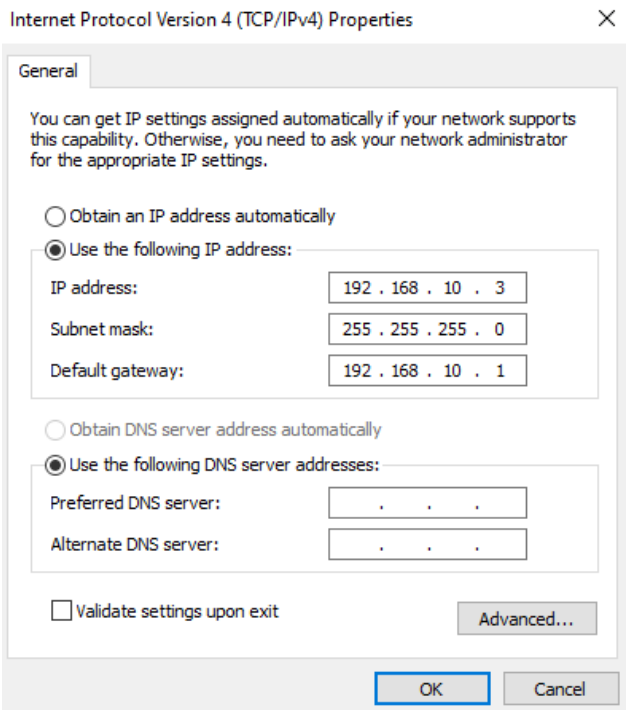
Jedna od glavnih dijagnstičkih naredba koje koristimo da provjerimo je li računalo spojeno na internet.

Izvođenje vježbe

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

Jesmo.

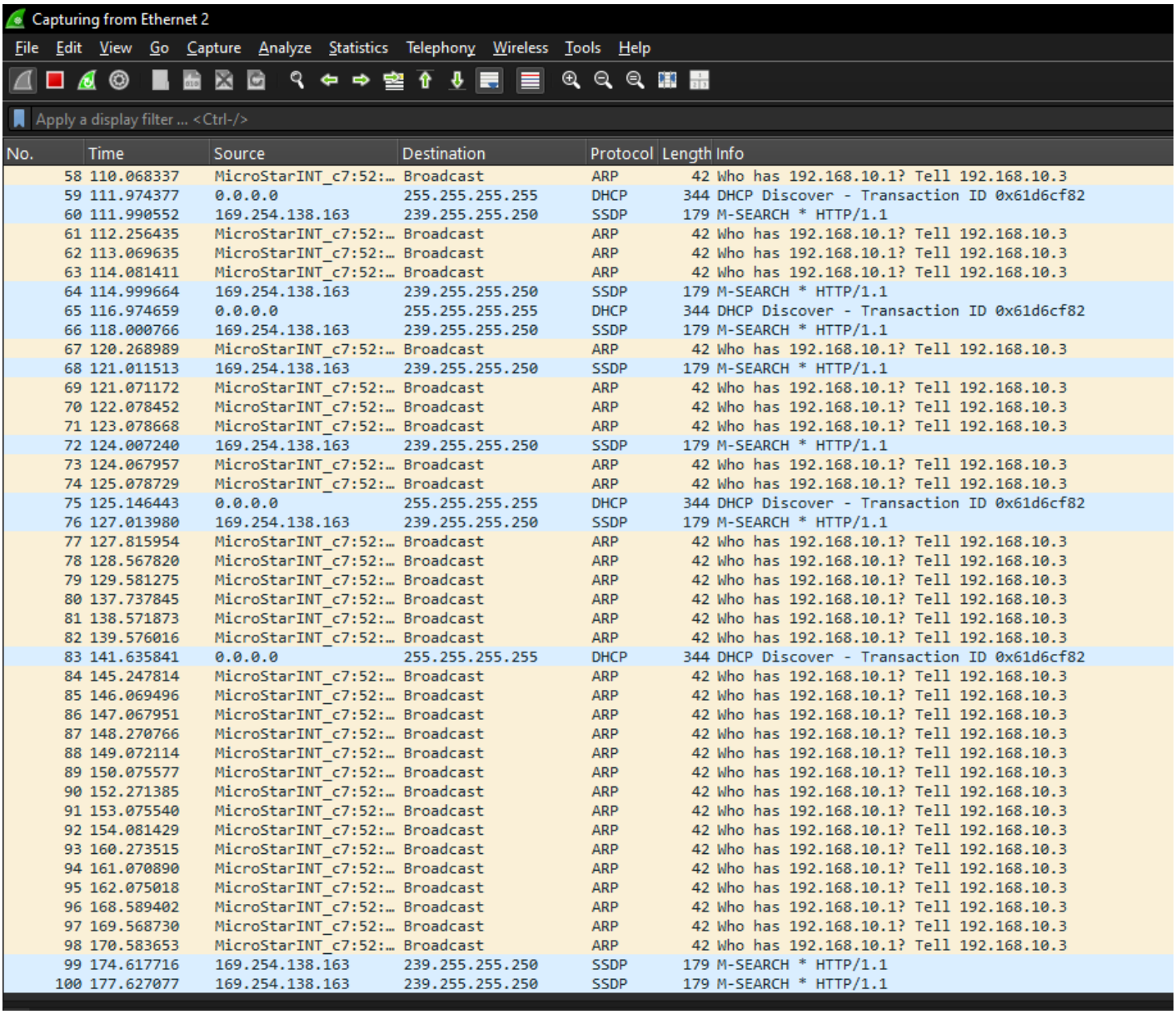
2.Konfigurirati računala za rad u mreži, pri čemu koristiti adresnu shemu prema tablici.



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

a)Koliko je točno okvira Wireshark „uhvatio“?

100



No.	Time	Source	Destination	Protocol	Length	Info
58	110.068337	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
59	111.974377	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x61d6cf82
60	111.990552	169.254.138.163	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
61	112.256435	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
62	113.069635	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
63	114.081411	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
64	114.999664	169.254.138.163	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
65	116.974659	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x61d6cf82
66	118.000766	169.254.138.163	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
67	120.268989	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
68	121.011513	169.254.138.163	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
69	121.071172	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
70	122.078452	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
71	123.078668	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
72	124.007240	169.254.138.163	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
73	124.067957	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
74	125.078729	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
75	125.146443	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x61d6cf82
76	127.013980	169.254.138.163	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
77	127.815954	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
78	128.567820	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
79	129.581275	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
80	137.737845	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
81	138.571873	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
82	139.576016	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
83	141.635841	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x61d6cf82
84	145.247814	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
85	146.069496	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
86	147.067951	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
87	148.270766	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
88	149.072114	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
89	150.075577	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
90	152.271385	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
91	153.075540	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
92	154.081429	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
93	160.273515	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
94	161.070890	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
95	162.075018	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
96	168.589402	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
97	169.568730	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
98	170.583653	MicroStarINT_c7:52:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
99	174.617716	169.254.138.163	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
100	177.627077	169.254.138.163	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1

b) Koje su oznake protokola na tim okvirima?

DHCP ,ARP, SSDP.

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

ARP povezuje MAC i IP adrese, DHCP dodjeljuje IP adrese, a SSDP

d) Analiziraj okvir koji u sebi nosi:

ARP paket (protokol) request te ispiši:

- polazišnu MAC adresu

```
Src: MicroStarINT_c7:52:c3 (04:7c:16:c7:52:c3)
```

- odredišnu MAC adresu

```
Dst: MicroStarINT_c7:52:da (04:7c:16:c7:52:da)
```

- polazišnu IP adresu

```
Sender IP address: 192.168.10.3
```

- odredišnu IP adresu

```
Target IP address: 192.168.10.1
```

ARP paket (protokol) reply te ispiši:

- polazišnu MAC adresu

```
Src: MicroStarINT_c7:52:da (04:7c:16:c7:52:da)
```

- odredišnu MAC adresu

```
Dst: MicroStarINT_c7:52:c3 (04:7c:16:c7:52:c3)
```

- Kolika je veličina svake od ovih adresa?

32 bita

- polazišnu IP adresu

```
Sender IP address: 192.168.10.1
```

- odredišnu IP adresu

```
Target IP address: 192.168.10.3
```

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

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?

4

b) Koji protokol pokreće naredba ping?

ICMP

c) Sastavni dio kojeg protokola je ICMP protokol?

IPv4

d) U koji okvir je enkapsuliran IP paket?

Ethernet 1

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?

192.168.10.1

g) Koja je MAC adresa polazišnog uređaja?

```
Src: MicroStarINT_c7:52:da (04:7c:16:c7:52:da)
```

h) Koja je MAC adresa odredišnog uređaja?

```
Dst: MicroStarINT_c7:52:c3 (04:7c:16:c7:52:c3)
```

i) Koja je oznaka vrste podataka u Ethernet okviru?

Type: IPv4 (0x0800)

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

IP adresa je 4 bajta ili 32 bita, a MAC adresa je 6 bajta ili 48 bita

k) Koja je veličina IP paketa kod ICMP protokola?

60

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

40

m) Postavi filter da se prati samo ICMP protokol.

Postavimo filter u Wiresharku, u pretraživač upišemo ICMP

n) Koliko je ICMP echo i reply paketa?

4 echo paketa I 4 reply paketa

o) Koji protokol pokreće naredba ping?

ICMP

p) Sastavni dio kojeg protokola je protokol ICMP?

IP

q) U koji okvir je enkapsuliran IP paket?

Ethernet 1