

LV2 – Osnovna analiza mrežnog prometa

Martin Barbarić

Adam Vidović

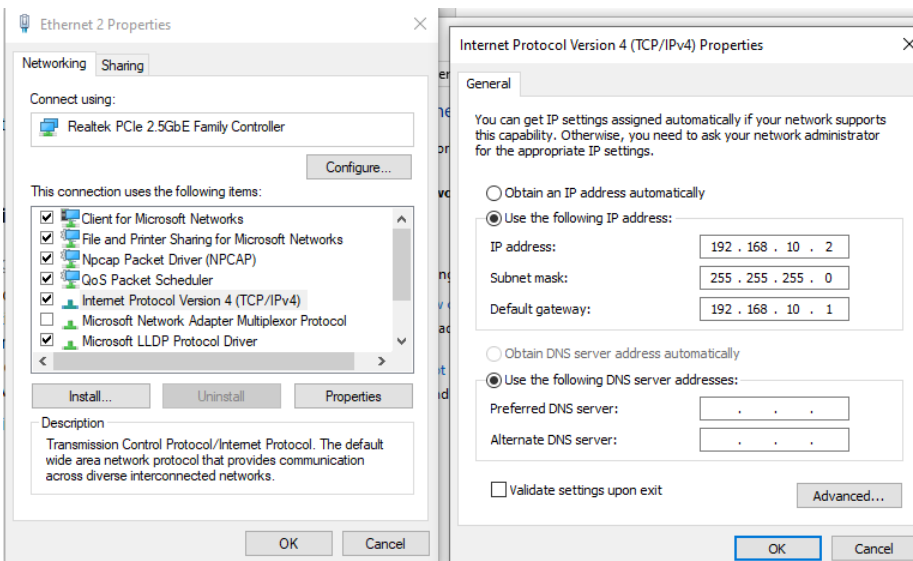
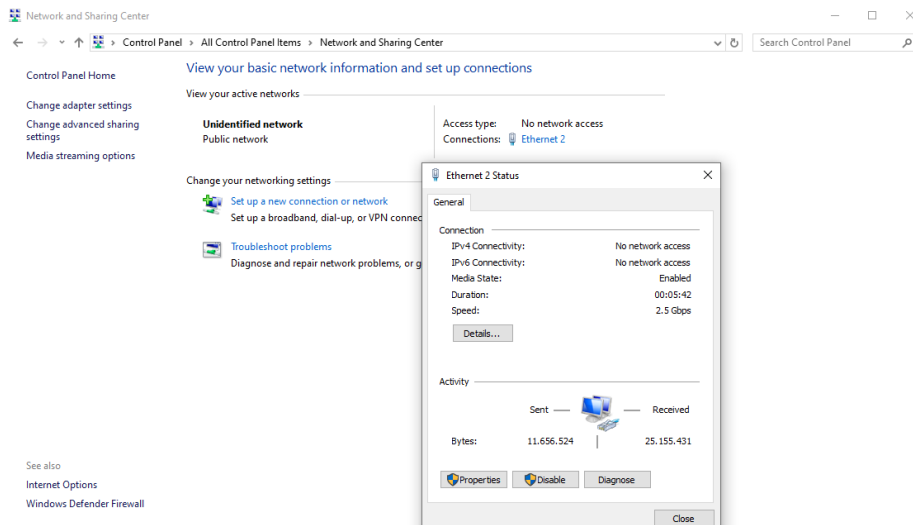
3.A

PRIPREMA ZA VJEŽBU

1. ARP (Address Resolution Protocol) koristi se za povezivanje IP adresa s fizičkim (MAC) adresama uređaja na lokalnoj mreži. Omogućuje uređajima na istoj mreži da komuniciraju pronalazeći MAC adresu odredišnog uređaja na temelju njegove IP adrese.
2. ICMP (Internet Control Message Protocol) koristi se za slanje kontrolnih poruka i obavijesti o greškama između uređaja na mreži. Omogućuje dijagnostiku mrežnih problema i obavještava o pogreškama poput nedostupnosti odredišta ili prekoračenja vremena prijenosa.
3. Naredba ping testira dostupnost uređaja na mreži slanjem ICMP "Echo Request" paketa i čekanjem "Echo Reply" odgovora. Koristi se za provjeru dostupnosti, mjerenje vremena odziva i otkrivanje mrežnih problema.

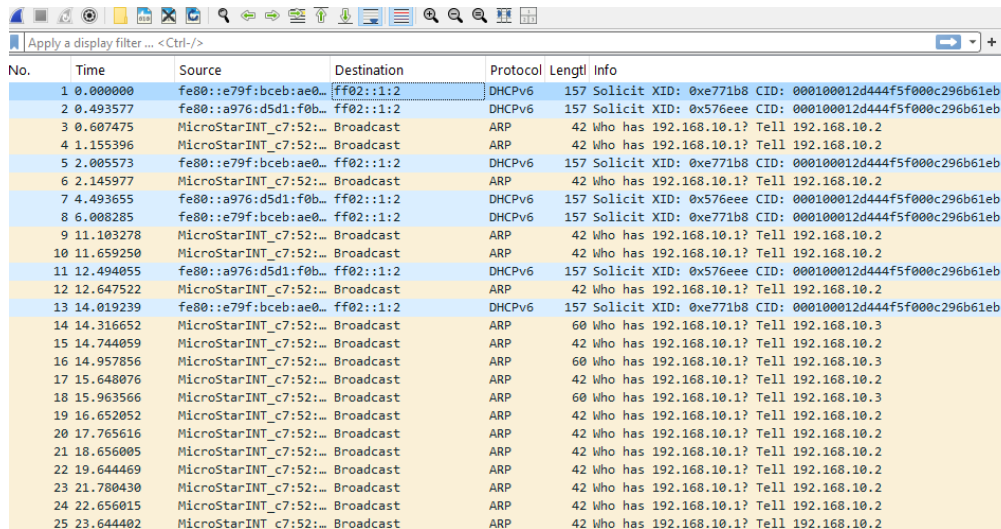
IZVOĐENJE VJEŽBE

1. Najprije smo oba računala spojili pomoću RJ45 konektora.
- 2.



3.

a)



The screenshot shows a Wireshark packet capture window with a display filter set to '<Ctrl-/>'. The packet list pane contains 25 entries. The first entry (No. 1) is a DHCPv6 Solicit packet from source fe80::e79f:bceb:ae0... to destination ff02::1:2. The second entry (No. 2) is a DHCPv6 Solicit packet from source fe80::a976:d5d1:f0b... to destination ff02::1:2. The third entry (No. 3) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The fourth entry (No. 4) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The fifth entry (No. 5) is a DHCPv6 Solicit packet from source fe80::e79f:bceb:ae0... to destination ff02::1:2. The sixth entry (No. 6) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The seventh entry (No. 7) is a DHCPv6 Solicit packet from source fe80::a976:d5d1:f0b... to destination ff02::1:2. The eighth entry (No. 8) is a DHCPv6 Solicit packet from source fe80::e79f:bceb:ae0... to destination ff02::1:2. The ninth entry (No. 9) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The tenth entry (No. 10) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The eleventh entry (No. 11) is a DHCPv6 Solicit packet from source fe80::a976:d5d1:f0b... to destination ff02::1:2. The twelfth entry (No. 12) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The thirteenth entry (No. 13) is a DHCPv6 Solicit packet from source fe80::e79f:bceb:ae0... to destination ff02::1:2. The fourteenth entry (No. 14) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The fifteenth entry (No. 15) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The sixteenth entry (No. 16) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The seventeenth entry (No. 17) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The eighteenth entry (No. 18) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The nineteenth entry (No. 19) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The twentieth entry (No. 20) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The twenty-first entry (No. 21) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The twenty-second entry (No. 22) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The twenty-third entry (No. 23) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The twenty-fourth entry (No. 24) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast. The twenty-fifth entry (No. 25) is an ARP request from source MicroStarINT_c7:52:... to destination Broadcast.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::e79f:bceb:ae0...	ff02::1:2	DHCPv6	157	Solicit XID: 0xe771b8 CID: 000100012d444f5f00c296b61eb
2	0.493577	fe80::a976:d5d1:f0b...	ff02::1:2	DHCPv6	157	Solicit XID: 0x576eee CID: 000100012d444f5f00c296b61eb
3	0.607475	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
4	1.155396	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
5	2.005573	fe80::e79f:bceb:ae0...	ff02::1:2	DHCPv6	157	Solicit XID: 0xe771b8 CID: 000100012d444f5f00c296b61eb
6	2.145977	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
7	4.493655	fe80::a976:d5d1:f0b...	ff02::1:2	DHCPv6	157	Solicit XID: 0x576eee CID: 000100012d444f5f00c296b61eb
8	6.008285	fe80::e79f:bceb:ae0...	ff02::1:2	DHCPv6	157	Solicit XID: 0xe771b8 CID: 000100012d444f5f00c296b61eb
9	11.103278	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
10	11.659250	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
11	12.494055	fe80::a976:d5d1:f0b...	ff02::1:2	DHCPv6	157	Solicit XID: 0x576eee CID: 000100012d444f5f00c296b61eb
12	12.647522	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
13	14.019239	fe80::e79f:bceb:ae0...	ff02::1:2	DHCPv6	157	Solicit XID: 0xe771b8 CID: 000100012d444f5f00c296b61eb
14	14.316652	MicroStarINT_c7:52:...	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.3
15	14.744059	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
16	14.957856	MicroStarINT_c7:52:...	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.3
17	15.648076	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
18	15.963566	MicroStarINT_c7:52:...	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.3
19	16.652052	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
20	17.765616	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
21	18.656005	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
22	19.644469	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
23	21.780430	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
24	22.656015	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
25	23.644402	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2

Wireshark je „uhvatio“ 25 okvira

b) Onake protokola su ARP i DHCPv6

c) ARP- prevodi IP adrese u MAC adrese uutar LAN-a

DHCPv6- koristi se za dovibanje adresa i drugih mrežnih postavki kao npr. Pretpostavljeni gateway, subnet maska i IP adrese DNS servera

d)

ARP paket request:

Sender MAC address: MicroStarINT_c7:52:8a (04:7c:16:c7:52:8a)

Sender IP address: 192.168.10.3

Target MAC address: MicroStarINT_c7:52:d1 (04:7c:16:c7:52:d1)

Target IP address: 192.168.10.2

ARP paket reply:

Sender MAC address: MicroStarINT_c7:52:d1 (04:7c:16:c7:52:d1)

Sender IP address: 192.168.10.2

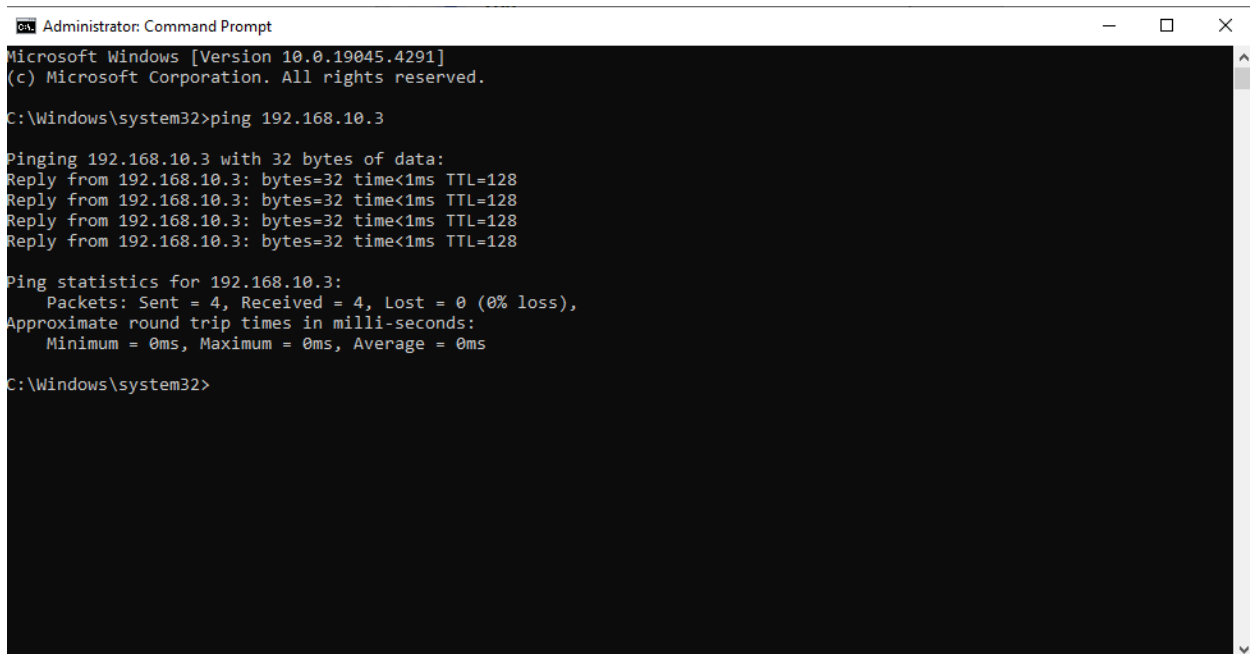
Target MAC address: MicroStarINT_c7:52:8a (04:7c:16:c7:52:8a)

Target IP address

MAC adresa je dugačka 6 bajta a IPv4 4 bajta

e) Glasi (00:00:00:00:00:00) zato što u početku nije poznata

4.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>
```

- a) Sve ukupno je 8 ICMP paketa, 4 zahtjeva i 4 odgovora
- b) Ping pokreće ICMP protokol
- c) ICMP je sastavio dio IP protokola
- d) IP paket je enkapsuliran u Ethernet okvir
- e) Source Address: 192.168.10.2

- f) Destination Address: 192.168.10.3
- g) Source: MicroStarINT_c7:52:d1 (04:7c:16:c7:52:d1)
- h) Destination: MicroStarINT_c7:52:8a (04:7c:16:c7:52:8a)
- i) Type: IPv4 (0x0800)
- j) MAC adresa je dugačka 6 bajta a IPv4 4 bajta
- k) Total Length: 60
- l) 40 bajta (total length – Header length= 60-20=40 bajta)
- m)

No.	Time	Source	Destination	Protocol	Length	Info
333	797.086096	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply
334	797.086618	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=128 (reque
335	798.101998	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply
336	798.102507	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=128 (reque
337	799.126675	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply
338	799.127198	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=128 (reque
339	800.150965	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (repl
340	800.151467	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=128 (reque

- n) Sve ukupno je 8 ICMP paketa, 4 zahtjeva i 4 odgovora
- o) Ping pokreće ICMP protokol
- p) ICMP je sastavio dio IP protokola
- q) IP paket je enkapsuliran u Ethernet II paket

5.

The screenshot shows a web browser window on the left and a Wireshark packet capture window on the right. The browser window displays a page titled 'Workbook' with a navigation menu and a list of items under the heading 'WEB sjediste primarno obrazovnog tipa'. The Wireshark window shows a detailed view of an ICMP Echo (ping) request packet, including the IP header and the ICMP payload.