

VJEZBA 2: Osnovna analiza mrežnog prometa

Jan Šotić, David Rudar

PRIPREMA:

- 1) ARP je komunikacijski protokol kojim se dobiva fizicka adresa na lokalnoj mrezi iz poznate mrezne adrese.
- 2) ICMP je komunikacijski protokol koji je ugradjen u svaki IP modul da bi omogućio mreznim prolazima ili racunalima slanje kontrolnih poruka o greskama. Zaduzen je samo za prijavljivanje gresaka, ali ne za njihovo ispravljanje.
- 3) Ping naredba je naredba naredbene naredbe koja se koristi za testiranje sposobnosti izvornog racunala da dosegne određeno određeno računalo. Ping naredba obično se koristi kao jednostavan način da se potvrdi da računalo može komunicirati preko mreže s drugim računalom ili mrežnim uređajem.

IZVOĐENJE VJEŽBE:

1. ...

2. ...

3. a) Uхватило je 25 Okvira kroz 25 redaka rada Wiresharka.

b) Oznake protokola su : ARP, NBNS, MDNS, LLMNR.

c) ARP- pise u pripremi

NBNS- protokol koji postoji da riješava imena na mreži bez potrebe za korištenje lokalnih host fileova ili DNS-a.

MDNS- razrješava imena hostova u IP adrese unutar malih mreža koje ne uključuju lokalni poslužitelji naziva

LLMNR- protokol temeljen na formatu paketa Domain Name System koji omogućuje i IPv4 i IPv6 hostovima da izvrše razrješenje imena za hostove na istoj lokalnoj vezi.

d) ARP REQUEST:

42	7.048344	AsrockIn_ce:9a:ec	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
46	8.081834	AsrockIn_ce:9a:ec	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
55	9.053503	AsrockIn_ce:9a:ec	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
59	10.056386	AsrockIn_ce:9a:ec	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
73	11.059156	AsrockIn_ce:9a:ec	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.2
2	0.149257	AsrockIn_ce:9b:e5	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.3
83	13.287253	AsrockIn_ce:9b:e5	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.3

>	Destination: Broadcast (ff:ff:ff:ff:ff:ff)
>	Source: AsrockIn_ce:9a:ec (70:85:c2:ce:9a:ec)
	Type: ARP (0x0806)
▼	Address Resolution Protocol (request)
	Hardware type: Ethernet (1)
	Protocol type: IPv4 (0x0800)
	Hardware size: 6
	Protocol size: 4
	Opcode: request (1)
	Sender MAC address: AsrockIn_ce:9a:ec (70:85:c2:ce:9a:ec)
	Sender IP address: 192.168.10.2
	Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
	Target IP address: 192.168.10.1

odredišna IP adresa: 192.168.10.1

ishodišna IP adresa: 192.168.10.2

odredišna MAC adresa: 00:00:00:00:00:00

ishodišna MAC adresa: 70:85:c2:ce:9a:ec

ARP REPLY:

2	0.149257	AsrockIn_ce:9b:e5	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.3
83	13.287253	AsrockIn_ce:9b:e5	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.3

>	Source: AsrockIn_ce:9b:e5 (70:85:c2:ce:9b:e5)
	Type: ARP (0x0806)
	Padding: 00000000000000000000000000000000
▼	Address Resolution Protocol (request)
	Hardware type: Ethernet (1)
	Protocol type: IPv4 (0x0800)
	Hardware size: 6
	Protocol size: 4
	Opcode: request (1)
	Sender MAC address: AsrockIn_ce:9b:e5 (70:85:c2:ce:9b:e5)
	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

ishodišna IP adresa: 192.168.10.3

odredišna IP adresa: 192.168.10.1

ishodišna MAC adresa: 70:85:c2:ce:9b:e5

odredišna MAC adresa: 00:00:00:00:00:00

e) ff:ff:ff:ff:ff:ff zato što je to broadcast adresa preko koje se šalje ARP zahtjev svim uređajima u mreži

4. a)

13	2.335624	192.168.10.3	192.168.10.2	ICMP	74 Echo (ping) reply	id=0x0001, seq=905/35075, tt...
----	----------	--------------	--------------	------	----------------------	---------------------------------

ICMP Echo: 74
reply paketa: 4

```
C:\Users\ucenik>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

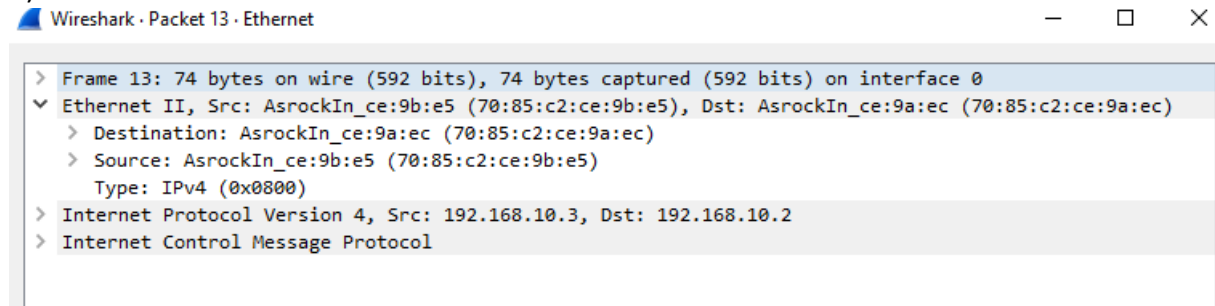
C:\Users\ucenik>
```

b) Protokol koji pokreće naredba ping je ICMP

c) ICMP protokol je sastavni dio IP protokola

d) U Ethernet okvir

e)



Polazišna IP adresa je: 192.168.10.3

f) Odredišna IP adresa je: 192.168.10.2

g) MAC adresa polazišnog računala je 70:85:c2:ce:9b:35

h) MAC adresa odredišnog računala je 70:85:c2:ce:9a:ec

i) 0x0800 – indicira ARP datagram

j) IP adresa: 60 bitova

MAC adresa: 48 bitova

k) 60 bitova

l) 20 bitova

m)

The screenshot shows a network traffic analysis window titled 'icmp'. The window displays a list of network packets with the following columns: No., Time, Source, Destination, Protocol, Length, and Info. The packets are ICMP Echo (ping) requests and replies. The requests are sent from 192.168.10.2 to 192.168.10.3, and the replies are sent from 192.168.10.3 to 192.168.10.2. The 'Info' column provides details such as ID, sequence number, and TTL for each packet.

No.	Time	Source	Destination	Protocol	Length	Info
33	5.376985	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=908/35843, ttl=128 ...
22	4.358227	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=907/35587, ttl=128 ...
19	3.340292	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=906/35331, ttl=128 ...
12	2.335334	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=905/35075, ttl=128 ...
34	5.377267	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=908/35843, ttl=128 ...
23	4.358591	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=907/35587, ttl=128 ...
20	3.340584	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=906/35331, ttl=128 ...
13	2.335624	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=905/35075, ttl=128 ...

5.

```

> Frame 2432: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▼ Ethernet II, Src: Routerbo_a6:8c:7f (74:4d:28:a6:8c:7f), Dst: AsrockIn_ce:9a:ec (70:85:c2:ce:9a:ec)
  > Destination: AsrockIn_ce:9a:ec (70:85:c2:ce:9a:ec)
  > Source: Routerbo_a6:8c:7f (74:4d:28:a6:8c:7f)
    Type: IPv4 (0x0800)
    Padding: 000000000000
▼ Internet Protocol Version 4, Src: 173.194.76.27, Dst: 192.168.50.14
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xa4 (DSCP: Unknown, ECN: Not-ECT)
  Total Length: 40
  Identification: 0xa6db (42715)
  > Flags: 0x0000
  Time to live: 111
  Protocol: TCP (6)
  
```

```

0000  70 85 c2 ce 9a ec 74 4d 28 a6 8c 7f 08 00 45 a4  p.....tM (.....E·
0010  00 28 a6 db 00 00 6f 06 b7 bc ad c2 4c 1b c0 a8  ·(.....o· .....L...
0020  32 0e 00 19 c3 f3 79 72 e6 8a dc 00 b5 7d 50 10  2.....yr .....}P·
0030  05 49 08 6f 00 00 00 00 00 00 00 00  ·I·o.....
  
```

No.: 2432 · Time: 5.220175 · Source: 173.194.76.27 · Destination: 192.168.50.14 · Protocol: TCP · Length: 60 · Info: 25 → 50163 [ACK] Seq=476 Ack=136153 Win=34636

Close Hel

7120	9.233610	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7486	9.317686	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7487	9.317686	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7488	9.318219	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7489	9.318219	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7490	9.318219	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7491	9.318219	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7492	9.318219	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7493	9.318219	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7494	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7495	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7496	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7497	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7498	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7499	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7500	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7501	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7502	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7503	9.319382	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200
7504	9.319622	104.16.126.63	192.168.50.14	UDP	1242 443 → 59239 Len=1200

7088	9.225960	192.168.50.14	104.16.125.63	UDP	1399 61786 → 443 Len=1357
7167	9.251644	192.168.50.14	104.16.125.63	UDP	94 61786 → 443 Len=52
7168	9.251668	192.168.50.14	104.16.125.63	UDP	94 61786 → 443 Len=52
7142	9.242306	192.168.50.14	104.16.125.63	UDP	96 61786 → 443 Len=54
7117	9.232880	192.168.50.14	104.16.125.63	UDP	97 61786 → 443 Len=55
7231	9.261947	192.168.50.14	104.16.125.63	UDP	120 61786 → 443 Len=78
7230	9.261923	192.168.50.14	104.16.125.63	UDP	130 61786 → 443 Len=88
7244	9.263853	192.168.50.14	104.16.125.63	UDP	137 61786 → 443 Len=95
7256	9.264248	192.168.50.14	104.16.125.63	UDP	137 61786 → 443 Len=95
7448	9.300504	192.168.50.14	104.16.125.63	UDP	137 61786 → 443 Len=95
7410	9.370015	192.168.50.14	104.16.125.63	UDP	137 61786 → 443 Len=95