Vježba 2: Osnovna analiza mrežnog prometa

Lovro Bartolec, Niko Mrkonjić 3.B

PRIPREMA ZA VJEZBU

1.ARP protokol je protokol mrežnog sloja koja nam od postojeće IP adrese odgovori sa MAC adresom povezanom s tom Ip adresom

2.ICMP protokol je komunikacijski protokol korišten da pošalje poruke o greškama.

3. Ping je administrativni alat koji služi za provjeru dostupnosti poslužitelja na računalnim mrežama temeljenim na IP protokolu.

IZVOĐENJE VJEŽBE

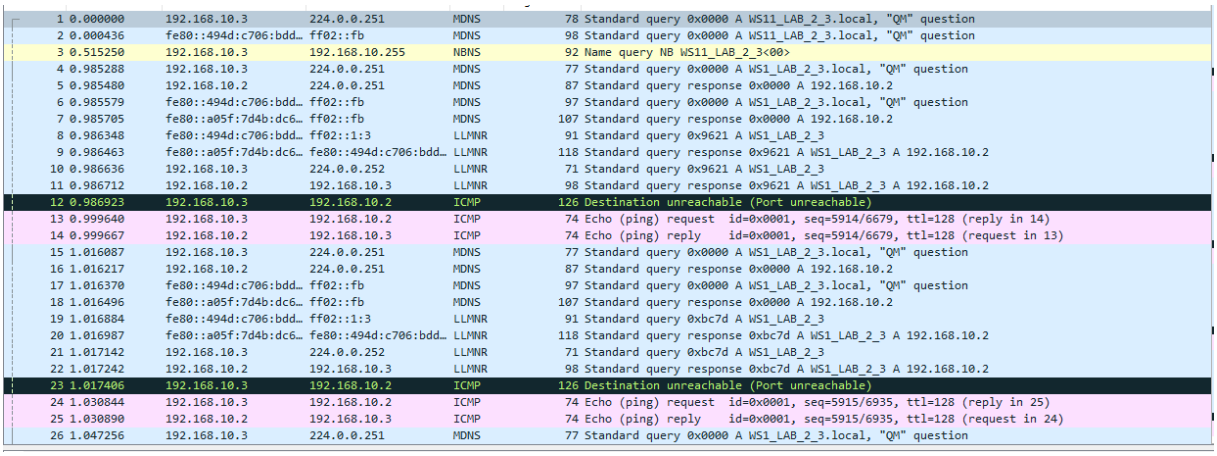
2.

```
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
```

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a05f:7d4b
   IPv4 Address. . . . . . . . . . . : 192.168.10.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
```

3.

a) 58 okvira



1	0.000000	192.168.10.3	224.0.0.251	MDNS	78	Standard query 0x0000 A WS11_LAB_2_3.local, "QM" question
2	0.000436	fe80::494d:c706:bdd…	ff02::fb	MDNS	98	Standard query 0x0000 A WS11_LAB_2_3.local, "QM" question
3	0.515250	192.168.10.3	192.168.10.255	NBNS	92	Name query NB WS11_LAB_2_3<00>
4	0.985288	192.168.10.3	224.0.0.251	MDNS	77	Standard query 0x0000 A WS1_LAB_2_3.local, "QM" question
5	0.985480	192.168.10.2	224.0.0.251	MDNS	87	Standard query response 0x0000 A 192.168.10.2
6	0.985579	fe80::494d:c706:bdd…	ff02::fb	MDNS	97	Standard query 0x0000 A WS1_LAB_2_3.local, "QM" question
7	0.985705	fe80::a05f:7d4b:dc6…	ff02::fb	MDNS	107	Standard query response 0x0000 A 192.168.10.2
8	0.986348	fe80::494d:c706:bdd…	ff02::1:3	LLMNR	91	Standard query 0x9621 A WS1_LAB_2_3
9	0.986463	fe80::a05f:7d4b:dc6…	fe80::494d:c706:bdd…	LLMNR	118	Standard query response 0x9621 A WS1_LAB_2_3 A 192.168.10.2
10	0.986636	192.168.10.3	224.0.0.252	LLMNR	71	Standard query 0x9621 A WS1_LAB_2_3
11	0.986712	192.168.10.2	192.168.10.3	LLMNR	98	Standard query response 0x9621 A WS1_LAB_2_3 A 192.168.10.2
12	0.986923	192.168.10.3	192.168.10.2	ICMP	126	Destination unreachable (Port unreachable)
13	0.999640	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=5914/6679, ttl=128 (reply in 14)
14	0.999667	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=5914/6679, ttl=128 (request in 13)
15	1.016087	192.168.10.3	224.0.0.251	MDNS	77	Standard query 0x0000 A WS1_LAB_2_3.local, "QM" question
16	1.016217	192.168.10.2	224.0.0.251	MDNS	87	Standard query response 0x0000 A 192.168.10.2
17	1.016370	fe80::494d:c706:bdd…	ff02::fb	MDNS	97	Standard query 0x0000 A WS1_LAB_2_3.local, "QM" question
18	1.016496	fe80::a05f:7d4b:dc6…	ff02::fb	MDNS	107	Standard query response 0x0000 A 192.168.10.2
19	1.016884	fe80::494d:c706:bdd…	ff02::1:3	LLMNR	91	Standard query 0xbc7d A WS1_LAB_2_3
20	1.016987	fe80::a05f:7d4b:dc6…	fe80::494d:c706:bdd…	LLMNR	118	Standard query response 0xbc7d A WS1_LAB_2_3 A 192.168.10.2
21	1.017142	192.168.10.3	224.0.0.252	LLMNR	71	Standard query 0xbc7d A WS1_LAB_2_3
22	1.017242	192.168.10.2	192.168.10.3	LLMNR	98	Standard query response 0xbc7d A WS1_LAB_2_3 A 192.168.10.2
23	1.017406	192.168.10.3	192.168.10.2	ICMP	126	Destination unreachable (Port unreachable)
24	1.030844	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=5915/6935, ttl=128 (reply in 25)
25	1.030890	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=5915/6935, ttl=128 (request in 24)
26	1.047256	192.168.10.3	224.0.0.251	MDNS	77	Standard query 0x0000 A WS1_LAB_2_3.local, "QM" question

b)MDNS, ICMP, LLMNR, ICMPv6

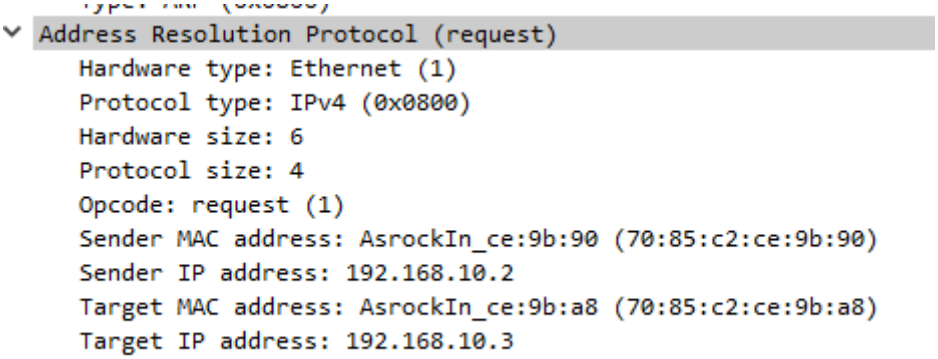
c)MDNS – protokol koji izvuče ime hosta od IP adrese

ICMP – komunikacijski protokol za slanje poruke o greškama

ICMPv6 – Komunikacijski protokol za slanje poruke o greškama za IPv6

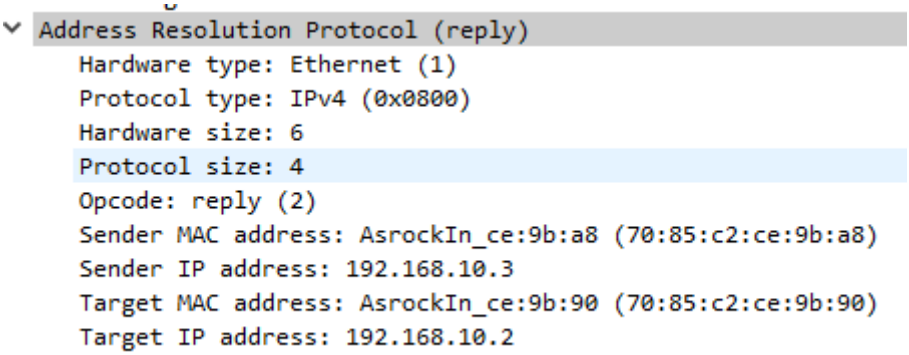
LLMNR – protokol koji služi da IPv4 i IPv6 odrede imena hostova koji su povezani.

d)ARP request :



```
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:90 (70:85:c2:ce:9b:90)
    Sender IP address: 192.168.10.2
    Target MAC address: AsrockIn_ce:9b:a8 (70:85:c2:ce:9b:a8)
    Target IP address: 192.168.10.3
```

ARP reply:



```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: AsrockIn_ce:9b:a8 (70:85:c2:ce:9b:a8)
    Sender IP address: 192.168.10.3
    Target MAC address: AsrockIn_ce:9b:90 (70:85:c2:ce:9b:90)
    Target IP address: 192.168.10.2
```

e)Tagret MAC adresa glasi FF:FF:FF:FF:FF (broadcast adresa), zato što traži koji su svi uređaji povezani u mreži.

4.

a)ICMP echo je 10 okvira, i 5 reply okvira.

23	1.989176	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=6492/23577, ttl=128 (reply in 24)
24	1.989203	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=6492/23577, ttl=128 (request in 23)
33	1.998213	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=6493/23833, ttl=128 (reply in 34)
34	1.998241	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=6493/23833, ttl=128 (request in 33)
43	2.007077	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=6494/24089, ttl=128 (reply in 44)
44	2.007110	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=6494/24089, ttl=128 (request in 43)
53	2.016055	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=6495/24345, ttl=128 (reply in 54)
54	2.016098	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=6495/24345, ttl=128 (request in 53)
63	2.024124	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=6496/24601, ttl=128 (reply in 64)
64	2.024173	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=6496/24601, ttl=128 (request in 63)

b)Ping pokreće ICMP protokol

c)ICMP je sastavni dio IP protokola.

d)IP protokol je enkapsuliran u Ethernet II okviru

e),f)

```
Source: 192.168.10.3
Destination: 192.168.10.2
```

g),h)

```
> Destination: AsrockIn_ce:9b:90 (70:85:c2:ce:9b:90)
> Source: AsrockIn_ce:9b:a8 (70:85:c2:ce:9b:a8)
```

i)

```
v Ethernet II, Src: AsrockIn_ce:9b:a8 (70:85:c2:ce:9b:a8), Dst: Asro
  > Destination: AsrockIn_ce:9b:90 (70:85:c2:ce:9b:90)
  > Source: AsrockIn_ce:9b:a8 (70:85:c2:ce:9b:a8)
    Type: IPv4 (0x0800)
```

0x0800

j) IP adresa ima duljinu 32 bita , mac adresa 48 bitova

k) veličina IP adrese u ICMP protokolu je 8 bajta.

l) veličina podatka u ICMP protokolu je 32 bajta

m)

icmp

No.	Time	Source	Destination	Protocol	Length	Info
22	1.987482	192.168.10.3	192.168.10.2	ICMP	126	Destination unreachable (Port unreachable)
23	1.989176	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=6492/23577, ttl=128 (reply in 24)
24	1.989203	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=6492/23577, ttl=128 (request in 23)
33	1.998213	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=6493/23833, ttl=128 (reply in 34)
34	1.998241	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=6493/23833, ttl=128 (request in 33)
43	2.007077	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=6494/24089, ttl=128 (reply in 44)
44	2.007110	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=6494/24089, ttl=128 (request in 43)
53	2.016055	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=6495/24345, ttl=128 (reply in 54)
54	2.016098	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=6495/24345, ttl=128 (request in 53)
63	2.024124	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=6496/24601, ttl=128 (reply in 64)
64	2.024173	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=6496/24601, ttl=128 (request in 63)