

LV02: Osnovna analiza mrežnog prometa

Priprema:

1. Što je i čemu služi protokol ARP?

Protokol ARP je protokol za prevođenje IP adresa u MAC adrese u lokalnoj mreži .

2. Što je i čemu služi protokol ICMP?

Protokol ICMP je protokol za dijagnosticiranje i izvještavanje o problemima u mrežnoj komunikaciji .

3. Što znaš o naredbi ping?

Naredba ping je naredba za testiranje dostupnosti i kašnjenja mrežnog odredišta ili usluge .

Izvođenje vježbe:

1. zadatak:



2. zadatak:

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. zadatak:

a. 32

b. DHCP, SSDP, BROWSER

c. SSDP-Simple Service Discovery Protocol (SSDP) mrežni je protokol temeljen na paketu internetskih protokola za oglašavanje i otkrivanje mrežnih usluga i informacija o prisutnosti.

DHCP (Dynamic Host Configuration Protocol) je mrežni protokol korišten od strane mrežnih računala za dodjelivanje IP adresa i ostalih mrežnih postavki

d. ARP Request

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: AsrockIn_ce:9a:f7 (70:85:c2:ce:9a:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ 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:f7 (70:85:c2:ce:9a:f7)
  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: 192.160.10.1
```

ARP Request

```
> Frame 15: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: AsrockIn_ce:9a:f7 (70:85:c2:ce:9a:f7), Dst: AsrockIn_ce:9a:f0 (70:85:c2:ce:9a:f0)
▼ 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:9a:f7 (70:85:c2:ce:9a:f7)
  Sender IP address: 192.168.10.2
  Target MAC address: AsrockIn_ce:9a:f0 (70:85:c2:ce:9a:f0)
  Target IP address: 192.168.10.3
```

e.

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: AsrockIn_ce:9a:f7 (70:85:c2:ce:9a:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ 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:f7 (70:85:c2:ce:9a:f7)
  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: 192.160.10.1
```

4. zadatak:

a. 4

b. ICMP

c. IPv4 protokola

d. Ethernet 1 okvir

e. 192.168.10.2

f. 192.168.10.3

g. (70:85:c2:ce:9a:f7)

h. (70:85:c2:ce:9a:f0)

i. Type: IPv4 (0x0800)

j. Veličina IP adrese je 4 bajta, a MAC adrese je 6 bajta

k. Total length: 60

l. Total length – Header length= 60-20=40

m. Stavimo ICMP u search box

n. 8 ih ima sve ukupno

o. ICMP

p. IP protokola

q. Ethernet 1 okvir

5. zadatak:

The screenshot shows a Wireshark capture of network traffic on an Ethernet interface. The packet list pane displays the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::	ff02::1:ff67:e0a0	ICMPv6	78	Neighbor Solicitation for fe80::e830:9acb:4967:e0a0
2	0.000000	fe80::e830:9acb:4967:e0a0	ff02::2	ICMPv6	62	Router Solicitation
3	0.000000	fe80::e830:9acb:4967:e0a0	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
4	0.086729	192.168.50.25	193.198.184.130	DNS	78	Standard query 0xf5f4 A mihaelarak.from.hr
5	0.086896	192.168.50.25	193.198.184.130	DNS	78	Standard query 0xf5f4 A mihaelarak.from.hr
6	0.088587	193.198.184.130	192.168.50.25	DNS	94	Standard query response 0xf5f4 A mihaelarak.from.hr A 161.53.160.228
7	0.088910	193.198.184.130	192.168.50.25	DNS	94	Standard query response 0xf5f4 A mihaelarak.from.hr A 161.53.160.228
8	0.089372	192.168.50.25	161.53.160.228	HTTP	881	GET /files/2023/09/LV01_Orak.pdf HTTP/1.1
9	0.090890	161.53.160.228	192.168.50.25	TCP	60	80 → 50474 [ACK] Seq=1 Ack=828 Win=501 Len=0
10	0.106495	161.53.160.228	192.168.50.25	HTTP	336	HTTP/1.1 304 Not Modified
11	0.136457	192.168.50.25	193.198.184.130	DNS	81	Standard query 0xf574 A services.bingapis.com
12	0.136612	192.168.50.25	193.198.184.130	DNS	81	Standard query 0xf574 A services.bingapis.com
13	0.137783	193.198.184.130	192.168.50.25	DNS	166	Standard query response 0xf574 A services.bingapis.com CNAME services-bingapis-com.e-0001.e-msedge.net
14	0.138052	193.198.184.130	192.168.50.25	DNS	207	Standard query response 0xf574 A services.bingapis.com CNAME services-bingapis-com.e-0001.e-msedge.net
15	0.138610	192.168.50.25	13.107.5.80	TCP	66	50476 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
16	0.139395	13.107.5.80	192.168.50.25	TCP	66	443 → 50476 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM
17	0.139450	192.168.50.25	13.107.5.80	TCP	54	50476 → 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
18	0.139819	192.168.50.25	13.107.5.80	TLsv1.2	649	Client Hello
19	0.140065	13.107.5.80	192.168.50.25	TCP	60	[TCP Window Update] 443 → 50476 [ACK] Seq=1 Ack=1 Win=262784 Len=0
20	0.140411	13.107.5.80	192.168.50.25	TCP	60	443 → 50476 [ACK] Seq=1 Ack=596 Win=262144 Len=0
21	0.146911	192.168.50.25	161.53.160.228	HTTP	642	GET /favicon.ico HTTP/1.1
22	0.190987	161.53.160.228	192.168.50.25	TCP	60	80 → 50474 [ACK] Seq=283 Ack=1416 Win=501 Len=0
23	0.195810	13.107.5.80	192.168.50.25	TLsv1.2	204	Server Hello, Change Cipher Spec, Encrypted Handshake Message
24	0.196018	192.168.50.25	13.107.5.80	TLsv1.2	105	Change Cipher Spec, Encrypted Handshake Message
25	0.196135	192.168.50.25	13.107.5.80	TLsv1.2	153	Application Data
26	0.196225	192.168.50.25	13.107.5.80	TLsv1.2	339	Application Data
27	0.196253	192.168.50.25	13.107.5.80	TLsv1.2	259	Application Data
28	0.196601	13.107.5.80	192.168.50.25	TCP	60	443 → 50476 [ACK] Seq=151 Ack=647 Win=262720 Len=0
29	0.196791	13.107.5.80	192.168.50.25	TCP	60	443 → 50476 [ACK] Seq=151 Ack=746 Win=262656 Len=0
30	0.196975	13.107.5.80	192.168.50.25	TCP	60	443 → 50476 [ACK] Seq=151 Ack=1031 Win=262464 Len=0
31	0.196975	13.107.5.80	192.168.50.25	TCP	60	443 → 50476 [ACK] Seq=151 Ack=1236 Win=262272 Len=0
32	0.204186	13.107.5.80	192.168.50.25	TLsv1.2	123	Application Data
33	0.204408	192.168.50.25	13.107.5.80	TLsv1.2	92	Application Data
34	0.204910	13.107.5.80	192.168.50.25	TCP	60	443 → 50476 [ACK] Seq=220 Ack=1274 Win=262720 Len=0
35	0.210746	13.107.5.80	192.168.50.25	TLsv1.2	92	Application Data
36	0.255642	192.168.50.25	13.107.5.80	TCP	54	50476 → 443 [ACK] Seq=1274 Ack=258 Win=2102016 Len=0
37	0.352446	13.107.5.80	192.168.50.25	TLsv1.2	568	Application Data, Application Data
38	0.402765	192.168.50.25	13.107.5.80	TCP	54	50476 → 443 [ACK] Seq=1274 Ack=772 Win=2101504 Len=0
39	0.449850	192.168.50.25	13.69.109.130	TCP	55	50264 → 443 [ACK] Seq=1 Ack=1 Win=8207 Len=1 [TCP segment of a reassembled PDU]
40	0.450468	13.69.109.130	192.168.50.25	TCP	60	443 → 50264 [ACK] Seq=1 Ack=2 Win=4106 Len=0
41	0.515344	fe80::e830:9acb:4967:e0a0	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
42	1.015373	fe80::e830:9acb:4967:e0a0	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::e830:9acb:4967:e0a0 (ovr) is at 70:85:c2:ce:9c:17
43	1.459606	161.53.160.228	192.168.50.25	HTTP	540	HTTP/1.1 302 Found
44	1.503757	192.168.50.25	161.53.160.228	TCP	54	50474 → 80 [ACK] Seq=1416 Ack=769 Win=1023 Len=0

The packet details pane for the selected packet (No. 1) shows:

- Ethernet II, Src: ASRockIn_ce:9c:17 (70:85:c2:ce:9c:17), Dst: IPv6mcast_ff:67:e0:a0 (ff02::1:ff67:e0a0)
- Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff67:e0a0

The packet bytes pane shows the raw hex and ASCII representation of the packet.