

Vježba 2: Osnovna analiza mrežnog prometa

Izradili: Marko Sesar i Josip Sremić

PRIPREMA ZA VJEŽBU

1. ARP (Address Resolution Protocol) je protokol koji služi računalima da uz poznatu IP adresu računala saznaju i njegovu MAC adresu.
2. ICMP (Internet Control Message Protocol) je protokol koji omogućuje provjeru pogrešaka i dijagnostiku u pijenosu podataka.
3. Naredba ping je dijagnostički alat koji služi za provjeru dostupnosti pojedinog hosta u mreži.

IZVOĐENJE VJEŽBE

3. a) Wireshark je uhvatio 19 okvira.

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

c) ARP (Address Resolution Protocol) je protokol koji služi računalima da uz poznatu IP adresu računala saznaju i njegovu MAC adresu.

NBNS (NetBIOS Name Service) je protokol koji ima sličnu svrhu kao DNS, odnosno on prevodi adrese koje su čitke ljudima u IP adrese.

MDNS (Multicast DNS) je protokol koji pretvara hostname u IP adresu unutar lokalnih mreža.

LLMNR (Link-Local Multicast Name Resolution) je protokol koji omogućuje hostovima da izvrše razrješenje imena za hostove na istoj lokalnoj vezi.

d) ARP REQUEST:

98	17.089332	AsrockIn_ce:9a:ec	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
100	17.891443	AsrockIn_ce:9a:ec	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
101	18.894284	AsrockIn_ce:9a:ec	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
110	19.928629	AsrockIn_ce:9a:ec	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
114	20.899979	AsrockIn_ce:9a:ec	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
123	21.887897	AsrockIn_ce:9a:ec	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
127	22.921468	AsrockIn_ce:9a:ec	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
136	23.892745	AsrockIn_ce:9a:ec	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
140	24.895590	AsrockIn_ce:9a:ec	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
1	0.000000	AsrockIn_ce:9b:e5	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
74	13.122726	AsrockIn_ce:9b:e5	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
75	13.997194	AsrockIn_ce:9b:e5	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
84	14.996957	AsrockIn_ce:9b:e5	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
146	28.125834	AsrockIn_ce:9b:e5	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3

```
> Frame 98: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: AsrockIn_ce:9a:ec (70:85:c2:ce:9a:ec), 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: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
```

Polazišna MAC adresa: AsrockIn_ce:9a:ec (70:85:c2:ce:9a:ec)

Odredišna MAC adresa: 00:00:00:00:00:00

Polazišna IP adresa: 192.168.10.2

Odredišna IP adresa: 192.168.10.1

ARP REPLY:

140	24.895590	AsrockIn_ce:9a:ec	Broadcast	ARP	60	Who has 192.168.10.1?	Tell 192.168.10.2
1	0.000000	AsrockIn_ce:9b:e5	Broadcast	ARP	42	Who has 192.168.10.1?	Tell 192.168.10.3
74	13.122726	AsrockIn_ce:9b:e5	Broadcast	ARP	42	Who has 192.168.10.1?	Tell 192.168.10.3
75	13.997194	AsrockIn_ce:9b:e5	Broadcast	ARP	42	Who has 192.168.10.1?	Tell 192.168.10.3
84	14.996957	AsrockIn_ce:9b:e5	Broadcast	ARP	42	Who has 192.168.10.1?	Tell 192.168.10.3
146	28.125034	AsrockIn_ce:9b:e5	Broadcast	ARP	42	Who has 192.168.10.1?	Tell 192.168.10.3

>	Frame 74: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
>	Ethernet II, Src: AsrockIn_ce:9b:e5 (70:85:c2:ce:9b:e5), 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: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

Polazišna MAC adresa: AsrockIn_ce:9a:ec (70:85:c2:ce:9a:ec)

Odredišna MAC adresa: 00:00:00:00:00:00

Polazišna IP adresa: 192.168.10.3

Odredišna IP adresa: 192.168.10.1

e) Odredišna MAC adresa kod prvog okvira ARP protokola je 00:00:00:00:00:00 zato što je to broadcast adresa.

4. a) 8 ICMP paketa, 4 zahtjeva i 4 odgovora.

b) ICMP protokol pokreće naredbu ping.

c) ICMP protokol je sastavni dio TCP/IP protokola.

d) IP paket je enkapsuliran u Ethernet okvir.

e) Polazišna IP adresa je: 192.168.10.3

f) Odredišna IP adrea je: 192.168.10.2

g) MAC adresa polazišnog uređaja:

h) MAC adresa odredišnog uređaja

i) vrsta podataka u Ethernet okviru: 0x0607.

j) veličina IP adrese: 4 bajta, veličina MAC adresa u paketima: 6 bajta

k) veličina IP paketa kod ICMP protokola: 60 bajta

l) veličina podataka u IP paketu kod ICMP protokola: 40 bajta

m) Postavi filter da se prati samo ICMP protokol.

5.)

The screenshot shows the Wireshark interface with a list of captured packets. The main pane displays a table of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The details pane below shows the structure of the selected packet (No. 16664), identifying it as an Ethernet II frame with an IPv4 header and an ICMP request.

No.	Time	Source	Destination	Protocol	Length	Info
16643	39.318785	161.53.160.228	192.168.50.15	TCP	60	80 → 49828 [ACK] Seq=1 Ack=440 Win=64128 Len=0
16644	39.318994	161.53.160.228	192.168.50.15	TCP	60	80 → 49829 [ACK] Seq=1 Ack=436 Win=64128 Len=0
16645	39.320357	161.53.160.228	192.168.50.15	TCP	1514	80 → 49828 [ACK] Seq=1 Ack=440 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
16646	39.320358	161.53.160.228	192.168.50.15	HTTP	207	HTTP/1.1 200 OK (text/css)
16647	39.320395	192.168.50.15	161.53.160.228	TCP	54	49828 → 80 [ACK] Seq=440 Ack=1614 Win=262656 Len=0
16648	39.320595	161.53.160.228	192.168.50.15	HTTP	701	HTTP/1.1 200 OK (text/css)
16649	39.344329	192.168.50.15	193.198.184.130	DNS	80	Standard query 0x26d8 A fonts.googleapis.com
16650	39.344438	192.168.50.15	193.198.184.130	DNS	80	Standard query 0xbb14 Unknown (65) fonts.googleapis.com
16651	39.344542	192.168.50.15	193.198.184.130	DNS	67	Standard query 0x1a6c A s.w.org
16652	39.344619	192.168.50.15	193.198.184.130	DNS	67	Standard query 0x5653 Unknown (65) s.w.org
16653	39.345673	193.198.184.130	192.168.50.15	DNS	96	Standard query response 0x26d8 A fonts.googleapis.com A 142.251.209.42
16654	39.345951	193.198.184.130	192.168.50.15	DNS	137	Standard query response 0xbb14 Unknown (65) fonts.googleapis.com SOA ns1.google.com
16655	39.345951	193.198.184.130	192.168.50.15	DNS	83	Standard query response 0x1a6c A s.w.org A 192.0.77.48
16656	39.345951	193.198.184.130	192.168.50.15	DNS	128	Standard query response 0x5653 Unknown (65) s.w.org SOA ns1.wordpress.org
16657	39.371879	192.168.50.15	161.53.160.228	TCP	54	49829 → 80 [ACK] Seq=436 Ack=648 Win=262144 Len=0
16658	39.722870	192.168.50.15	52.123.128.14	TCP	66	49830 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
16659	39.723928	52.123.128.14	192.168.50.15	TCP	66	443 → 49830 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
16660	39.724000	192.168.50.15	52.123.128.14	TCP	54	49830 → 443 [ACK] Seq=1 Ack=1 Win=263424 Len=0
16661	39.724470	192.168.50.15	52.123.128.14	TLSv1.2	571	Client Hello
16662	39.725261	52.123.128.14	192.168.50.15	TCP	60	443 → 49830 [ACK] Seq=1 Ack=518 Win=4194048 Len=0
16663	39.726766	52.123.128.14	192.168.50.15	TCP	1514	443 → 49830 [ACK] Seq=1 Ack=518 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]
16664	39.726991	52.123.128.14	192.168.50.15	TCP	1514	443 → 49830 [ACK] Seq=1461 Ack=518 Win=4194048 Len=1460 [TCP segment of a reassembled PDU]

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: AsrockIn_ce:9b:a8 (70:85:c2:ce:9b:a8), 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:9b:a8 (70:85:c2:ce:9b:a8)
Sender IP address: 192.168.50.24
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.50.18