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.

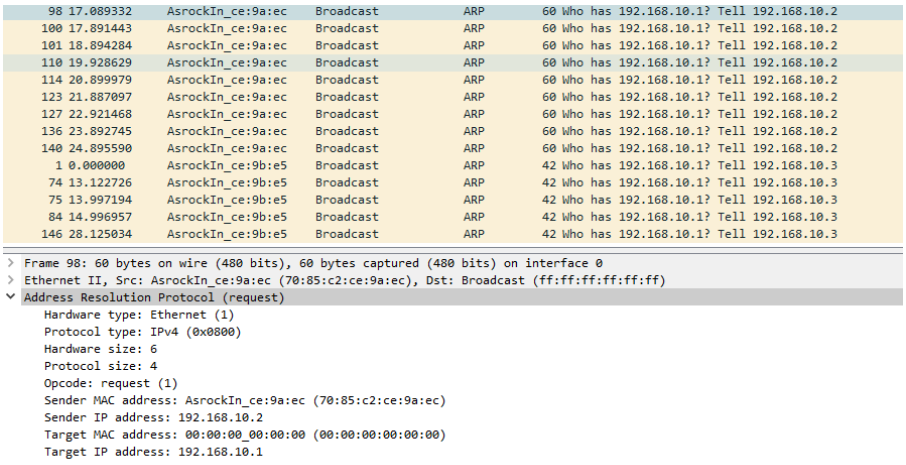
c) ARP (Address Resolution Protocol) je protokol koji služi računalima da uz poznatu IP adresu računala saznaju i njegovu MAC adresu.

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:

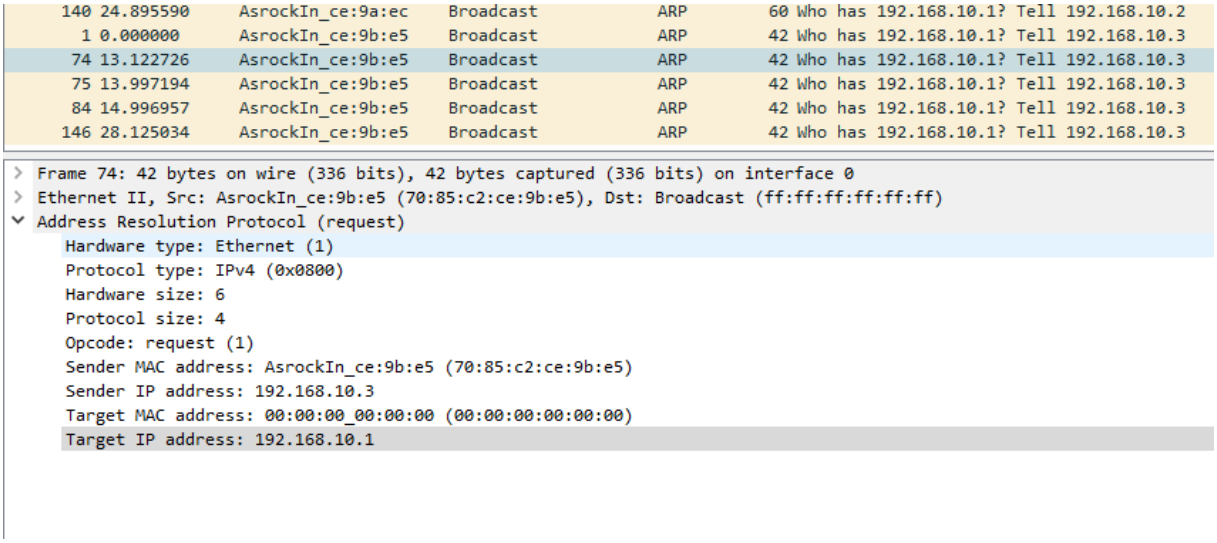


```
    98 17.089332    AsrockIn_ce:9a:ec    Broadcast           ARP         60 Who has 192.168.10.1? Tell 192.168.10.2
   100 17.891443    AsrockIn_ce:9a:ec    Broadcast           ARP         60 Who has 192.168.10.1? Tell 192.168.10.2
   101 18.894284    AsrockIn_ce:9a:ec    Broadcast           ARP         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 21.887097    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 28.125034    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)
v 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:



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.)