Tehnička škola Ruđera Boškovića

Zagreb, Getaldićeva 4

Niko Josipović

Osnovna analiza mrežnog prometa

LABORATORIJSKA VJEŽBA

Zagreb, listopad 2024.

CILJ VJEŽBE

Učenik će znati samostalno pratiti inapraviti osnovnu analizizu prometa na vezi.

PRIPREMA ZA VJEŽBU

1. **Što je i čemu služi protokol ARP?**
   - ARP (Address Resolution Protocol) je komunikacijski protokol kojim se povezuje IP adresa i fiksna fizička adresa nekog uređaja na lokalnoj mreži (LAN) poznata pod nazivom MAC. Iz logičke (IP) adrese se dobiva fizička (MAC) adresa.

2. **Što je i čemu služi protokol ICMP?**
   - ICMP je komunikacijski protokol koji je ugrađen u svaki IP modul kako bi usmjerinicima ili računalima omogućio slanje kontrolnih poruka o greškama. Uloga ICMP je prijavljivanje grešaka, u komunikaciji, **bez njihovog ispravljanja.**

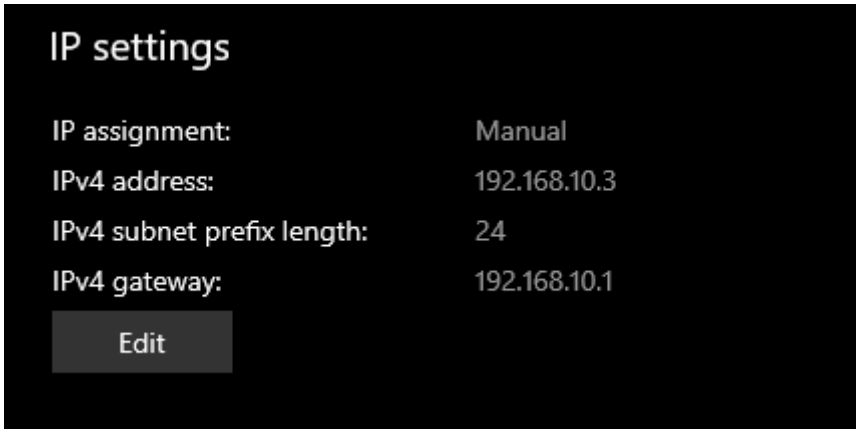
3. **Što znaš o naredbi ping?**
   - Ping je osnovni mrežni alat koji služi za provjeru dostupnosti određenog hosta povezanog u IP mrežu. To postiže slanjem paketa sa ICMP porukom prema odredišnom računalu. Šalje se paket echo request, a iščekuje ICMP echo response.

IZVOĐENJE VJEŽBE

1. Povezati dva susjedna računala u P2P spoj.

2. Konfigurirati računala za rad u mreži, prema tablici:

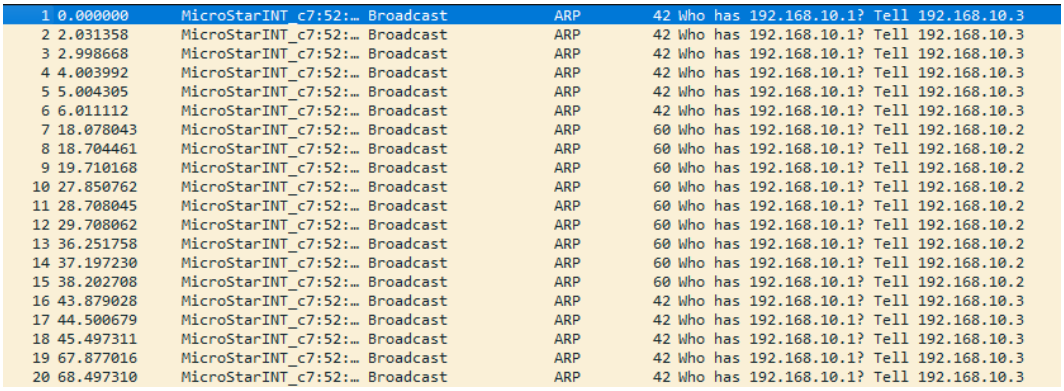
Oznaka na shemi	PC1	PC2
Naziv radne stanice	WSx	WSy
IP adresa	192.168.10.2	192.168.10.3
Subnet maska	255.255.255.0	255.255.255.0
Default Gateway	192.168.10.1	192.168.10.1



3. Pokrenuti program Wireshark. Pričekati da se prikaže prvih dvadesetak redaka, a onda zaustaviti hvatanje (Capture – Stop).

a) Koliko je točno okvira Wireshark „uhvatio“?

- 20 okvir



1	0.000000	MicroStarINT_c7:52:…	Broadcast	ARP	42 Who has 192.168.10.1? Tell 192.168.10.3
2	2.031358	MicroStarINT_c7:52:…	Broadcast	ARP	42 Who has 192.168.10.1? Tell 192.168.10.3
3	2.998668	MicroStarINT_c7:52:…	Broadcast	ARP	42 Who has 192.168.10.1? Tell 192.168.10.3
4	4.003992	MicroStarINT_c7:52:…	Broadcast	ARP	42 Who has 192.168.10.1? Tell 192.168.10.3
5	5.004305	MicroStarINT_c7:52:…	Broadcast	ARP	42 Who has 192.168.10.1? Tell 192.168.10.3
6	6.011112	MicroStarINT_c7:52:…	Broadcast	ARP	42 Who has 192.168.10.1? Tell 192.168.10.3
7	18.078043	MicroStarINT_c7:52:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.2
8	18.704461	MicroStarINT_c7:52:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.2
9	19.710168	MicroStarINT_c7:52:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.2
10	27.850762	MicroStarINT_c7:52:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.2
11	28.708045	MicroStarINT_c7:52:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.2
12	29.708062	MicroStarINT_c7:52:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.2
13	36.251758	MicroStarINT_c7:52:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.2
14	37.197230	MicroStarINT_c7:52:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.2
15	38.202708	MicroStarINT_c7:52:…	Broadcast	ARP	60 Who has 192.168.10.1? Tell 192.168.10.2
16	43.879028	MicroStarINT_c7:52:…	Broadcast	ARP	42 Who has 192.168.10.1? Tell 192.168.10.3
17	44.500679	MicroStarINT_c7:52:…	Broadcast	ARP	42 Who has 192.168.10.1? Tell 192.168.10.3
18	45.497311	MicroStarINT_c7:52:…	Broadcast	ARP	42 Who has 192.168.10.1? Tell 192.168.10.3
19	67.877016	MicroStarINT_c7:52:…	Broadcast	ARP	42 Who has 192.168.10.1? Tell 192.168.10.3
20	68.497310	MicroStarINT_c7:52:…	Broadcast	ARP	42 Who has 192.168.10.1? Tell 192.168.10.3

b) Koje su oznake protokola na tim okvirima?

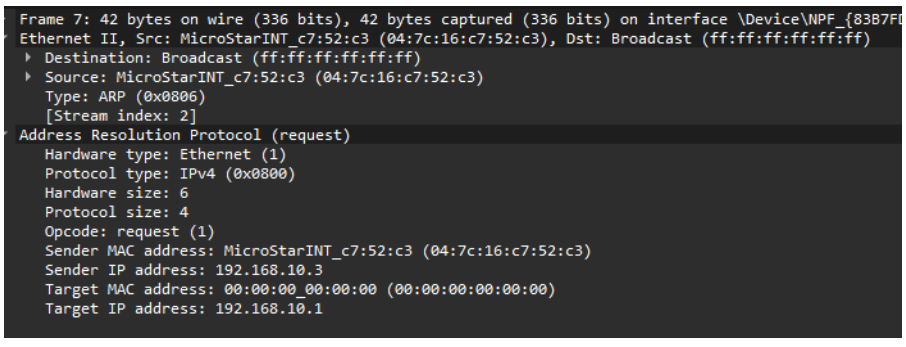
- ARP protokol

c) Koristeći dostupne informacije sa predavanja/Interneta opiši kratko funkcije tih protokola.

- ARP je komunikacijski protokol kojim se povezuje IP adresa i fiksna fizička adresa nekog uređaja na lokalnoj mreži (LAN) poznata pod nazivom MAC. Iz logičke (IP) adrese se dobiva fizička (MAC) adresa

d) Analiziraj okvir koji u sebi nosi:

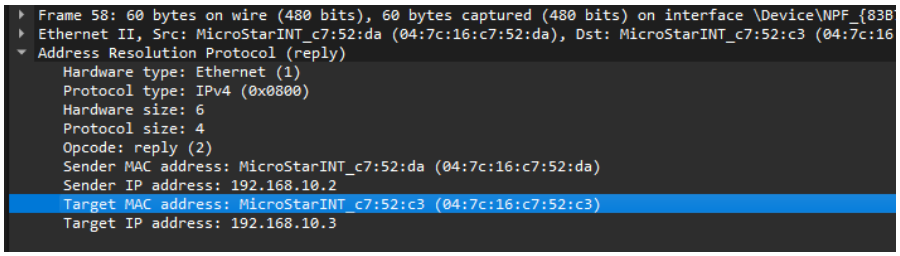
ARP paket (protokol) request te ispiši:



```
Frame 7: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{83B7F
Ethernet II, Src: MicroStarINT_c7:52:c3 (04:7c:16:c7:52:c3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: MicroStarINT_c7:52:c3 (04:7c:16:c7:52:c3)
    Type: ARP (0x0806)
    [Stream index: 2]
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: MicroStarINT_c7:52:c3 (04:7c:16:c7:52:c3)
    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
```

- polazišnu MAC adresu: **04:7c:16:c7:52:c3**
- odredišnu MAC adresu: **ff:ff:ff:ff:ff:ff (broadcast)**
- polazišnu IP adresu: **192.168.10.3**
- odredišnu IP adresu: **192.168.10.1**

ARP paket (protokol) reply te ispiši:



- polazišnu MAC adresu: **04:7c:16:c7:52:da**
- odredišnu MAC adresu: **04:7c:16:c7:52:c3**
- Kolika je veličina svake od ovih adresa? **6 bajta**
- polazišnu IP adresu: **192.168.10.2**
- odredišnu IP adresa: **192.168.10.3**

4. U istom spoju računala pomoću Wiresharka analiziraj ICMP promet korištenjem naredbe ping sa jednog računala na drugo.

a) Koliko je ICMP echo i reply paketa?

- Ima **osam** ICMP echo i reply paketa

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request
2	0.000536	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply
3	1.005244	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request
4	1.005716	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply
5	2.015927	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request
6	2.016356	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply
7	3.035222	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request
8	3.035731	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply

b) Koji protokol pokreće naredba ping?

- ICMP

c) Koji protokol pokreće naredba ping?

- IP protokol

d) Koji protokol pokreće naredba ping?

- Enkapsuliran u Ethernet II. Paket

Izaberi jedan redak koji se odnosi na protokol ICMP, ispiši njegov sadržaj te odgovori na slijedeća pitanja:

e) Koja je polazišna IP adresa?

- Polazišna IP adresa: 192.168.10.2

f) Koja je odredišna IP adresa?

- Odredišna IP adresa: 192.168.10.3

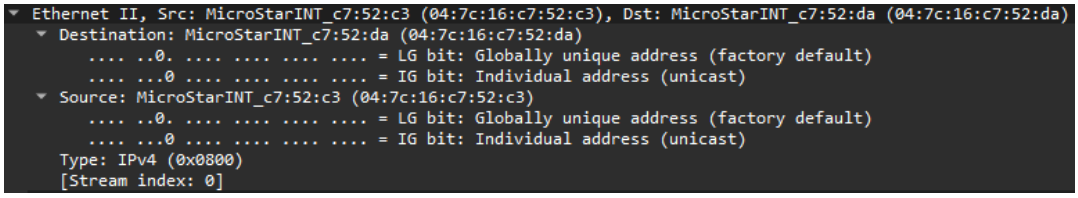
g) Koja je MAC adresa polazišnog uređaja?

- 04:7c:16:c7:52:c3

h) Koja je MAC adresa odredišnog uređaja?

- 04:7c:16:c7:52:da

i) Koja je oznaka vrste podataka u Ethernet okviru?



- Vrsta podataka: Ipv4 (0x0800)

j) Koja je veličina IP adrese, a koja MAC adrese u okvirima/paketima?

- IP adrese je 4 bajta, a MAC adrese 6 bajta

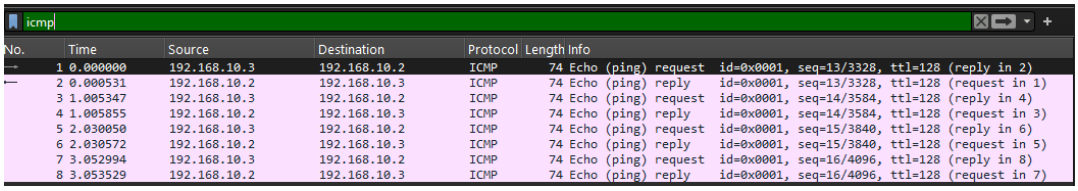
k) Koja je veličina IP paketa kod ICMP protokola?

- 60 bajta („Total lenght“)

l) Koja je veličina podataka u IP paketu kod ICMP protokola?

- 40 bajta -> „Total lenght“ - „Header lenght“

m) Postavi filter da se prati samo ICMP protokol.



5. Računala ponovno spojiti u školsku mrežu i provjeriti mrežne postavke. Učitati tri web stranice i pratiti promet na vezi pomoću alata Wireshark računala na drugo.