Marko Gregl, Borna Kolak 3.C

LV-02 Osnovna analiza mrežnog prometa

Priprema za vježbu

U pisanoj formi odgovori na slijedeća pitanja:

1. Što je i čemu služi protokol ARP?

ARP (eng. Address Resolution Protocol) je protokol koji se koristi za mapiranje IP adresa na MAC adrese unutar lokalne mreže. Služi za otkrivanje MAC adresa drugih uređaja kako bi se omogućilo slanje okvira na odgovarajuće odredište.

2. Što je i čemu služi protokol ICMP?

ICMP (eng. Internet Control Message Protocol) je protokol koji se koristi za razmjenu kontrolnih poruka i obavještenja između računala u mreži. Služi za dijagnostiku i upravljanje mrežom te omogućava informiranje o greškama i dostupnosti u mreži.

3. Što znaš o naredbi ping?

Naredba ping se koristi za provjeru dostupnosti računala ili uređaja u mreži putem ICMP zahtjeva. Šalje ICMP "echo request" pakete ciljnom uređaju i očekuje "echo reply" pakete kao odgovor. Koristi se za testiranje povezanosti i latencije u mreži.

IZVOĐENJE VJEŽBE

1. zadatak

Povezati dva susjedna računala odgovarajućim kabelom te uspostaviti P2P spoj.

Topologija:

2. zadatak

Konfigurirati računala za rad u mreži, pri čemu koristiti adresnu shemu prema tablici:

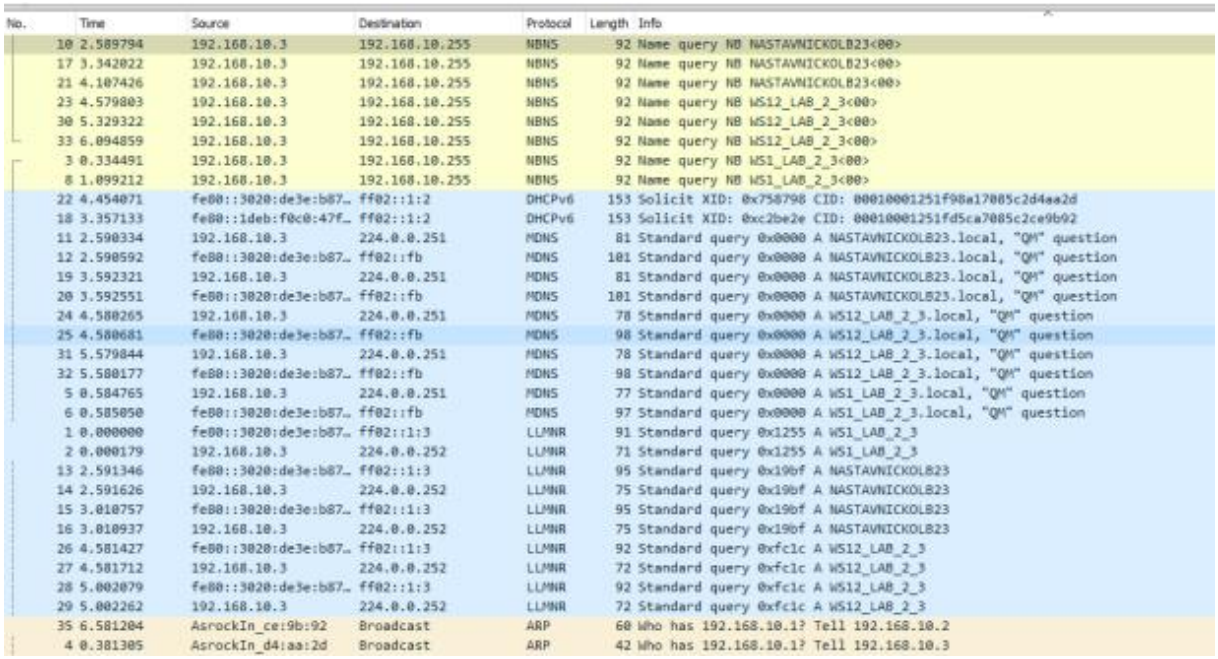
Oznaka na shemi	PC1	PC2
Naziv radne stanice	WSx	WSy
IP adresa	192.168.10.2	192.168.10.3
Subnet maska	255.255.255.0	255.255.255.0
Default Gateway	192.168.10.1	192.168.10.1

3. zadatak

Pokrenuti program Wireshark.

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

a) Koliko je točno okvira Wireshark „uhvatio“?



No.	Time	Source	Destination	Protocol	Length	Info
10	2.589794	192.168.10.3	192.168.10.255	NBNS	92	Name query NB NASTAVNICKOLB23<00>
17	3.342022	192.168.10.3	192.168.10.255	NBNS	92	Name query NB NASTAVNICKOLB23<00>
21	4.107426	192.168.10.3	192.168.10.255	NBNS	92	Name query NB NASTAVNICKOLB23<00>
23	4.579803	192.168.10.3	192.168.10.255	NBNS	92	Name query NB WS12_LAB_2_3<00>
30	5.329322	192.168.10.3	192.168.10.255	NBNS	92	Name query NB WS12_LAB_2_3<00>
33	6.094859	192.168.10.3	192.168.10.255	NBNS	92	Name query NB WS12_LAB_2_3<00>
3	0.334491	192.168.10.3	192.168.10.255	NBNS	92	Name query NB WS1_LAB_2_3<00>
8	1.099212	192.168.10.3	192.168.10.255	NBNS	92	Name query NB WS1_LAB_2_3<00>
22	4.454071	fe80::3020:de3e:b87…	ff02::1:2	DHCPv6	153	Solicit XID: 0x758798 CID: 00010001251f98a17085c2d4aa2d
18	3.357133	fe80::1deb:f0c0:47f…	ff02::1:2	DHCPv6	153	Solicit XID: 0xc2be2e CID: 00010001251fd5ca7085c2ce9b92
11	2.590334	192.168.10.3	224.0.0.251	MDNS	81	Standard query 0x0000 A NASTAVNICKOLB23.local, "QM" question
12	2.590592	fe80::3020:de3e:b87…	ff02::fb	MDNS	101	Standard query 0x0000 A NASTAVNICKOLB23.local, "QM" question
19	3.592321	192.168.10.3	224.0.0.251	MDNS	81	Standard query 0x0000 A NASTAVNICKOLB23.local, "QM" question
20	3.592551	fe80::3020:de3e:b87…	ff02::fb	MDNS	101	Standard query 0x0000 A NASTAVNICKOLB23.local, "QM" question
24	4.580265	192.168.10.3	224.0.0.251	MDNS	78	Standard query 0x0000 A WS12_LAB_2_3.local, "QM" question
25	4.580681	fe80::3020:de3e:b87…	ff02::fb	MDNS	98	Standard query 0x0000 A WS12_LAB_2_3.local, "QM" question
31	5.579844	192.168.10.3	224.0.0.251	MDNS	78	Standard query 0x0000 A WS12_LAB_2_3.local, "QM" question
32	5.580177	fe80::3020:de3e:b87…	ff02::fb	MDNS	98	Standard query 0x0000 A WS12_LAB_2_3.local, "QM" question
5	0.584765	192.168.10.3	224.0.0.251	MDNS	77	Standard query 0x0000 A WS1_LAB_2_3.local, "QM" question
6	0.585050	fe80::3020:de3e:b87…	ff02::fb	MDNS	97	Standard query 0x0000 A WS1_LAB_2_3.local, "QM" question
1	0.000000	fe80::3020:de3e:b87…	ff02::1:3	LLMNR	91	Standard query 0x1255 A WS1_LAB_2_3
2	0.000179	192.168.10.3	224.0.0.252	LLMNR	71	Standard query 0x1255 A WS1_LAB_2_3
13	2.591346	fe80::3020:de3e:b87…	ff02::1:3	LLMNR	95	Standard query 0x19bf A NASTAVNICKOLB23
14	2.591626	192.168.10.3	224.0.0.252	LLMNR	75	Standard query 0x19bf A NASTAVNICKOLB23
15	3.010757	fe80::3020:de3e:b87…	ff02::1:3	LLMNR	95	Standard query 0x19bf A NASTAVNICKOLB23
16	3.010937	192.168.10.3	224.0.0.252	LLMNR	75	Standard query 0x19bf A NASTAVNICKOLB23
26	4.581427	fe80::3020:de3e:b87…	ff02::1:3	LLMNR	92	Standard query 0xfc1c A WS12_LAB_2_3
27	4.581712	192.168.10.3	224.0.0.252	LLMNR	72	Standard query 0xfc1c A WS12_LAB_2_3
28	5.002079	fe80::3020:de3e:b87…	ff02::1:3	LLMNR	92	Standard query 0xfc1c A WS12_LAB_2_3
29	5.002262	192.168.10.3	224.0.0.252	LLMNR	72	Standard query 0xfc1c A WS12_LAB_2_3
35	6.581204	AsrockIn_ce:9b:92	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
4	0.381305	AsrockIn_d4:aa:2d	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3

Wireshark je uhvatio 32 okvira

b) Koje su oznake protokola na tim okvirima?

Oznake protokola na tim okvirima su NBNS, DHCPv6, MDNS, LLMNR, ARP

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

ARP je komunikacijski protokol kojim se dobiva fizička adresa na lokalnoj mreži iz

poznate mrežne adrese

NBNS je protokol za „name resolution“. Protokol je jednak kao i LLMNR, ali koristi UDP

paket umjesto Multicast paketa. Pretraživači se njime koriste nakon što korištenje LLMNR

protokola nije uspjelo.

d) Analiziraj okvir koji u sebi nosi:

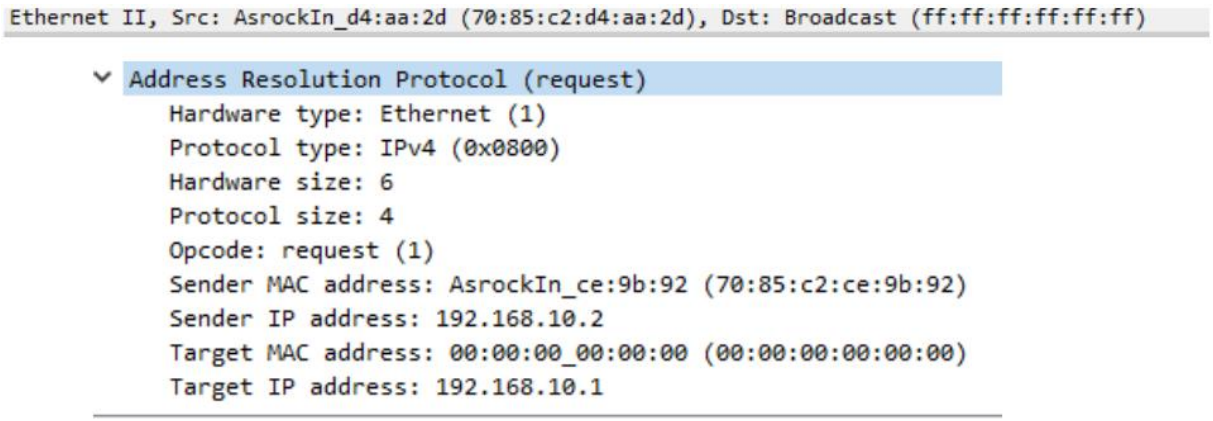
ARP paket (protokol) request te ispiši:

- polazišnu MAC adresu

- odredišnu MAC adresu

- polazišnu IP adresu

- odredišnu IP adresu



ARP paket (protokol) – reply te ispiši:

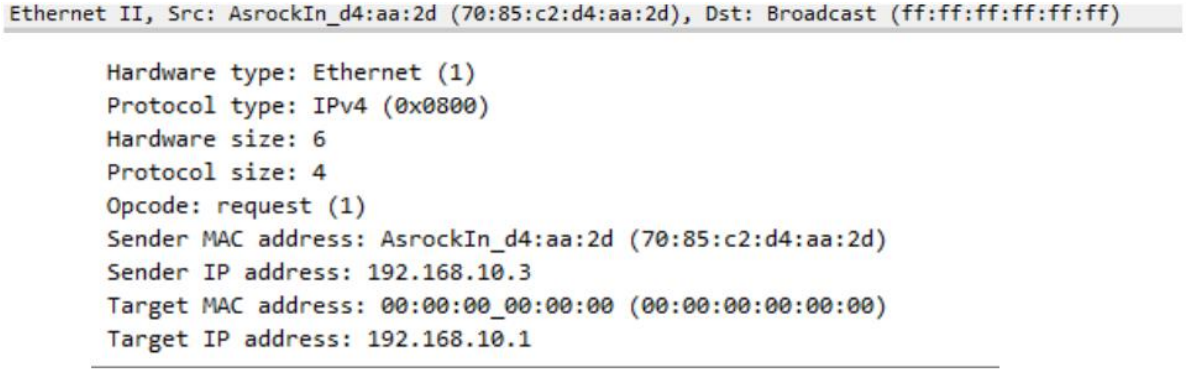
- polazišnu MAC adresu

- odredišnu MAC adresu

- Kolika je veličina svake od ovih adresa?

- polazišnu IP adresu

- odredišnu IP adresu



e) Kako glasi odredišna MAC adresa prvog Ethernet okvira kod ARP protokola i zašto?

Odredišna MAC adresa prvog Ethernet okvira kod ARP protokola će biti "broadcast"

(FF:FF:FF:FF:FF:FF) jer se ARP zahtjev šalje svim uređajima u mreži kako bi se pronašla

odgovarajuća MAC adresa.

4. zadatak

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?

8 su ICMP echo i reply paketa , 4 odgovora i 4 zahtjeva

b) Koji protokol pokreće naredba ping?

Naredba ping pokreće ICMP protokol.

c) Sastavni dio kojeg protokola je ICMP protokol?

ICMP je sastavni dio IP protokola.

d) U koji okvir je enkapsuliran IP paket?

IP paket je enkapsuliran u Ethernet okvir.

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

e) Koja je polazišna IP adresa?

```
Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.10.3
```

f) Koja je odredišna IP adresa?

```
Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.10.3
```

g) Koja je MAC adresa polazišnog uređaja?

```
Ethernet II, Src: AsrockIn_ce:9b:92 (70:85:c2:ce:9b:92), Dst: AsrockIn_d4:aa:2d (70:85:c2:d4:aa:2d)
```

h) Koja je MAC adresa odredišnog uređaja?

```
Ethernet II, Src: AsrockIn_ce:9b:92 (70:85:c2:ce:9b:92), Dst: AsrockIn_d4:aa:2d (70:85:c2:d4:aa:2d)
```

i) Koja je oznaka vrste podataka u Ethernet okviru?

```
▾ Ethernet II, Src: AsrockIn_d4:aa:2d (70:85:c2:d4:aa:2d), Dst: AsrockIn_ce:9b:92 (70:85:c2:ce:9b:92)
  › Destination: AsrockIn_ce:9b:92 (70:85:c2:ce:9b:92)
  › Source: AsrockIn_d4:aa:2d (70:85:c2:d4:aa:2d)
    Type: IPv4 (0x0800)
```

IPv4 0x0800 označava IPv4 paket dok 0x0806 označava ARP paket

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

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

k) Koja je veličina IP paketa kod ICMP protokola?

Veličina IP paketa kod ICMP protokola je 60 bajta

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

Veličina podataka u IP paketu je 40

5. Zadatak

Računala ponovno spojiti u školsku mrežu i provjeriti mrežne postavke.