TEHNIČKA ŠKOLA
RUĐERA BOŠKOVIĆA
Zagreb, Getaldićeva 4

Nastavni predmet	RAČUNALNE MREŽE_3H
Naslov cjeline	Djelovanje u mrežnom sloju
Naslov jedinice	Vježba 2: Osnovna analiza mrežnog prometa

Marko Dalić i Filip Ćorković, 3.C

PRIPREMA ZA VJEŽBU

1. **Što je i čemu služi protokol ARP?**
   ARP protokol (Address Resolution Protocol) je komunikacijski protokol za određivanje fizičkih adresa.
2. **Što je i čemu služi protokol ICMP?**
   Ugrađen u svaki IP modul kako bi usmjernicima i računalima omogućio slanje kontrolnih poruka o greškama, ne osigurava pouzdan prijenos podataka.
3. **Što znaš o naredbi ping?**

   Ping je administrativna funkcija koja služi za provjeru dostupnosti poslužitelja na računalnim mrežama temeljenim na IP protokolu.

IZVOĐENJE VJEŽBE

- Pokrenuti program za praćenje protokola Wireshark ✓
- Odabrati mrežnu karticu na kojoj će se pratiti promet podataka ✓
- Pokrenuti praćenje prometa na mrežnoj kartici ✓

1. zadatak

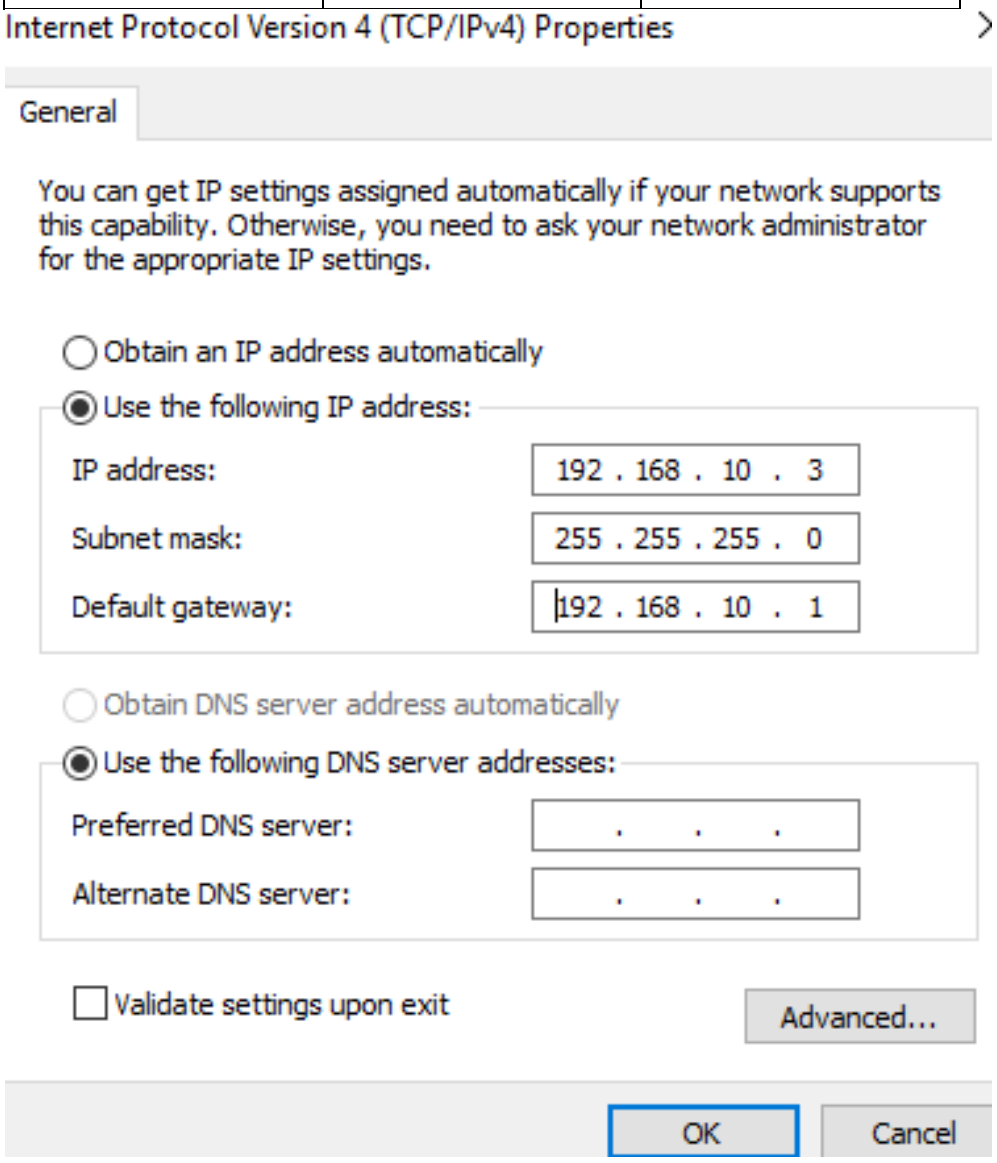
Povezati dva susjedna računala odgovarajućim kabelom te uspostaviti P2P spoj. ✓

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

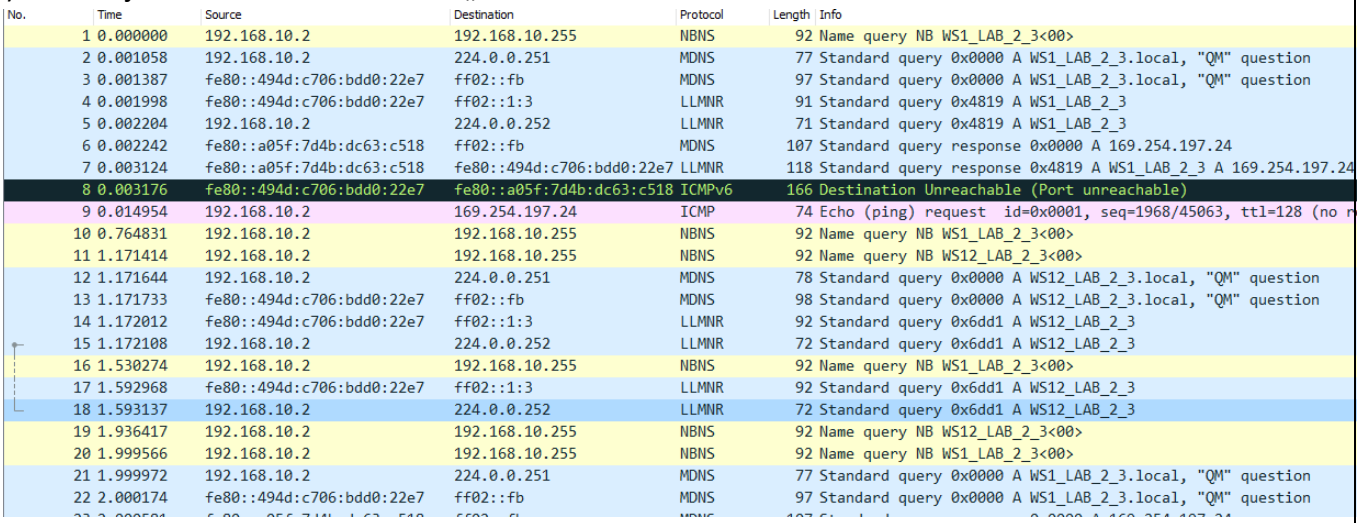


3. zadatak

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
1	0.000000	192.168.10.2	192.168.10.255	NBNS	92	Name query NB WS1_LAB_2_3<00>
2	0.001058	192.168.10.2	224.0.0.251	MDNS	77	Standard query 0x0000 A WS1_LAB_2_3.local, "QM" question
3	0.001387	fe80::494d:c706:bdd0:22e7	ff02::fb	MDNS	97	Standard query 0x0000 A WS1_LAB_2_3.local, "QM" question
4	0.001998	fe80::494d:c706:bdd0:22e7	ff02::1:3	LLMNR	91	Standard query 0x4819 A WS1_LAB_2_3
5	0.002204	192.168.10.2	224.0.0.252	LLMNR	71	Standard query 0x4819 A WS1_LAB_2_3
6	0.002242	fe80::a05f:7d4b:dc63:c518	ff02::fb	MDNS	107	Standard query response 0x0000 A 169.254.197.24
7	0.003124	fe80::a05f:7d4b:dc63:c518	fe80::494d:c706:bdd0:22e7	LLMNR	118	Standard query response 0x4819 A WS1_LAB_2_3 A 169.254.197.24
8	0.003176	fe80::494d:c706:bdd0:22e7	fe80::a05f:7d4b:dc63:c518	ICMPv6	166	Destination Unreachable (Port unreachable)
9	0.014954	192.168.10.2	169.254.197.24	ICMP	74	Echo (ping) request id=0x0001, seq=1968/45063, ttl=128 (no r
10	0.764831	192.168.10.2	192.168.10.255	NBNS	92	Name query NB WS1_LAB_2_3<00>
11	1.171414	192.168.10.2	192.168.10.255	NBNS	92	Name query NB WS12_LAB_2_3<00>
12	1.171644	192.168.10.2	224.0.0.251	MDNS	78	Standard query 0x0000 A WS12_LAB_2_3.local, "QM" question
13	1.171733	fe80::494d:c706:bdd0:22e7	ff02::fb	MDNS	98	Standard query 0x0000 A WS12_LAB_2_3.local, "QM" question
14	1.172012	fe80::494d:c706:bdd0:22e7	ff02::1:3	LLMNR	92	Standard query 0x6dd1 A WS12_LAB_2_3
15	1.172108	192.168.10.2	224.0.0.252	LLMNR	72	Standard query 0x6dd1 A WS12_LAB_2_3
16	1.530274	192.168.10.2	192.168.10.255	NBNS	92	Name query NB WS1_LAB_2_3<00>
17	1.592968	fe80::494d:c706:bdd0:22e7	ff02::1:3	LLMNR	92	Standard query 0x6dd1 A WS12_LAB_2_3
18	1.593137	192.168.10.2	224.0.0.252	LLMNR	72	Standard query 0x6dd1 A WS12_LAB_2_3
19	1.936417	192.168.10.2	192.168.10.255	NBNS	92	Name query NB WS12_LAB_2_3<00>
20	1.999566	192.168.10.2	192.168.10.255	NBNS	92	Name query NB WS1_LAB_2_3<00>
21	1.999972	192.168.10.2	224.0.0.251	MDNS	77	Standard query 0x0000 A WS1_LAB_2_3.local, "QM" question
22	2.000174	fe80::494d:c706:bdd0:22e7	ff02::fb	MDNS	97	Standard query 0x0000 A WS1_LAB_2_3.local, "QM" question

b) Koje su oznake protokola na tim okvirima?

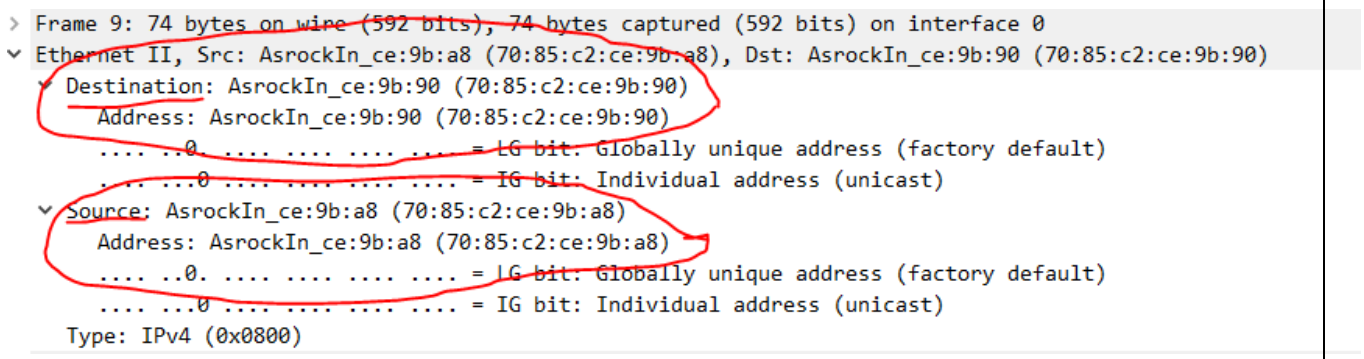
MBNS i ARP

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

ARP - komunikacijski protokol kojim se dobiva fizička adresa na lokalnoj mreži iz poznate mrežene adrese

NBNS - protokol za "name resolution"; protokol je jednak kao i LLMNR, ali koristi UDP pakete umjesto multicast paketa. Pretaržívači 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: 70:85:c2:ce:9b:90
- odredišnu MAC adresu: 70:85:c2:ce:9b:a8
- polazišnu IP adresu: 192.168.10.2
- odredišnu IP adresu: 192.168.10.1

ARP paket (protokol) – reply te ispiši:

- polazišnu MAC adresu
- odredišnu MAC adresu
- Kolika je veličina svake od ovih adresa?
- polazišnu IP adresu 192.168.10.2
- odredišnu IP adresu : 192.168.10.1

e) Kako glasi odredišna MAC adresa prvog Ethernet okvira kod ARP protokola i zašto?
ff:ff:ff:ff:ff:ff, kako bi pronašao mrežne adrese drugih računala

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

b) Koji protokol pokreće naredba ping?
ICMP

c) Sastavni dio kojeg protokola je ICMP protokol?
IP

d) U koji okvir je enkapsuliran IP paket?

Ethernet

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

e) Koja je polazišna IP adresa?
192.168.10.2

f) Koja je odredišna IP adresa?

192.168.10.3

g) Koja je MAC adresa polazišnog uređaja?
70:85:c2:ce:9b:90

h) Koja je MAC adresa odredišnog uređaja?
70:85:c2:ce:9b:a8

i) Koja je oznaka vrste podataka u Ethernet okviru?
0x0800

j) Koja je veličina IP adrese, a koja MAC adrese u okvirima/paketima?
MAC adresa - 6 bajtova
IP adresa – 4 bajta

k) Koja je veličina IP paketa kod ICMP protokola?
60 bajtova

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

e) Postavi filter da se prati samo ICMP protokol. ✓

f) Koliko je ICMP echo i reply paketa?
8 ICMP paketa, 4 zahtjeva i 4 odgovora

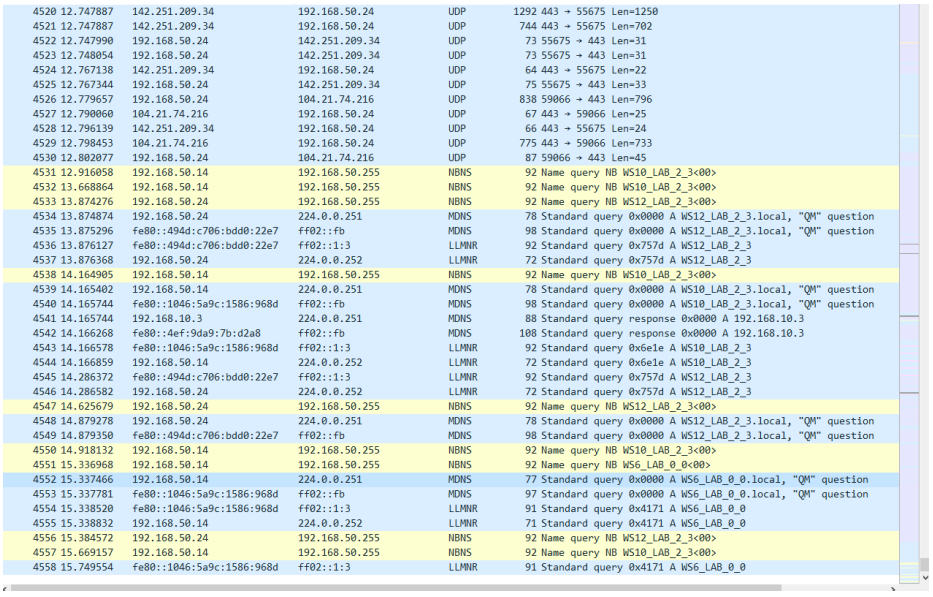
g) Koji protokol pokreće naredba ping?
ICMP

h) Sastavni dio kojeg protokola je protokol ICMP?
IP

i) U koji okvir je enkapsuliran IP paket?
U ethernet II. paket

5. Zadatak

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



4520	12.747887	142.251.209.34	192.168.50.24	UDP	1292 443 → 55675 Len=1250
4521	12.747887	142.251.209.34	192.168.50.24	UDP	744 443 → 55675 Len=702
4522	12.747990	192.168.50.24	142.251.209.34	UDP	73 55675 → 443 Len=31
4523	12.748054	192.168.50.24	142.251.209.34	UDP	73 55675 → 443 Len=31
4524	12.767138	142.251.209.34	192.168.50.24	UDP	64 443 → 55675 Len=22
4525	12.767344	192.168.50.24	142.251.209.34	UDP	75 55675 → 443 Len=33
4526	12.779657	192.168.50.24	104.21.74.216	UDP	838 59066 → 443 Len=796
4527	12.790060	104.21.74.216	192.168.50.24	UDP	67 443 → 59066 Len=25
4528	12.796139	142.251.209.34	192.168.50.24	UDP	66 443 → 55675 Len=24
4529	12.798453	104.21.74.216	192.168.50.24	UDP	775 443 → 59066 Len=733
4530	12.802077	192.168.50.24	104.21.74.216	UDP	87 59066 → 443 Len=45
4531	12.916058	192.168.50.14	192.168.50.255	NBNS	92 Name query NB WS10_LAB_2_3<00>
4532	13.668864	192.168.50.14	192.168.50.255	NBNS	92 Name query NB WS10_LAB_2_3<00>
4533	13.874276	192.168.50.24	192.168.50.255	NBNS	92 Name query NB WS12_LAB_2_3<00>
4534	13.874874	192.168.50.24	224.0.0.251	MDNS	78 Standard query 0x0000 A WS12_LAB_2_3.local, "QM" question
4535	13.875296	fe80::494d:c706:bdd0:22e7	ff02::fb	MDNS	98 Standard query 0x0000 A WS12_LAB_2_3.local, "QM" question
4536	13.876127	fe80::494d:c706:bdd0:22e7	ff02::1:3	LLMNR	92 Standard query 0x757d A WS12_LAB_2_3
4537	13.876368	192.168.50.24	224.0.0.252	LLMNR	72 Standard query 0x757d A WS12_LAB_2_3
4538	14.164905	192.168.50.14	192.168.50.255	NBNS	92 Name query NB WS10_LAB_2_3<00>
4539	14.165402	192.168.50.14	224.0.0.251	MDNS	78 Standard query 0x0000 A WS10_LAB_2_3.local, "QM" question
4540	14.165744	fe80::1046:5a9c:1586:968d	ff02::fb	MDNS	98 Standard query 0x0000 A WS10_LAB_2_3.local, "QM" question
4541	14.165744	192.168.10.3	224.0.0.251	MDNS	88 Standard query response 0x0000 A 192.168.10.3
4542	14.166268	fe80::4ef:9da9:7b:d2a8	ff02::fb	MDNS	108 Standard query response 0x0000 A 192.168.10.3
4543	14.166578	fe80::1046:5a9c:1586:968d	ff02::1:3	LLMNR	92 Standard query 0x6e1e A WS10_LAB_2_3
4544	14.166859	192.168.50.14	224.0.0.252	LLMNR	72 Standard query 0x6e1e A WS10_LAB_2_3
4545	14.286372	fe80::494d:c706:bdd0:22e7	ff02::1:3	LLMNR	92 Standard query 0x757d A WS12_LAB_2_3
4546	14.286582	192.168.50.24	224.0.0.252	LLMNR	72 Standard query 0x757d A WS12_LAB_2_3
4547	14.625679	192.168.50.24	192.168.50.255	NBNS	92 Name query NB WS12_LAB_2_3<00>
4548	14.879278	192.168.50.24	224.0.0.251	MDNS	78 Standard query 0x0000 A WS12_LAB_2_3.local, "QM" question
4549	14.879350	fe80::494d:c706:bdd0:22e7	ff02::fb	MDNS	98 Standard query 0x0000 A WS12_LAB_2_3.local, "QM" question
4550	14.918132	192.168.50.14	192.168.50.255	NBNS	92 Name query NB WS10_LAB_2_3<00>
4551	15.336968	192.168.50.14	192.168.50.255	NBNS	92 Name query NB WS6_LAB_0_0<00>
4552	15.337466	192.168.50.14	224.0.0.251	MDNS	77 Standard query 0x0000 A WS6_LAB_0_0.local, "QM" question
4553	15.337781	fe80::1046:5a9c:1586:968d	ff02::fb	MDNS	97 Standard query 0x0000 A WS6_LAB_0_0.local, "QM" question
4554	15.338520	fe80::1046:5a9c:1586:968d	ff02::1:3	LLMNR	91 Standard query 0x4171 A WS6_LAB_0_0
4555	15.338832	192.168.50.14	224.0.0.252	LLMNR	71 Standard query 0x4171 A WS6_LAB_0_0
4556	15.384572	192.168.50.24	192.168.50.255	NBNS	92 Name query NB WS12_LAB_2_3<00>
4557	15.669157	192.168.50.14	192.168.50.255	NBNS	92 Name query NB WS10_LAB_2_3<00>
4558	15.749554	fe80::1046:5a9c:1586:968d	ff02::1:3	LLMNR	91 Standard query 0x4171 A WS6_LAB_0_0