

RAČUNALNE MREŽE

UPUTE ZA LABORATORIJSKE VJEŽBE

UVOD: PACKET TRACER

Uslijed novonastale situacije uzrokovane epidemijom COVID-19 osmišljen je online ekvivalent laboratorijskih vježbi iz kolegija Računalne mreže (RM). Simulacijsko okruženje Packet Tracer (PT) odabrano je radi jednostavnosti korištenja i široke raspoloživosti u svrhu edukacije.

UPUTE ZA INSTALACIJU

Za praćenje online vježbi iz RM potrebno je instalirati simulator PT na svoje računalo. To je program tvrtke Cisco koji služi za simuliranje rada mreže i mrežnih uređaja (računala, switchevi, routeri, bežične pristupne točke i sl.).

Kako je navedeno na web-stranicama Cisco Networking Akademije [1], PT možete instalirati na računalo nakon što se besplatno registrirate i odslušate uvodni tečaj koji će vas upoznati sa osnovama korištenja simulatora [2]. Nije potrebno detaljno odslušati tečaj, nego ga samo "proletjeti" naredbom "next", jer ćemo na uvodnoj laboratorijskoj vježbi naučiti sve najbitnije što ćemo koristiti tijekom semestra.

Ukoliko želite, starije verzije programa možete skinuti (bez tečaja) sa web-stranice [3].

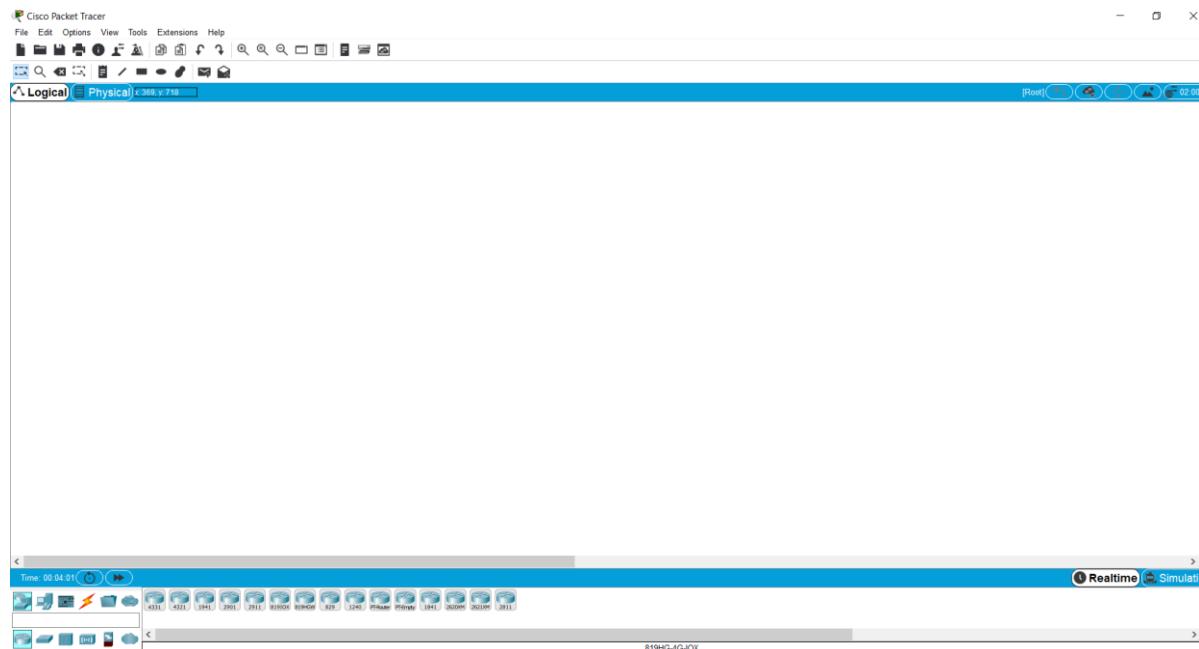
Kada se ulogirate u svoj kreirani account (nakon besplatne registracije), omogućit će vam se pristup My NetAcad dashboard-u sa tečajem, a mogućnost preuzimanja i instalacije alata PT nalazi se na tabu Resources → Download Packet Tracer. Ova verzija uputa za laboratorijske vježbe temelji se na Packet Tracer-u 7.3.0. iz 2019. godine.

The screenshot shows the Cisco Networking Academy website. At the top, there's a navigation bar with links for Networking Academy, My NetAcad, Resources, Courses, Careers, and More. A search bar and user profile information for 'Marina' are also at the top right. Below the navigation, there's a breadcrumb trail: Home / Resources / Download Cisco Packet Tracer. A dropdown menu is open over the 'Resources' link, showing options like 'Certification Exams & Discounts', 'Find an Academy', 'Download Packet Tracer' (which is highlighted in blue), 'All Resources', and 'Alumni Courses'. Below this, the main content area has a title 'Download Cisco Packet Tracer'. It includes a sub-headline 'The best way to learn about networking is to do it.', a brief description of what Cisco Packet Tracer is, and a list of reasons to use it. At the bottom, there's a section titled 'Learn more on how to use Packet Tracer' with a link to an introduction course.

GRAFIČKO KORISNIČKO SUČELJE

Grafičko sučelje simulatora sastoji se od zaglavlja sa tabovima koji služe za standardno upravljanje projektom, koji se u ovom slučaju naziva Packet Tracer Activity File (sa ekstenzijom *.pkt). Tako se na primjer na traci izbornika može pronaći opcije kao što su spremanje kreirane topologije, otvaranje postojeće mrežne topologije, pomoć pri korištenju alata, pristup tutorijalima itd.

Srednji dio sučelja je radna površina na koju se "povlače" mrežni uređaji po principu "drag-and-drop". Mrežni uređaji se nalaze na samom dnu sučelja (donji lijevi kut). Potrebno je još uočiti dva principa rada mreže kreirane u PT-u, a to su simulacijski (simulation) način rada i realtime način rada u „realnom“ vremenu.



CILJ UVODNE VJEŽBE

Glavni cilj je upoznati se sa grafičkim sučeljem alata i naučiti kako izgraditi mrežnu topologiju.

Ostali ciljevi:

- Kreirati jednostavnu lokalnu mrežu (Local Area Network, LAN) sa računalima povezanim na switch i računalima povezanim na hub
- Testirati konekciju unutar svake od dviju manjih LAN mreža
- Povezati mreže u jedan veći LAN i verificirati konekciju unutar mreže
- Osim osnovnih naredbi **ipconfig** i **ping**, upoznati se sa još nekim osnovnim mrežnim naredbama.

TEORIJSKI PREDUVJETI

Uvodna vježba je modificirana prema [4]. Ova vježba podrazumijeva osnovno znanje o LAN mreži, pojam IP adresе, ICMP, DNS, ARP protokol. Teorijski dijelovi ove skripte preuzeti su iz [5].

IP (Internet Protocol)

IP je protokol mrežne razine koji je temelj Internet mreže i većine današnjih lokalnih mreža. Namjena mu je osigurati prijenos podataka (IP datagrama) između raznorodnih mreža, što uključuje dva zadatka: adresiranje i usmjeravanje. Adresiranje omogućuje identificiranje izvorišta i odredišta datagrama, dok usmjeravanje omogućuje dostavu datagrama do odredišta najoptimalnijim putem.

IP protokol je nepouzdani bespojni protokol, dakle ne uspostavlja logički kanal kao spojevni protokoli, pa ne nudi zaštitu od gubitka datagrama. Kako je rukovanje datogramima zasebno za svaki od njih, kao i zbog drugih karakteristika Internet mreže, moguće je da niz datagrama poslan prema odredištu stigne do njega redoslijedom različitim od onog kod slanja, a moguća je i pojava višestrukih kopija istog datagrama. Trenutno su u upotrebi dvije varijante IP protokola: IPv4 i IPv6.

Adresiranje ima ulogu identificirati svako računalo, odnosno čvor u IP mreži, a jedinstvena identifikacija svakog čvora je omogućena uz pomoć IP adrese. Ona mora sadržavati identifikaciju mreže u kojoj se čvor nalazi, kao i samo računalo unutar mreže (čvor). IP adrese u IPv4 protokolu su duljine 32 bita.

IP adrese se najčešće zapisuju u tzv. dotted quad formi, gdje se svaki oktet iz 32 bita adrese predstavlja svojim decimalnim ekvivalentom. Primjerice, 161.53.168.12. je decimalni ekvivalent binarne adrese 10100001 00110101 10101000 00001100.

ICMP (Internet Control Message Protocol)

ICMP je razvijen za komuniciranje usmjernika (računala koja usmjeravaju IP datagram od izvorišta do odredišta), međusobno, kao i s izvořišnim računalima da bi se izvijestilo o eventualnoj pogrešci nastaloj u obradi paketa (nedostupnost mreže, zagušenje, itd.).

Neke ICMP poruke su:

- Echo request - šalje se da bi se dobila informacija o dostupnosti nekog odredišta.
- Echo reply - odgovor na Echo request.
- Redirection – preusmjerenje, kada se u tablici nađe kraći put do odredišta.
- Destination Unreachable - nedostupnost računala, mreže, porta ili protokola.
- Time Exceeded - obavještava izvorište da je paketu isteklo "vrijeme života" (Time to Live vrijednost je TTL=0).
- Parameter Problem - usmjernik je naišao na nekonzistentnost unutar zaglavlja.
- Source Quench - zahtjev izvorištu za smanjenjem brzine slanja paketa, paket odbačen.

Program Ping koristi ICMP Echo Request poruku da bi odredio da li je odredište aktivno i dostupno. Svako računalo koje podržava Internet Protocol (IP) protokol podržava i ICMP protokol. Dostupnost računala u lokalnoj mreži može se testirati naredbom

`ping <IP adresa računala>.`

DNS (Domain Name Service)

Kako je i decimalna notacija IP adresa nezgodna za pamćenje uvedena je DNS usluga koja IP adrese zamjenjuje hijerarhijski organiziranim sustavom imena.

Na primjer, IP adresa 161.53.167.47 ima svoj DNS ekvivalent www.fesb.hr pri čemu je .hr top-level (vrhovna) domena, a .fesb je sekundarna.

Imena vrhovnih domena su standardizirana (.com, .org, .edu, itd + domene država). Računala koja pružaju DNS uslugu su DNS poslužitelji, koji su također organizirani hijerarhijski. DNS poslužitelj sadrži zapise o određenom broju računala unutar jedne ili više lokalnih mreža (DNS zone). Ukoliko se želi saznati IP adresa računala izvan zone, DNS poslužitelji kontaktira poslužitelj iz zone traženog računala i formira odgovor.

DNS imena računala koriste se u najvećem broju mrežnih aplikacija. Izravan kontakt se DNS poslužiteljem moguć je naredbom

```
nslookup <IP ili DNS zapis>
```

Ukoliko se upit postavlja za računalo izvan zone DNS servera (potpis servera je u prve dvije linije odgovora), odgovor je "Non-authoritative" tipa, odnosno dobiven je od DNS servera van zone računala koje je postavilo upit.

ARP (Address Resolution Protocol)

ARP je protokol koji omogućuje dostavu datagrama mrežne razine (IP) računalu koje se nalazi na lokalnoj mreži Ethernet. ARP protokol ustavlja vezu između mrežne adrese i fizičke adrese računala. Radi se o mapi IP-MAC adresa, tako da ako je poznata IP adresa računala kojem se dostavlja IP datagram, ARP protokolom se doznaje njegova MAC adresa, formira Ethernet okvir s IP datagramom u podatkovnom dijelu okvira i MAC adresom odredišnog računala u zaglavljtu Ethernet okvira.

Svako računalo koje se nalazi na lokalnoj mreži održava listu parova IP-MAC adresa (ARP cache), koja je dostupna naredbom

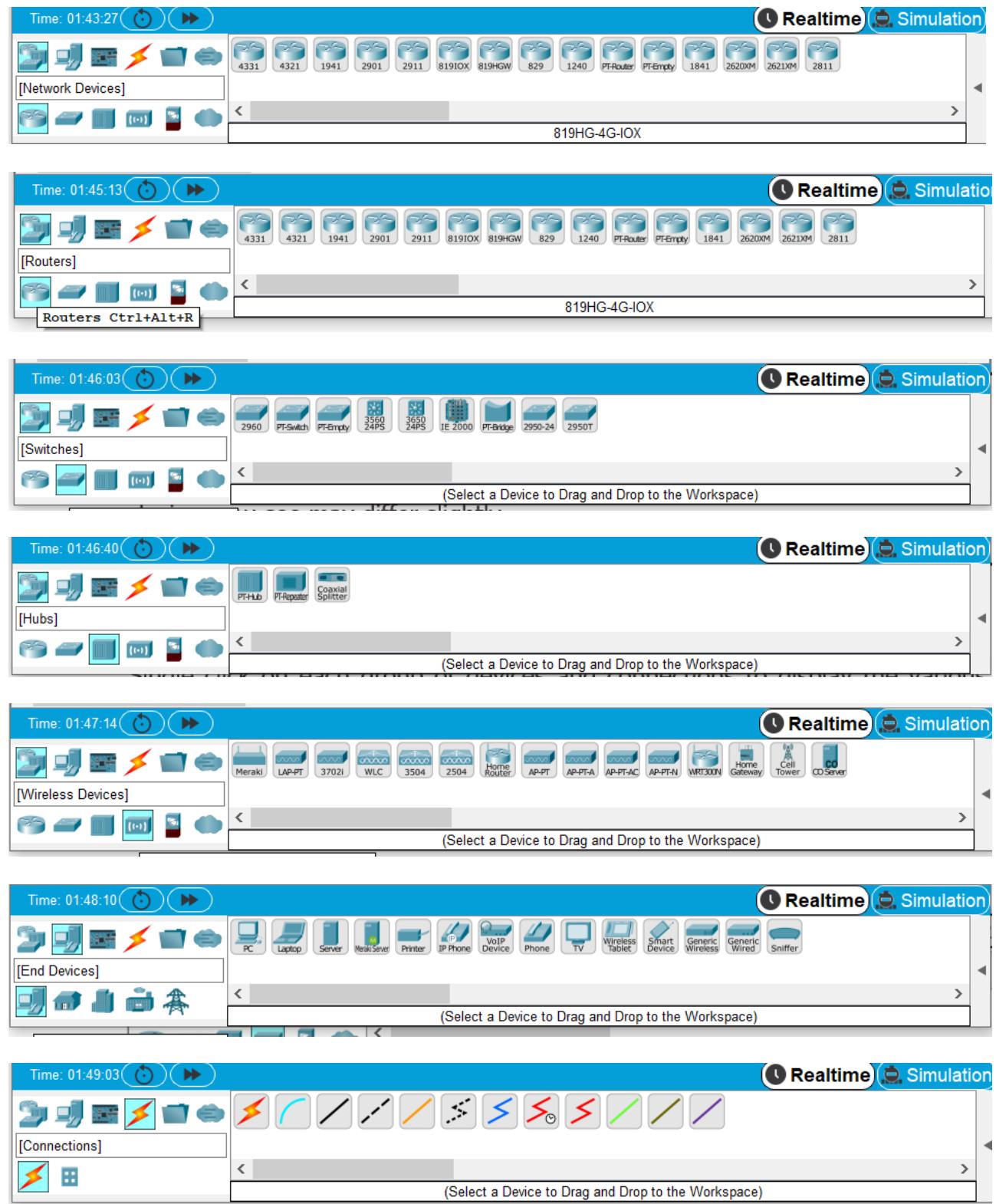
```
arp -a.
```

Kod formiranja Ethernet okvira najprije se pretražuje ARP cache, ukoliko se tu ne pronađe tražena MAC adresa, emitira se broadcast upit, na kojeg će odgovoriti ono računalo koje ima traženu IP adresu. Odgovor se sastoji od para IP-MAC adrese i spremi se u ARP cache, jer je velika vjerojatnost da će nam uskoro opet trebati.

RARP – reverzni ARP protokol ima suprotnu ulogu: za danu MAC adresu traži odgovarajuću IP adresu. Dynamic Host Configuration Protocol (DHCP) protokol je poboljšanje RARP protokola koji omogućuje automatsku konfiguraciju računala kod spajanja na mrežu.

ODABIR MREŽNIH UREĐAJA I KONEKCIJA U SIMULATORU

Počinjemo kreiranje mrežne topologije tako što odabiremo mrežne uređaje i medije (kabele) s kojima ćemo ih povezati. U PT-u se mogu koristiti razni tipovi uređaja i mrežnih konekcija. Lijevi klik mišem na svaku od grupe uređaja i konekcija otvara više različitih opcija.



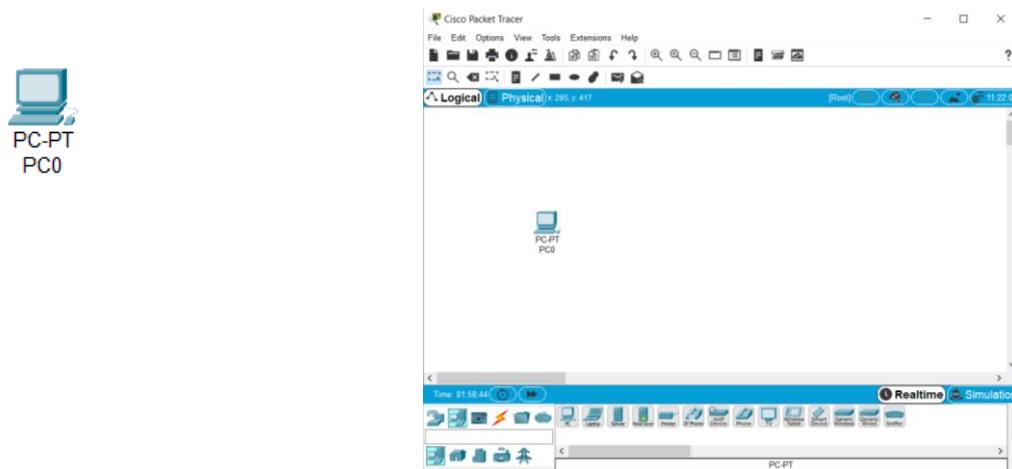
IZGRADNJA MREŽNE TOPOLOGIJE

DODAVANJE KRAJNJIH UREĐAJA (HOSTS)

Kliknite na krajnje uređaje (End Devices) i odaberite PC.



Primaknite cursor prema radnoj površini i primijetite kako se cursor pretvori u znak plus +. Klikom na radnu površinu dovodimo na nju prvi PC host.

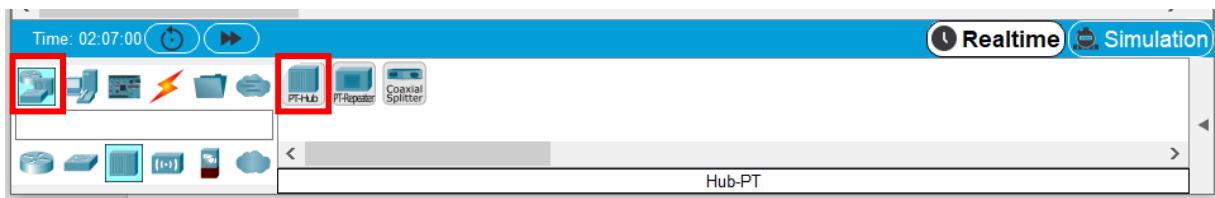


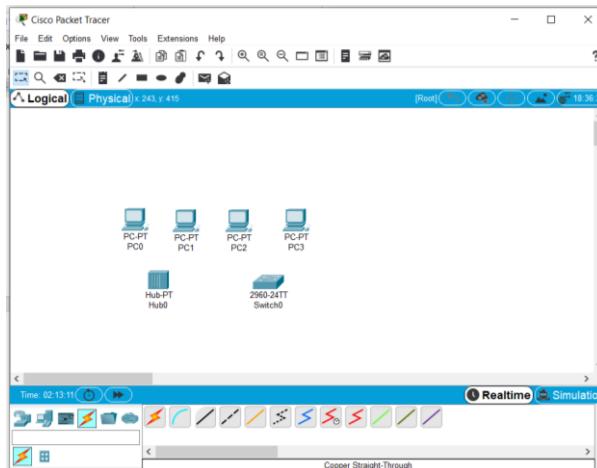
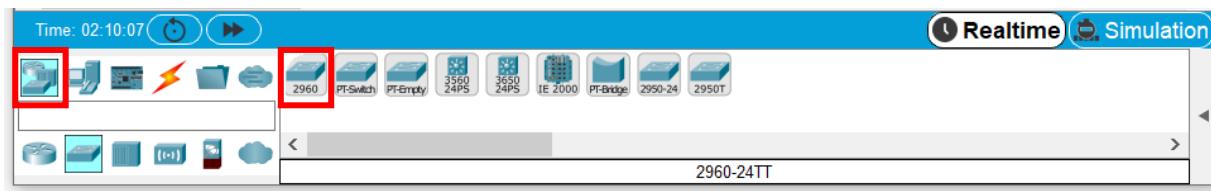
Dodajte još tri PC hosta na radnu površinu.



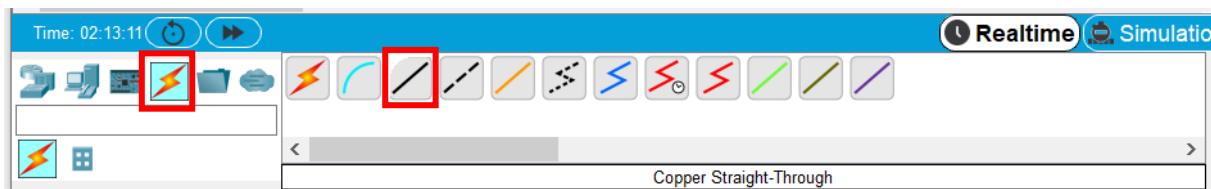
POVEZIVANJE HOSTOVA NA HUB I SWITCH

Odaberite hub i dodajte ga na radnu površinu ispod PC0 i PC1. Istim postupkom odaberite switch i postavite ga "ispod" računala PC2 i PC3 na radnoj površini.



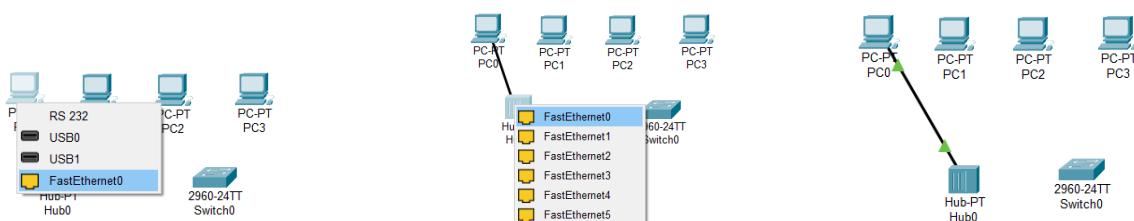


Povežite računala PC0 i PC1 na hub, te računala PC2 i PC3 na switch korištenjem copper straight-through kabela.

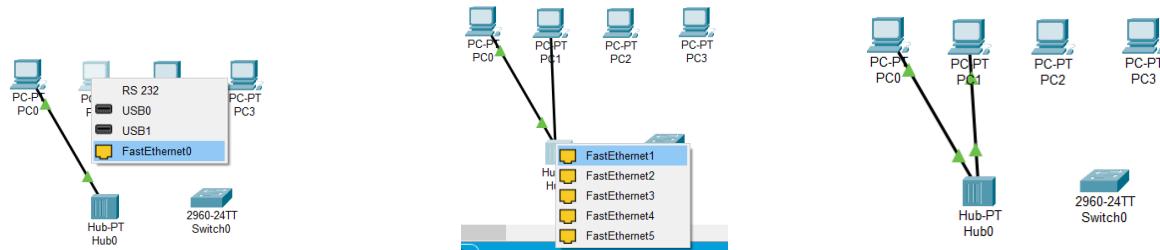


Primjerice, za povezivanje PC0 na hub, potrebno je napraviti iduće korake:

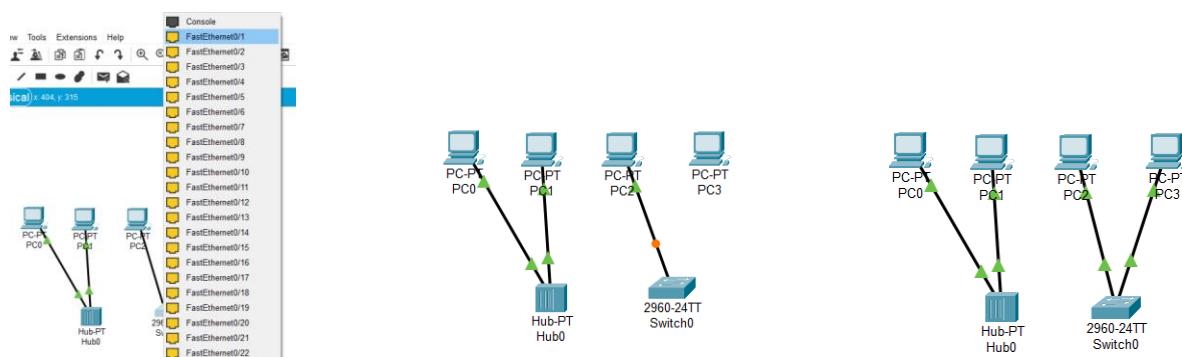
- Kliknuti jednom na PC0 i odabratи FastEthernet
- Povući kursor do hub-a
- Kliknuti jednom na hub i odabratи FastEthernet 0 (to je Port 0)
- Primijetite kako se pojavilo zeleno svjetlo na PC0 Ethernet konektoru i na portu od hub-a, što pokazuje da je link aktiviran.



Na isti način povezati PC1 na Port 1 od hub-a. Redni broj porta nije bitan, računalo možemo povezati na bilo koji slobodan port na hub-u.



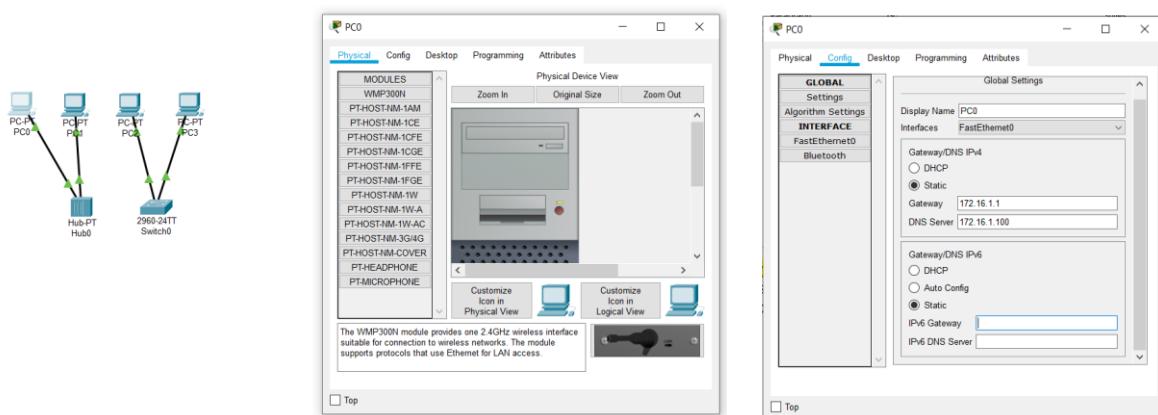
Prateći iste korake, povezati računala PC2 i PC3 na switch Port FastEthernet 0/1 i FastEthernet 0/2. Primijetite kako je broj portova na switch-u mnogo veći od broja portova na hub-u. Također, zeleno svjetlo na linku pojavi se malo kasnije nego u prethodnom slučaju - ponekad je potrebno pričekati i do 30 sekundi da se veza „podigne“.



KONFIGURIRANJE IP ADRESA RAČUNALA

Kako bi hostovi mogli komunicirati u mreži, potrebno im je konfigurirati IP adrese i mrežnu masku. O njima će detaljnije biti riječi u nekoj od narednih vježbi, a za sada ćemo ih samo upisivati prema uputama.

Kliknite jednom na računalo PC0 i odaberite konfiguracijski (Config) tab.

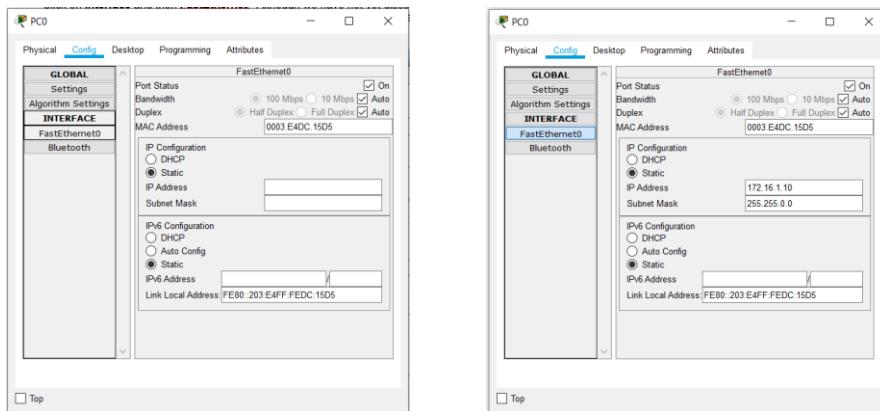


Unutar Config tab-a, kliknite na postavke (Settings), gdje možete promijeniti ime za PC0, unijeti Default Gateway i IP adresu DNS servera. Ovo bi zapravo trebala biti IP adresa lokalnog usmjernika, o čemu će više riječi biti u narednim vježbama. Ako želite, ovdje

možete unijeti Gateway IP adresu 172.16.1.1 i DNS Server IP adresu 172.16.1.100, iako ih nećemo koristiti u današnjoj vježbi.

Kliknite na konfiguraciju Interface FastEthernet0 sučelja. Iako ćemo o IP adresama i mrežnim maskama detaljno govoriti u nekoj od narednih vježbi, postavite računalu PC0 statičku IP adresu 172.16.1.10 i mrežnu masku 255.255.0.0. Primijetimo da možemo mijenjati i brzinu sučelja. Primjerice, FastEthernet podrazumijeva brzinu Etherneta 100 Mbps, a možemo odabrati i 10 Mbps Ethernet link.

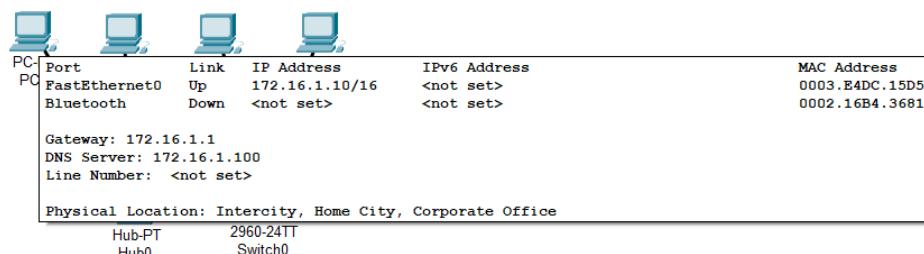
Ne trebamo tu ništa mijenjati nego ostavimo opciju "Auto". To znači da mrežna kartica hosta pregovara sa interfaceom mrežnog uređaja. Ako je host povezan na switch ili hub koji podržava 100 Mbps Ethernet, onda mrežna kartica odabire 100 Mbps (Fast Ethernet). Inače, će odabrati 10 Mbps Ethernet ako switch ili hub mogu samo podržati tu brzinu.



Ugasite na "x" te će se sve promjene na računalu PC0 automatski spremiti. Ponovite postavljanje mrežnih adresa za ostale hostove i to prema idućim konfiguracijama:

<u>Host</u>	<u>IP Address</u>	<u>Subnet Mask</u>
PC0	172.16.1.10	255.255.0.0
PC1	172.16.1.11	255.255.0.0
PC2	172.16.1.12	255.255.0.0
PC3	172.16.1.13	255.255.0.0

Postavke možemo provjeriti tako da prođemo cursorom miša preko određenog PC-ja. Na slici ispod je primjer za PC0:

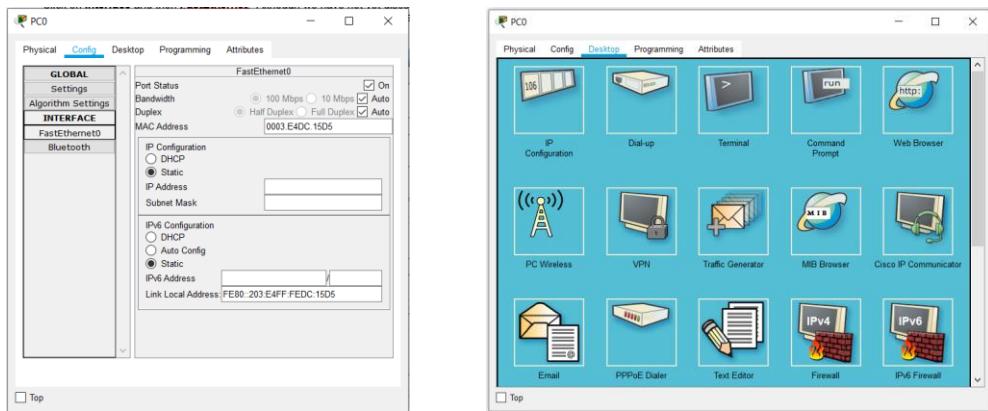


TESTIRANJE KOMUNIKACIJE UNUTAR LAN MREŽA

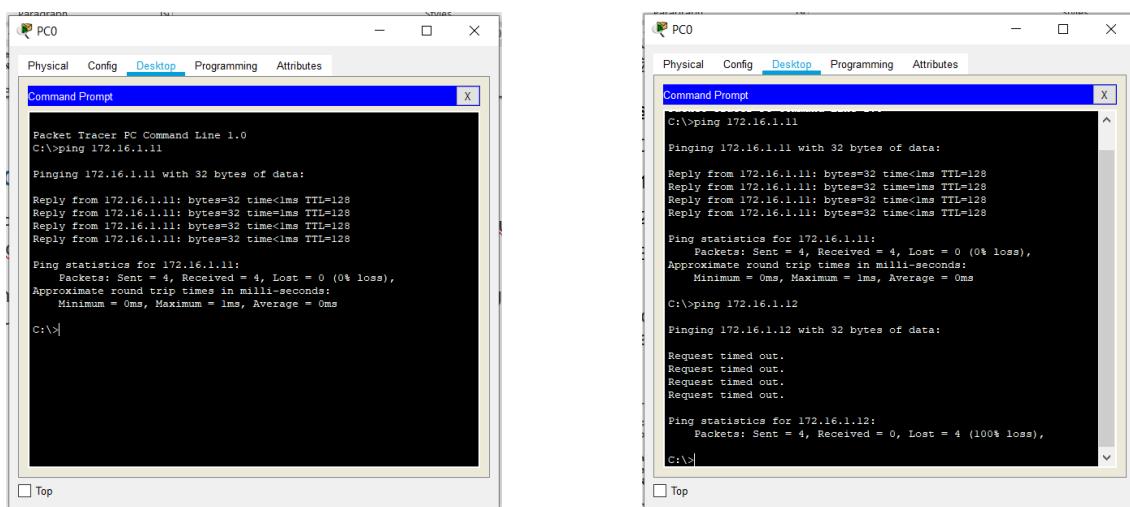
Korištenjem ICMP protokola i naredbe "ping" možemo testirati komunikaciju unutar LAN-ova. Kliknite na PC0 i odaberite Desktop tab, a zatim Command Prompt.

Recimo da želimo testirati je li računalo PC1 dostupno na mreži. Njegova IP adresa je 172.16.1.11, pa u Command Prompt unosimo naredbu

ping 172.16.1.11 < pritisnite enter >.



Rezultat nam kaže da PC0 vidi računalo PC1 na mreži (jer su na istom LAN-u). Poslana su 4 paketa od 32 byta sa računala PC1 i oni su svi uredno primljeni – statistika izgubljenih paketa je 0%. Da slučajno nismo dobili odgovor od čvora PC1, to bi značilo da nešto nije u redu s našom mrežom i trebalo bi provjeriti IP adresu čvora PC1 koju "pingamo".



Isto provjeravamo i za računalo PC2. Naravno, kako PC0 i PC2 nisu na istoj LAN mreži, oni ne mogu komunicirati. Vidimo da su sada svi poslani paketi izgubljeni i nema odgovora od PC2.

Osim prolaskom mišem preko određenog računala, IP adresu možemo provjeriti i u Command Prompt-u uz pomoć naredbe

ipconfig < pritisnite enter >.

Znači, na računalu čiju adresu želimo provjeriti, odaberemo Desktop → Command Prompt i upišemo gornju naredbu u terminal. Rezultat za pojedina računala je prikazan na slici ispod:

```

PC0:
Pinging 172.16.1.12 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:>ipconfig

FastEthernet0 Connection:(default port)
    Link-local IPv6 Address.....: FE80::260:47FF:FE0E:C79C
    IP Address.....: 172.16.1.1
    Subnet Mask.....: 255.255.0.0
    Default Gateway.....: 0.0.0.0

Bluetooth Connection:
    Link-local IPv6 Address.....: ::
    IP Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: 0.0.0.0
C:>

PC1:
Packet Tracer PC Command Line 1.0
C:>ipconfig

FastEthernet0 Connection:(default port)
    Link-local IPv6 Address.....: FE80::202:17FF:FE0B:59BB
    IP Address.....: 172.16.1.11
    Subnet Mask.....: 255.255.0.0
    Default Gateway.....: 0.0.0.0

Bluetooth Connection:
    Link-local IPv6 Address.....: ::
    IP Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: 0.0.0.0
C:>

PC2:
Packet Tracer PC Command Line 1.0
C:>ipconfig

FastEthernet0 Connection:(default port)
    Link-local IPv6 Address.....: FE80::290:CFF:FEAD:8824
    IP Address.....: 172.16.1.12
    Subnet Mask.....: 255.255.0.0
    Default Gateway.....: 0.0.0.0

Bluetooth Connection:
    Link-local IPv6 Address.....: ::
    IP Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: 0.0.0.0
C:>

PC3:
C:>ipconfig

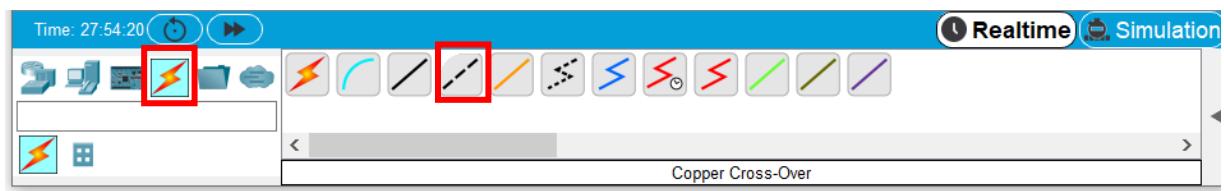
FastEthernet0 Connection:(default port)
    Link-local IPv6 Address.....: FE80::207:ECFF:FEDE:394C
    IP Address.....: 172.16.1.13
    Subnet Mask.....: 255.255.0.0
    Default Gateway.....: 0.0.0.0

Bluetooth Connection:
    Link-local IPv6 Address.....: ::
    IP Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: 0.0.0.0
C:>

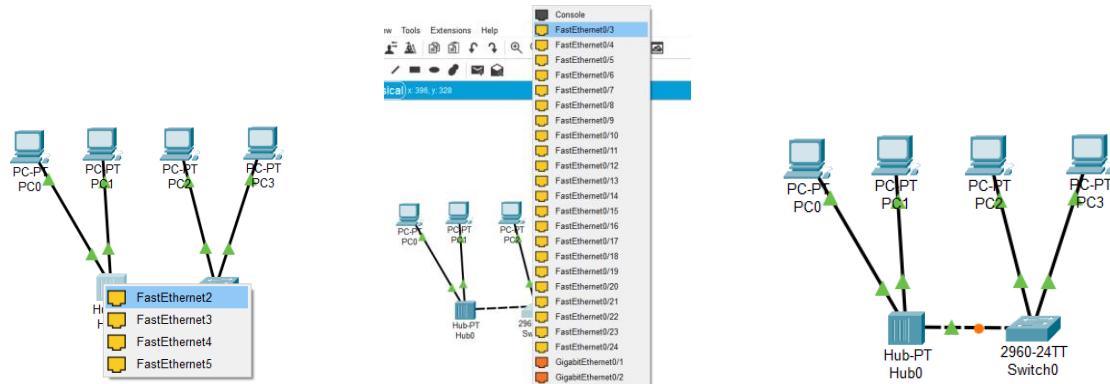
```

POVEZIVANJE LAN MREŽA

Povežimo ove dvije LAN mreže u jednu veću i to povezivanjem hub-a i switch-a. Za to koristimo Cross-over kabel iz skupine Connections.



Kliknite na cross-over i dovedite ga do hub-a uz pomoć kursora miša. Odaberite prvi slijedeći dostupni port na hub-u (to je FastEthernet 2). Za povezivanje na switch dovedite cursor do switch-a i odaberite FastEthernet 0/3. Pričekajte nekoliko trenutaka da se veza uspostavi i konekcije pozelene na oba porta.



VERIFIKACIJA KONEKCIJE UNUTAR MREŽE

Pokušajte sada provjeriti dostupnost računala PC2 sa PC0. Vidimo da je komunikacija sada uspješna i paketi su primljeni.

```

PC0
Physical Config Desktop Programming Attributes
Command Prompt
Link-local IPv6 Address.....: FE80::260:47FF:FE0E:C79C
IP Address.....: 172.16.1.1
Subnet Mask.....: 255.255.0.0
Default Gateway.....: 0.0.0.0
Bluetooth Connection:
Link-local IPv6 Address.....: ::
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
C:\>ping 172.16.1.12
Pinging 172.16.1.12 with 32 bytes of data:
Reply from 172.16.1.12: bytes=32 time=1ms TTL=128
Reply from 172.16.1.12: bytes=32 time=2ms TTL=128
Reply from 172.16.1.12: bytes=32 time=1ms TTL=128
Reply from 172.16.1.12: bytes=32 time=1ms TTL=128
Ping statistics for 172.16.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
C:\>

```



```

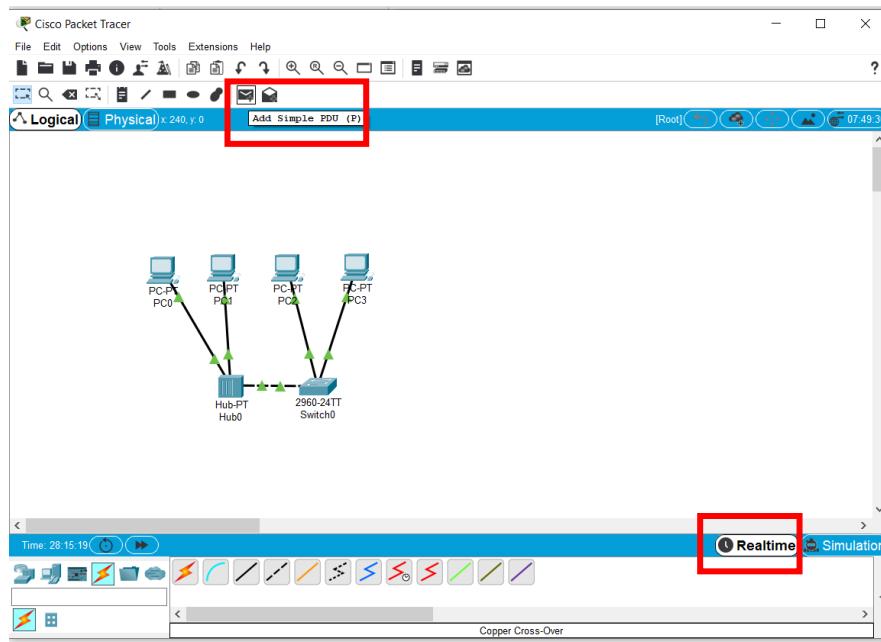
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Fing statistics for 172.16.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::260:47FF:FE0E:C79C
IP Address.....: 172.16.1.1
Subnet Mask.....: 255.255.0.0
Default Gateway.....: 0.0.0.0
Bluetooth Connection:
Link-local IPv6 Address.....: ::
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
C:\>arp -a
Internet Address      Physical Address      Type
172.16.1.11           0002.17eb.59bb      dynamic
172.16.1.12            0090.0cad.8824      dynamic
C:\>

```

Kad unesemo arp -a možemo vidjeti sadržaj ARP cachea na PC0. Vidimo da je računalo slalo IP pakete na IP adrese 172.16.1.11 i 172.16.1.12, te su uspješno mapirane mrežne IP adrese i fizičke adrese računala koje smo tražili na mreži.

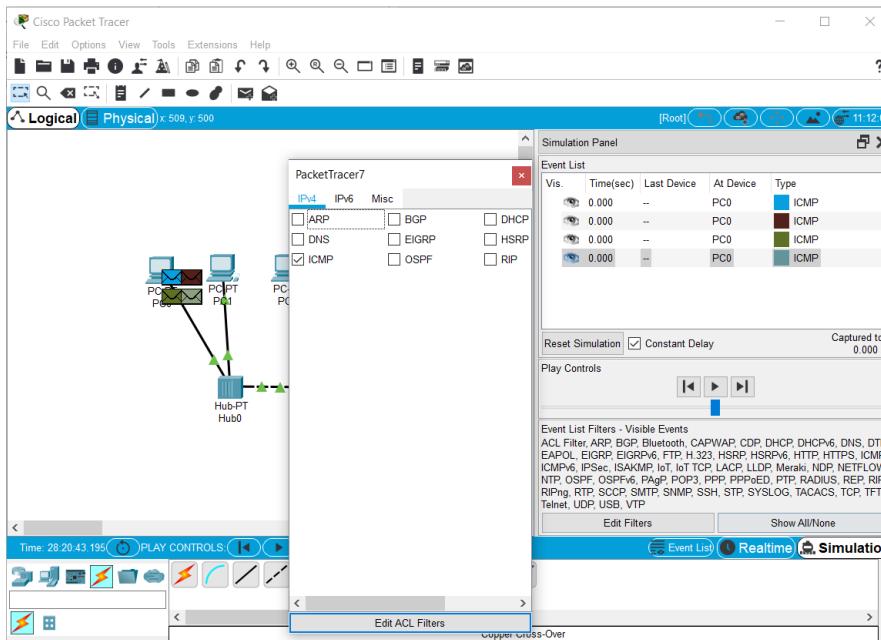
VERIFIKACIJA KONEKCIJE U REALTIME MODU

Napravimo isto kao u gornjem primjeru, ali korištenjem realtime načina rada u alatu PT. Prvo kliknemo na realtime i odaberemo simple Packet Datagram Unit (PDU) koja se koristi u svrhu ping programa. Kada označimo PDU, kliknemo na PC0 pa na PC2 jer tu konekciju želimo provjeriti. Vidimo da je konekcija uspješna i nema grešaka.



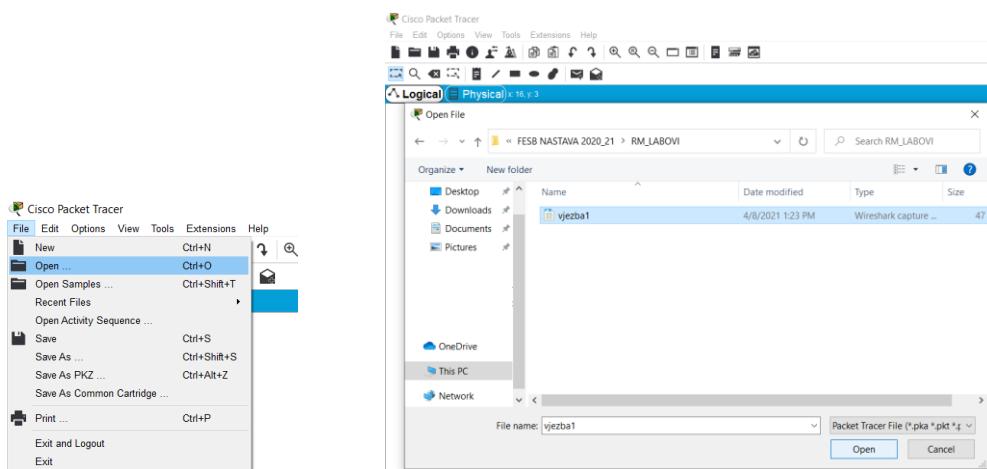
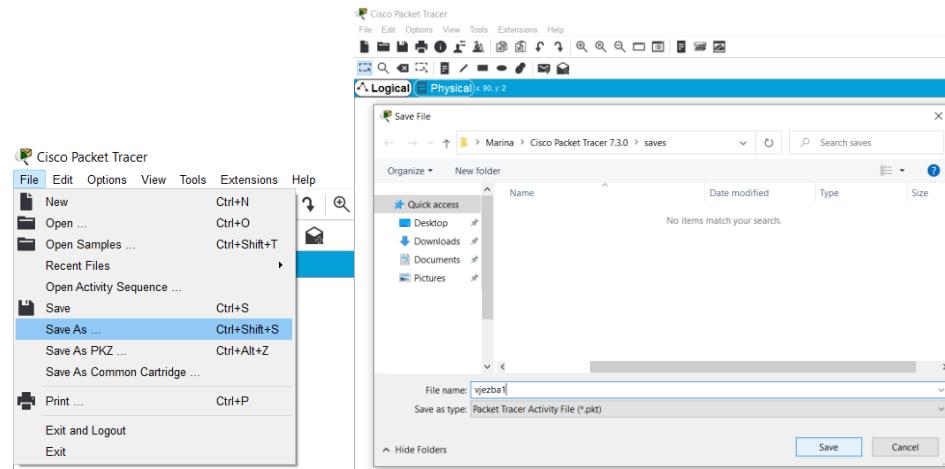
VERIFIKACIJA KONEKCIJE U SIMULACIJSKOM MODU

Testirajmo istu komunikaciju u simulacijskom modu. Prvo odaberimo simulacijski način rada i Edit Filters u kojem sve označimo osim ICMP protokola. Pratimo kako paket putuje od izvorišta do odredišta.



SPREMANJE I OTVARANJE POSTOJEĆE MREŽNE TOPOLOGIJE

Kreiranu mrežnu topologiju je potrebno spremiti kao file sa ekstenzjom *.pkt, a slike ispod pokazuju kako se taj file sprema na računalu i kako otvoriti postojeću topologiju.



ZADATAK ZA UVODNU VJEŽBU (PREDAJA IZVJEŠTAJA):

Napraviti novi projekt u programu PT i kreirati mrežu kako je pokazano na vježbi. Upoznati se sa osnovnim dijelovima PT sučelja, vježbati dodavanjem novih uređaja i računala u mrežu te dodjeljivati IP adrese. Testirati komunikaciju unutar mreže i verificirati svoje znanje o osnovnim mrežnim naredbama.

VJEŽBA 1: PODMREŽAVANJE

CILJ VJEŽBE

Glavni cilj je naučiti kako razvrstavamo IP adrese i kako funkcionira podmrežavanje. Uključeni su primjeri koji su prilagođeni sa [6] i pomažu u povezivanju gradiva.

TEORIJSKI PREDUVJETI

Podrazumijeva se osnovno razumijevanje binarnih i decimalnih brojeva. Pojmovi koje trebamo definirati prije samog početka su:

- IP adresa - jedinstveni identifikator dodijeljen jednom hostu ili sučelju u mreži.
- Podmreža (subnet) - dio mreže koji dijeli određenu adresu podmreže.
- Mrežna maska (subnet mask) - 32-bitna kombinacija koja se koristi za opisivanje dijela adrese koji se odnosi na podmrežu, i dijela za identifikaciju računala u mreži.
- Sučelje (interface) - mrežna veza.

RAZUMIJEVANJE IP ADRESA

Ponovimo da se IP adresa koristi za jedinstvenu identifikaciju uređaja na mreži. Sastoji se od 32 bita, koji se uz pomoć mrežne maske mogu podijeliti na mrežni dio i host dio.

Primjer IPv4 adrese:

1 0 1 0 0 0 0 1 0 0 1 1 0 1 0 1 0 1 1 0 1 0 1 0 1 1 0 0 0 1 0 1 0 1

Za lakše čitanje, bitovi su podijeljeni u osmorce (oktete) odvojene točkom (1 oktet = 8 bita):

1 0 1 0 0 0 0 1 . 0 0 1 1 0 1 0 1 . 1 0 1 0 1 0 1 1 . 0 0 0 1 0 1 0 1

Svaka osmorka se zapiše kao dekadski broj:

$$10100001_{(2)} = 161_{(10)}$$

$$00110101_{(2)} = 53_{(10)}$$

$$10101011_{(2)} = 171_{(10)}$$

$$00010101_{(2)} = 21_{(10)}$$

Vrijednost u svakom oktetu se kreće od 0 do 255, ili 00000000 - 11111111 u binarnoj verziji.

Konačno, IPv4 adresu iz gornjeg primjera ćemo zapisati u obliku:

161.53.171.21

Od navedenih 32 bita adrese, prvih nekoliko je **adresa mreže**, a ostatak je **adresa računala u toj mreži**.

MREŽNA MASKA

Definira koliko bitova IP adrese se odnosi na adresu mreže (identifikacija mreže), a koliko na adresu računala u toj mreži (identifikacija hostova).

Mrežna maska je niz jedinica i nakon toga niz nula, a ima ukupno 32 bita:

- pozicije na kojima se nalaze jedinice znače da se ti bitovi IP adrese odnose na adresu mreže
- pozicije na kojima su u mrežnoj maski nule znače da se ti bitovi IP adrese odnose na adresu računala u toj mreži

Primjer, za adresu 161.53.171.21:

IP adresa:	1 0 1 0 0 0 0 1 . 0 0 1 1 0 1 0 1 . 1 0 1 0 1 0 1 1 . 0 0 0 1 0 1 0 1
Mrežna maska:	1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 0 0 0 0 . 0 0 0 0 0 0 0 0

Napomena:

Gore je prikazana proizvoljna mrežna maska (izmišljena), i prema ovakvoj mrežnoj maski prvih 20 bitova IP adrese (to su bitovi slijeva odnosno značajniji bitovi) adresiraju mrežu u kojoj se nalazi računalo, a posljednjih 12 bitova (oni desni dakle manje značajni bitovi) adresiraju računalo u toj mreži.

Sva računala u ovoj mreži će imati istih prvih 20 bitova (adresa te mreže u kojoj se nalaze), a razlikovat će se po adresi računala u mreži (jer IP adresa svakog računala mora biti jedinstvena).

Za lakše čitanje, i mrežna maska se zapisuje kao 4 dekadska broja odvojena točkom, pa bi za gornji primjer pisali:

IP adresa:	161.53.171.21
Mrežna maska:	255.255.240.0

CIDR FORMAT

Classless Interdomain Routing (CIDR) format je uveden kako bi se poboljšala upotreba adresnog prostora i skalabilnost usmjeravanja na Internetu. To je bilo potrebno zbog brzog rasta Interneta i rasta veličine IP tablica usmjeravanja u internetskim usmjerivačima [6].

U CIDR formatu, IP mreža je predstavljena prefiksom, dakle format zapisa se sastoji od IP adrese i duljine mrežne maske:

IP adresa / broj bitova koji se odnose na adresu mreže

Za gornji primjer, to je: 161.53.171.21 / 20

Ponovimo još jednom kako je prefiks zapravo duljina, odnosno broj krajnje lijevih bitova maske koji su u jedinici. Ako uzmemmo još jedan primjer, za mrežu:

IP adresa:	172.16.0.0
Mrežna maska:	255.255.0.0

CIDR format se može prikazati kao: 172.16.0.0 / 16.

ADRESIRANJE RAČUNALA U MREŽI

Koliko računala možemo (maksimalno) imati u mreži kojoj je mrežna maska 255.255.240.0?

Za adresiranje računala u toj mreži imamo na raspolaganju 12 bitova, a s 12 bitova možemo dobiti $2^{12} = 4096$ različitih adresa.

Adresa sa svim nulama u dijelu za adresu računala se tradicionalno uzima kao adresa te mreže i ne koristi se za adresiranje računala. Također, adresa sa svim jedinicama u dijelu za adresu računala je broadcast (univerzalna) adresa u toj mreži i pakete s tom adresom primaju sva računala u mreži.

IP adresa:	1 0 1 0 0 0 0 1 . 0 0 1 1 0 1 0 1 . 1 0 1 0 1 0 1 1 . 0 0 0 1 0 1 0 1
Mrežna maska:	1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 0 0 0 0 . 0 0 0 0 0 0 0 0

Adresa mreže:	1 0 1 0 0 0 0 1 . 0 0 1 1 0 1 0 1 . 1 0 1 0 0 0 0 0 . 0 0 0 0 0 0 0 0
Broadcast adresa:	1 0 1 0 0 0 0 1 . 0 0 1 1 0 1 0 1 . 1 0 1 0 1 1 1 1 . 1 1 1 1 1 1 1 1

Dakle, za adresiranje računala imamo na raspolaganju $2^{12} - 2 = 4096 - 2 = 4094$ adresa, pa je to maksimalan broj računala koji možemo imati u mreži. Adresa mreže se dobije logičkom operacijom AND koja se radi bit po bit između IP adrese i mrežne maske.

NASTANAK KLASA IP ADRESA

U početku razvoja Interneta zainteresiranim korporacijama dodjeljivane su adrese s 8 bitova za adresu mreže:

9.0.0.0 / 8	- IBM
10.0.0.0 / 8	- ARPANET
12.0.0.0 / 8	- AT&T
13.0.0.0 / 8	- Xerox
17.0.0.0 / 8	- Apple
19.0.0.0 / 8	- Ford
56.0.0.0 / 8	- US postal service
...	

Svaka od ovih adresa ima mjesta za $2^{(32-8)} - 2 = 2^{24} - 2$ računala tj. za preko 16 milijuna računala.

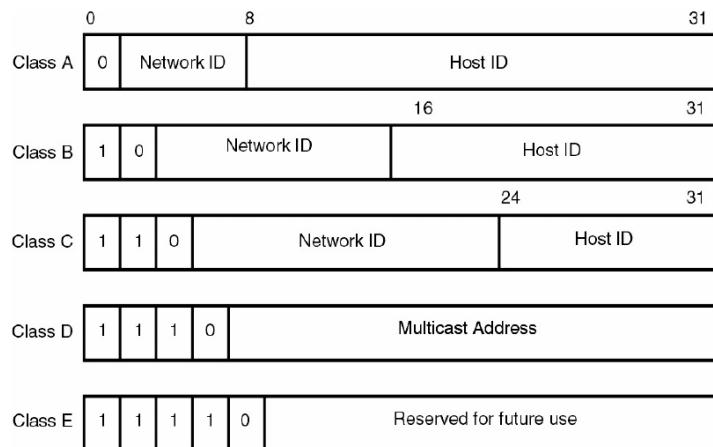
Problem: većina adresa ostaje neiskorišteno, a uskoro će nestati ovakvih /8 mreža!

Rješenje:

Uvođenje više klasa IP adresa, za svaku klasu različit broj bitova se odnosi na adresu mreže (dok se ostatak odnosi na adresu računala u mreži).

Klase koje imaju više bitova za adresu mreže mogu adresirati više mreža, ali u svakoj mreži manje računala.

Sve do tada podijeljene adrese su imale najvažniji bit prvog okteta nula (prvi oktet je bio manji od 128). Odlučeno je da takve adrese imaju 8 bitova za adresu mreže (i 24 bita za adresu računala). Ta klasa IP adresa nazvana je **klasa A**. Postoji ukupno 5 klase mreža, to su klasa A, B, C, D i E. Koncentrirat ćemo se u vježbi na klase od A do C, jer su klase D i E adrese posebne namjene rezervirane za multicast i eksperimentalnu upotrebu.



Na gornjoj slici [5] su prikazani detalji o pojedinoj klasi IP adresa. Identifikator mreže (network ID) sadrži oznaku za tip klase kojoj IP adresa pripada. Kodovi klasa su redom:

Klasa A → prvi bit = 0

Klasa B → prva dva najznačajnija bita = 10

Klasa C → prva tri najznačajnija bita = 110

Klasa D → prva četiri najznačajnija bita = 1110

Klasa E → prvih pet najznačajnijih bitova = 11110

U adresi **klase A** prvi oktet je mrežni dio, a okteti 2, 3 i 4 (sljedeća 24 bita) služe za adresiranje računala u toj mreži. Adrese klase A koriste se za velike mreže koje imaju više od 65 536 hostova (opravdano, do $2^{24}-2 = 16\ 777\ 214$ računala). U klasi A postoji $2^{7-3} = 125$ mreža (jer je osim dvije rezervirane IP adrese, rezervirana i adresa sa svim nulama).

U adresi **klase B** prva dva okteta su mrežni dio, a okteti 3 i 4 (16 bitova) namijenjeni su podmrežavanju. Adrese klase B koriste se za mreže koje imaju između 256 i $2^{16}-2 = 65\ 534$ hostova. U klasi B postoji $2^{14}-2 = 16\ 382$ mreže.

U adresi **klase C** prva tri okteta su mrežni dio, a oktet 4 (8 bitova) namijenjen je podmrežama i hostovima. Koristi se za mreže s manje od $2^8-2 = 254$ računala. U klasi C postoji $2^{21}-2 = 2\ 097\ 150$ mreža.

Iz karakteristika formata pojedine klase IP adresa lako možemo zaključiti kojoj klasi neka IP adresa pripada. Raspon IP adresa u pojedinoj klasi je:

Klasa A → 0.0.0.0 - 127.255.255.255

Klasa B → 128.0.0.0 - 191.255.255.255

Klasa C → 192.0.0.0 - 223.255.255.255

Klasa D → 224.0.0.0 - 239.255.255.255

Klasa E → 240.0.0.0 - 255.255.255.255

Kako smo već vidjeli, po dvije IP adrese iz svakog raspona su rezervirane: adresa računala koja binarno ima sve jedinice je tzv. **broadcast adresa** za dotičnu mrežu (koja služi za slanje poruka cijeloj mreži na kojoj se neko računalo nalazi), a ona sa svim nulama identificira mrežu.

Usmjernici na Internetu usmjeravaju promet prema odredištu tako da (pojednostavljenno!!!):

- pogledaju kojoj klasi pripada adresa odredišta i zaključe koliko bitova u adresi se odnosi na adresu mreže
- zaključe koja je adresa mreže u kojoj je odredište
- router u svojoj tablici usmjeravanja pogleda u kojem smjeru treba proslijediti promet koji ide u tu mrežu i usmjere promet prema tamo (ustvari, prema routerima koji znaju kako su raspoređene adrese u toj mreži). Bitovi koji se odnose na adresu računala u toj mreži ih ne zanimaju
- na ovaj način paket stigne u mrežu u kojoj se nalazi odredište. Pri tom se „mreža“ ne odnosi na LAN u kojem je odredište, nego na cijelu mrežu kojoj pripada njegova adresa (npr ako je to adresa iz neke B klase, onda je njegova mreža s nekoliko desetaka tisuća računala i većim brojem routera koji obavljaju usmjeravanje unutar te mreže)
- tek routeri koji se nalaze bliže odredištu (u njegovoj mreži) počinju gledati i bitove koji se odnose na adresu računala

Već smo vidjeli da mrežna maska pomaže saznati koji dio adrese identificira mrežu, a koji dio adrese identificira računalo. Mreže klase A, B i C imaju zadane (default) mrežne maske, kao što je prikazano ovdje:

Klasa A → 255.0.0.0

Klasa B → 255.255.0.0

Klasa C → 255.255.255.0

Ponovimo kako iz IP adrese (ovaj put uz zadanu mrežnu masku) prepoznati mrežni dio (network ID) i dio gdje je adresa računala (host ID):

Neka je zadana IP adresa klase A → 8.20.15.1 koja ima zadanu masku: 255.0.0.0.

Pretvorimo adresu i masku u binarni oblik:

$8.20.15.1 = 00001000.00010100.00001111.00000001$

$255.0.0.0 = 11111111.00000000.00000000.00000000$

Adresni bitovi koji imaju odgovarajuće bitove maske postavljene u 1 predstavljaju mrežni ID. Bitovi adrese koji imaju odgovarajuće bitove maske postavljene na 0 predstavljaju ID računala.

$8.20.15.1 = \boxed{00001000}.\boxed{00010100}.\boxed{00001111}.\boxed{00000001}$

$255.0.0.0 = 11111111.00000000.00000000.00000000$

Net ID = 00001000 = 8

Host ID = 00010100.00001111.00000001 = 20.15.1

POSTUPAK PODMREŽAVANJA

Podmrežavanje omogućuje stvaranje više logičkih mreža koje postoje unutar jedne mreže klase A, B ili C. Samim postupkom dodajemo više bitova u mrežni dio adrese nego što je propisano nekom klasom.

Prilikom procesa podmrežavanja, prvo proširimo zadanu masku s nekim bitovima iz dijela adrese koji se odnosi na host ID kako bi dobili ID podmreže. Na primjer, za mrežu klase C 204.17.5.0 koja ima zadanu masku 255.255.255.0, podmreže možemo stvoriti na ovaj način:

204.17.5.0	- 11001100.00010001.00000101. 000 00000
255.255.255.224	- 11111111.11111111.11111111.111 00000

Proširivanjem maske sa 255.255.255.0 na 255.255.255.224 smo uzeli tri najznačajnija bita (označena plavom bojom) s izvornog dijela gdje se nalazio host ID i od njih ćemo napraviti podmreže. S ova tri bita moguće je stvoriti osam podmreža (2^3). S preostalih pet bitova host ID-a, svaka podmreža može imati do 32 adrese hosta (2^5), od kojih se 30 stvarno može dodijeliti uređaju (2^5-2), jer ID-evi hosta sa svim nulama ili svim jedinicama nisu dopušteni (broadcast adresa i adresa mreže).

Raspisemo sve moguće kombinacije sa tri bita:

204.17.5.0	- 11001100.00010001.00000101. 000 00000
	001 00000
	010 00000
	...
	111 00000

Tako su stvorene slijedeće podmreže (mrežnu masku ćemo zapisati u CIDR formi):

Podmreža 1 → 204.17.5.0 / 27

Raspon adresa računala u mreži je od 1 do 30, jer je:

204.17.5.0	- 11001100.00010001.00000101. 000 00000
	00000001
	00000010
	00000011
	...
	00011110

Podmreža 2 → 204.17.5.32 / 27

Raspon adresa računala u mreži je od 33 do 62, jer je:

204.17.5.32	- 11001100.00010001.00000101. 001 00000
	00100001
	00100010
	00100011
	...
	00111110

Podmreža 3 → 204.17.5.64 / 27	i raspon adresa računala od 65 do 94
Podmreža 4 → 204.17.5.96 / 27	i raspon adresa računala od 97 do 126
Podmreža 5 → 204.17.5.128 / 27	i raspon adresa računala od 129 do 158
Podmreža 6 → 204.17.5.160 / 27	i raspon adresa računala od 161 do 190
Podmreža 7 → 204.17.5.192 / 27	i raspon adresa računala od 193 do 222
Podmreža 8 → 204.17.5.224 / 27	i raspon adresa računala od 225 do 254

Naravno da što više bitova uzmemo od host dijela za masku podmreže, to ćemo moći napraviti više podmreža. Međutim, što je više podmreža dostupno, to nam manje adresa hosta ostane na podmreži. Na primjeru gore, mreža klase C od 204.17.5.0 i maska od 255.255.255.224 (/ 27) omogućila nam je da imamo osam podmreža, svaka s 32 adresama hosta (od kojih se 30 može dodijeliti uređajima).

Da smo koristili masku od 255.255.255.240 (/ 28), račun bi bio:

204.17.5.0	- 11001100.00010001.00000101.00000000
255.255.255.240	- 11111111.11111111.11111111.1111 0000

Budući da sada imamo četiri bita za izradu podmreža, preostala su nam samo četiri bita za adrese hosta. Dakle, u ovom slučaju možemo imati do 16 podmreža, od kojih svaka može imati do 16 adresa računala (od kojih se 14 može dodijeliti uređajima).

Uzmimo za primjer jednu mrežu klase B, na primjer 172.16.0.0 /21

Možemo lako vidjeti da je sada moguće stvoriti puno više podmreža nego s mrežom klase C. Kako ćemo izračunati broj mogućih podmreža i broj mogućih adresa hostova na mreži?

172.16.0.0	- 10101100.00010000.00000000.00000000
255.255.248.0	- 11111111.11111111.1111 000.00000000

Za podmreža sada koristimo pet bitova iz izvornih bitova host dijela. To nam omogućuje da imamo 32 podmreža (2^5). Nakon korištenja pet bitova za podmreža, ostaje nam 11 bitova za adrese hosta. To omogućuje svakoj podmreži da ima 2048 adresa računala (2^{11}), od kojih se 2046 može dodijeliti uređajima.

Napomena:

U gornjim primjerima smo mrežu dijelili na podmreže jednakе veličine. Ali, mreža se može podijeliti i na podmreže različitih veličina, kao što ćemo vidjeti u slijedećem primjeru.

PRIMJER PODMREŽAVANJA CARNET MREŽE

Slučaj 1. Pogledajmo jednu adresu B klase (koja je dodijeljena Carnetu) i pokušajmo je podijeliti na manje mreže koje Carnet dodijeli pojedinim sveučilištima (ovisno o tome koliko koje sveučilište treba računala za adresiranje sada i u predviđenoj budućnosti).

Primjer: mreža iz B klase 161.53.0.0 / 16

1 0 1 0 0 0 0 1 . 0 0 1 1 0 1 0 1 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 0

Označimo najznačajnijih 16 bitova adrese crvenom bojom jer nam CIDR prefiks / 16 kaže da je najznačajnijih 16 bitova mrežne maske postavljeno u jedinicu. Znači da su nam preostali bitovi host dijela (također 16 bitova) dostupni za podmrežavanje.

Pretpostavimo da ZG i ST sveučilišta trebaju po 6000 adresa, OS sveučilište treba 3000 adresa, a DU treba 1500 adresa za adresiranje računala.

Pošto adresiramo hostove, onda uzimamo najmanje značajne bitove, to jest uzimamo onliko najmanje značajnih bitova ili bitova sa krajnje desnog dijela mrežne adrese, ovisno o tome koliko uređaja želimo adresirati.

Na temelju toga određujemo novu mrežnu masku za pojedina sveučilišta.

Carnet	161.53. 0 0 0 0 0 0 0 . 0 / 16	(ima ukupno $2^{16}-2 \approx 65k$ adresa)
ZG – 6k adresa	161.53. 0 0 0 0 0 0 0 . 0 / 19	(161.53.0.0 / 19)
ST – 6k adresa	161.53. 0 0 1 0 0 0 0 0 . 0 / 19	(161.53.32.0 / 19)
OS – 3k adresa	161.53. 0 1 0 0 0 0 0 0 . 0 / 20	(161.53.64.0 / 20)
DU – 1,5k adresa	161.53. 0 1 0 1 0 0 0 0 . 0 / 21	(161.53.80.0 / 21)

Kako vidimo u gornjem rješenju, DU treba samo 1500 adresa, pa nam je dovoljno uzeti 11 zadnjih bitova označenih crnom bojom (jer je $2^{11} = 2048$). Primijetimo kako 10 bitova nije dovoljno jer je $2^{10} = 1024$. Zato je CIDR prefiks /21, odnosno mrežna maska ima sve jedinice osim zadnjih (krajnje desnih) 11 nula.

Nadalje, OS treba duplo više adresa, njih 3000, pa trebamo uzeti zadnjih 12 bitova mrežne maske za adresiranje hostova na tom sveučilištu ($2^{12} = 4096$). Istom logikom, CIDR prefiks je /20, jer smo uzeli jedan bit više u mrežnoj maski.

Kako to nije dovoljno za ST i ZG, jer oni trebaju svaki po 6000 adresa, prefiks njihove IP adrese u CIDR formi će biti /19 sa ukupno 13 bitova uzetih u mrežnoj maski ($2^{13} = 8192$).

Što se tiče identifikacije samih mreža na pojedinom sveučilištu, svi su dio Carnetove velike mreže pa imaju prvih (najznačajnijih) 16 bitova istih → **161.53.**

Sada kad smo odvojili bitove za adresiranje računala, vidimo da imamo slobodnih tri bita mrežnog dijela adrese (u trećem oktetu) koje treba dodijeliti za ZG i ST, četiri bita dostupna za adresu OS sveučilišta i pet bitova dostupnih za DU. Nadalje, potrebno je ZG dodijeliti prvu dostupnu kombinaciju za identifikaciju mreže sa tri bita, a to je **000**. Kako više taj identifikator nije moguć, za ST uzimamo prvu iduću kombinaciju sa tri bita, a to je **001**.

Sveučilištu OS dodjeljujemo prvu iduću kombinaciju koja nema prethodne bitove koji su već dodijeljeni, znači prvu kombinaciju koja ne započinje sa 000 ili 001, a to je **0100**.

Kod DU se radi o puno manje računala koje treba adresirati pa smo uzeli manje bitova s kraja, i ostalo nam je više bitova (pet) dostupnih za adresu mreže. Istom logikom, uzimamo prvu dostupnu kombinaciju sa pet bitova koja ne započinje sa prethodno iskorištenim kombinacijama 000, 001, 0100, a to je **01010**.

Ovakvim podmrežavanjem Carnetove mreže zainteresiranim sveučilištima su dodijeljene samo neke od raspoloživih adresa, dok ostale adrese ostaju (za sada) neiskorištene. Od njih

će se moći stvoriti nove podmreže unutar Carnetove mreže kada to zatraže neke druge organizacije (npr. RI ili ZD sveučilište)

Slučaj 2. U idućem slučaju radimo daljnje podmrežavanje mreže ST sveučilišta na mreže za pojedine fakultete prema "prijavljenim" potrebama. Želimo da se od 8000 adresa dodijeljenih ST sveučilištu, FESB-u i EFST-u omogući po 2000 adresa, a PFST 500 adresa.

ST –	161.53. 0 0 1 0 0 0 0 0 . 0 / 19	(ukupno 6k adresa)
FESB – 2k adresa	161.53. 0 0 1 0 0 0 0 0 . 0 / 21	
EFST – 2k adresa	161.53. 0 0 1 0 1 0 0 0 . 0 / 21	
PFST – 500 adresa	161.53. 0 0 1 1 0 0 0 . 0 / 23	

Kako nam treba po 2000 adresa za FESB i EFST, to znači da je 11 bitova potrebno ($2^{11}=2048$), odnosno ostaje nam $32-11=21$ bit za adresu podmreže, dakle CIDR će biti /21. Preostala tri najznačajnija bita mrežnog dijela adrese (u trećem oktetu) postavimo na prvu slobodnu kombinaciju sa dva bita, a to je **00**. Analogno, za EFST postavimo na prvu slijedeću kodnu riječ, a to je **01**.

Kako nam treba samo 500 adresa za PFST, to znači da je 9 bitova potrebno ($2^9=512$), odnosno ostaje nam $32-9=23$ bita za adresu podmreže, dakle CIDR će biti /23. Preostale bitove u trećem oktetu koje su nam potrebne za identifikaciju mreže treba postaviti na prvu dostupnu kombinaciju (ovaj put sa četiri bita), a koja ne započinje sa 00 ni 01, a to je **1000**.

KORIŠTENJE MREŽNE MASKE

Mrežnu masku koriste krajnja računala povezana na mrežu i routeri u mreži, ali za različite stvari i različite maske za istu IP adresu.

Krajnja računala koriste masku kako bi znali koji su bitovi adrese isti za sva računala u njihovom LANu, pa na temelju toga mogu zaključiti je li odredište za paket koji žele poslati u njihovom LANu ili izvan njega. Ako je u LANu onda šalju paket odmah na MAC adresu odredišta, a ako nije onda šalju paket na MAC adresu default gateway-a (MAC odredište je gateway, a IP odredište je ono pravo IP odredište).

Mrežne maske koriste i usmjernici kako bi znali kojoj u kojoj mreži se nalazi odredište za neki paket. Za istu IP adresu routeri mogu koristiti različite mrežne maske: najudaljeniji router cijelu mrežu odrede prema klasi kojoj pripada adresa (tada je mrežna maska onolika koliku ta klasa propisuje), a routeri u toj mreži onda koriste drugačije maske za odrediti da je to odredište u podmreži **podmreža_X**, a onda neki drugi routeri koriste opet treću masku za odrediti da je ta adresa u pod-podmreži **podmreža_X_c** itd...

Tako će prema gornjem primjeru na nekom Carnetovom routeru, u tablicama usmjeravanja pisati iduće:

161.53. 0. 0 / 19	ZG
161.53. 32.0 / 19	ST
161.53. 64.0 / 20	OS
161.53. 80.0 / 21	DU

Na routerima u mreži Splitskog sveučilišta će pisati:

FESB **161.53.32.** 0 / 21
 EFST **161.53.40.** 0 / 21
 PFST **161.53.48.** 0 / 23

Dakle, routeri koriste masku kako bi odredili u kojoj mreži ili podmreži se nalazi odredište. Možemo reći da i krajnja računala koriste masku za istu stvar, s tim što krajnja računala razlikuju samo 2 mreže: njihov LAN i sve druge mreže.

USMJERAVANJE UNUTAR ISTE MREŽE

Pretpostavimo da je Carnetova mreža B klase 161.53.0.0 / 16 podmrežena prema gornjem primjeru. Kao što je već rečeno, routeri usmjeravaju pakete prema odredištu tako što pogledaju koja je IP adresa odredišta u IP zaglavljiju paketa, odrede kojoj mreži pripada odredišna IP adresa i zaključe kojom stazom je najbolje proslijediti taj paket prema odredišnoj mreži. Neka je na Internetu neki paket s IP adresom odredišta 161.53.35.144. Pojednostavljeni, routeri na Internetu će prema toj adresi zaključiti da je odredište u mreži B klase i to u mreži 161.53.0.0, a svi oni znaju gdje je ta mreža i kojim putem je najbolje poslati paket prema toj mreži. Ovi routeri, dakle, usmjeravaju samo na temelju adrese cijele mreže A, B ili C klase, tj. na temelju prvih 8, 16 ili 24 bita adrese odredišta.

Kada paket konačno dođe do Carnetove mreže, Carnetovi routeri počinju gledati i sljedećih nekoliko bitova adrese odredišta, budući da oni znaju kako je Carnetova mreža podmrežena.

Stoga Carnetovi routeri pakete unutar svoje mreže usmjeravaju prema sljedećim pravilima:

- svi paketi kojima je odredište u ovoj mreži imaju prvih 16 bitova 161.53
- ako su prva 3 bita trećeg okteta jednaki 000 usmjeriti u podmrežu ZG sveučilišta
- ako su prva 3 bita trećeg okteta jednaki 001 usmjeriti u podmrežu ST sveučilišta
- ako su prva 4 bita trećeg okteta jednaki 0100 usmjeriti u podmrežu OS sveučilišta
- ako je prvih 5 bitova trećeg okteta jednak 01010 usmjeriti u podmrežu DU sveučilišta

U slučaju naše adrese (161.53.35.144) treći oktet je jednak 00100011. Dakle, ovaj paket će routeri u Carnetovoj mreži usmjeriti prema ST sveučilištu.

Kada paket dođe do ST, tada routeri u mreži ST sveučilišta znaju kako je ta mreža podmrežena i unutar nje usmjeravaju pakete prema sljedećim pravilima:

- svi paketi kojima je odredište u ovoj mreži imaju prvih 16 bitova 161.53 i onda još 3 bita 001
- ako su sljedeća 2 bita (bitovi 4 i 5 u trećem oktetu adrese) jednak 00, usmjeriti u podmrežu FESB-a
- ako su sljedeća 2 bita (bitovi 4 i 5 u trećem oktetu adrese) jednak 01, usmjeriti u podmrežu EFST-a
- ako su sljedeća 4 bita (bitovi 4-7 u trećem oktetu adrese) jednak 1000, usmjeriti u podmrežu PFST-a

U slučaju naše adrese, bitovi 4 i 5 u trećem oktetu su 00 tako da će se paket usmjeriti prema FESB-ovoj mreži. Router (ili routeri) na FESB-u će isporučiti paket računalu na FESB-u koji ima adresu 161.53.35.144.

ZADACI ZA VJEŽBU 1 (PREDAJA IZVJEŠTAJA):

Riješite zadatke.

Zadatak 1. Ispisati mrežnu masku u dekadskom, binarnom i CIDR format za podmreže dovivene od mreže 172.18.0.0 uz uvjet da se dobije barem 3 podmreže. Za svaku podmrežu napisati adresu mreže te broadcast adresu.

Zadatak 2. Ispisati mrežnu masku u dekadskom, binarnom i CIDR format za podmreže dovivene od mreže 10.0.0.0 uz uvjet da svaka podmreža ima barem 3000 računala. Za svaku podmrežu napisati adresu mreže te broadcast adresu.

Zadatak 3. Koliko host-ova možemo adresirati sa mrežnom maskom 255.255.240.0? Obavezno napisati postupak!

Zadatak 4. Koja je broadcast adresa i koja je adresa mreže u kojoj se nalazi računalo s IP adresom 192.168.242.5/20?

Zadatak 5. Imamo mrežu čija IP adresa pripada klasi B i želimo napraviti 29 podmreža. Koju mrežnu masku moramo uzeti i zašto?

Zadatak 6. Provjerite jesu li dva računala s IP adresama 172.16.17.30/20 i 172.16.28.15/20 na istoj podmreži i zašto? Potvrditi računski.

Zadatak 7. Popunite slijedeću tablicu.

IP addressa	Klasa kojoj pripada	Broj bitova za podmreže i broj bitova hosta	Broj mogućih podmreža	Broj mogućih hostova
10.25.66.154/23	A	15 / 9	32768	510
172.31.254.12/24				
192.168.20.123/28				
63.24.89.21/18				
128.1.1.254/20				
208.100.54.209/30				

Zadatak 8. Prateći primjer podmrežavanja Carnet mreže, napravite podjelu mreže klase C sa IP adresom 204.17.5.0 koja ima zadanu masku 255.255.255.0, na mrežu za 100 računala, mrežu sa 50 računala i mrežu od 10 računala.

VJEŽBA 2: a) MREŽNE POSTAVKE NA VLASTITOM RAČUNALU

CILJ PRVOG DIJELA VJEŽBE

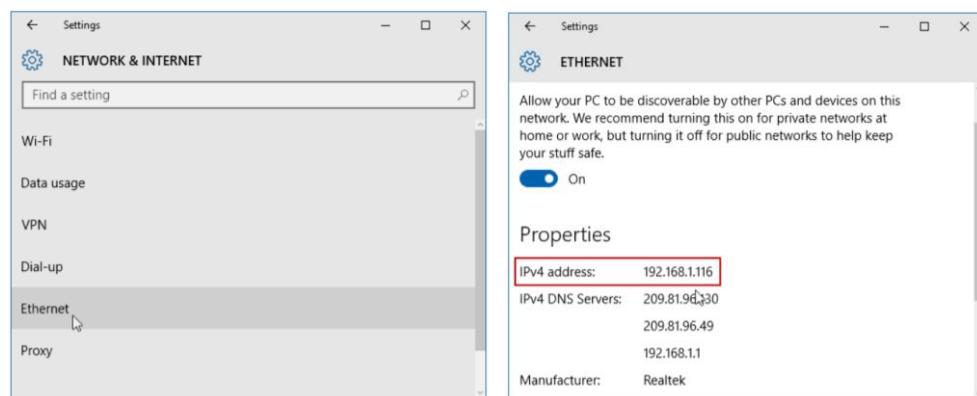
Primijeniti znanje sa uvodne vježbe i naučiti kako se mrežne postavke mogu postaviti na vlastitom računalu.

KAKO SAZNATI SVOJU IP ADRESU NA WINDOWS 10 RAČUNALU

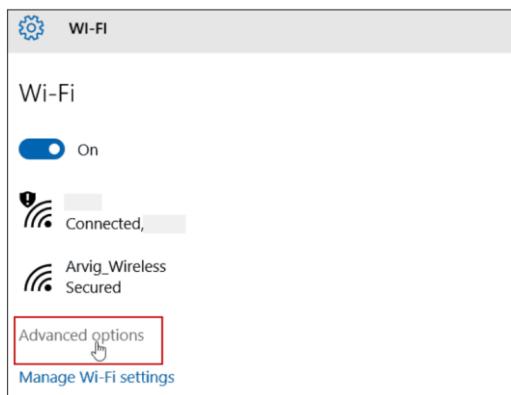
Podsjetimo se da je IP adresa vašeg računala (kao dio internet protokola), adresa koja pruža jedinstveni identitet vašeg uređaja na mreži. Bilo da se radi o lokalnoj mreži unutar intraneta u tvrtkama, vašem domu ili masivnoj mreži poput Interneta. Svako web mjesto koje posjetite na Internetu također koristi jedinstvenu IP adresu [7].

Postoji nekoliko načina na koje možete pronaći svoju IP adresu. Počnimo s najjednostavnijom metodom koja vam omogućuje upotrebu korisničkog sučelja Windows operacijskog sustava.

Na primjer, idite na Postavke → Mreža i Internet. Zatim odaberite Wi-Fi ili Ethernet (ovisno o načinu povezivanja uređaja). Autor je u donjem primjeru spojen na Ethernet, pa je odabrao tu opciju. Potrebno se pomaknuti dolje do odjeljka Svojstva (Properties) i vidjet ćete podatke o svojoj IPv4 adresi.



Ukoliko ste povezani na Wi-Fi, pronađenje vaših IP adresa će biti malo drugačije. Potrebno je ići na Postavke → Mreža i Internet, a zatim odabrati Napredne opcije. Ponovno se treba pomaknuti do odjeljka Svojstva kako bi se pronašla IP adresa uređaja.



Drugi način za pronađak IP adrese je preko terminala (Command Prompt) nakon što unesete naredbu

ipconfig < pritisnite enter >.

```
Administrator: Command Prompt
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : 
Ethernet adapter Ethernet 2:
Connection-specific DNS Suffix . . . . . : fesb.fesb.hr
Link-local IPv6 Address . . . . . : fe80::e10e:8fe%2:221:baec%3
Autoconfiguration IPv4 Address . . . . . : 169.254.186.236
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . . . . . : nsfhome.net
Link-local IPv6 Address . . . . . : fe80::e10e:8fe%4:192.168.137.25
IPv4 Address . . . . . : 192.168.137.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.137.1
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : 
D:\>
```

Vidjeli smo u prethodnoj vježbi kako možemo pomoći naredbe ping provjeriti da li je odredište aktivno/dostupno. Provjerimo da li možemo pristupiti web stranici www.fesb.hr. Vidimo pozitivan odgovor prema odredištu (od 4 poslana paketa, svi su primljeni).

```
Command Prompt
Microsoft Windows [Version 10.0.18363.1082]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Marina>ping www.fesb.hr

Pinging web4.fesb.hr [161.53.167.47] with 32 bytes of data:
Reply from 161.53.167.47: bytes=32 time=53ms TTL=54
Reply from 161.53.167.47: bytes=32 time=24ms TTL=54
Reply from 161.53.167.47: bytes=32 time=60ms TTL=54
Reply from 161.53.167.47: bytes=32 time=24ms TTL=54

Ping statistics for 161.53.167.47:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 60ms, Average = 40ms

C:\Users\Marina>nslookup www.fesb.hr
Server: speedport.ip
Address: 192.168.1.1

Non-authoritative answer:
Name: web4.fesb.hr
Address: 161.53.167.47
Aliases: www.fesb.hr
```

```
Command Prompt
C:\Users\Marina>ping 161.53.167.47

Pinging 161.53.167.47 with 32 bytes of data:
Reply from 161.53.167.47: bytes=32 time=22ms TTL=54
Reply from 161.53.167.47: bytes=32 time=22ms TTL=54
Reply from 161.53.167.47: bytes=32 time=23ms TTL=54
Reply from 161.53.167.47: bytes=32 time=23ms TTL=54

Ping statistics for 161.53.167.47:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 23ms, Average = 22ms
```

Također, kad god pretražujemo Internet i upišemo web stranicu u web preglednik, naše računalo komunicira s drugim uređajem kojeg nazivamo web server. On prima upit (na primjer www.fesb.hr), ali on ne zna što je "www.fesb.hr", on samo zna IP adresu i tu uskače DNS. Prije nego što browser pošalje upit na web server, on prvo pita DNS server koji je IP adresa od "www.fesb.hr". DNS možete shvatiti kao ogroman imenik koji povezuje imena sa brojevima, dakle on na sličan način mapira web stranice s njihovim IP adresama. Prema toj

logici, pretraživanje web stranica bismo mogli raditi i direktno preko IP adrese od "www.fesb.hr", umjesto preko imena (kako vidimo na slici gore uz pomoć naredbe nslookup to je 161.53.167.47). Naravno, nama je to jako neprirodno, puno je lakše pamtitи imena nego brojeve, tako da DNS obavlja posao pamćenja IP adresa za nas. Na gornjoj slici pokazali smo kako provjeriti navedeno uz pomoć naredbe ping.

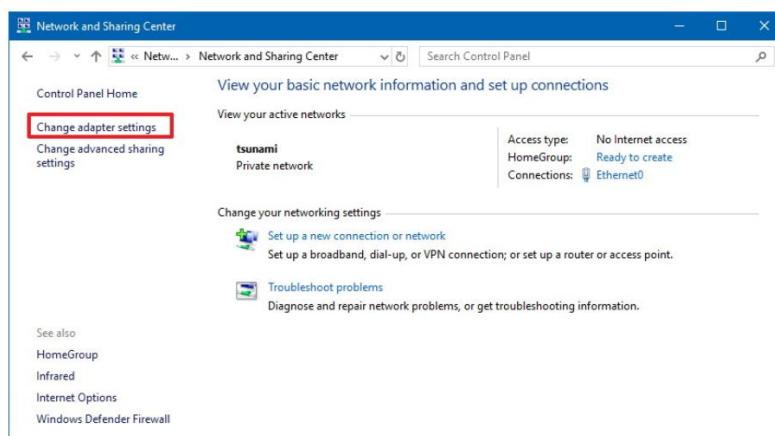
POSTAVLJANJE STATIČKE IP ADRESE NA WINDOWS 10 RAČUNALU

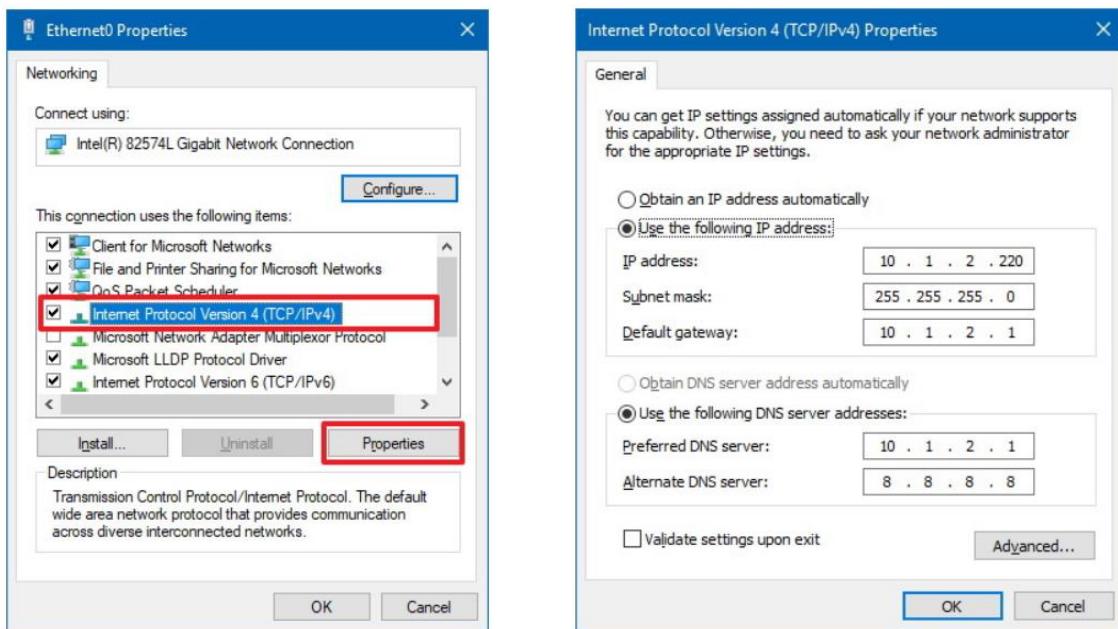
IP adresa se može postaviti na računalu na razne načine. Za dinamičko dodjeljivanje IP adresa zaslužan je Dynamic Host Configuration Protocol (DHCP) i koristi se najčešće kad mreža ima jako puno računala ili ako se računala povremeno spajaju na mrežu. Većina današnjih operacijskih sustava podržava DHCP poslužitelj. On olakšava konfiguraciju mreže jer eliminira ručno dodavanje mrežnih postavki i omogućava da su dodijeljene IP adrese ispravne i da u mreži nema sukoba adresa. Ovaj protokol može osim IP adrese dodjeliti i mrežnu masku, adresu default gateway-a i adresu DNS poslužitelja [8].

U sustavu Windows 10 često vam može zatrebatи postavljanje statičke IP adrese na vaš uređaj, to jest promjena vaše mrežne konfiguracije. Na primjer, ako želite dijeliti podatke s računalima na mreži, dijeliti datoteke ili pisač na lokalnoj mreži i slično.

Koraci za postavljanje statičke IPv4 adrese su idući [9]:

Prvo otvorite upravljačku ploču (Control Panel) → Mreža i Internet (Network and Sharing). Kliknite na opciju Promjeni postavke adaptera (Change adapter settings) u lijevom navigacijskom dijelu prozora, pa desnom tipkom miša kliknite mrežni adapter i odaberite opciju Svojstva (Properties). Odaberite opciju Internet Protocol Version 4 (TCP / IPv4) → Svojstva.





Odaberite opciju "Koristi sljedeću IP adresu" i postavite IP adresu (npr. Na gornjoj slici je to 10.1.2.220), mrežnu masku (npr. 255.255.255.0), te default gateway (obično IP adresa vašeg usmjerivača, npr. 10.1.2.1). U odjeljku "Koristite sljedeći set adresa DNS poslužitelja" postavite preferirani DNS poslužitelj (npr. 10.1.2.1), a izborno možete postavite alternativni DNS poslužitelj koji će vaše računalo koristiti ako ne može pristupiti željenom poslužitelju.

VJEŽBA 2: b) LOKALNE MREŽE ETHERNET

CILJ DRUGOG DIJELA VJEŽBE

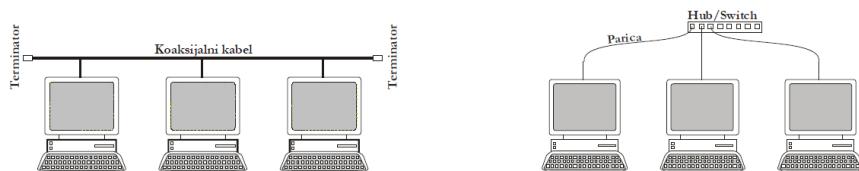
Primijeniti znanje s prethodnih vježbi na praktičnom primjeru u PT simulatoru. Teorijski dijelovi su preuzeti iz [5], a praktični dio vježbe prilagođen je prema [10], [11].

ETHERNET LAN MREŽA

Lokalna mreža omogućuje veliku brzinu prijenosa podataka i malo kašnjenje, a ograničena je na računala unutar prostorije ili zgrade (kratak doseg). Najčešće se koriste lokalne mreže tipa Ethernet, s ograničenjem brzine sa 10 megabita u sekundi (10 Mbps) na 100 Mbps za brzi Ethernet i 1000 Mbps za gigabitni Ethernet. Osim po brzini, lokalne mreže Ethernet mogu se podijeliti i po vrsti komunikacijskog medija koji se koristi za prijenos podataka (fizička razina ISO-OSI modela) pa postoje

- Ethernet na parici (Base-T) koji je daleko najčešća instalacija,
- varijante s koaksijalnim kablovima (Base 5 i Base 2) korištene u prošlosti,
- varijanta s optičkim vlaknima (Base-F) koja je dosta skuplja i stoga se rjeđe koristi.

Slijedi prikaz dvije karakteristične lokalne mreže:



LAN mreža na gornjoj slici lijevo je Base 5/2 i temelji se na koaksijalnim kabelima. Mrežne kartice sadrže koaksijalni konektor, na koji se priključuje tzv. T koaksijalni konektor, koji omogućuje spajanje svih računala u lokalnoj mreži u niz, pri čemu je bitno uočiti da sva računala koriste isti komunikacijski kabel (višespojni medij). Posljedica je takve organizacije da u određenom trenutku samo jedno računalo može slati podatke na lokalnu mrežu. Te podatke primaju sva računala koja su priključena na višespojni medij, a ako neko od računala u tom trenutku pokuša poslati podatke na mrežu nastupa kolizija (collision), stoga se koristi i termin domena kolizije za skup računala koji koriste isti višespojni medij.

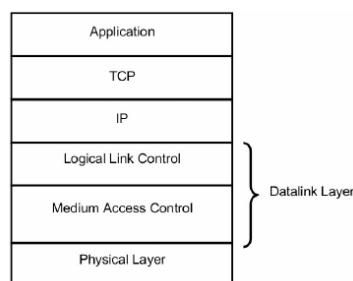
Protokol na kojem se temelji dijeljenje zajedničkog medija u Ethernet mreži je **MAC protokol** (Media Access Control). Mrežna kartica koja želi poslati podatke na medij osluškuje stanje medija i čeka trenutak kada medij postane slobodan (Carrier Sense). Kako više uređaja osluškuje zajednički medij ovaj pristup se naziva **Carrier Sense Multiple Access** (CSMA). Budući da signalu kojeg šalje jedna stanica treba određeno vrijeme da stigne do ostalih stanica, može se dogoditi da neka stanica počne slati podatke iako neka druga stanica već šalje, te dolazi do sudara (kolizije). Nastanak kolizije očituje se kroz nagli porast napona na vodu, a podaci koji su trenutno na mediju su izgubljeni i potrebna je retransmisija. Postupak otkrivanja sudara se naziva **Collision Detection** (CD). Ethernet mreže koriste oba navedena postupka, odnosno CSMA/CD.

Druga mreža na gornjoj slici desno temelji se na paricama uz pomoć kojih su računala spojena na hub (zvjezdiste) ili switch (prospoјnik). **Hub** je mrežni uređaj koji signal (paket) koji dobije na prijemnoj parici nekog od priključenih računala prosljedi na predajne parice svih ostalih priključenih računala, eventualno ga i pojača i očisti od šuma, ali nema inteligentnih funkcija u smislu čitanja podataka iz niza bitova koje primi.

Switch je intelligentniji od hub-a, budući da čita podatke iz primljenih paketa (okvira) i na temelju njih određuje na koji od svojih priključaka će poslati paket. Pritom ne može nastupiti kolizija jer se okvir ne prosljeđuje na sve priključke kao kod hub-a, već samo onom računalu kojem su podaci namijenjeni. **Broadcast okvire**, naravno, switch prosljeđuju na sve svoje portove osim dolaznog. Njihovo prosljeđivanje ograničava se uređajima više razine (to su router i gateway), tj. ovi uređaji odvajaju tzv. **broadcast domene**.

PROTOKOLI LOKALNE MREŽE ETHERNET

Na slici dolje lijevo prikazane su Ethernet podrazine u TCP/IP skupu protokola.



Fizička razina kod Ethernet mreža definira kodiranje/dekodiranje i prijem/predaju električnog signala, generiranje prembule. **Podatkovna razina** (datalink layer) je podijeljena u dva dijela:

- MAC pod razina koja implementira funkcije pristupa mediju
- LLC razina koja prihvata podatke od nadređene razine (najčešće IP), formira okvire lokalne mreže, popunjava polja adresa i kontrolne sume, a kod prijema okvira testira njegovu ispravnost, odvaja podatkovni dio od zaglavljiva okvira i prosljeđuje ga nadređenoj razini.

Ethernet II okvir je prikazan na idućoj slici:

8 okteta	6 okteta	6 okteta	2 okteta	46 do 1500 okteta	4 okteta
Preamble	Odredišna adresa	Izvořišna adresa	Tip okvira	Podaci i dopuna	CRC

Dva su polja iz zaglavja jako bitna: **odredišna i izvořišna adresa** adresiraju dva računala (mrežne kartice) koji izmjenjuju okvire. Svaka kartica unutar svoje ROM memorije ima upisanu adresu, koja je jedinstvena, tj. ne postoji dvije kartice koje imaju identičnu (MAC) adresu. Ona je duljine 6 okteta, pri čemu su gornja tri okteta identifikacija proizvođača kartice, a donja tri su vrijednost koju dodjeljuje proizvođač. Ukoliko je mreža kreirana uz korištenje hub-a ili koaksijalnih kabela, svaki okvir koji se pojavi na mreži prihvati svaka kartica, ali se nadređenoj razini (najčešće IP) prosljeđuju podaci samo u tri slučaja:

- ako je odredišna adresa jednaka adresi kartice,
- ako je odredišna adresa broadcast (0xFFFF FFFF FFFF),
- bezuvjetno, ako je kartica u tzv. promiskuitetnom modu, kod testiranja.

Polje **Tip okvira** (Frame Type ili EtherType) definira protokol korišten na mrežnoj razini, i kod najčešćeg protokola mrežne razine (IP) iznosi 0x0800.

Preamble služi za sinkronizaciju po bitu i okviru, a sastoji se od 7 okteta oblika 10101010 te zadnjeg okteta oblika 10101011.

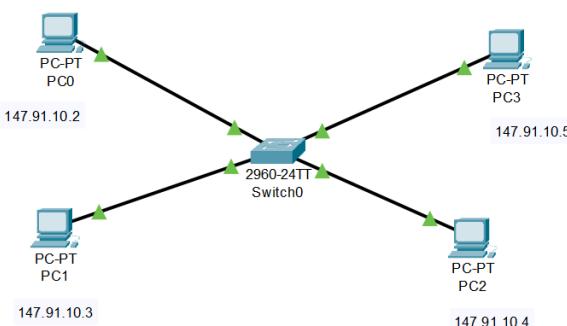
Podaci su paket protokola nadređene razine (najčešće IP paket), a **CRC** je ciklička zaštita koja se dodaje u svrhu detektiranja pogreški prilikom primanja okvira.

Sada je moguće detaljnije opisati rad switch-a. **Switch** analizira promet preko svojih ulaza i gradi tablicu, koja mu omogućuje da Ethernet okvir prosljedi na onaj svoj priključak na koji je spojena mrežna kartica s MAC adresom koja se nalazi u polju Odredišna adresa (Destination Address) zaglavlja okvira. Spomenuta switch tablica ili tablica MAC adresa sadrži parove MAC adresa - port. Svakom priključku switch-a može biti pridruženo više MAC adresa ukoliko je na njega spojen hub s više priključenih računala. Ukoliko je mreža kreirana uz korištenje switch-a, okviri koji dolaze do mrežne kartice bit će samo oni koji imaju odredišnu MAC adresu identičnu MAC adresi kartice, ili **broadcast okviri**.

POVEZIVANJE RAČUNALA NA SWITCH U ETHERNET LAN

Kako je već navedeno, switch-evi i hub-ovi imaju više ethernet portova koji su međusobno povezani i kada želimo dodati novo računalo u mrežu, trebamo ga povezati na slobodan ethernet port. Ponovimo kako je osnovna razlika između switch-a i hub-a to što **hub** svaki paket koji primi na nekom od portova šalje na sve ostale portove bez obzira na sadržaj tog paketa. Problem kod hub-a je što može izazvati zagušenje mreže proslijednjem nepotrebnih poruka, ali zato ima jednostavnu konfiguraciju i nisku cijenu. **Switch** s duge strane provjerava odredišnu adresu u okviru primljenog paketa i na temelju toga šalje paket na odgovarajući port te izbjegava zagušenje mreže.

Kreirajmo zvjezdastu topologiju mreže kao na slijedećoj slici:



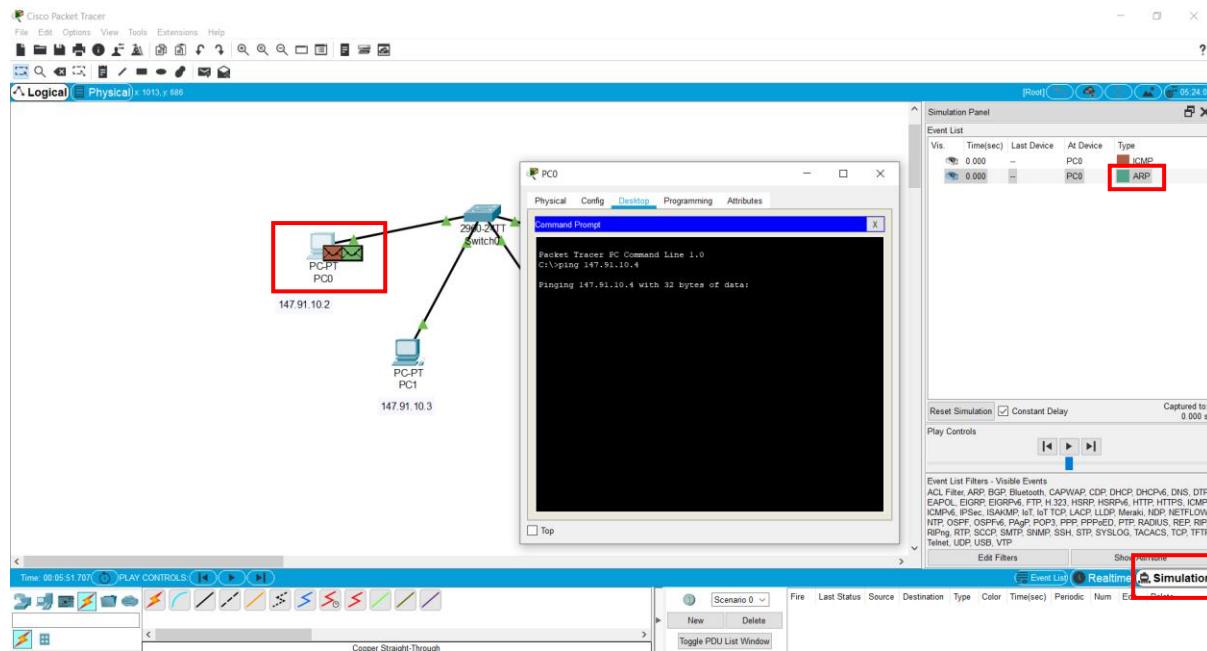
IP adrese svakog računala naznačene su kao labele, dok je mrežna maska postavljena svima na 255.255.0.0. **Provjerite jesu li računala na istoj mreži i koja je adresa mreže!**

Testirajmo vezu između računala korištenjem ping komande u simulacijskom modu. Tako ćemo moći pratiti putanje paketa korak po korak i analizirati sadržaj paketa u svakom koraku na putu od izvorišta do odredišta. Za testiranje ove opcije potrebno je aktivirati simulacijski mod, zatim otvoriti Command Prompt računala PC0 i unijeti komandu:

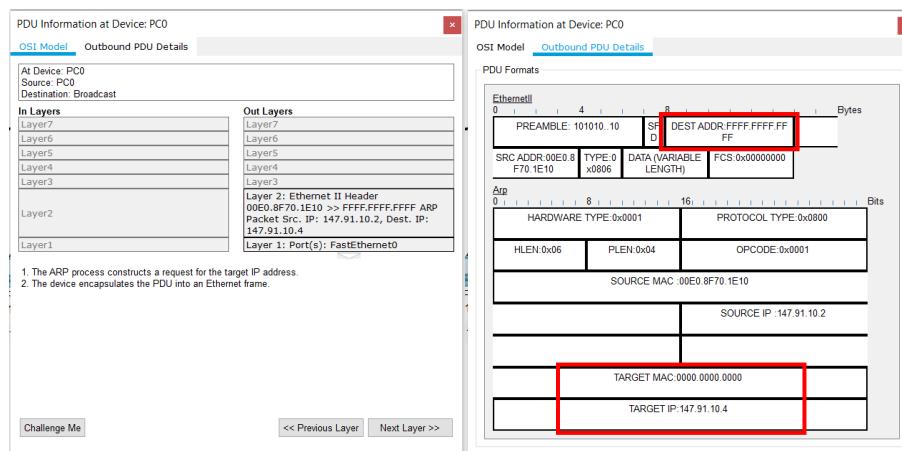
```
ping 147.91.10.4
```

U Packet Tracer simulaciji koja je prikazana na slici ispod možemo vidjeti da su nakon unosa komande ping kod računala PC0 kreirana 2 paketa (smeđi i zeleni paketić). Značenje ovih paketa se može naći u simulacijskom prozoru sa desne strane (Simulation Panel) gdje piše da su to paketi tipa ICMP i ARP. **ICMP** (Internet Control Message Protocol) paketi se koriste za testiranje komunikacije odnosno ostvarenih veza između računala. **ARP** (Address

Resolution Protocol) služi za određivanje fizičke (MAC) adrese računala kojem je namijenjena poruka. Uspješno slanje poruke zahtijeva da u okviru polja za odredište zaglavlja ethernet paketa stoji MAC adresa odredišnog računala. Izvođeno računalo međutim zna samo IP adresu odredišnog računala i nema nikakvu informaciju o njegovoj MAC adresi. ARP upit se šalje svim računalima u okviru mreže i svako računalo koje dobije ovu poruku provjerava da li odredišna IP adresa odgovara njegovoj IP adresi. Ono računalo koje prepozna svoju IP adresu šalje natrag ARP odgovor u kojem se nalazi njegova MAC adresa. Nakon uspješno određene MAC adrese izvođe može sastaviti Ethernet okvir s tom adresom kao odredištem, a sadržaj okvira će biti ICMP poruka (ping upit).

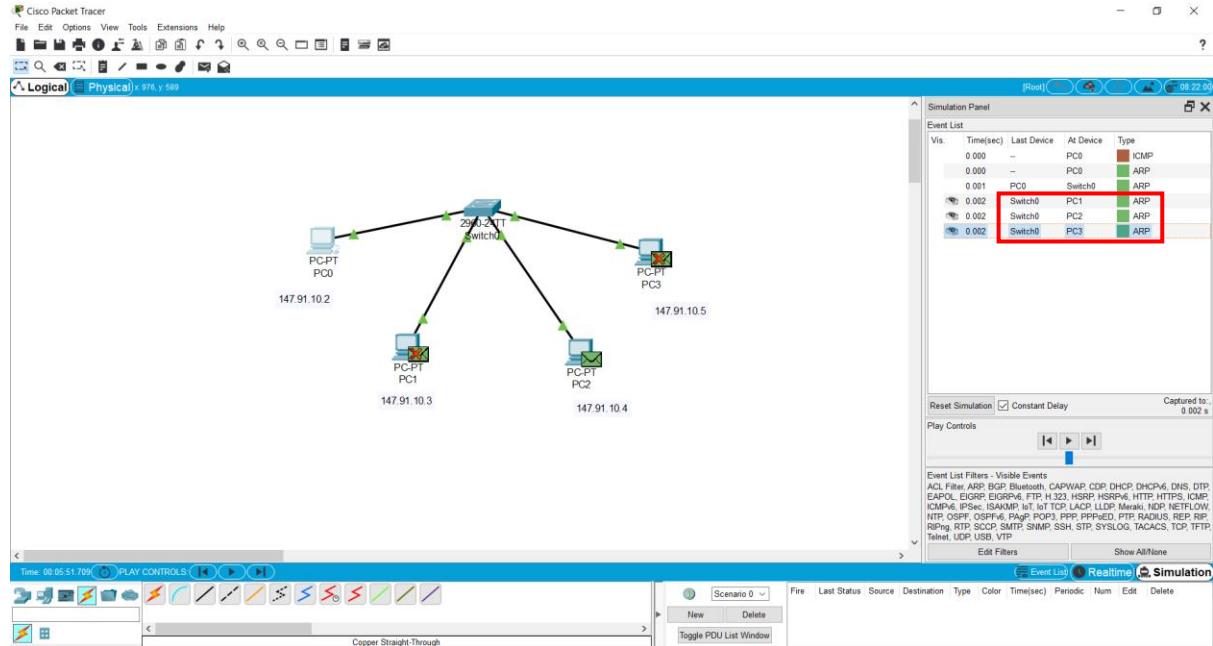


Slijedeći korak u simulaciji se izvršava klikom na Capture/Forward. Sadržaj svakog paketa se može analizirati klikom na obojeni kvadrat pored naziva paketa u okviru liste događaja na desnoj strani. Dolje lijevo je prikazan apstraktni opis slojevitne arhitekture mreže prema OSI-modelu i vidimo izlazni FastEthernet0 port na fizičkom sloju koji potječe od računala PC0 i kako se odlazni PDU formira u Ethernet okvir. Sadržaj odlaznog ARP paketa i Ethernet okvira je dan na slici desno.

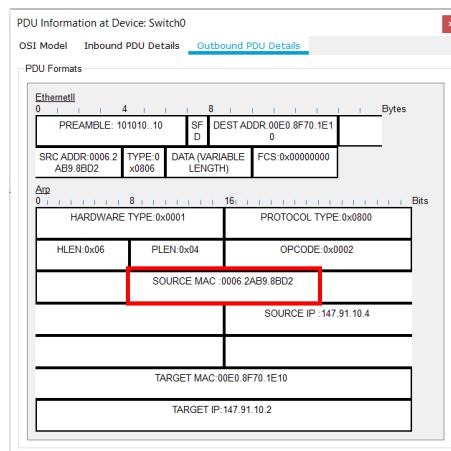


Kako nije poznata MAC adresa računala koji ima IP adresu 147.91.10.4, PC0 šalje ARP poruku svima (broadcast adresa FFFF.FFFF.FFFF). U okviru polja za podatke smještena je IP

adresa odredišta i prazno polje u koje odgovarajuće računalo treba upisati svoju MAC adresu. Izvršavanjem simulacije dalje vidi se da switch ovu ARP poruku prosljeđuje svim računalima u mreži, tj. u simulacijskom panelu vidimo tri ARP poruke. Računala PC1 i PC3 ne prepoznaju IP adresu koja se traži jer nije njihova i ignoriraju ovu poruku (prikazano crvenim križićem) dok računalo PC2 prepoznaže poruku i šalje nazad odgovor.

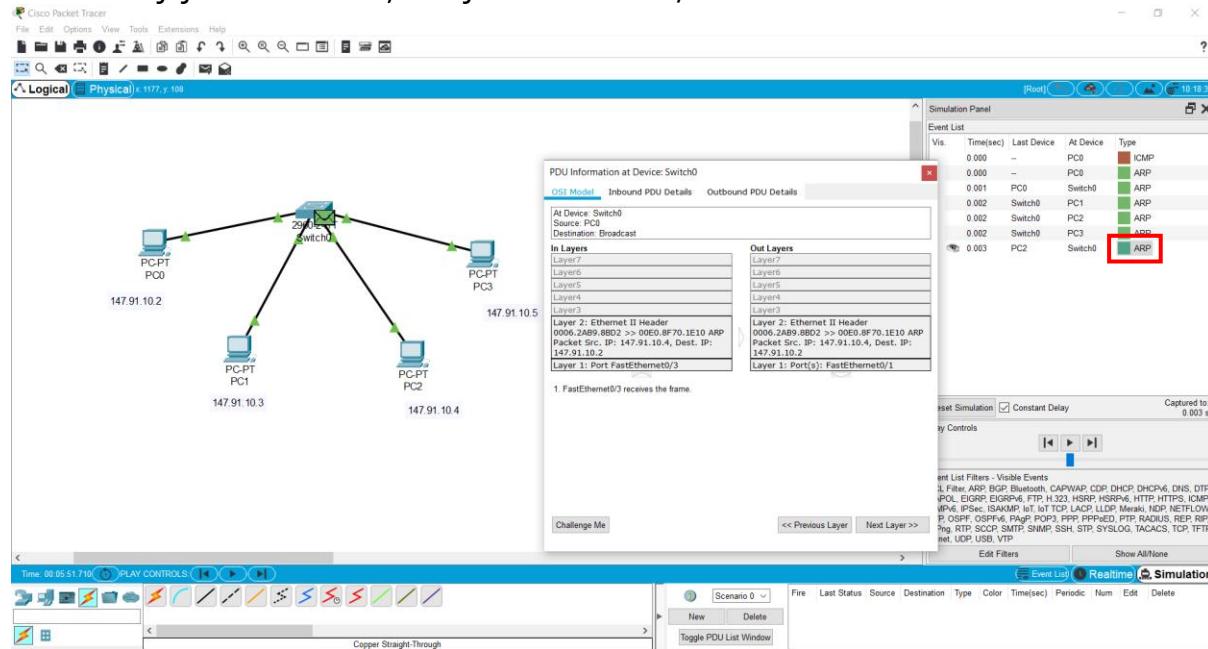


Pogledajmo dolje sadržaj ARP paketa koji se šalje kao odgovor računala PC2 na switch (to je na switch-u ulazni Inbound PDU), a to je ujedno i paket koji će se dalje u idućem koraku poslati od switch-a prema izvořnom računalu PC0 (to je označeno kao izlazni Outbound PDU sa switch-a na PC0). Upisana je MAC adresa računala PC2 kojeg je računalo PC0 i htjelo dohvatiti (MAC adresa od PC2 je 0006.2AB9.8BD2 i to je sada source MAC jer potječe od PC2), dok destination MAC pripada računalu PC0 i to je 00E0.8F70.1E10 (jer se odgovor šalje računalu PC0). Usput, primijetimo da je MAC adresa duljine 48 bita (12*4 bita).

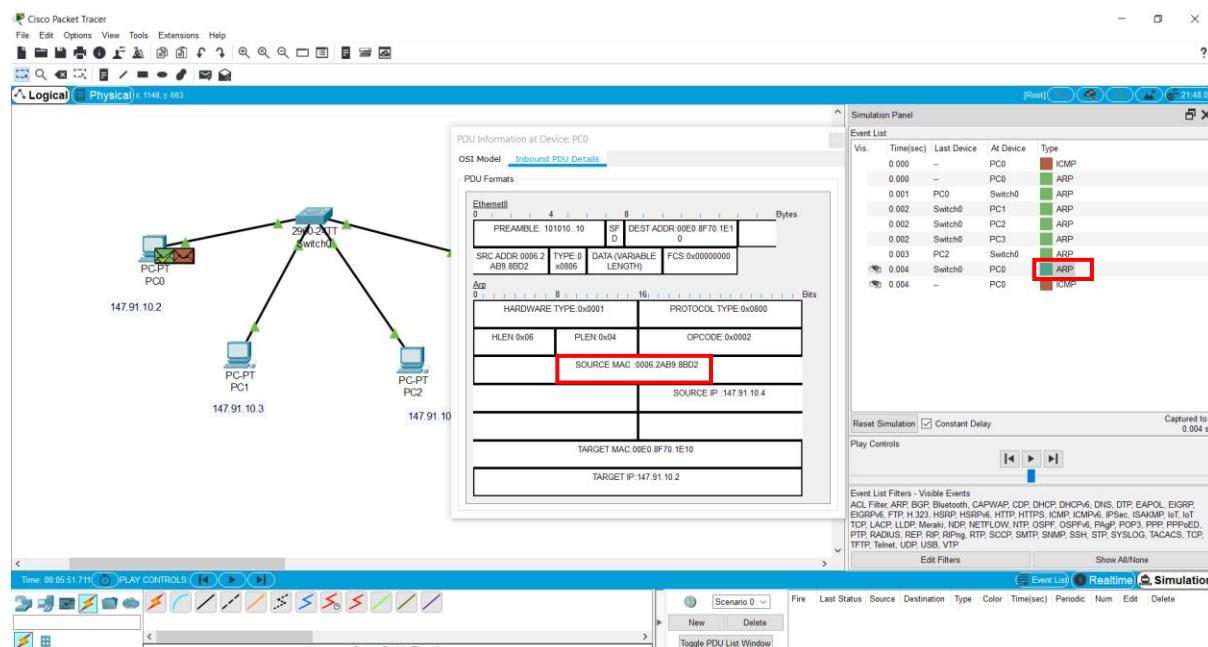


Na donjoj slici možemo popratiti slojevitu komunikaciju prema OSI referentnom modelu. Na lijevom tj. ulaznom stack-u vidimo kako switch na fizičkom sloju (OSI Layer 1) i to na portu FastEthernet0/3 prima PDU kao odgovor od PC2. Nakon toga na podatkovnom sloju (OSI Layer 2) formira Ethernet okvir.

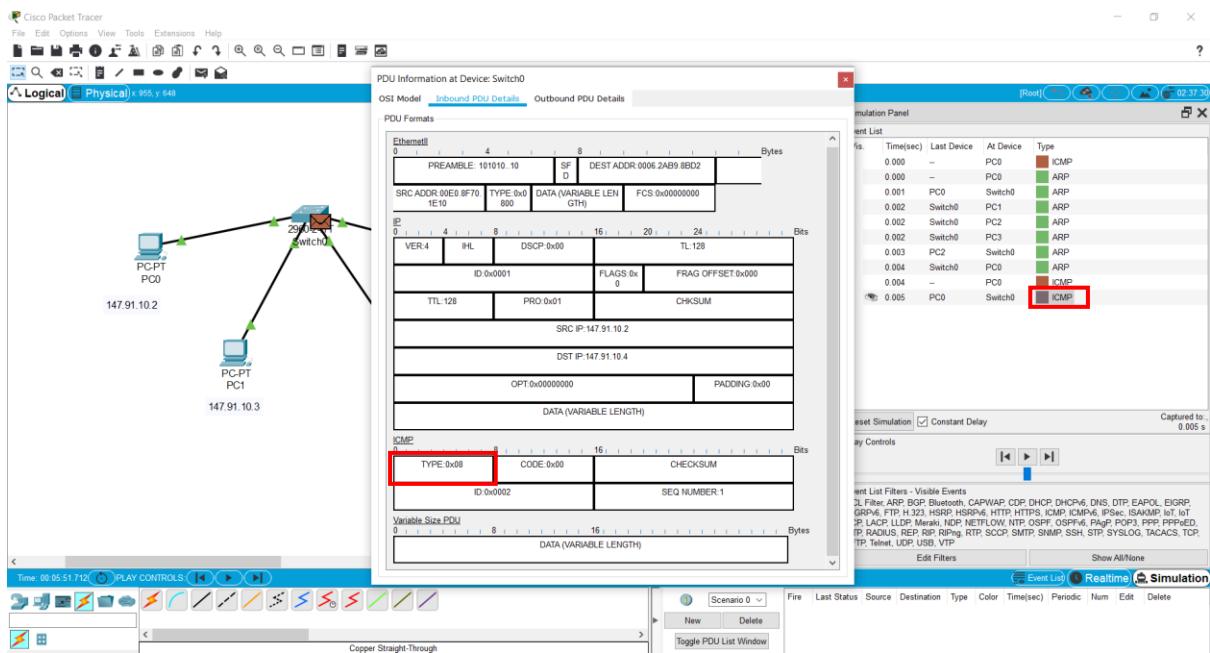
Također, na desnom tj. izlaznom stack-u OSI modela vidimo kako switch šalje okvir na izlazni port. Kada gledamo fizičku razinu za izlazni PDU, on se proslijeđuje samo na port switch-a koji je vezan za PC0, a to je FastEthernet0/1.



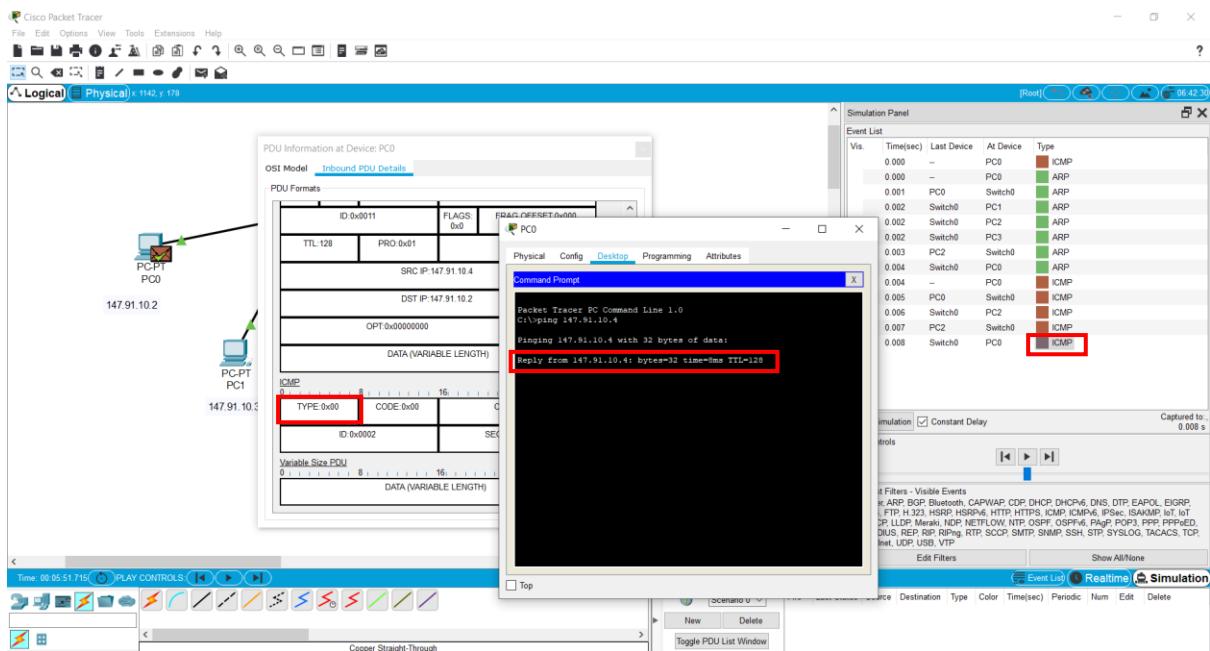
Nastavite idući korak simulacije kako bi se ARP paket prosljedio sa switch-a na PC0. Uredaj nakon primitka paketa na portu FastEthernet0 odvaja PDU od Ethernet okvira i analizira se ARP okvir. Uredaj ažurira svoju ARP tablicu sa informacijama o MAC adresi od PC2 dobivenim iz ARP okvira. Nakon toga će računalo PC0 poslati ICMP poruku na switch.



ICMP paket kojeg PC0 šalje na switch je Echo Request, što možemo vidjeti po 8-bitnom tipu ICMP poruke u zaglavljtu paketa (kod 0x08). Sama ICMP poruka je enkapsulirana unutar IP paketa.



Izvršite nekoliko dalnjih koraka simulacije dok se ne dobije prvi ICMP odgovor od PC2 do PC0. Pogledajte detalje ICMP poruke koja je došla kao 8-bitni tip Echo Reply (kod 0x00).

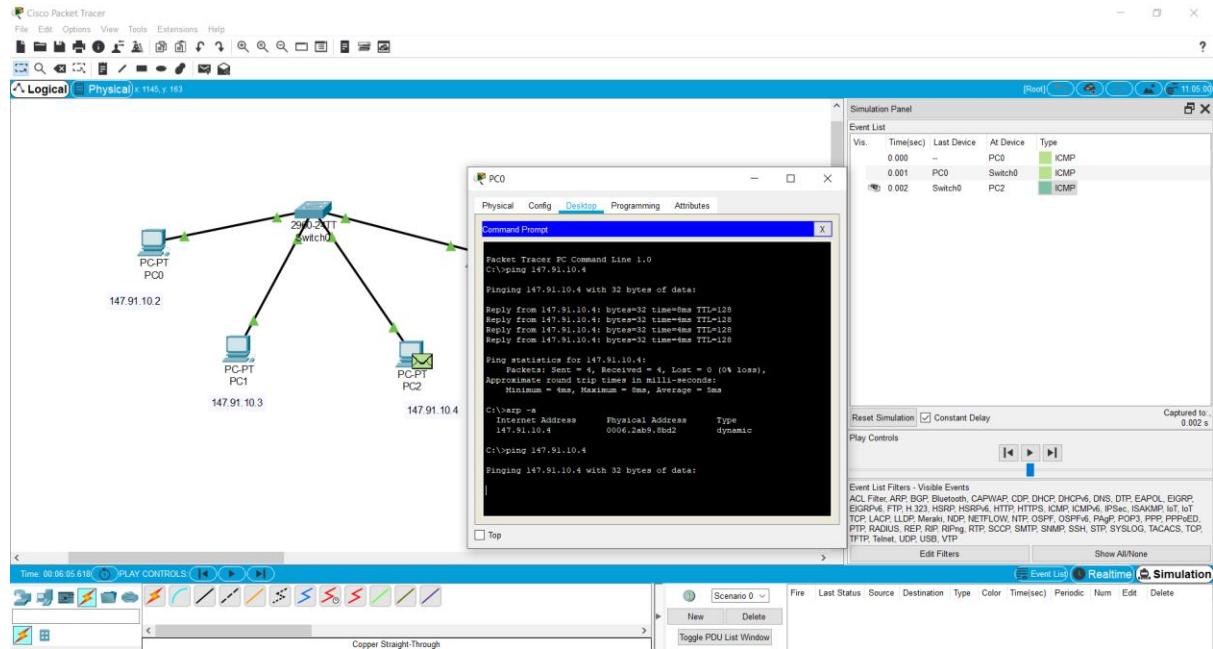


Nastavite simulaciju sve dok svi paketi podataka u Command Promptu nisu primljeni, tj. dok ping naredba nije do kraja izvršena (PC0 je primio sve ICMP Echo Reply poruke).

Nakon toga provjerite ARP tablicu na računalu PC0 uz pomoć naredbe **arp -a**. Možemo vidjeti da je u tablicu upisan par IP adresa računala PC2 - MAC adresa računala PC2, što znači kako je računalo PC0 sada "saznalo" MAC adresu od PC2 pa mu neće više trebati ARP protokol za buduću komunikaciju sa PC2 (osim ako mu izbrisemo zapise u ARP tablici uz pomoć naredbe **arp -d**).

Dakle, nakon uspješno određene MAC adrese odredišnog računala PC2, ova adresa se sprema u mrežnoj kartici računala PC0 i nastavlja se komunikacija slanjem ICMP poruka.

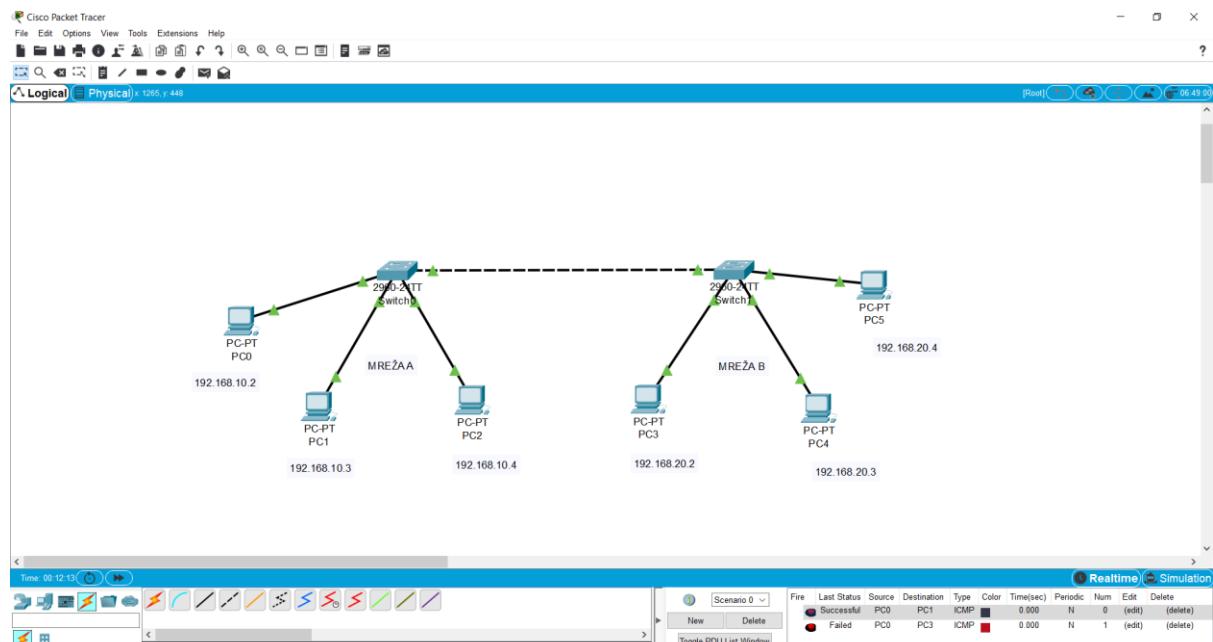
Pokušajte sada ponovno pingati računalo PC2 sa PC0 i uočite promjene u simulaciji, tj. kako više nema ARP paketa nego se šalju direktno ICMP poruke.



Spremite Packet Tracer topologiju pod nazivom **ime_prezime_zadatak1.pkt**.

KOMUNIKACIJA IZMEĐU LAN MREŽA

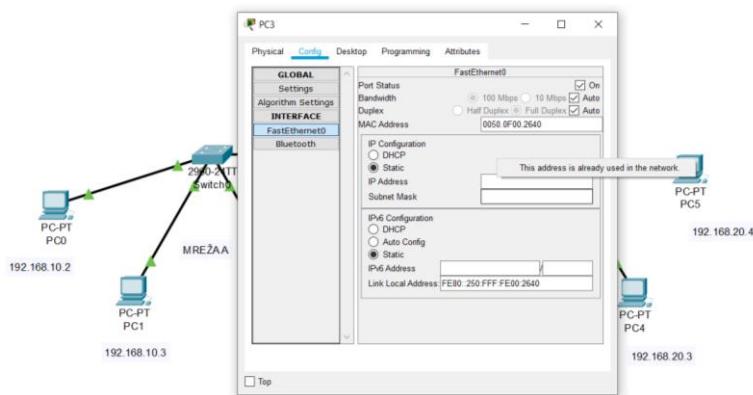
Kreirajmo novu Packet Tracer topologiju sa dvije različite LAN mreže i nazovimo ih mreža A i mreža B. Adrese mreža A i B su 192.168.10.0/24 i 192.168.20.0/24 (podsjetimo se da 24 bita adrese predstavljaju adresu mreže dok je 8 bita namijenjeno adresi računala). U svakoj mreži nalaze se po 3 računala sa odgovarajućim IP adresama prema slici.



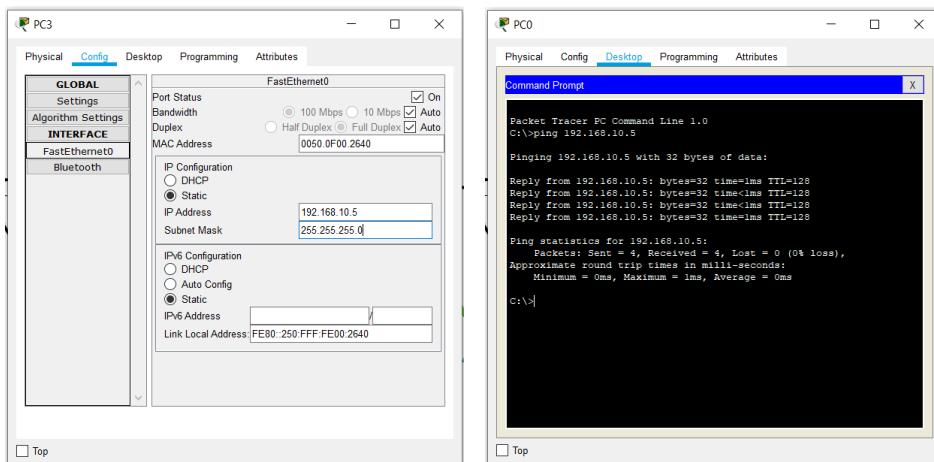
Provjerimo komunikaciju unutar mreže A (od PC0 do PC2) i komunikaciju između mreža (od PC0 do PC3) u Realtime načinu rada i vidimo da je prva komunikacija uspješna, a druga nije.

Razlog tome je što su računala u prvom slučaju u istoj mreži, a u drugom u različitim mrežama iako su switch-evi povezani Copper Cross-Over kabelom.

Postavite računalu PC3 ispravnu IP adresu kako bi bio u istom LAN-u dakle u mreži A i kako bi mogao komunicirati sa PC0. Za početak, pokušajte računalu PC3 promijeniti IP adresu u 192.168.10.2. Vidimo da tu adresu ne možemo dodijeliti jer je ona već dodijeljena računalu PC0 – dakle, vidimo da IP adresa u mreži **mora biti jedinstvena**.



U idućem scenariju dodijelimo IP adresu 192.168.10.5/24 i ponovno testirajmo komunikaciju PC0 i PC3. Vidimo da smo uspješno prebacili računalo PC3 u mrežu A i da je komunikacija u mreži sada uspješna.



Spremite Packet Tracer topologiju pod nazivom **ime_prezime_zadatak2.pkt**.

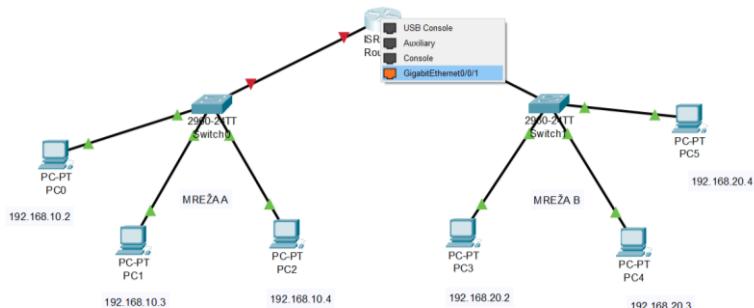
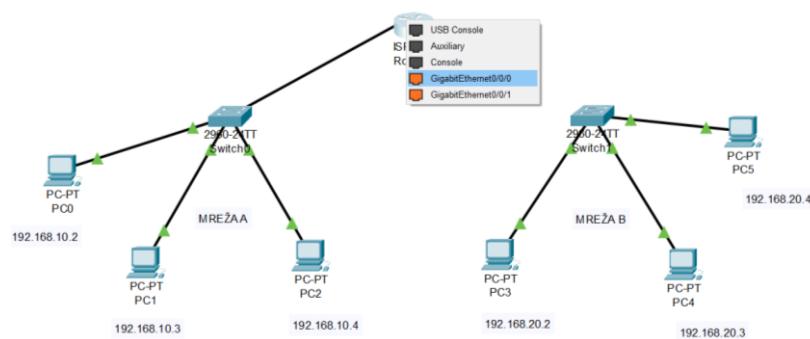
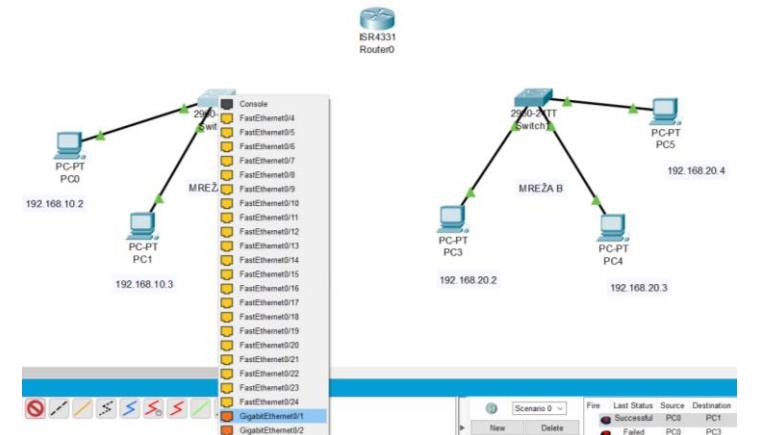
POVEZIVANJE LAN MREŽA PREKO ROUTERA

Vratimo sada računalu PC3 njegovu „staru“ adresu iz mreže B (to je bila IP adresa 192.168.20.2). Također, izbrišimo vezu između switch-evi. Kako možemo ostvariti komunikaciju između ovih naših odvojenih LAN mreža?

Ukoliko želimo povezati ove dvije mreže, ili omogućiti da se računala iz pojedinih mreža spoje na Internet, potreban nam je uređaj više razine – **usmjernik ili router**.

Dakle, dodajmo router i povežimo ga na oba switch-a korištenjem Copper Straight-Trough kabela. Na switch-evima ovaj put odaberimo GigabitEthernet 0/1 portove, a na routeru

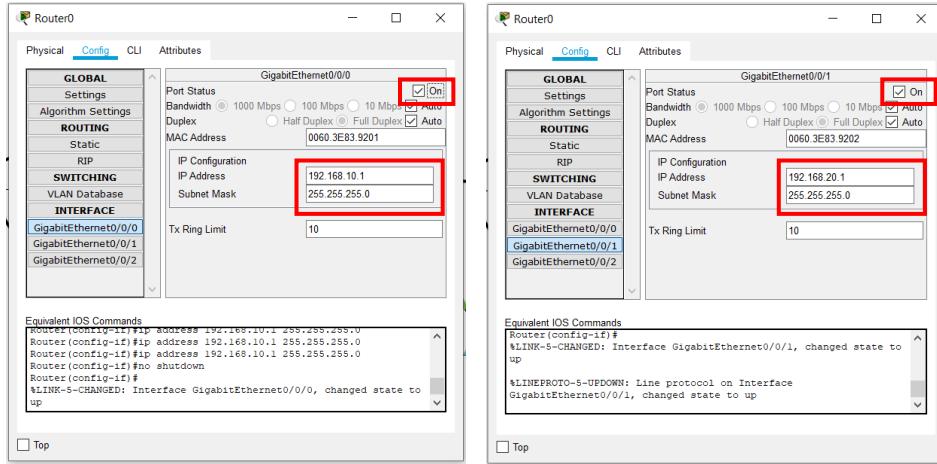
pažljivo odaberimo GigabitEthernet 0/0/0 port za switch od mreže A i GigabitEthernet 0/0/1 port za switch od mreže B.



Portovi na sučelju GigabitEthernet 0/0/0 i 0/0/1 router-a pripadaju odgovarajućim mrežama A i B i uzimaju adrese iz odgovarajućeg opsega adresa. Router predstavlja vezu (gateway) između mreža. Obično postoji jedan podrazumijevani router kojem se šalju svi podaci čije odredište nije u našoj lokalnoj mreži. Ovaj router se naziva **default gateway** i obično ima najnižu adresu iz dostupnog opsega adresa. Port router-a na koji je spojena naša lokalna mreža je i dalje dio naše mreže, tj. to je krajnja točka lokalne mreže na putu prema drugim mrežama ili Internetu.

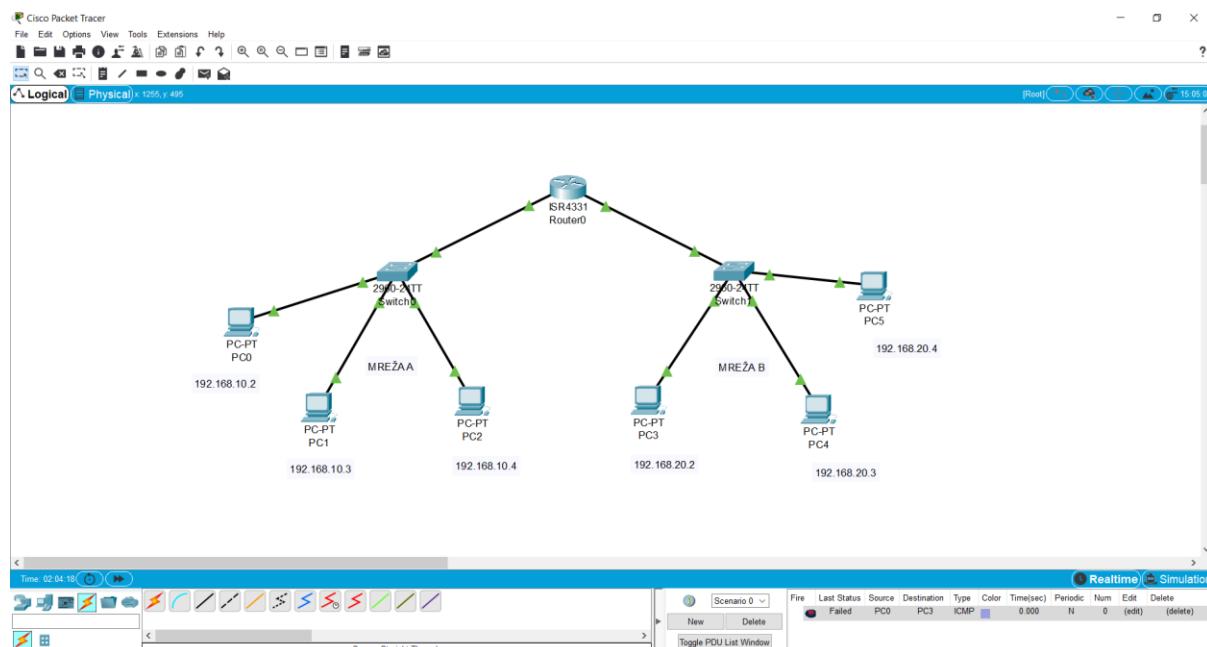
Postavimo tako IP adrese na sučeljima router-a, i to redom IP adresu 192.168.10.1 na sučelju prema mreži A i IP adresu 192.168.20.1 na sučelju prema mreži B. Primijetite da su adrese na sučeljima router-a odabrane tako da budu dio mreže na koju su spojeni.

Adrese priključaka router-a se u praksi podešavaju iz komandne linije međutim mogu se podesiti i pomoću grafičkog okruženja. Potrebno je kliknuti na router i pod tab-om Config pronaći GigabitEthernet 0/0/0 u kategoriji sučelja (Interface) kako je prikazano na slici dolje lijevo. Unesite IP adresu i odgovarajuća mrežna maska će se automatski postaviti. Isto ponovite i za sučelje GigabitEthernet 0/0/1 (slika dolje desno).



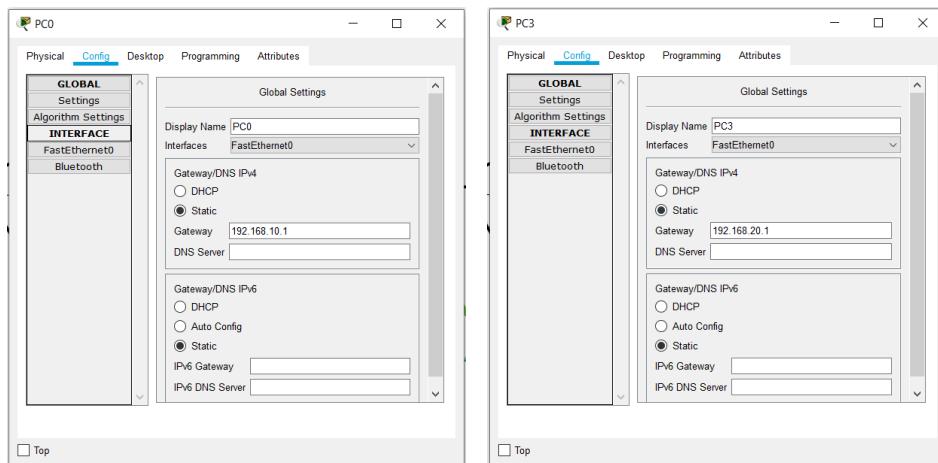
Nakon podešavanja IP adrese potrebno je aktivirati odgovarajući priključak router-a odabirom polja On u okviru grafičkog okruženja kao što je prikazano na gornjim slikama. Primijetite kako se sa svakim odabirom na grafičkom sučelju prilikom definiranja postavki routera automatski izvršavaju komande koje su ekvivalentne odabranim postavkama. Automatsko izvršavanje komandi je prikazano u donjem dijelu prozora.

Testirajmo sada komunikaciju od PC0 do PC3.

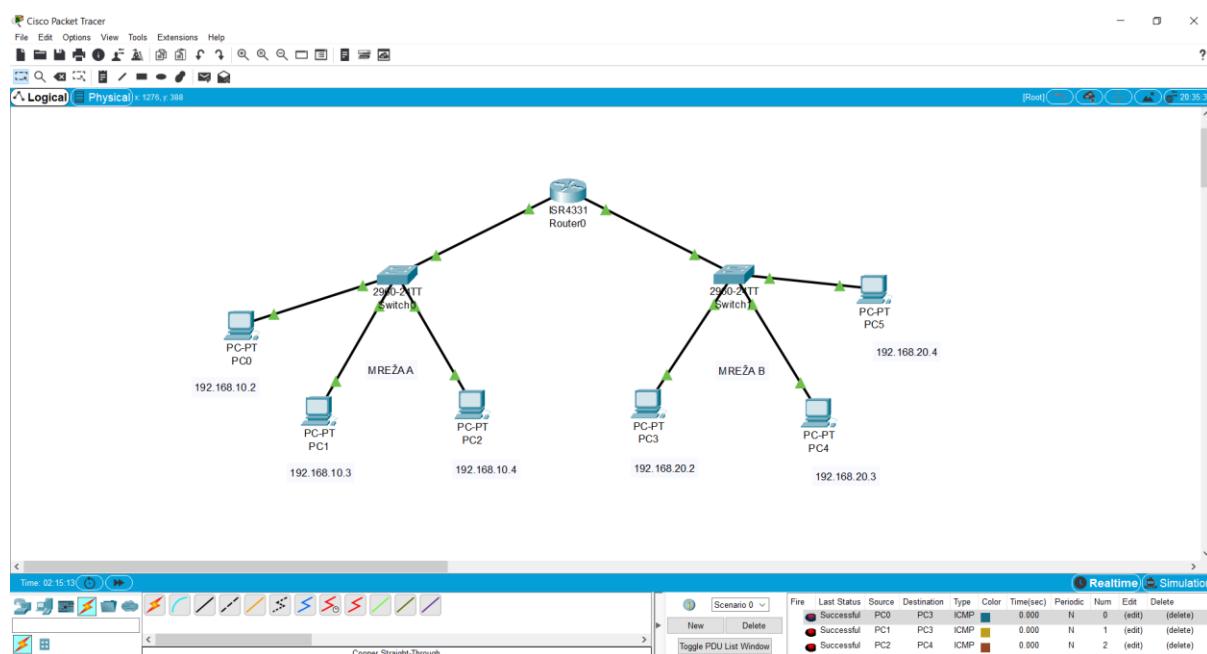


Komunikacija nije uspješna, jer je potrebno svim računalima u pojedinim LAN-ovima postaviti adresu odgovarajućeg default gateway-a, pazeći pritom na koje sučelje je pojedina mreža povezana. Tako je default gateway za sva računala iz mreže A potrebno postaviti na 192.168.10.1, a default gateway za sva računala iz mreže B treba biti 192.168.20.1.

Postupak kojim se primjerice postavlja adresa default gateway za računala PC0 i PC3 prikazan je na idućoj slici:



Provjerite da je komunikacija između LAN mreža A i B sada uspješno omogućena:

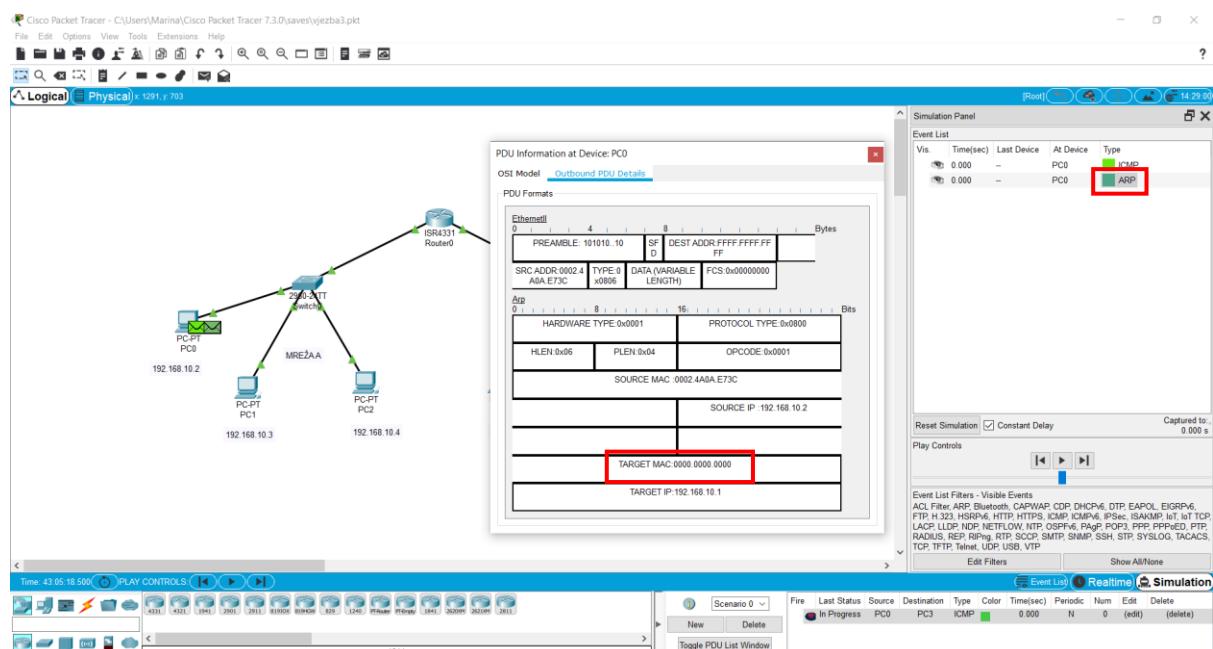
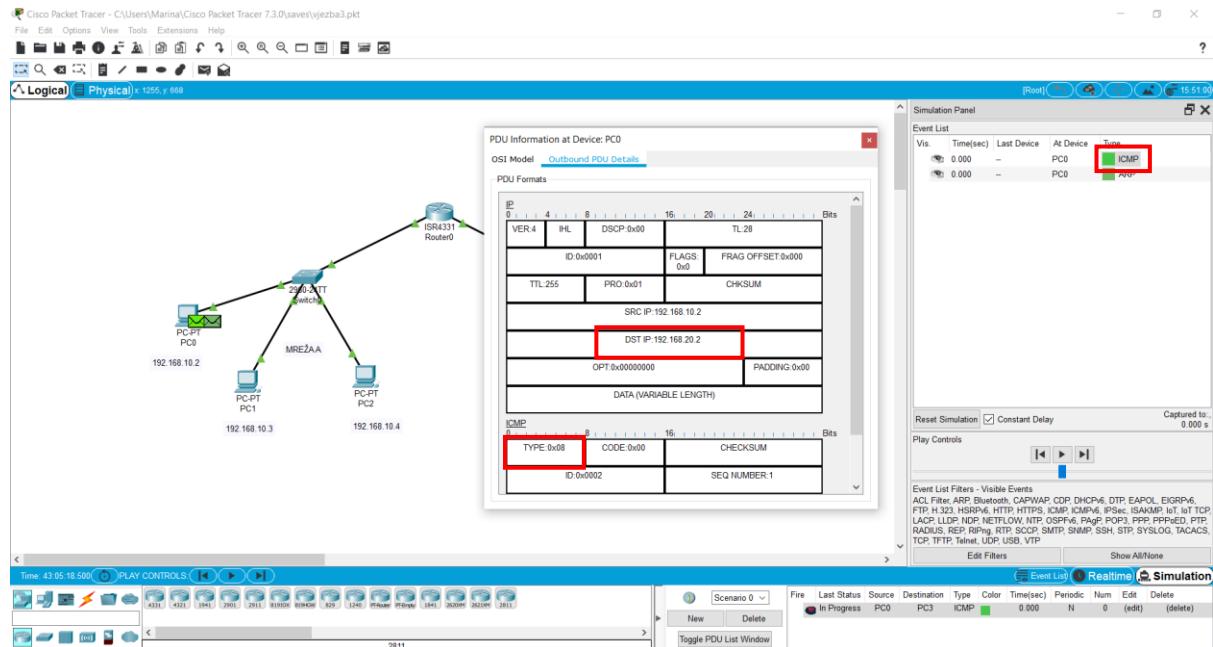


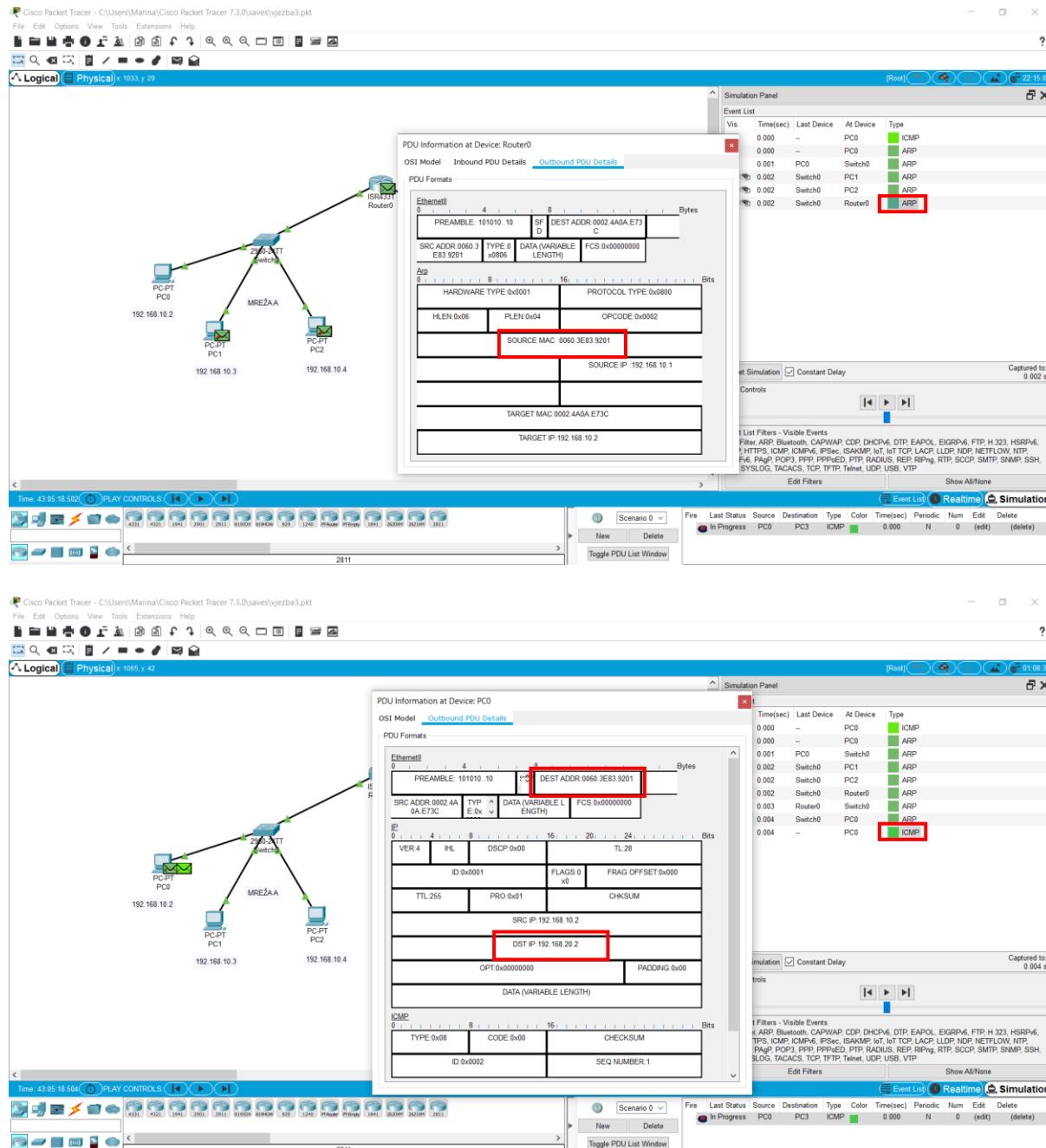
Ponovimo: default gateway je adresa na koju računalo šalje sve podatke čije odredište nije u lokalnoj mreži promatranog računala. Stoga prilikom slanja podataka računalo prvo provjeri je li odredište u njegovoj lokalnoj mreži. To se radi usporedbom mrežnog dijela IP adrese promatranog računala (izvorišta) i odredišta. Ako su ti dijelovi jednaki, računalo zaključi da je odredište u njegovoj lokalnoj mreži i sastavi okvir s MAC adresom odredišnog računala (ako je ne zna dozna je korištenjem ARP-a). S druge strane, ako računalo zaključi da odredište nije u njegovoj lokalnoj mreži, onda podatke koje želi poslati (npr. neki IP paket) stavi u okvir kojem je odredište MAC adresa default gateway-a (opet, ako ne zna tu MAC adresu dozna je korištenjem ARP-a).

Pratite pakete u simulacijskom modu od PC0 do PC3. Prvi paket je ICMP i računalo kreira poruku Echo Request (tip 0x08). Odredišna IP adresa je 192.168.20.2 i ona nije u istoj

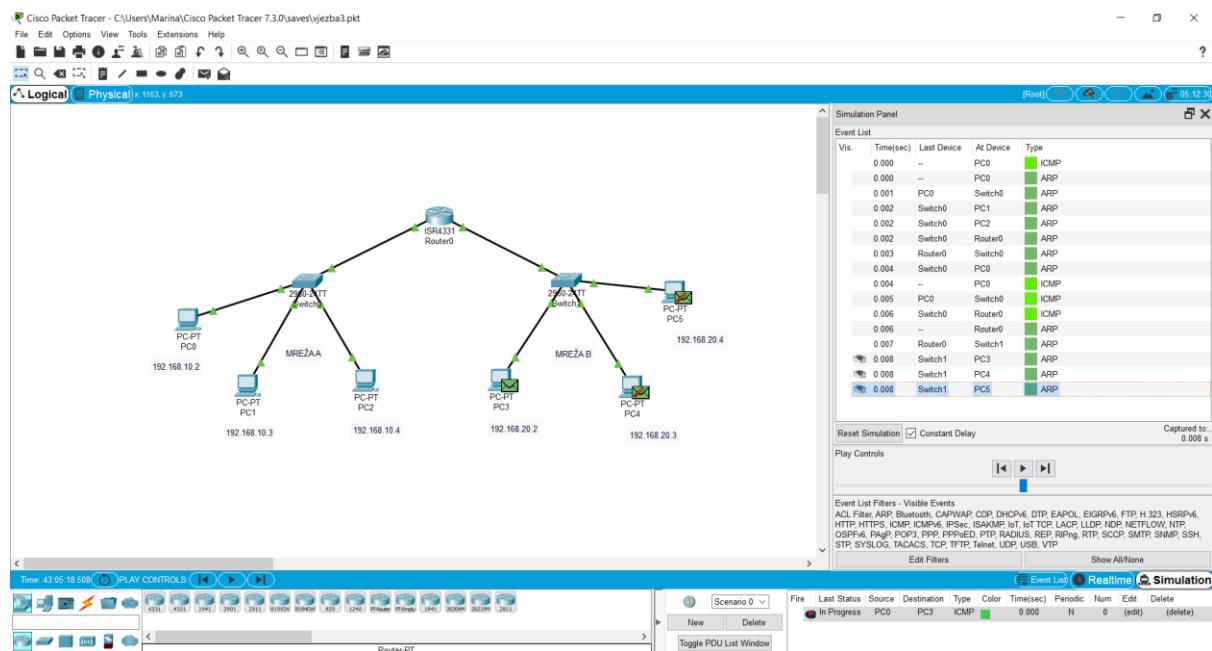
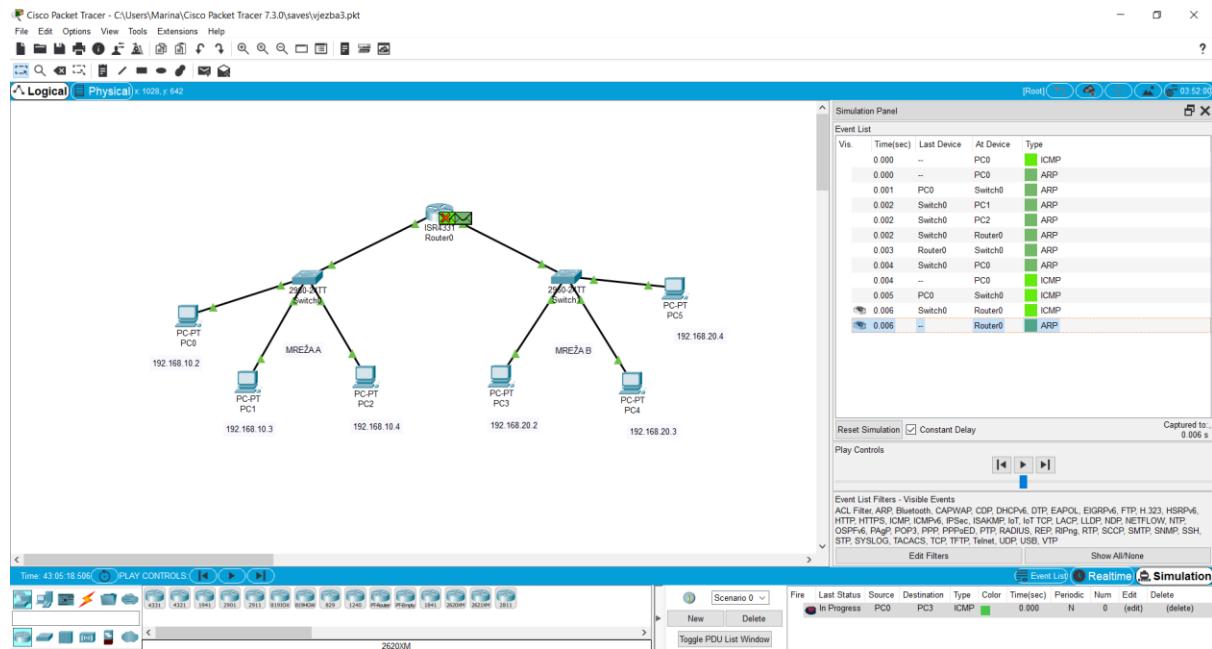
podmreži kao adresu od računala PC0. Zato će uređaj pokušati poslati poruku na default gateway koji je postavljen.

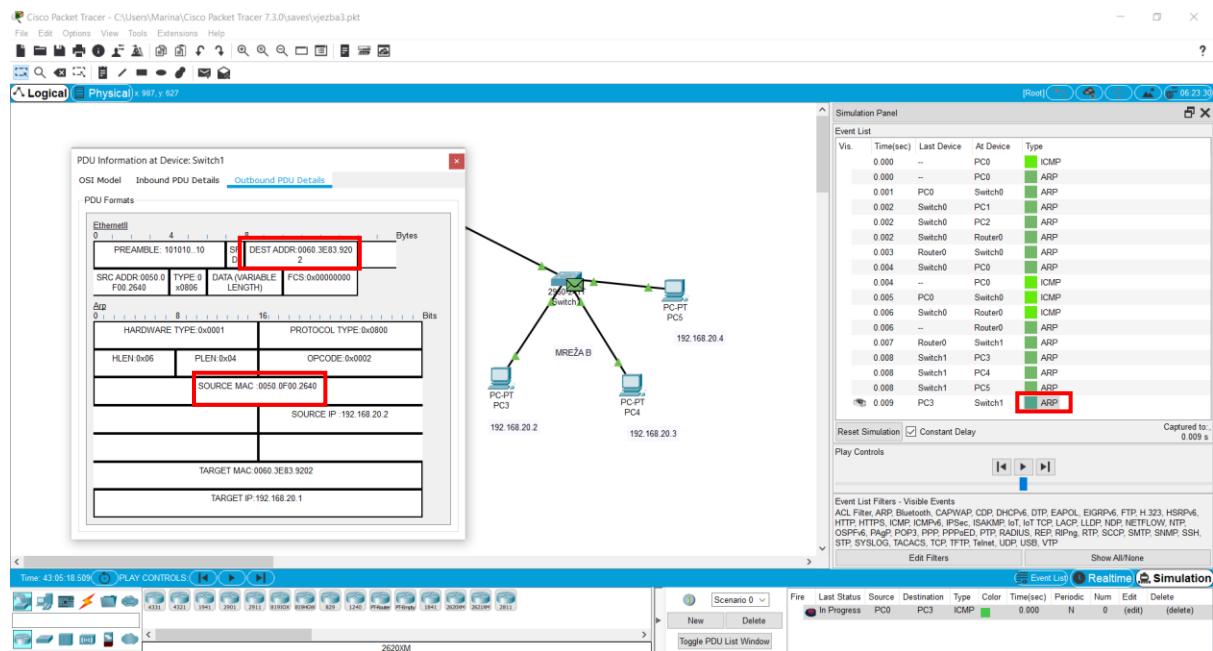
Kako bi izvorišno računalo doznalo MAC adresu router-a, formira se ARP zahtjev u kojem vidimo da je destination IP address postavljen na adresu default gateway-a 192.168.10.1. Switch formira tri ARP paketa i šalje ih na sva tri povezana uređaja i jedini koji prepozna svoj target IP je router koji u ARP odgovor upisuje svoju MAC adresu i šalje ga na switch. Switch proslijeđuje ARP odgovor na PC0 koji sada formira ICMP poruku koja je spremna za slanje. Primijetite kako je sada u paketu dodano Ethernet II zaglavlje koje govori da je odredišni MAC na koji se okvir treba poslati MAC adresa router-a. S druge strane, u zaglavljiju IP paketa je kao adresa odredišta navedena IP adresa konačnog odredišta (PC3). Na temelju ove adrese će IP proces na routeru odrediti kamo dalje treba poslati paket kako bi došao do konačnog odredišta.



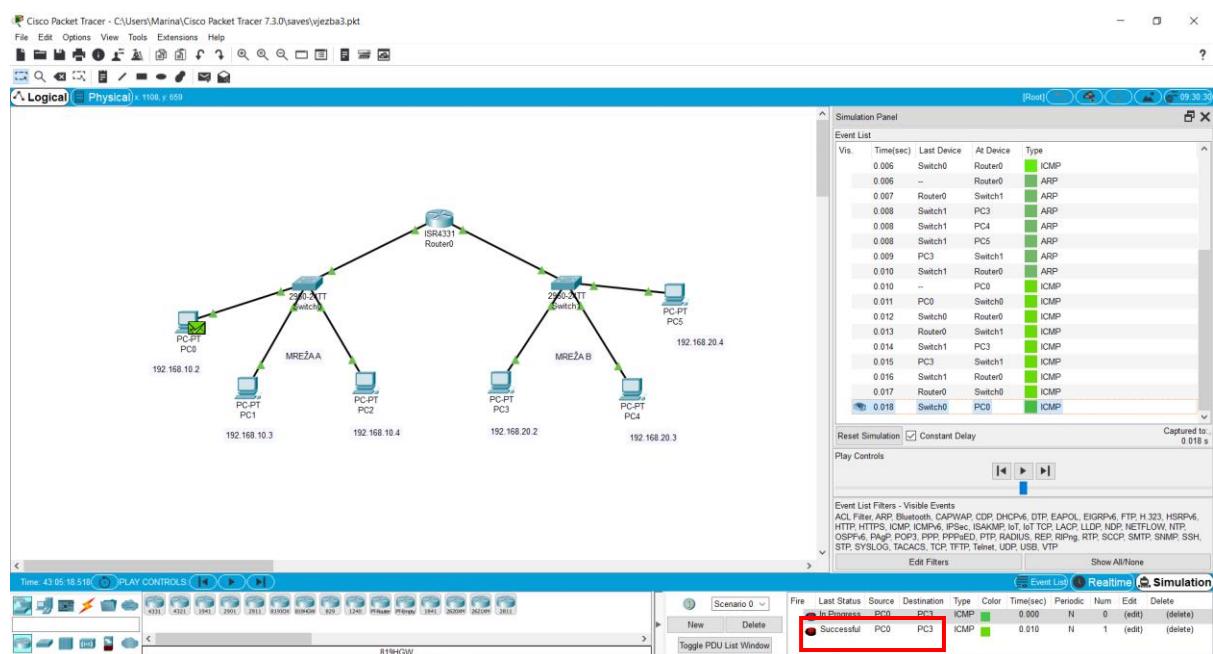


Izvrtite nekoliko dalnjih koraka simulacije dok ICMP paket ne dođe do routera i uočite crveni križić koji označava da router nije finalno odredište (njegov IP ne odgovara odredišnom IP-u). Router „zna“ da taj ICMP zahtjev treba proslijediti računalu s navedenom odredišnom adresom, a po IP adresi tog odredišta zna da se ono nalazi u mreži koja je spojena s njegove desne strane, tj. na njegov priključak s adresom 192.168.20.1. Ipak, ono što router još ne zna je MAC adresu tog odredišta pa stoga samo odbaci ICMP upit, ali i pokuša doznati MAC adresu odredišta kako bi mu ubuduće mogao prosljeđivati podatke. Zato router sa svoga desnog priključka šalje ARP upit na switch pa s njega na sva tri spojena uređaja. Naravno, odgovara računalo PC3 koje prepozna svoj target IP u ulaznom paketu i upisuje svoju MAC adresu u izlazni paket, tj. u njegovo IP zaglavje. MAC adresa odredišta u ARP odgovoru je, naravno, MAC adresa desnog sučelja na routeru, onoga s IP adresom 192.168.20.1.





Kada je router primio ARP paket i doznao MAC adresu računala PC3, pošaljite još jedan ICMP paket od PC0 do PC3 uz pomoć naredbe Create Simple PDU. Popratite kako paket putuje do svog odredišta i konačno kako je krajnji rezultat komunikacije uspješan.



Spremite Packet Tracer topologiju pod nazivom **ime_prezime_zadatak3.pkt**.

ZADACI ZA VJEŽBU 2 (PREDAJA IZVJEŠTAJA):

Kreirati sve tri mrežne topologije u alatu Packet Tracer kako je pokazano na vježbi. Predati sve konfiguracije pod nazivom:

- **ime_prezime_zadatak1.pkt**
- **ime_prezime_zadatak2.pkt**
- **ime_prezime_zadatak3.pkt**.

VJEŽBA 3: VIRTUALNE LOKALNE MREŽE

CILJ VJEŽBE

Cilj ove vježbe je simulacijom pokazati princip rada virtualnih lokalnih mreža (VLAN) u različitim scenarijima te objasniti neke probleme koji se mogu pojaviti u praktičnoj primjeni VLAN mreža. Vježba je prilagođena sa [12], [13].

TEORIJSKI PREDUVJETI

Podrazumijeva se osnovno razumijevanje idućih teorijskih pojmove:

- Lokalna mreža
- Mrežna IP adresa računala i postavljanje statičke IP adrese
- Mrežna maska, podmreža
- ARP protokol
- Broadcast domena, IP adresa broadcast paketa
- Naredbe „ping“ i „ipconfig“

MOTIVACIJA ZA UVOĐENJE VLAN MREŽA

BROADCAST I MULTICAST PROMET

Broadcast i multicast u smislu dostavljanja prometa je sličan. Informacija poslana broadcastom ili multicastom dolazi do svih odnosno do grupe odabralih uređaja unutar iste mreže (subneta). Upravo takav tip poruka koji sa jedne točke u mreži dolazi do svih krajnjih uređaja stvara nepotrebnu potrošnju resursa (mrežnog kapaciteta) u današnjim mrežama. Danas se smatra da je LAN jedna broadcast domena. Pod tim se misli da ako neko računalo posalje broadcast podatke preko svojeg LAN-a, primit će ih svako računalo koje je priključeno na isti LAN. Krajnja točka broadcast domene router preko kojeg je mreža povezana s drugim mrežama (u prethodnoj vježbi smo upoznali gateway; ukoliko računala iz različitih LAN mreža žele komunicirati, komunikacija se mora odvijati preko routera, a router stvara i dodatno kašnjenje zbog čega se cijeli proces komunikacije produžuje).

LAN SE MORA NALAZITI NA ISTOM FIZIČKOM PODRUČJU

Kako bismo računala mogli povezati pomoću switch-a, ona se trebaju nalaziti na istom fizičkom području. Također, da bismo dva switcha mogli međusobno povezati, ukoliko ne upotrebljavamo uređaje 3. sloja, oni se moraju nalaziti na istom fizičkom području.

Strategija u rješavanju navedenih problema jest da se smanji broj kolizija ali i eliminira dodatni mrežni promet koji većinom čine tzv. "Broadcast" i "Multicast" paketi. Ovim dolazimo do paradoksalne situacije: mrežu smo uveli da bismo međusobno povezali sva računala, a ta ista mreža efikasno radi samo ako je podijelimo na manje dijelove.

VLAN koncept je smisljen da razriješi ovaj problem, tj. da mreža ostane fizički povezana, ali da se smanji broj kolizija i intenzitet Broadcast i Multicast prometa – "virtualnom" podjelom na manje dijelove.

Kada se ne koriste VLAN-ovi cijela mreža je jedna broadcast domena. Ako imamo veći broj korisnika, a to znači i veću broadcast domenu postoji veća mogućnost tzv. broadcast oluje (broadcast storm) koji može značajno narušiti performanse mreže. Dobro je povezati korisnike koji pripadaju istoj skupini i često komuniciraju (npr. rade isti posao), a bez uporabe VLAN-ova nemoguće je fizički udaljene skupine korisnika povezati u istu domenu.

Gledano sa sigurnosnog aspekta ako je veliki broj korisnika u istoj domeni postoji velika mogućnost napada ili krađe podataka. Zbog svega navedenog, poželjno je razdvojiti određenu vrstu korisnika i izolirati ju od ostalih, a za to se u današnjim računalnim mrežama koristi tehnologija virtualnih lokalnih mreža.

VIRTUALNA LOKALNA MREŽA

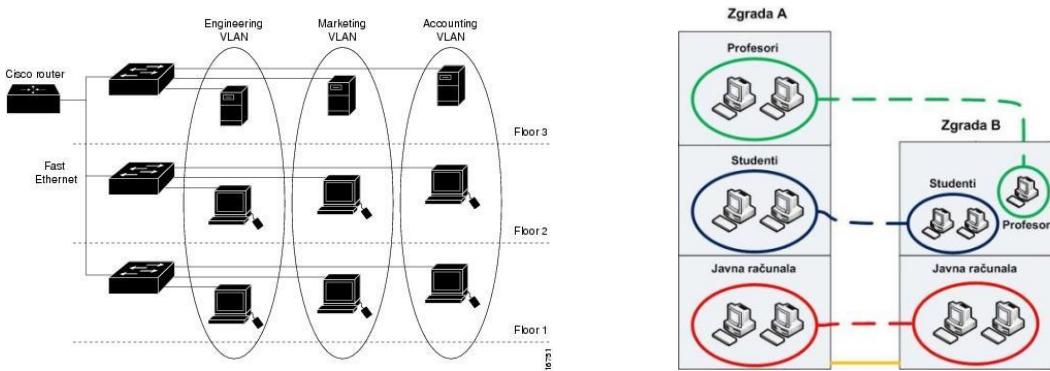
Virtualna lokalna mreža (engl. Virtual Local Area Network – VLAN) je mreža kod koje je logička organizacija mreže različita od fizičke organizacije. Dakle, kada želimo napraviti VLAN radimo podjelu jedne te iste fizičke LAN mreže na više odvojenih logičkih mreža (VLAN-ova) pri čemu nam nisu potrebne nikakve fizičke promjene, već se mreža odvaja logički u potpuno odvojene VLAN-ove konfiguriranjem switch-eva na željeni način.

Mrežu tako možemo podijeliti na više VLAN-ova na jednostavan i jeftin način, jer ne treba fizički premještati računala, prespajati kable, provoditi dodatne kable, uvoditi dodatnu mrežnu opremu i slično. Također se dosta lako može mijenjati konfiguracija na switch-u koja određuje koje računalo pripada kojem VLAN-u.

VLAN-ovi nam daju fleksibilnost jer fizičku mrežu možemo „modelirati“ u bilo kakvu logičku mrežu. Implementacijom VLAN-ova podizemo i razinu sigurnosti razdvajanjem prometa (komunikacije) između VLAN-ova, rješavamo nepotrebno nakupljanje broadcast prometa i time povećavamo performanse, pojednostavljujemo administraciju i smanjujemo troškove mreže. Do pojave VLAN-ova jedini način blokiranja takvog prometa je bio moguć uređajem koji radi na trećem sloju (OSI modela) npr. routerom. Znači da bi blokirali broadcast ili multicast poruke i tako riješili nepotrebni gubitak bandwidth-a moramo odvojiti broadcast domene ruterom ili kreirati dodatne podmreže.

VLAN-ovi omogućavaju mrežnom administratoru logičko segmentiranje LAN-a u različite broadcast domene, a pošto je segmentiranje logičko, uređaji u istom logičkom segmentu ne moraju biti na fizički istim lokacijama. Znači da korisnici u različitim sobama, katovima, zgradama itd. mogu pripadati istom logičkom segmentu odnosno VLAN-u. VLAN-ovi dozvoljavaju kreiranje broadcast domena bez korištenja uređaja trećeg sloja OSI modela kao što je router. Ipak za komunikaciju između VLAN-ova moramo koristiti uređaj trećeg sloja (Layer 3 switch).

Na donjoj slici lijevo [14] dan je primjer triju VLAN-ova, a na slici desno [15] je primjer koji pokazuje opravdanost korištenja VLAN-ova uz pomoć kojeg je napravljena organizacija mreže fakulteta. Profesori iz zgrada A i B su stavljeni u isti VLAN i tako odvojeni od studentskih i javnih računala. Dakle, iako su javna, studentska i računala profesora spojena na isti switch, njihov promet je odvojen i praktički je nemoguće nekome iz jednog VLAN-a vidjeti promet drugog VLAN-a.



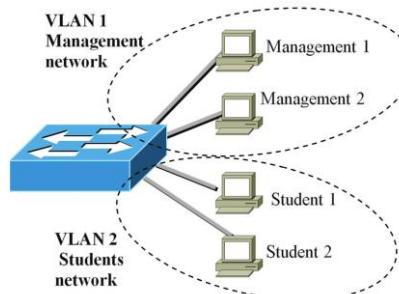
PRINCIP RADA VLAN-a

Postoji više načina konfiguriranja VLAN-ova, a najčešće korišteni su **MAC-based VLAN** i **port-based VLAN**.

Kod VLAN-a koji se temelji na MAC adresama (**MAC-based VLAN**), switch-evi u LAN-u se konfiguriraju tako da se na njima kreira potreban broj VLAN-ova te se napravi popis u kojem se definira koje računalo (tj. njegova MAC adresa) pripada kojem VLAN-u. Switchevi znaju koja MAC adresa im je spojena na koji priključak te po tom priključku šalju samo promet koji pripada VLAN-u spojenog računala. Ukoliko se računalo prebaci na neki drugi priključak, switch to detektira i jednostavno po tom novom priključku počne slati promet koji pripada VLAN-u premještenog računala. Na ovoj vježbi neće se obrađivati MAC-based VLAN.

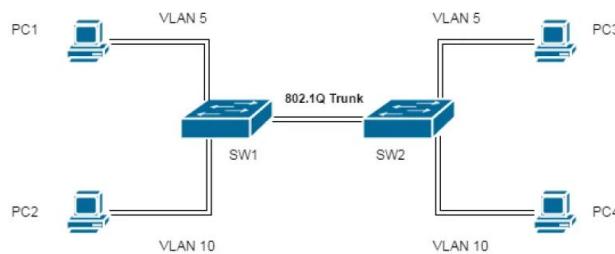
Kod VLAN-a temeljenog na portovima (**port-based VLAN**) koji će se obrađivati u ovoj vježbi, switch-evi se konfiguriraju tako da se na njima kreira potreban broj VLAN-ova te se svaki port switcha dodijeli nekom VLAN-u. Switch će po svakom portu slati samo promet onog VLAN-a kojemu je taj port pridružen. Ovako konfigurirani portovi nazivaju se access portovi.

Povezivanje računala u više VLAN mreža pomoću jednog switch-a [16]:



Na slici je prikazan switch na kojem postoje dva VLAN-a. Na switch su spojena 4 računala, odvojena u različite VLAN-ove. Svako računalo vidi samo ono računalo koje se nalazi u istom VLAN-u. Bez „vanjske“ pomoći, podatak iz jednog VLAN-a ne može prijeći u drugi VLAN.

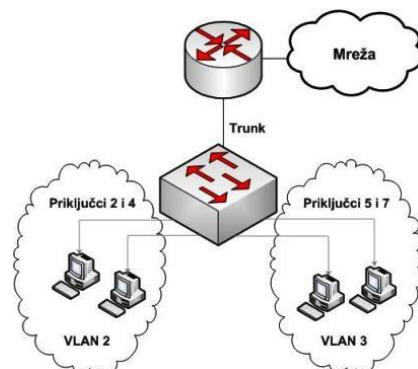
Povezivanje istih VLAN mreža preko više switch-eva [17]:



Na slici su prikazana dva switch-a koji povezuju 4 računala. Pretpostavimo da je potrebno podijeliti ovu LAN mrežu na dva VLAN-a (VLAN5 i VLAN10), pri čemu PC1 i PC3 pripadaju jednom, a PC2 i PC4 drugom VLAN-u. Potrebno je na oba switcha kreirati 2 VLAN-a (5 i 10) te portove na koji su spojena računala na oba switcha pridijeliti odgovarajućim VLAN-ovima. To su access portovi koji prenose samo promet VLAN-a kojem su pridijeljeni. Međutim, preko linka koji povezuje switcheve SW1 i SW2 treba prolaziti promet oba VLAN-a, kako bi PC1 i PC3 mogli komunicirati, baš kao i PC2 i PC4. Stoga se ti portovi na switch-evima ne konfiguriraju kao access, nego kao trunk portovi. Trunk portovi mogu prenositi promet koji pripada većem broju VLAN-ova, a potrebno je navesti koji VLAN-ovi se propuštaju preko porta (po default-u se svi propuštaju).

Dakle, portovi na switch-evima se mogu konfigurirati kao jedan od dva tipa:

- access port – ako je preko njega switch povezan s računalom, hub-om ili nekom trećim uređajem koji u sebi nema VLAN funkcionalnost
- trunk port – ako je preko njega switch povezan s nekim uređajem koji ima VLAN funkcionalnost (npr. s drugim switch-em)



Važno je napomenuti da priključci switcha koji se nalaze u različitim VLAN-ovima ne mogu komunicirati izravno, već im je za to potreban router [15]. Sučelje routera (engl. interface) treba podijeliti na onoliko pod sučelja koliko postoji VLAN-ova. Svakom od tih virtualnih sučelja se dodjeljuje IP adresa iz raspona pojedinog VLAN-a, a to je ujedno adresa predefiniranog izlaza (engl. default gateway) za taj VLAN. Osim adrese na pod sučelju je potrebno definirati kojem VLAN-u pripada te koji "trunking" protokol koristi.

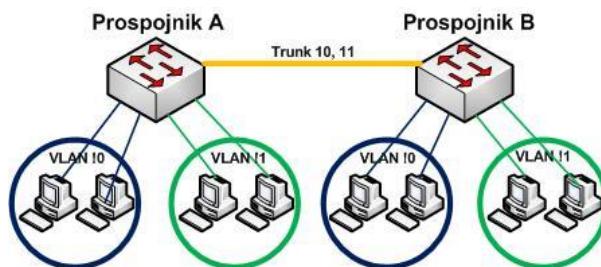
TIPOVI SPAJANJA U VLAN MREŽAMA

IEEE 802.1Q je protokol koji se koristi u konfiguraciji VLAN-ova. Protokol se temelji na označavanju Ethernet okvira koji se razmjenjuju između više switch-eva (koji definiraju više različitih VLAN mreža) kako bi se znalo kojoj VLAN mreži paket treba biti proslijeđen. Dijelovi mreže koji su VLAN „svjesni“ (npr. switch) mogu dodavati VLAN oznake na pakete, stoga kada paket dođe do VLAN „svjesnog“ dijela mreže, njemu se dodaje oznaka kojem VLAN-u pripada i ovisno o tome kojem VLAN-u može biti proslijeđen. Na svakom okviru se mora moći pročitati točno jedan VLAN kojem pripada.

Sada se može i detaljnije objasniti razlika između trunk i access linkova.

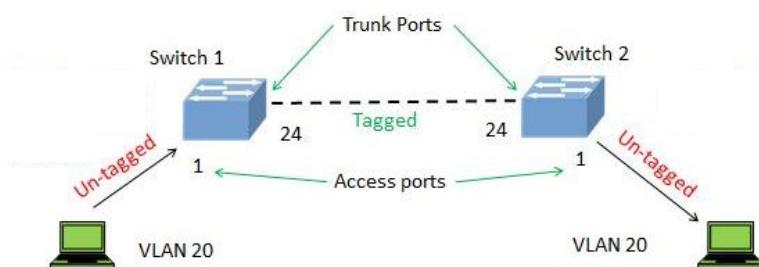
1. TRUNK LINK (VLAN „svjesni“ uređaji)

Svi spojeni uređaji moraju podržavati VLAN tehnologiju, moraju sadržavati specifični format zaglavlja okvira koji govori o pripadnosti VLAN-u. Moguće je konfigurirati trunk linkove da filtriraju promet odgovarajućih VLAN-ova. Trunk link je označena (engl. tagged) veza kojom se spajaju switch-evi međusobno ili switch i router. Kroz trunk link se propušta promet na način da se točno zna koji promet je namijenjen kojem VLAN-u. Ovime npr. računala spojena na VLAN 10 switch-a A i računala spojena na VLAN 10 switch-a B mogu komunicirati međusobno kao da su u lokalnoj mreži (slika dolje [15]). Na trunk vezi mora se specificirati koji VLAN-ovi se propuštaju.



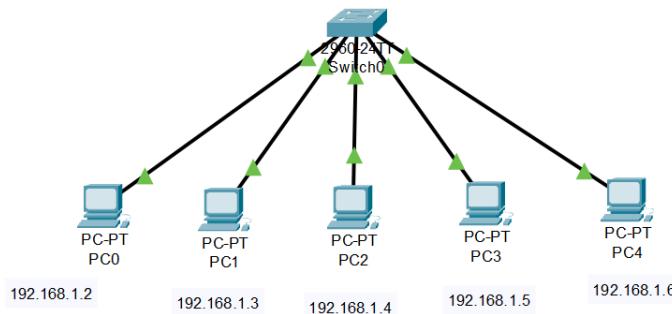
2. ACCESS LINK (VLAN „nesvjesni“ uređaji)

Access link je neoznačena (engl. untagged) veza na kojoj promet ulazi ili izlazi bez oznake VLAN-a. To su priključci switch-a na koje se povezuju računala ili drugi uređaji. Ako se promet sa određenog access priključka šalje kroz trunk link tom prometu se dodaje oznaka (engl. tag) definiranog VLAN-a. Priključci switch-a koji se nalaze u različitim VLAN-ovima ne mogu komunicirati izravno, već im je za to potreban uređaj koji radi na mrežnoj razini (3.sloj) router ili switch. Na donjoj slici [18] je prikazan TRUNK link sa trunk portovima kojima se prenose frameovi različitih VLAN-ova, ali i ACCESS linkovi sa ACCESS portovima koji pripadaju odgovarajućem VLAN-u.



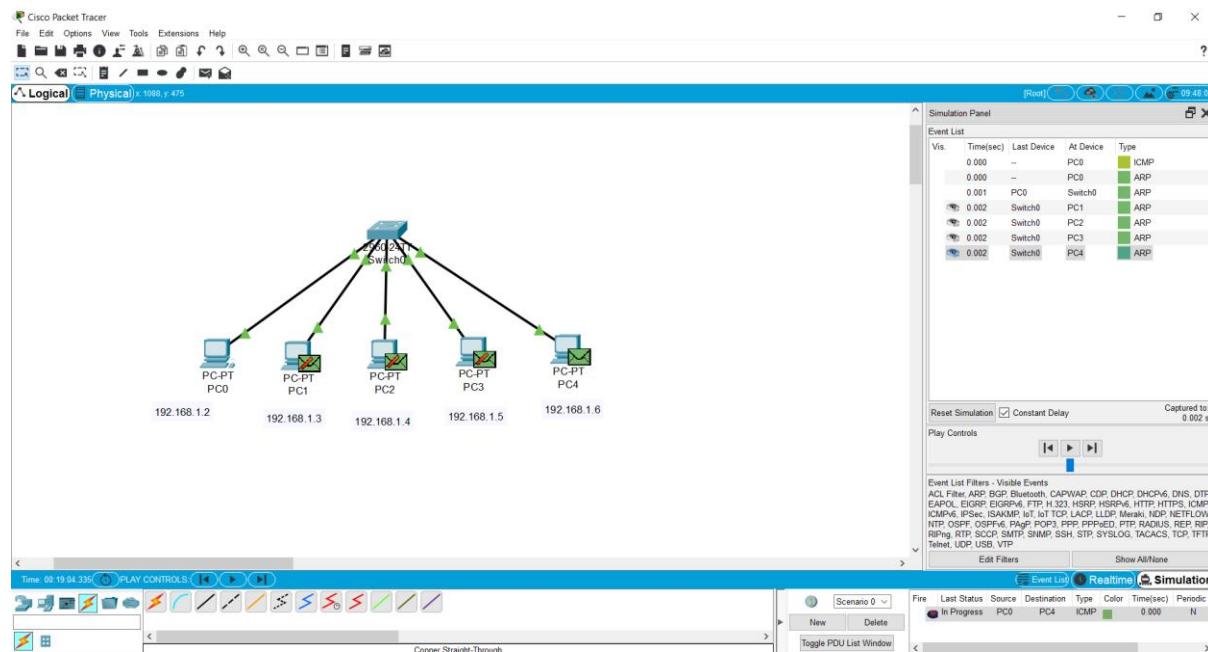
POVEZIVANJE RAČUNALA U VLAN-OVE UZ POMOĆ JEDNOG SWITCH-A

U prvom zadatku ćemo simulirati jedan od najjednostavnijih načina implementacije VLAN mreža, a to je kada više računala spojimo na jedan switch i portove na tom switch-u podijelimo u različite VLAN mreže. U tom zadatku ćemo pokazati kako možemo konfigurirati switch-eve za takav način rada.

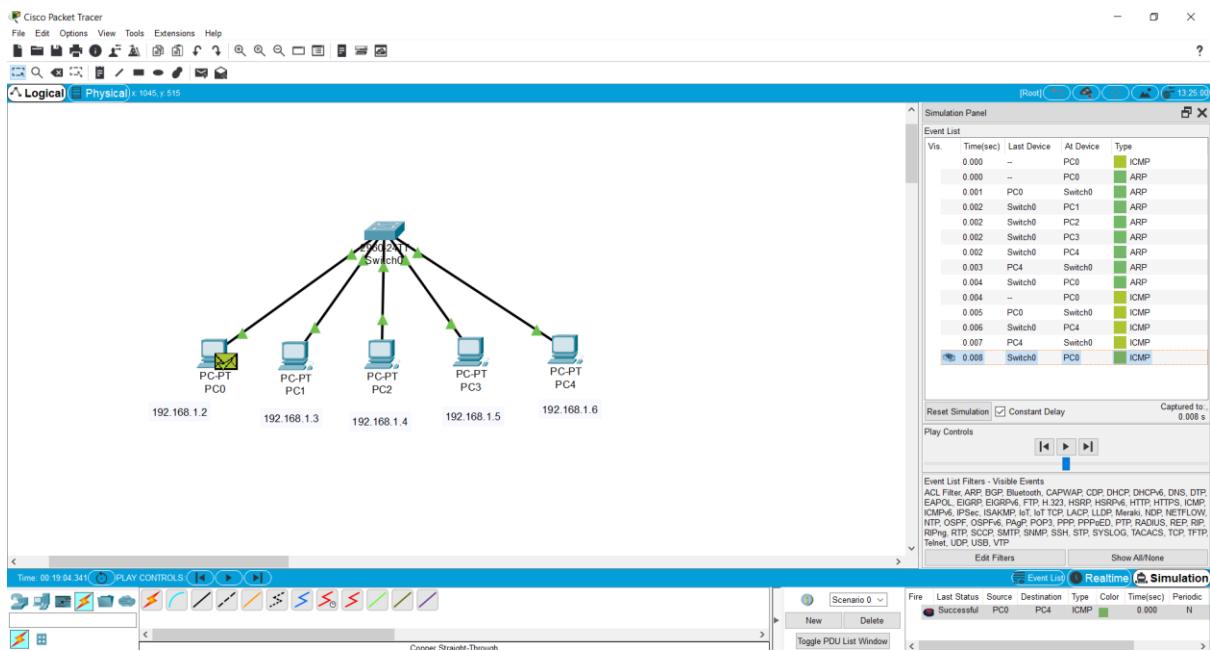


Za početak, povežite 5 računala na switch u lokalnu mrežu prema gornjoj slici. Kod povezivanja računala na switch počnite spajati računala na port Fa 0/2, pa Fa 0/3, Fa 0/4, Fa 0/5 i Fa 0/6 kako bi port Fa 0/1 na switch-u ostao rezerviran za trunk port koji će nam trebati kasnije u vježbi. Dodijelit ćemo svim računalima statičku IP adresu (IP adrese su vam zadane na slici) i mrežnu masku da sva računala budu na istoj mreži. Sada su sva računala u jednome jedinome VLAN-u - to je VLAN 1 koji je default kod Cisca.

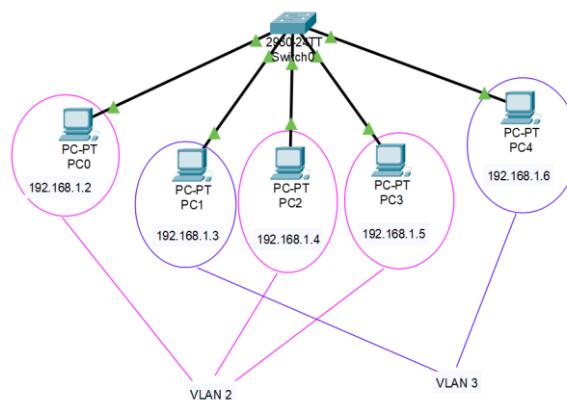
Napravimo naredbu ping između neka dva računala (npr. PC0 do PC4) u simulacijskom modu i pogledajmo kako paket uspješno putuje do svog odredišta. Prvo se formira ARP zahtjev koji se šalje na switch kako bi se doznala MAC adresa računala PC4. Switch proslijeđuje četiri ARP paketa na svaki od spojenih računala nakon čega mu PC4 odgovara.



Kada dobije ARP odgovor od switch-a, PC0 formira ICMP Echo Request paket te mu se u konačnici vrati ICMP Echo Reply. Izvršite simulaciju kako biste se uvjerili da je komunikacija uspješna te da ping procesom potvrđujemo da je odredište dostupno i aktivno.



Podijelimo sada računala ove jedne lokalne mreže u različite VLAN-ove, pri čemu treba imati na umu da je VLAN 1 rezerviran za konfiguraciju kod Packet Tracera i ne smije se dirati. Znači, potrebno je definirati dva nova VLAN-a koja ćemo nazvati VLAN 2 i VLAN 3 i dodijeliti portove na switch-u određenom VLAN-u. Računala PC0, PC3 i PC2 neka pripadaju VLAN-u 2, a računala PC1 i PC4 VLAN-u 3.



VLAN je potrebno konfigurirati na switch-u i tako mrežni administratori rade u praksi. Klikom na switch možemo odabrati konfiguracijski tab za ulazak u terminal i direktno unositi naredbe, ali mi ćemo u ovoj vježbi konfiguraciju VLAN-ova raditi grafički. Primijetite u svakom koraku kako se u donjem dijelu pojavljuju ekvivalentne naredbe iz terminala.

Prvo je potrebno dodati VLAN-ove. Na switch-u u Config tabu kliknemo na VLAN Database i dodat ćemo dva nova VLAN-a. Za sada on ima defaultne VLAN-ove (od Cisca), a mi dodamo VLAN rednog broja 2 kojeg nazovemo "studenti" i VLAN rednog broja 3 kojeg nazovemo "profesori" (ime nije važno i može biti bilo koje, ono što je bitno je redni broj – jer on je taj koji se upisuje u zaglavlje poslanog paketa da se on označi na ispravan način). Nakon što unesete redni broj i ime VLAN-a kliknete Add, kako bi se taj VLAN dodao u bazu na switch-u. Primijetite ekvivalentnu naredbu u komandnoj liniji koju smo mogli unijeti u terminalu switch-a kako bismo postigli istu funkcionalnost.

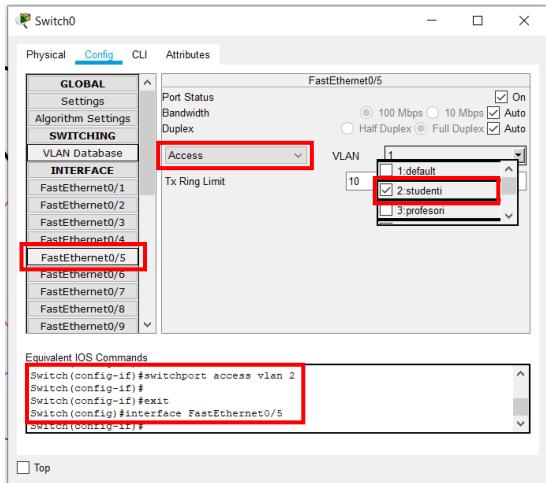
The screenshots illustrate the creation of VLANs 2 and 3:

- Screenshot 1:** Shows the Global Settings page. The "VLAN Database" option is selected in the left sidebar. The "Add" button in the VLAN Configuration section is highlighted.
- Screenshot 2:** Shows the VLAN Configuration page for VLAN 2. It lists VLAN No 1 (default), VLAN No 2 (studenti), and VLAN No 3 (profesori). The "Add" button is highlighted again. The equivalent IOS command shown is `Switch(vlan)#vlan 2 name studenti`.
- Screenshot 3:** Shows the VLAN Configuration page for VLAN 3. It lists VLAN No 1 (default), VLAN No 2 (studenti), and VLAN No 3 (profesori). The "Add" button is highlighted. The equivalent IOS command shown is `Switch(vlan)#vlan 3 name profesori`.

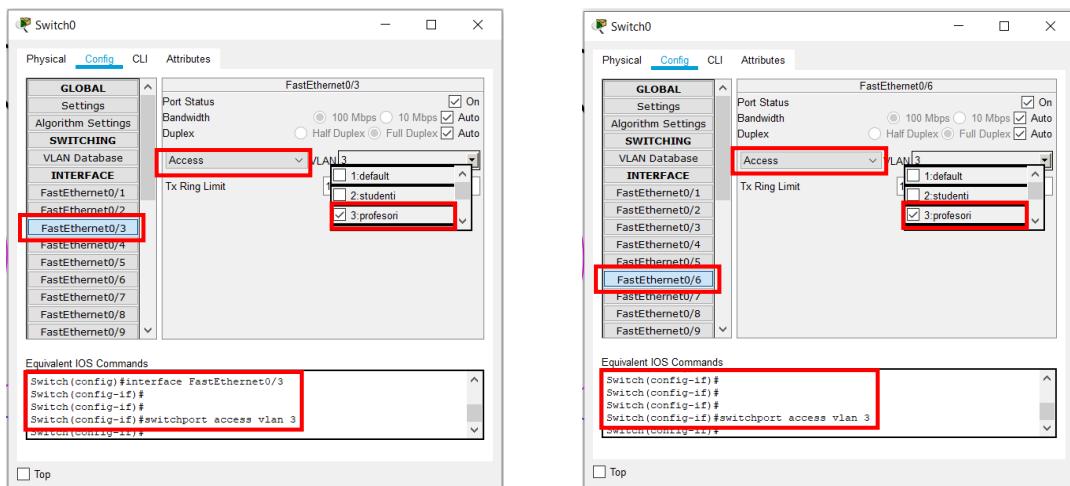
Ono što još trebamo napraviti je prvo portove na switch-u na kojima su spojeni PC0, PC2 i PC3 dodati u VLAN 2. Rekli smo na samome početku da će to biti Fa 0/2, Fa 0/4 i Fa 0/5, pa provjerite jeste li baš na te portove spojili računala kako biste mogli pratiti daljnje upute. Kliknemo na željeni port u listi s lijeve strane (na donjoj slici lijevo to je Fa 0/2) i označite ga kao ACCESS port i dodijelite u VLAN 2. Isto napravite za ostale portove Fa 0/4 i Fa 0/5.

The screenshots show the configuration of FastEthernet0/2 and FastEthernet0/4 ports as ACCESS ports in VLAN 2:

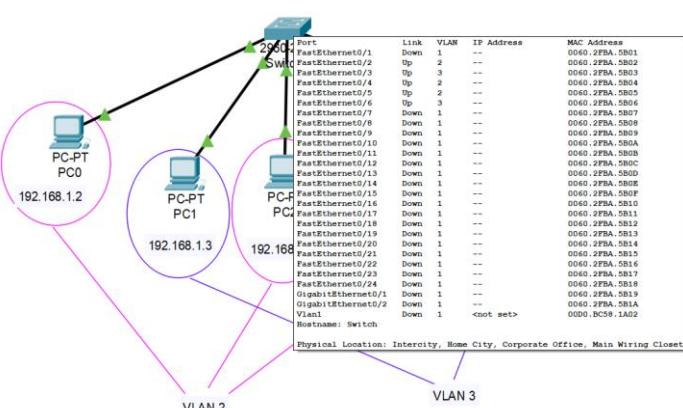
- Screenshot 1:** Shows the configuration for FastEthernet0/2. The "Access" option is selected in the VLAN dropdown menu. The "2:studenti" checkbox is checked under the VLAN list. The equivalent IOS command shown is `Switch(config)#interface FastEthernet0/2`.
- Screenshot 2:** Shows the configuration for FastEthernet0/4. The "Access" option is selected in the VLAN dropdown menu. The "2:studenti" checkbox is checked under the VLAN list. The equivalent IOS command shown is `Switch(config)#interface FastEthernet0/4`.



Portove na switch-u na kojima su spojeni PC1 i PC4 (Fa 0/3 i Fa 0/6) treba dodati u VLAN 3.



Prije nego što krenemo dalje, provjerimo da smo sve portove doveli u željene VLAN-ove prema početnoj slici. Za to je dovoljno samo "proći" mišem preko ikone switch-a.



U sljedećem zadatku ćemo provjeriti je li konfiguracija dobro napravljena i pokušat ćemo uspostaviti komunikaciju između računala iz istog VLAN-a te između računala iz različitih VLAN-ova. Na temelju tih komunikacija, doći ćemo do zaključka o osnovnoj karakteristici VLAN mreža.

KOMUNIKACIJA U VLAN-u I IZMEĐU VLAN MREŽA

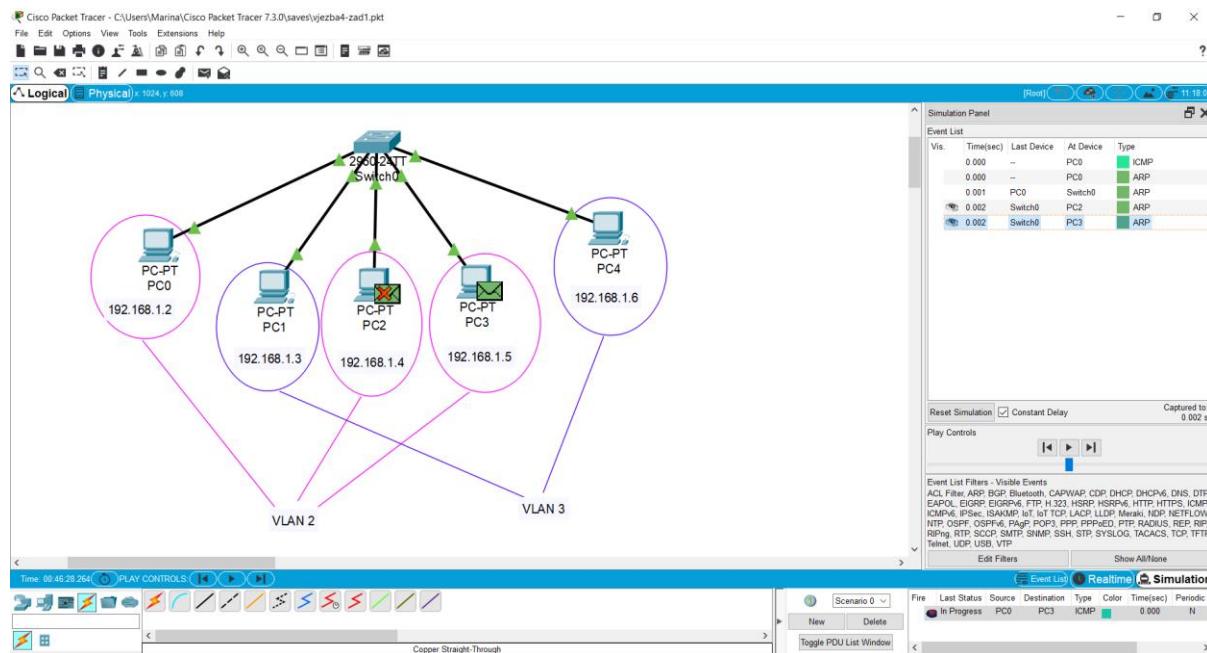
Testirajmo komunikaciju između računala:

- Unutar istoga VLAN-a

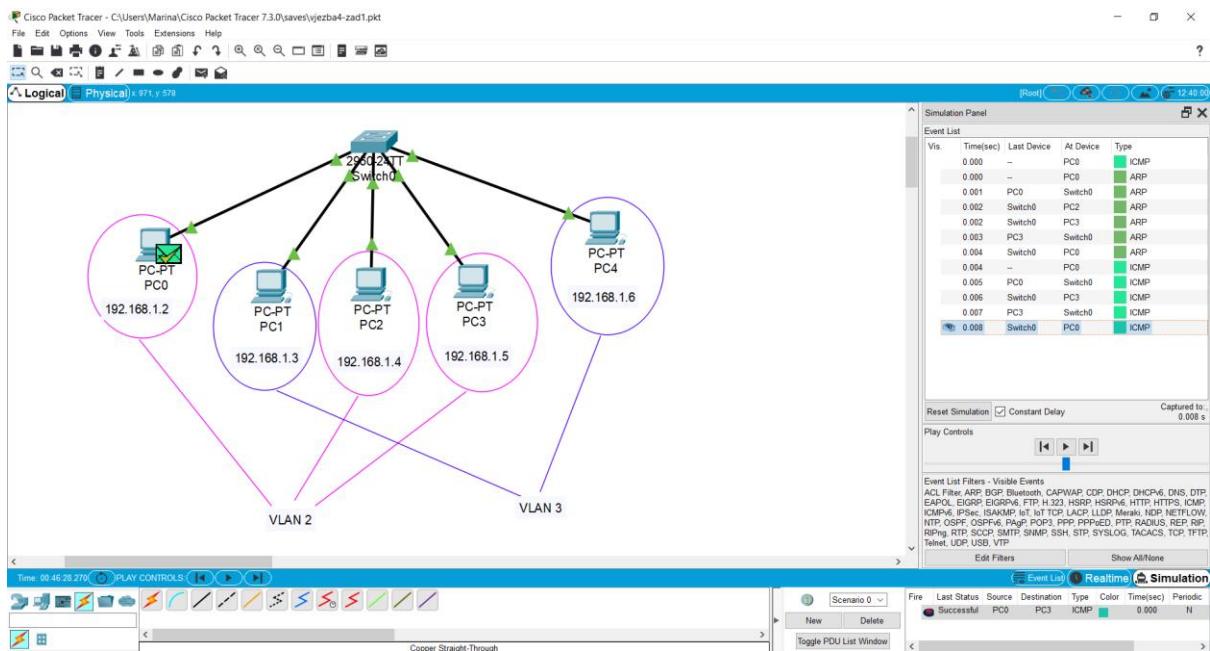
Napravite ping u simulacijskom modu između računala PC0 i PC3 te između PC1 i PC4.

Primjer za komunikaciju između računala PC0 i PC3 je dan u nastavku. Računalo PC0 formira ARP zahtjev i šalje na switch koji prosljeđuje paket svim onim računalima iz njegovog VLAN-a (to su PC2 i PC3).

S obzirom da broadcast paket poslan s jednog računala unutar nekog VLAN-a prime sva računala koja pripadaju tom istom VLAN-u, a koja su spojena na isti switch kao i izvorišno računalo, možemo zaključiti da je VLAN zapravo jedna **broadcast domena**.



Na ARP zahtjev odgovara PC3 sa svojom MAC adresom i vraća se ARP odgovor nakon kojeg slijedi ICMP te je komunikacija PC0 i PC3 uspjela.



Isto napravite i za provjeru komunikacije između računala PC1 i PC4.

b) Između različitih VLAN-ova

Napravimo ping između računala PC0 i PC4. Postupak je isti kao u prethodnom slučaju. Kako PC4 već postoji u MAC tablici od PC0 (provjerite uz pomoć naredbe **arp -a**), izbrišite zapise u ARP tablici od PC0 kako bismo opet vidjeli gdje putuju ARP paketi (naredba **arp -d**).

```

Packet Tracer PC Command Line 1.0
C:\>arp
Internet Address      Physical Address      Type
192.168.1.5            00d0.b427.040e      dynamic
192.168.1.6            0001.4220.877e      dynamic
C:\>

```

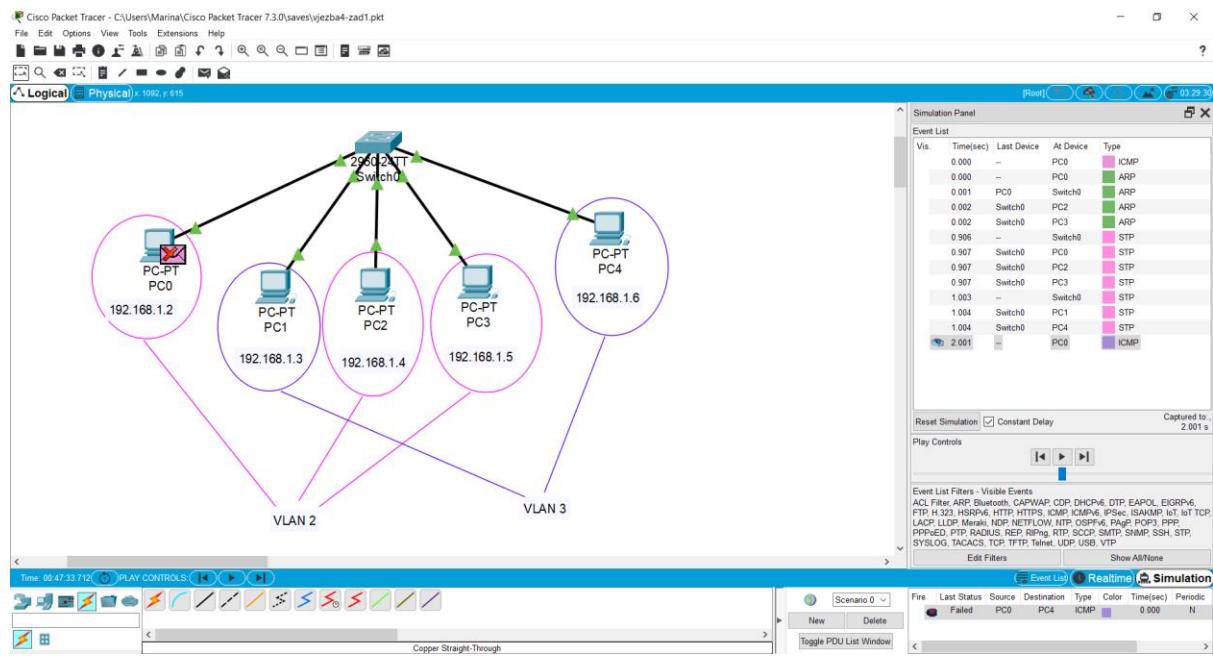


```

Packet Tracer PC Command Line 1.0
C:\>arp
Internet Address      Physical Address      Type
192.168.1.5            00d0.b427.040e      dynamic
192.168.1.6            0001.4220.877e      dynamic
C:\>arp -d
C:\>

```

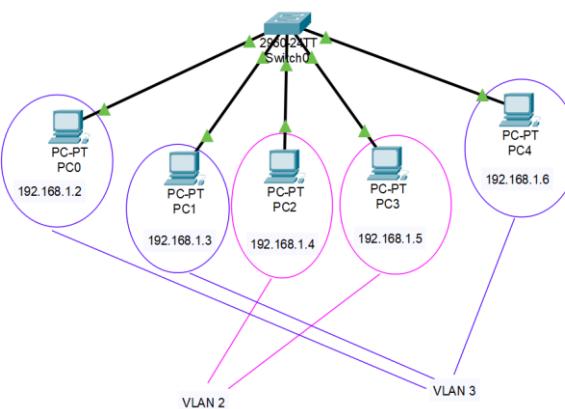
Vidimo da su ARP paketi opet poslani samo računalima PC2 i PC3 i switch nije primio ARP odgovor, koji bi trebao proslijediti na PC0. Komunikacija između računala PC0 i PC4 nije uspjela, odnosno računalo PC4 nije dostupno sa PC0.



Pitanje 1. Zašto je komunikacija u primjeru pod a) uspješna, a u primjeru pod b) nije?

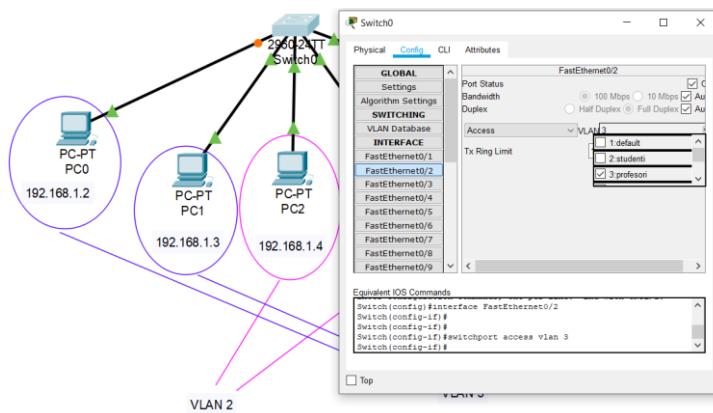
PREMJEŠTANJE RAČUNALA IZ JEDNOG VLAN-A U DRUGI

U trećem zadatku ćemo pokazati kako možemo jednostavno premjestiti računalo iz jedne VLAN mreže u drugu. Premjestimo tako računalo PC0 iz VLAN-a 2 u VLAN 3. Pritome je potrebno port na switchu na kojem je spojen host PC0 dodijeliti VLAN-u 3.

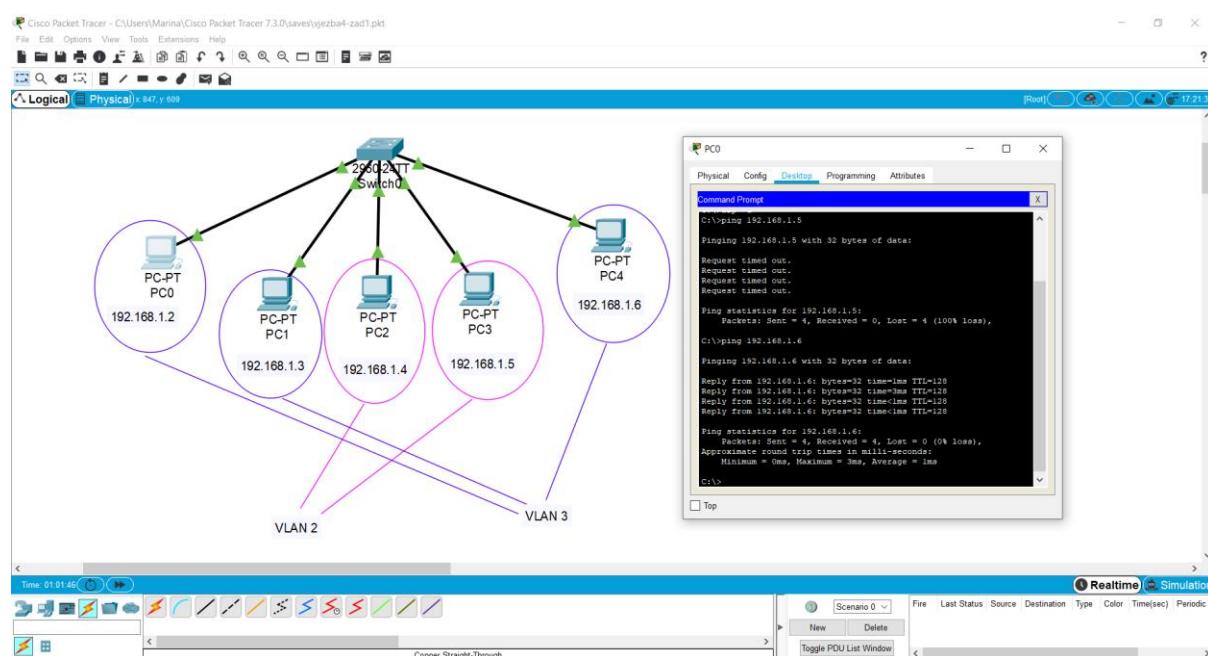


Cilj nam je pokazati nedostatak stvaranja VLAN mreža pomoću portova na switch-u, jer se strano računalo vrlo jednostavno može uključiti u VLAN mrežu tako što se samo priključi kabelom na željeni port i na taj način poremeti sigurnost odgovarajuće VLAN mreže. Upravo tu situaciju ćemo ovdje pokazati.

Potrebno je opet napraviti konfiguraciju na switch-u te prebaciti port na kojem je spojeno računalo PC0 (port Fa 0/2) u VLAN 3. Stoga, kliknite na switch te u Config tabu odaberite taj port i promijenite VLAN redni broj kojem pripada.



Pitanje 2. Testirajte sada komunikaciju između PC0 i PC3 te PC0 i PC4. Koja komunikacija je uspjela i zašto?



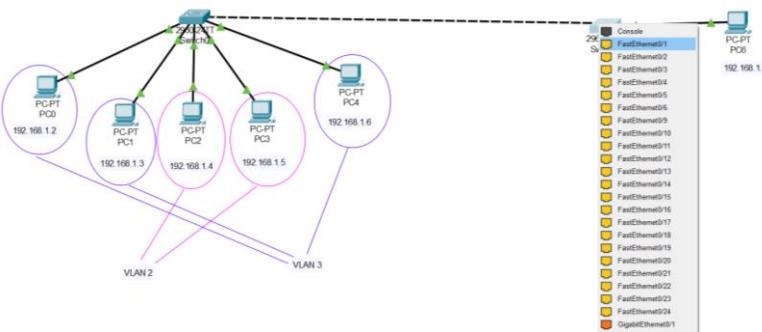
POVEZIVANJE VLAN MREŽA UZ POMOĆ DVAJU SWITCH-EVA

Računala mogu kao u prethodnim scenarijima biti spojena na isti switch i pripadati različitim VLAN-ovima, ali mogu biti spojena i na različite switch-eve, a pripadati istome VLAN-u. Upravo to ćemo pokazati u ovom zadatku.

Proširite prethodnu topologiju tako šta ćete dodati još jedan switch na koji su spojena dva računala. Računala spajati na port Fa 0/7 i Fa 0/8 kako bi mogli lakše pratiti na kojim su portovima sva računala redom te kako bi port Fa 0/1 i na drugom switch-u ostao rezerviran za trunk port koji će nam trebati kasnije.

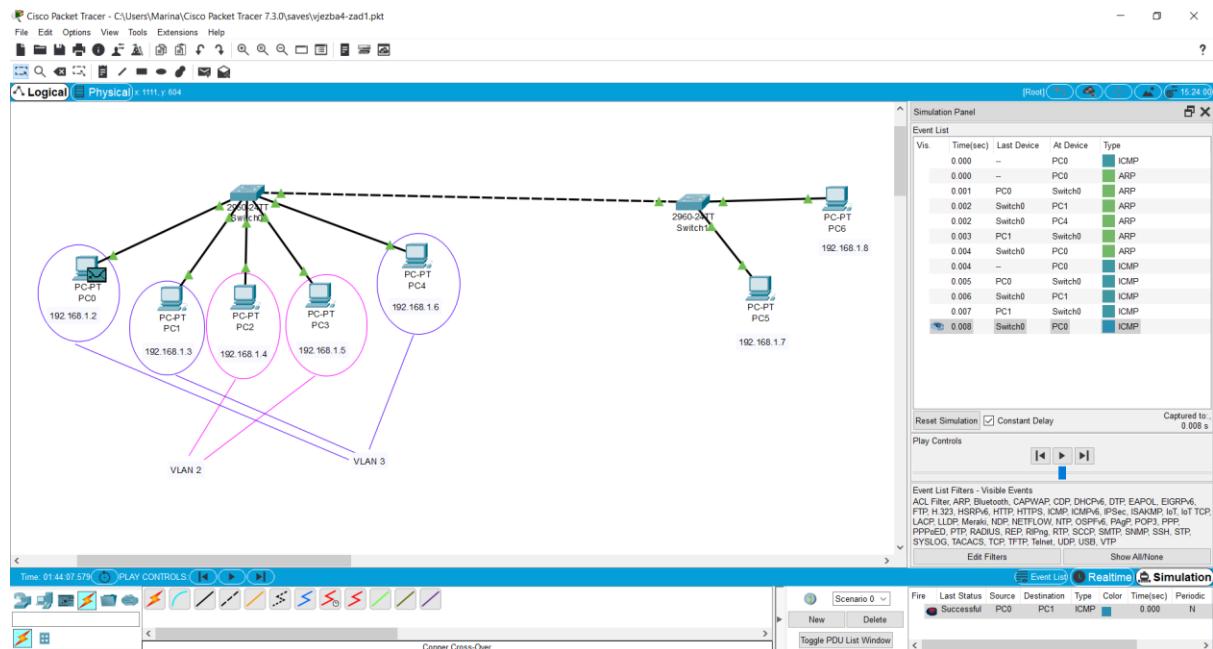


Pripazite da budu ispravne IP adrese na novim računalima (da sva računala budu na istoj mreži), pa im dodijelite IP adrese 192.168.1.7 i 192.168.1.8. Novi switch povežite sa starim uz pomoć Copper Cross-Over kabela i to na onaj port koji smo sačuvali na oba switch-a (port Fa 0/1).



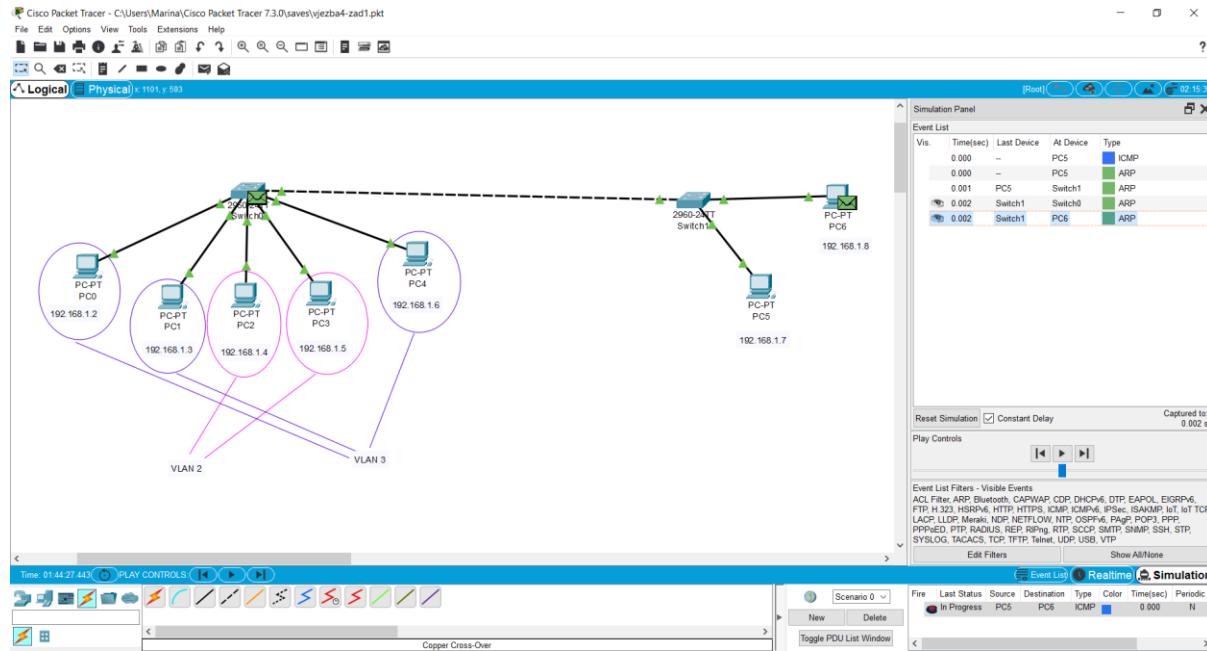
Sada su svi portovi na novom switch-u ACCESS portovi koji po defaultu pripadaju VLAN-u 1, tako da računala PC5 i PC6 pripadaju novome VLAN-u. To znači da sada zapravo imamo ukupno tri VLAN-a u našoj Packet Tracer topologiji.

Pokušajte pingati sa PC0 na PC1 (računala su u VLAN-u 3).

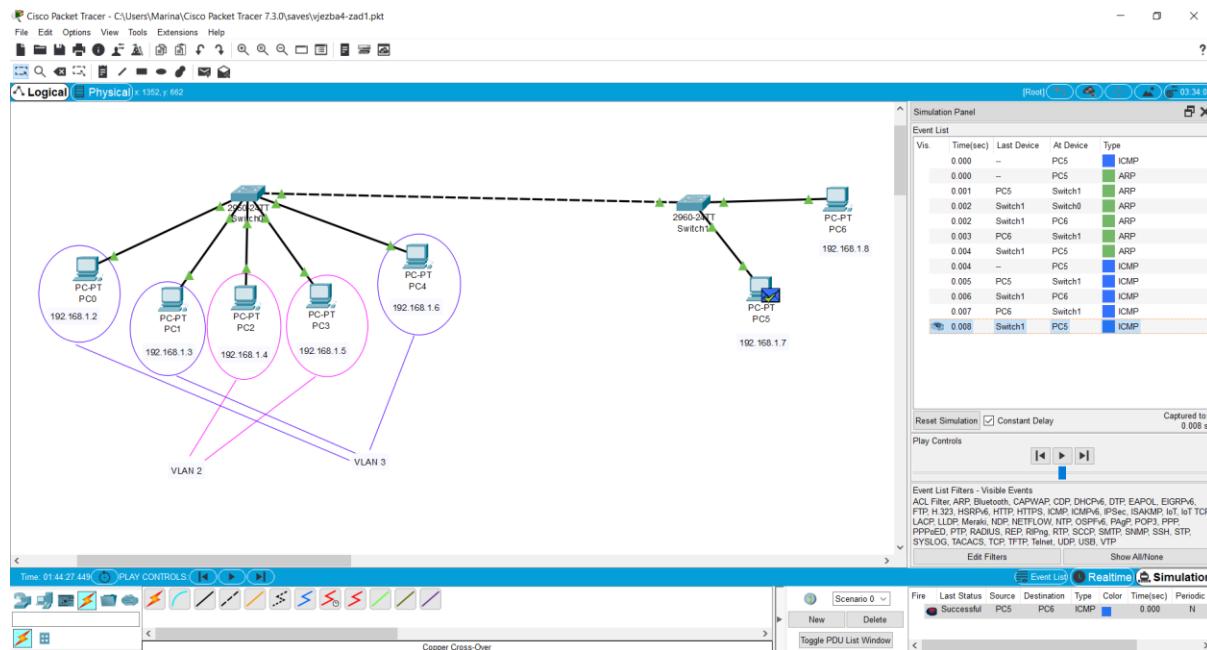


Vidimo na gornjoj slici kako se opet broadcast paket šalje cijelom VLAN-u kojem pripada računalo PC0 (računalima PC1 i PC4), a ne i desnoj strani mreže spojenoj na novi switch. To je zato što su računala na novom switch-u trenutno u zasebnom VLAN-u (VLAN 1). Njemu

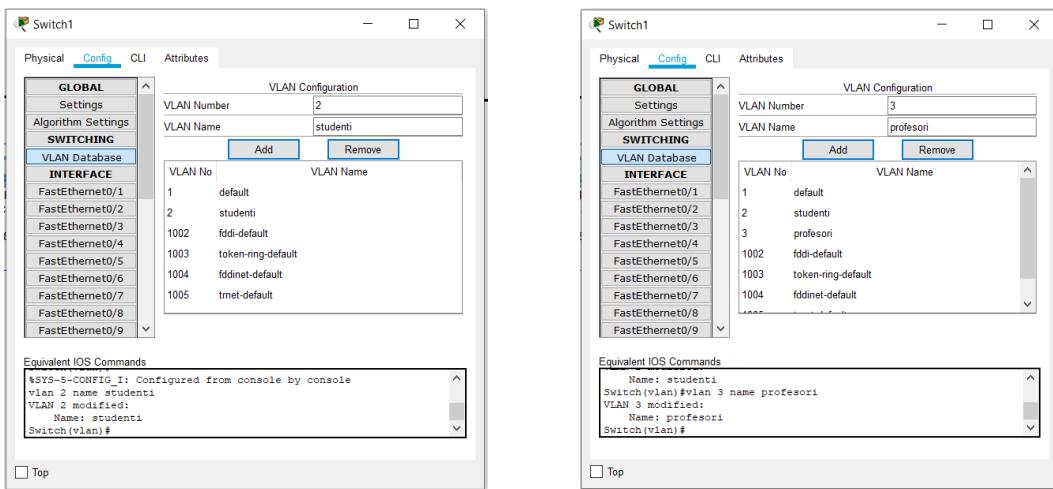
pripadaju četiri uređaja (PC5, PC6, switch0 i switch1). Provjerite pinganjem u simulacijskom modu sa računala PC5 na PC6.



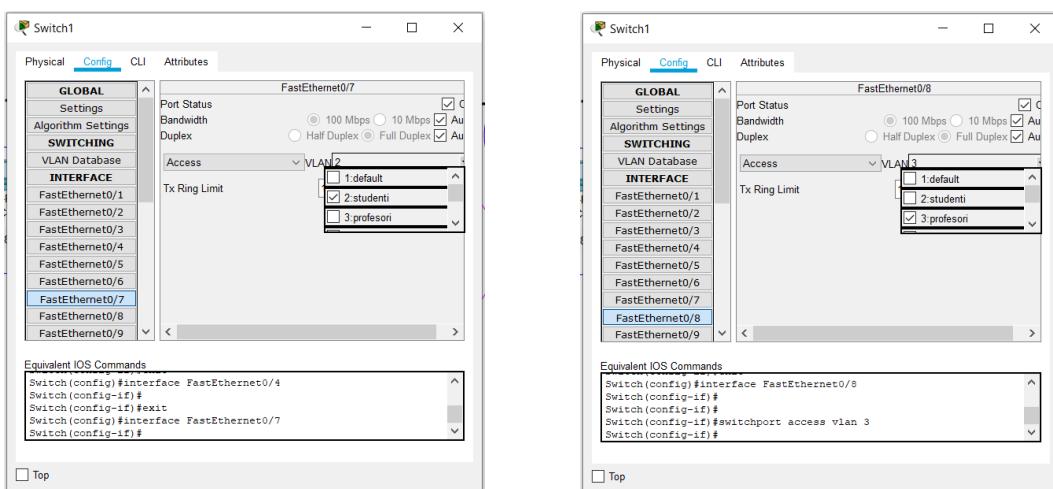
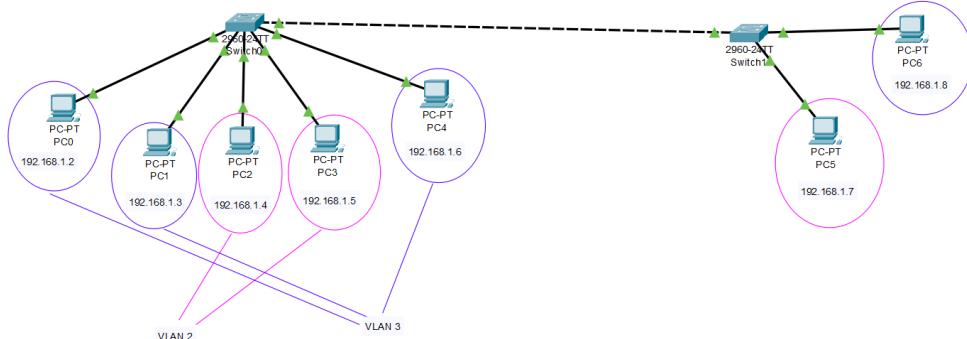
Vidimo da se ARP paket šalje sa switcha1 na sve uređaje u VLAN-u 1, a to su switch0 i PC6.



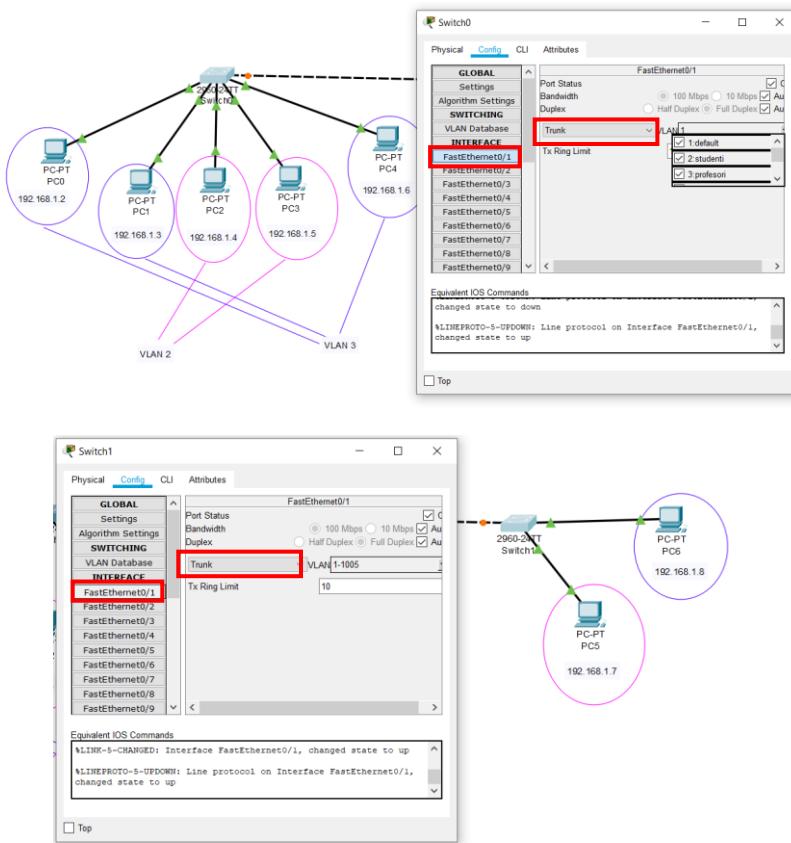
Sada od ova dva računala na novom switch-u, jednoga dodijelimo u crveni (VLAN 2), a drugoga u plavi (VLAN 3). Znači trebamo prvo kreirati VLAN-ove na novom switch-u pa kliknemo na switch1 i u Config tabu odaberemo VLAN Database. Dodamo dva VLAN-a (važno je da redni brojevi budu 2 i 3 kao što je na starome switch-u).



Iduće što moramo učiniti je na novom switch-u dodijeliti ova dva access porta od računala PC5 i PC6 u VLAN-ove prema donjoj slici (PC5 u VLAN 2 i PC6 u VLAN 3).



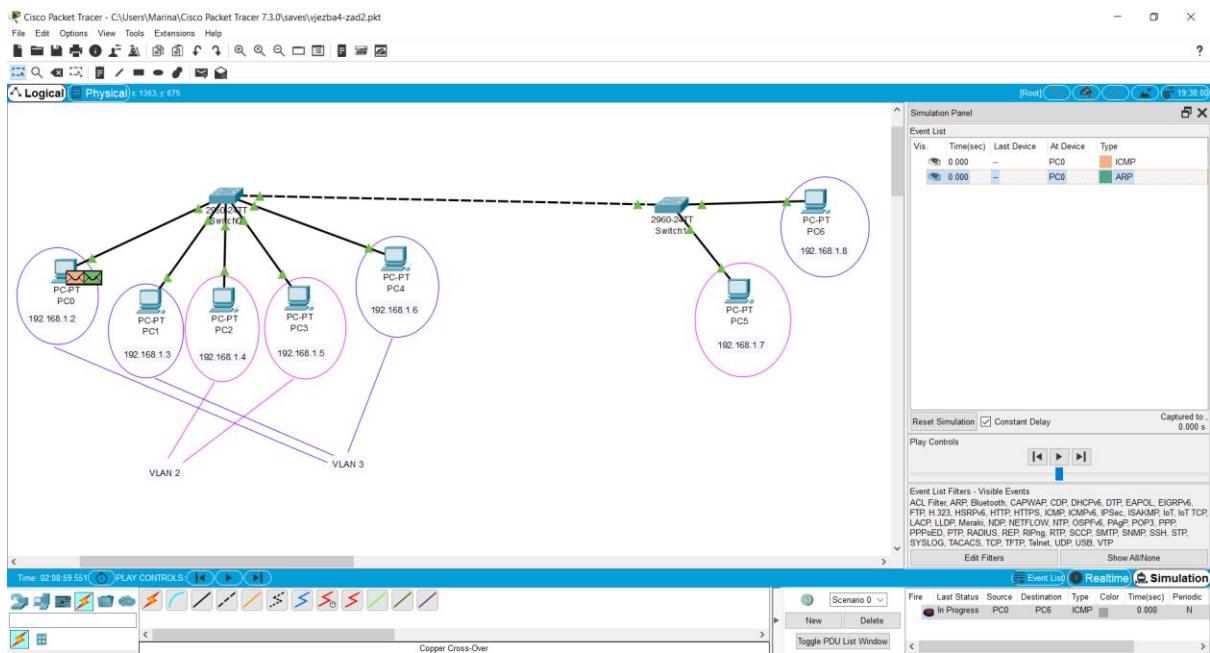
Još moramo postaviti trunk port na novom i na starom switch-u, kako bi se mogao između switch-eva slati VLAN taggirani promet pojedinih VLAN-ova. Sjetite se da smo ostavili Fa0/1 na oba switch-a upravo za potrebe trunk porta. Kliknite na switch0 i u Config tabu odaberite port Fa0/1 pa trunk. Primijetite kako će se automatski odabrati redni brojevi svih VLAN-ova jer nam trunk port omogućava VLAN taggirani promet. Isti postupak ponovite i za switch1.



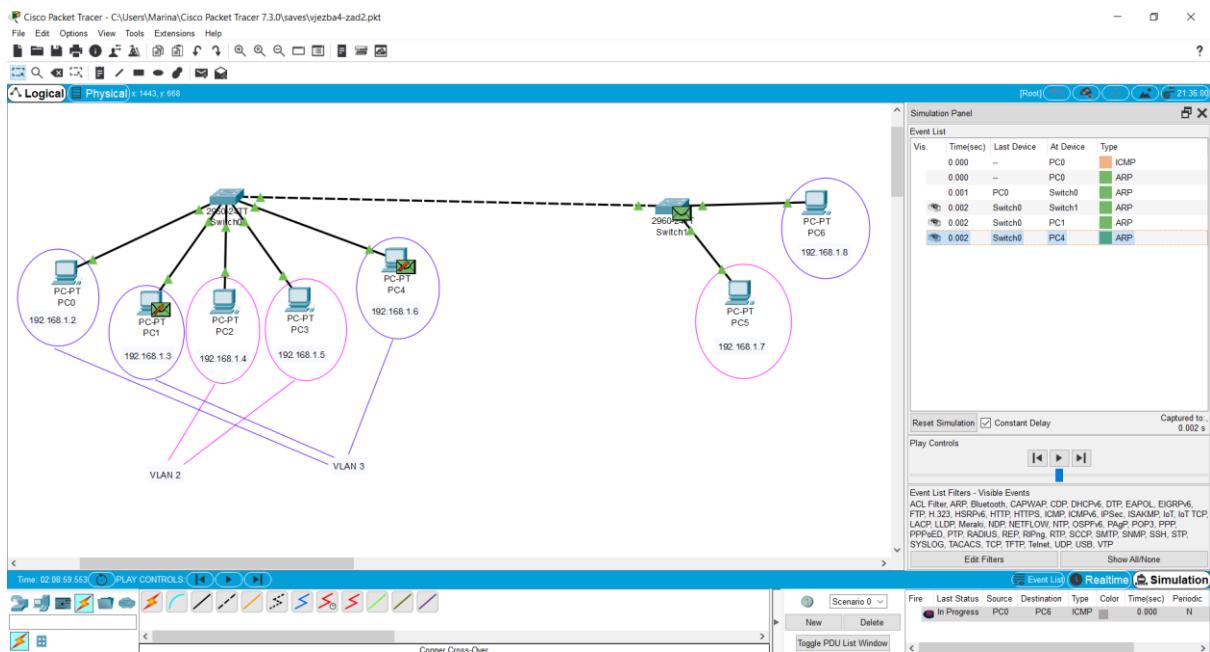
Pitanje 3. Zašto switch-eve ne možemo spojiti access linkom nego moramo trunk linkom?

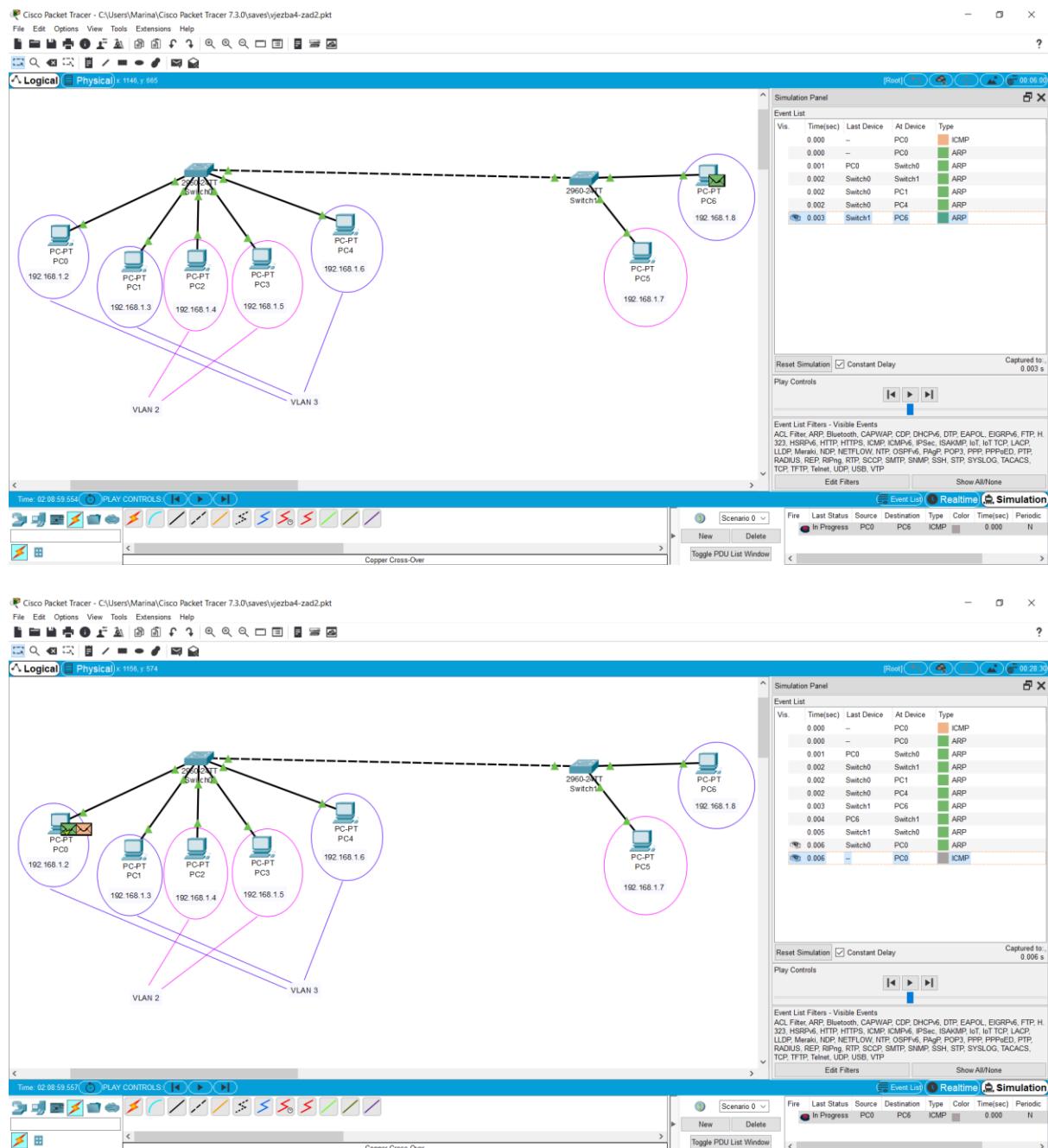
VERIFIKACIJA KOMUNIKACIJE U VLAN MREŽI I IZMEĐU VLAN-ova

Verificirajte komunikaciju između hostova koji su spojeni na različite switch-eve ali pripadaju istoj VLAN mreži. Na primjer, ping između PC0 i PC6 i pratite putanju u simulacijskom modu.

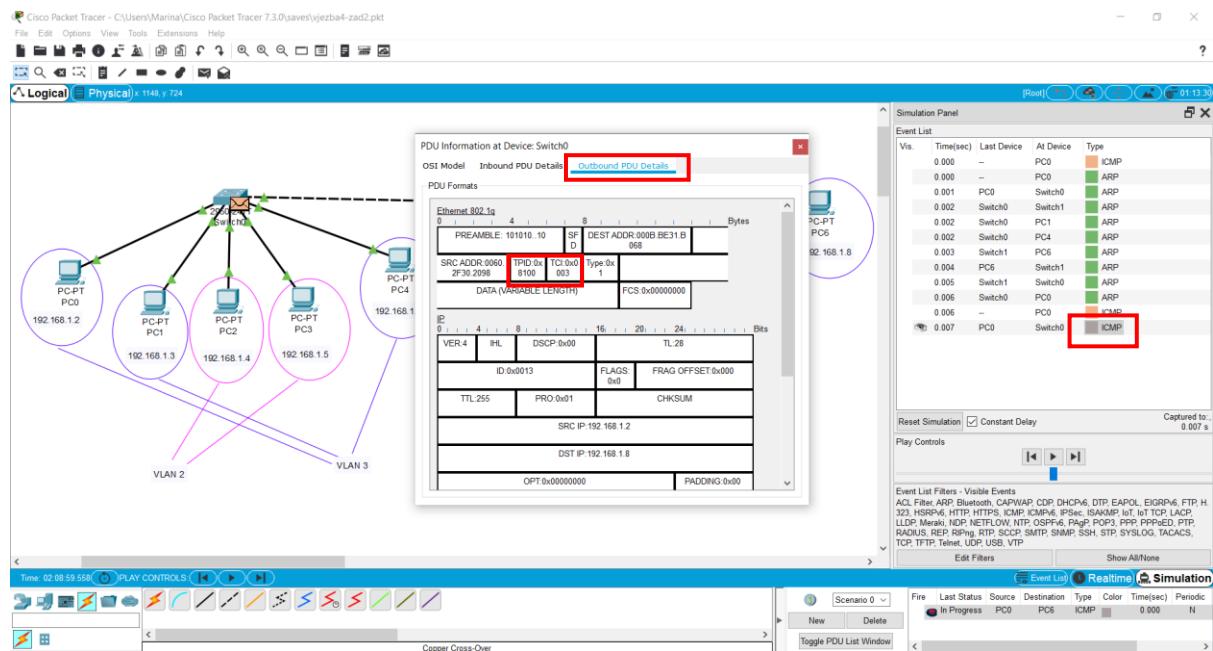


Opet ne zna MAC adresu od PC6 pa se ARP šalje cijeloj mreži. Sada su to PC1 i PC4, ali i novi switch. Paket se propušta dalje i do PC6 jer je na switch-evima omogućen trunk port (tj. između njih je trunk link).

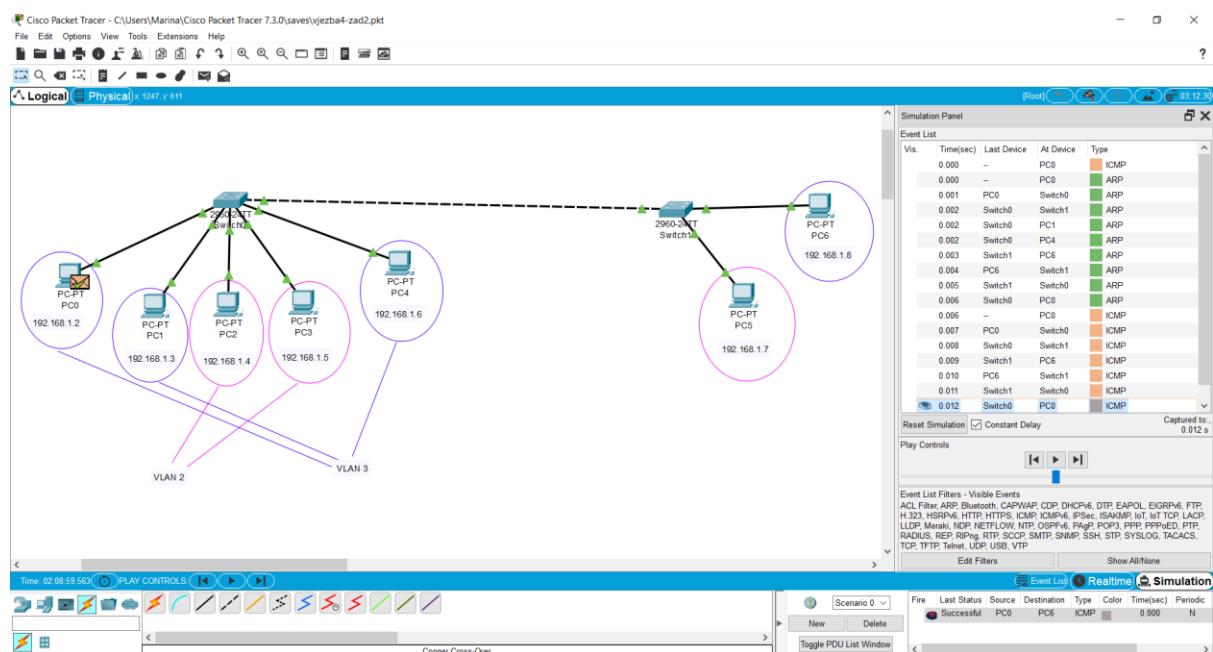




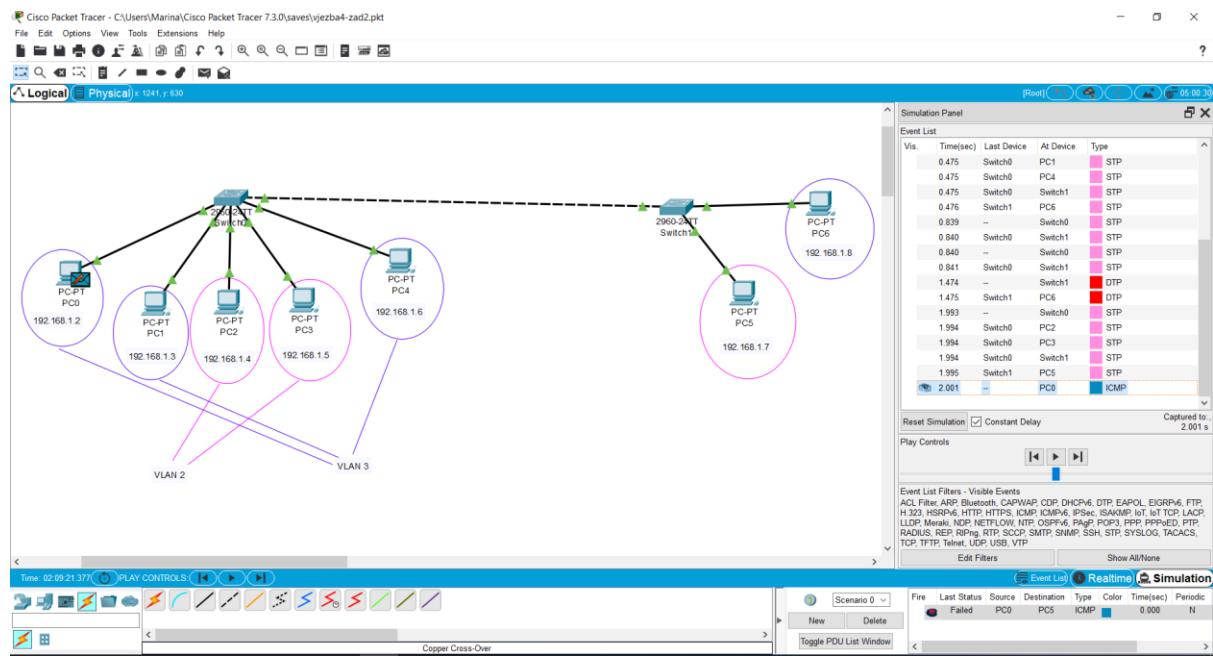
Analizirajte sadržaj Ethernet okvira na switch-u prije nego se pušta na trunk link. Između izvorišne MAC adrese i oznake tipa okvira trebao bi biti umetnut TPID (Tag Protocol Identifier) koji govori da je okvir tagiran po 802.1Q standardu za VLAN mrežu i ima vrijednost 0x8100. Također bi se trebao vidjeti TCI (Tag Control Information) koji sadrži VID (VLAN identifikator). U našem slučaju je VID=3 jer se šalje promet od VLAN-a 3, tj. pingamo od PC0 do PC6 koji pripadaju VLAN-u s rednim brojem 3.



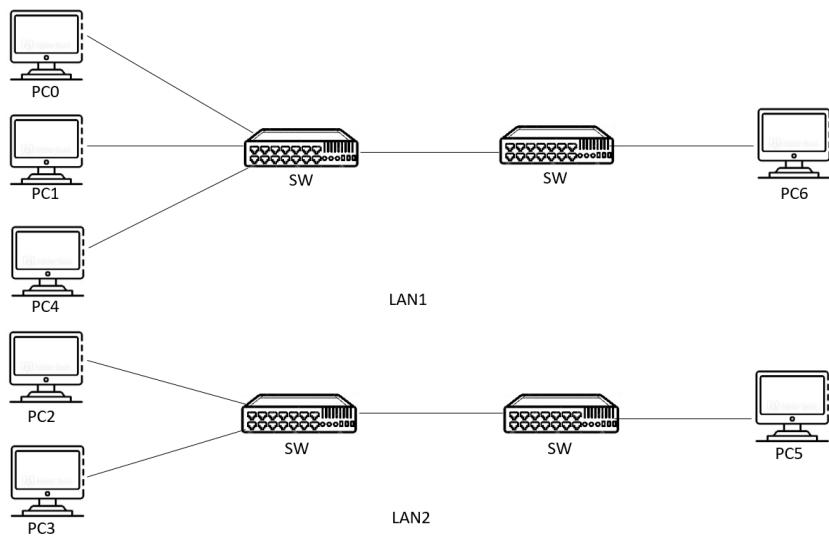
Izvršite simulaciju do kraja i komunikacija unutar VLAN-a je uspješna.



Pitanje 4. Pošaljite paket između VLAN-ova, konkretno od PC0 do PC5. Je li komunikacija između VLAN-ova uspješna?



Ova mreža ovako konfigurirana kao gore vam je kao da imamo dvije skroz odvojene LAN mreže. Skica logičke mreže dana je ispod:



U posljednjem zadatku ćemo pokazati da sva računala iz VLAN-a moraju imat adrese iz iste (pod)mreže.

POVEZNICA IZMEĐU VLAN-A I PODMREŽE

Sve što smo do sada pokazali je ispravno, ali nije baš kao u praksi. Naime, ako dijelimo jednu LAN mrežu (kojoj su dodijeljene neke IP adrese koje pripadaju istoj mreži) na više VLAN-ova, onda bi ispravno bilo podijeliti tu cijelu mrežu adresa na dvije podmreže i računalima iz jednog VLAN-a dodijelit adrese iz jedne podmreže, a računalima iz drugog VLAN-a dodijelit adrese iz druge podmreže.

Zašto je to važno?

Zato jer da bi se mogao, jednom kad dodamo router u ovu mrežu, preko toga routera (na temelju IP adresa) promet sa jednog VLAN-a prenijeti na drugi VLAN. Inače to neće biti moguće, jer kako ćemo reći routeru na kojem portu mu je koja mreža. Ovako će mu sve što potjeće iz jedne podmreže biti na jednom portu, a sve što je iz druge podmreže će mu biti na drugome portu.

Na primjer, u gornjim primjerima smo koristili mrežu 192.168.1.0/24.

Mrežu sada podijelimo na dvije podmreže, što znači da uzmemo 1 bit od mrežnog dijela za mrežu, a preostalih 7 bitova je za hostove.

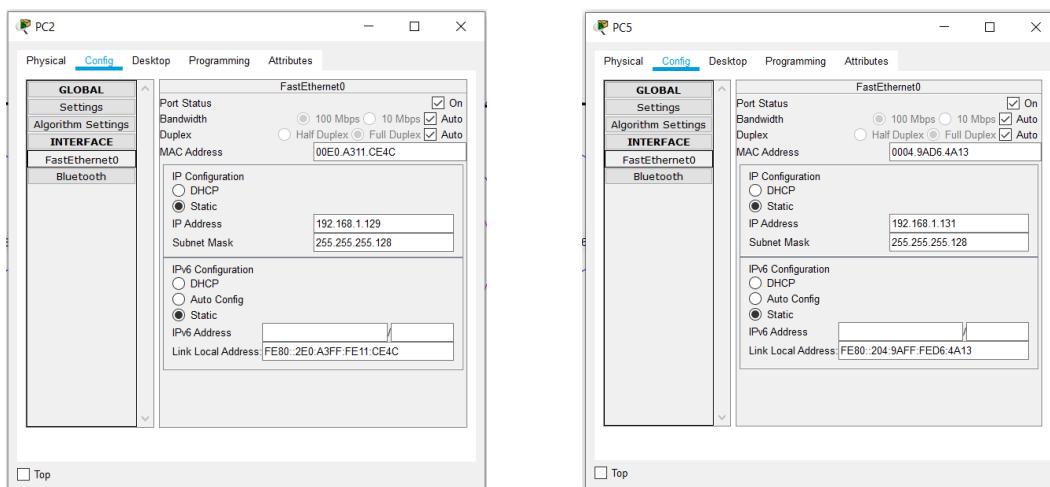
Mrežna maska je sada 255.255.255.128.

Dobijemo 2 podmreže:

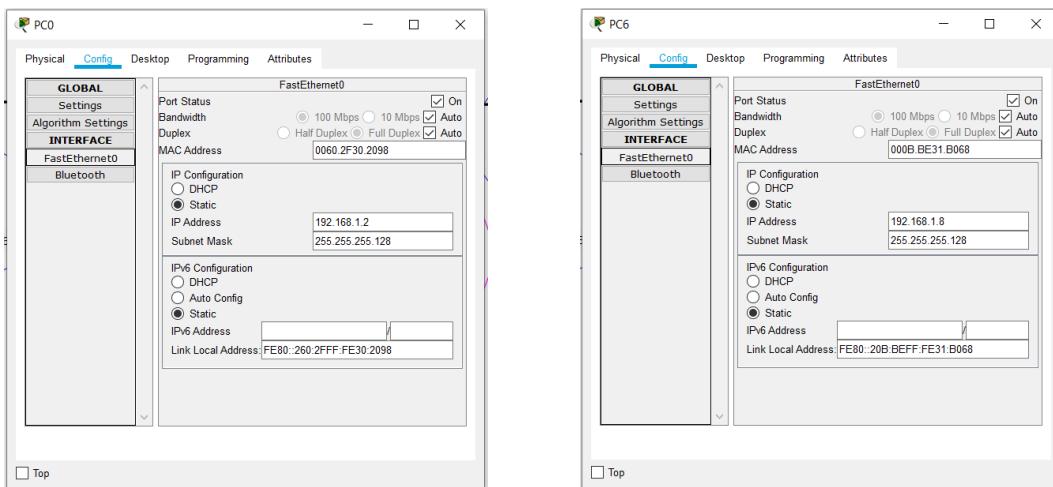
- 192.168.1.0 - 192.168.1.127
 - 192.168.1.0 je adresa podmreže
 - 192.168.1.127 je broadcast adresa
 - 192.168.1.1 do 192.168.1.126 je raspon hostova
- 192.168.1.128 - 192.168.1.255
 - 192.168.1.128 je adresa podmreže
 - 192.168.1.255 je broadcast adresa
 - 192.168.1.129 do 192.168.1.254 je raspon hostova

Dodijelite svim računalima iz VLAN-a 2 IP adrese iz prve podmreže i svim računalima iz VLAN-a 3 IP adrese iz druge podmreže. Ne zaboravite promijeniti mrežnu masku. Pinganjem testirajte komunikaciju unutar VLAN-a i između VLAN-ova.

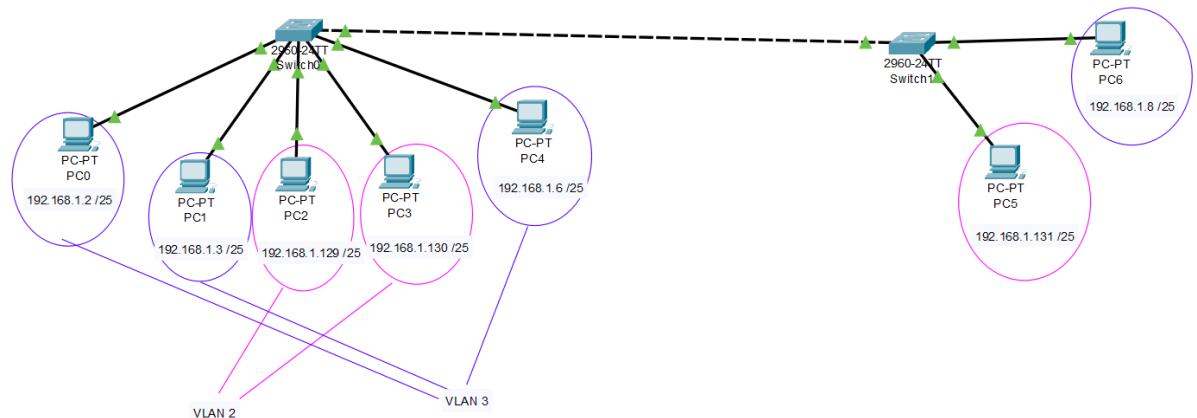
Primjer postavljanja IP adresa i mrežne maske u VLAN-u 2:



Primjer postavljanja IP adresa i mrežne maske u VLAN-u 3:



Pitanje 5. Pošaljite paket između VLAN-ova i unutar VLAN-a. U kojem slučaju je komunikacija uspješna, a u kojima nije i zašto?



ZADACI ZA VJEŽBU 3 (PREDAJA IZVJEŠTAJA):

Odgovoriti na pitanja koja su zadana tijekom vježbe.

Svaki odgovor potkrijepiti simulacijom u alatu Packet Tracer kako je pokazano na vježbi i predati sve konfiguracije pod nazivom:

- **ime_prezime_odgovor1(pkt)**
- **ime_prezime_odgovor2(pkt)**
- **ime_prezime_odgovor3(pkt)**
- **ime_prezime_odgovor4(pkt)**
- **ime_prezime_odgovor5(pkt)**.

VJEŽBA 4: USMJERAVANJE NA INTERNETU

CILJ VJEŽBE

Cilj ove vježbe je simulirati dinamičko usmjeravanje i pokazati princip rada RIP protokola. Vježba je prilagođena sa [19].

TEORIJSKI PREDUVJETI

Podrazumijeva se osnovno razumijevanje idućih teorijskih pojmove:

- Lokalna mreža
- Mrežna IP adresa računala i postavljanje statičke IP adrese
- ARP protokol
- Postavljanje adrese default gateway-a

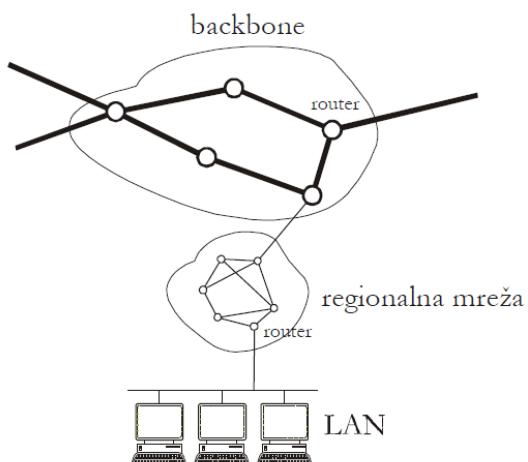
Teorijski dijelovi vježbe u nastavku preuzeti su sa [5].

USMJERAVANJE NA INTERNETU

Usmjeravanje kod paketskih mreža ima primarnu ulogu osigurati dostupnost od izvorišta do odredišta toka podataka, a sekundarnu pri tome utjecati na optimalno iskorištenje mreže i kvalitetu usluge. Usmjernik (router) je sustav s više mrežnih priključaka, koji svoj rad temelji na **algoritmu usmjeravanja** (routing algorithm). Algoritam usmjeravanja određuje na koji od priključaka proslijediti datagram koji pristigne na jedan od njih (forwarding). Odluka o usmjeravanju donosi se na temelju sadržaja **tablice usmjeravanja** (routing table).

ARHITEKTURA USMJERAVANJA NA INTERNETU

Prvobitno su usmjernici unutar Interneta bili organizirani hijerarhijski, što je bilo naslijede ranije ARPANET arhitekture. Postojaо je centralni sustav (jezgra) mreže, kroz čije su usmjernike (core gateways) prolazile informacije o usmjeravanju među svim mrežama Interneta. Rastom Interneta, naglo je rasla i količina usmjerivačkih informacija koje je jezgra trebala obraditi, te je to postao i glavni nedostatak hijerarhijskog modela.



Novi model usmjeravanja zasniva se na ravnopravnim nezavisnim (autonomnim) sustavima. Svaki nezavisni sustav sastoji se od grupe mreža koje su pod istom administrativnom upravom. Arhitektura Internet mreže dana je na gornjoj slici.

Osnovna mreža (Backbone), povezuje vanjske usmjernike i predstavlja najvišu razinu. Paketi IP protokola isporučuju se optimalnim putem do usmjernika preko kojega je dostupna osnovna podmreža odredišta.

Osnovna podmreža (Autonomous system) predstavljena je s jednom ili više adresnih klasa, a karakterizirana je vlastitom administracijom adresa. Dijeli se na podmreže s fiksnom (klase) ili varijabilnom (adresna maska) mrežnom adresom. Najčešće je ostvarena jednostavnom do srednje složenom mrežom unutrašnjih usmjernika na koje su povezane podmreže. IP paketi se usmjeravaju optimalnim putem do usmjernika preko kojega je dostupna podmreža odredišta.

Podmreža (Subnetwork) je dio Interneta koji obuhvaća jednu zonu prostiranja (broadcast domain) lokalne mreže, a čija je mrežna IP adresa određena klasom ili mrežnom maskom. Podmreža je s osnovnom podmrežom povezana najčešće samo jednim usmjernikom, koji za računala podmreže predstavlja osnovni usmjernik (default gateway). Pakete koji dolaze na podmrežu osnovni usmjernik pakira u okvire s MAC adresom odredišta i proslijedi ih lokalnom mrežom.

Pakete koji idu van iz podmreže, izvorište pakira u okvire s MAC adresom osnovnog usmjernika, koji će ih proslijediti dalje kroz osnovnu podmrežu.

Paketi kojima je izvorište i odredište na istoj podmreži (unutar granica zone prostiranja), odredište pakira u okvir s MAC adresom odredišta i šalje ga direktno odredištu.

U sva tri slučaja, pripadnost paketa podmreži određuje se na osnovu mrežnog dijela IP adrese, a pretvorba IP adrese odredišta ili usmjernika u MAC adresu obavlja se korištenjem ARP protokola.

S obzirom na takvu podjelu razlikujemo sljedeće vrste usmjernika:

- **vanjske usmjernike** koji obavljaju usmjeravanje i razmjenjuju informacije o usmjeravanju između različitih nezavisnih sustava. Takvi sustavi koriste vanjske usmjerivačke protokole (npr. BGP-Border Gateway Protocol).
- **unutrašnje usmjernike** koji usmjeravaju pakete unutar nezavisnih sustava. Takvi sustavi koriste unutrašnje usmjerivačke protokole (npr. RIP-Routing Information Protocol, OSPF-Open Shortest Path First, EIGRP-Enhanced Interior Gateway Routing Protocol).

Algoritmi/protokoli usmjeravanja se također mogu podijeliti u sljedeće dvije grupe:

- statički (neadaptivni) algoritmi ne uzimaju u obzir topologiju mreže, njen opterećenje i sl. već se put paketa od točke A do točke B određuju unaprijed i postavlja kod pokretanja usmjernika.
 - **Shortest Path algoritam** - Veze između usmjernika opisuju se karakterističnim parametrima: udaljenost, brzina, kašnjenje, cijena, i sl. Mijenjanjem težine koja se pridaje jednom od ili više navedenih parametara određuje se najkraći put po zadanim parametrima.

- **Flooding** - Ovaj algoritam se sastoji u proslijđivanju primljenog paketa na sve priključke osim izvođenog. Kako se na taj način generira golem promet kopija datagrama, koriste se razne optimizacije kako bi se taj problem smanjio.
- adaptivni algoritmi uzimaju u obzir parametre rada mreže, te u skladu s njima mijenjaju sadržaj tablice usmjeravanja.
- **Distance Vector Routing** - Svaki usmjernik održava tablicu vektora, koja sadrži "udaljenost" do odredišta i preko kojeg priključka ga je moguće dosegnuti. Usmjernici međusobno komuniciraju i mijenjaju tablicu vektora u skladu s promjenama u radu mreže. Primjeri ovog algoritma su EIGRP, te RIP - prvi algoritam usmjeravanja Interneta, koji se i danas koristi, ali na manjim mrežama.
- **Link State Routing** - "Udaljenost" iz prethodnog algoritma podrazumijevala je duljinu reda čekanja (queue) u određenom smjeru. S uvođenjem više linija različitih brzina, ali i njegovih drugih slabosti 1979. se prelazi na Link State Routing algoritme (npr. OSPF), kod kojeg svaki usmjernik ima nekoliko zadataka:
 - upoznati susjedne usmjernike i njihove adrese, odrediti kašnjenje ili cijenu do svakog od njih,
 - konstruirati paket s podacima iz prvog zadatka i poslati ga ostalim usmjernicima (flooding)
 - odrediti najkraću putanju do svakog svih ostalih usmjernika.

TABLICE USMJERAVANJA I RIP

Da bi olakšali traženje optimalnog puta usmjernici održavaju tablice usmjeravanja. One sadrže niz informacija potrebnih za usmjeravanje i odabir najboljeg puta, primjerice:

- parove `adresa_odredišta-slijedeći_usmjernik` koji govore usmjerniku da se odgovarajuće odredište može dosegnuti na optimalan način ako se pošalje na navedeni sljedeći usmjernik. Dakle, usmjernici ne drže informacije o potpunom putu paketa već sadrže samo prvi sljedeći korak na tom putu. Odredište može biti mreža, računalo ili posebna oznaka koja označava osnovni usmjernik.
- mrežnu masku za određeno odredište
- metriku - koja definira mehanizam za uspoređivanje kakvoće pojedinih smjerova
- ime mrežnog sučelja koje koristi navedeni smjer
- da li je smjer ispravan, koristi li usmjernike ili je vezan izravnom vezom i sl.
- vrijeme kada je pojedini smjer posljednji put ažuriran.

Unutar tablice usmjeravanja postoji posebna adresa kojom se definira osnovni smjer (default route) i najčešće je to adresa koja sadrži sve nule (0.0.0.0). Na osnovni smjer šalju se svi paketi za koje se ne može pronaći odredište unutar tablice usmjeravanja (bilo bi nepraktično da svaki usmjernik ima u tablici usmjeravanja sva moguća odredišta). Osnovni smjer definiran je adresom osnovnog usmjernika (default gateway). Dakle, kada paket stigne na neki usmjernik, on provjerava tablicu usmjeravanja ne bi li našao odgovarajuću odredišnu adresu (računala ili njegovu mrežnu adresu) i ako je ne pronađe, šalje je na vlastiti osnovni usmjernik.

RIP (Routing Information Protocol) je još vrlo popularan unutrašnji protokol za usmjeravanje. RIP omogućuje usmjernicima i računalima razmjenu informacija o usmjerivačkim smjerovima unutar Internet mreže. Zasniva se na algoritmu "vektora udaljenosti" i to tako da odabire smjer s najmanjim "brojem koraka" (brojem usmjernika koje paket treba proći na putu do odredišta) kao najbolji. Najduži prihvatljivi smjer unutar RIP usmjerivačke tablice može imati najviše 15 koraka (za >15 RIP smatra da se odredište ne može doseći). RIP pamti samo najbolji put do odredišta, tj. ako nova informacija nudi bolji smjer (manji broj koraka), nova informacija zamjenjuje staru.

Kada neki RIP usmjernik detektira prekid jedne od svojih vlastitih veza on ažurira svoju tablicu (postavlja broj koraka za taj smjer na 16) i susjednim usmjernicima šalje vlastitu usmjerivačku tablicu. Svaki usmjernik koji primi ovu poruku ažurira vlastitu tablicu i šalje je dalje – promjena se propagira mrežom.

Za prijenos dijelova vlastite usmjerivačke tablice RIP koristi UDP datagrame. Ukoliko računalo nije usmjernik ono također može motriti ove RIP poruke, ali ne šalje vlastitu tablicu. To je tzv. "tihi" RIP proces (**silent RIP**). RIP ne osigurava mehanizam za prijavu pogreški izvořnom računalu kada dođe do pogreški pri usmjeravanju. Tu funkciju obavlja ICMP protokol.

RIP proces svakih 30 sekundi šalje čitavu usmjerivačku tablicu svojim susjedima. Ako nakon 180 sekundi usmjernik nije dobio potvrdu smjera u tablici, on proglašava smjer neispravnim (broj koraka postavlja >15), a ukoliko nakon dalnjih 120 sekundi (najčešće) ne dobije potvrdu smjera, on ga briše iz tablice usmjeravanja. Ukoliko usmjernik detektira prekid neke veze on, po ažuriranju vlastite tablice, odmah šalje svoju tablicu susjednim usmjernicima ne čekajući istek 30 sekundi (**triggered update**).

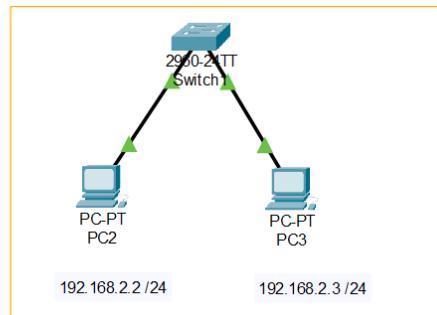
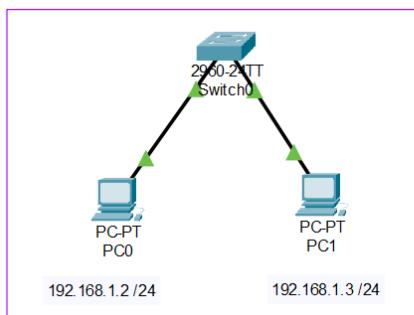
Osim ograničavanja najvećeg broja koraka na 15, RIP protokol uključuje i niz dodatnih svojstava koja omogućuju stabilniji rad:

- **Podijeljena obzorja** (Split Horizons) - Ovo svojstvo proizlazi iz činjenice da nije korisno slati informaciju o smjerovima u onom smjeru iz kojeg smo tu informaciju i primili. Ovim sprječavamo stvaranje usmjerivačkih petlji između 2 usmjernika.
- **Ažuriranje prekinutih smjerova** (Poison Reverse Updates) - Ovo svojstvo namijenjeno je nalaženju i sprječavanju usmjerivačkih petlji između tri ili više računala, a temelji se na tome da povećavanje broja koraka za pojedini smjer obično ukazuju na pojavu usmjerivačke petlje. Stoga se pri uočavanju ovakvih smjerova šalju paketi (Poison reverse update poruke) koje brišu takve smjerove iz usmjerivačkih tablica.
- **Zadržavanje promjene izbrisanih smjerova** (Hold-downs) - Budući da ažuriranje smjerova koji su prekinuti ne dolazi istovremeno na svaki usmjernik, može se dogoditi da usmjernik koji još nije obaviješten o prekidu veze šalje redovite poruke u kojima navodi da je takav smjer još ispravan. Usmjernik koji primi takvu poruku, a već je obaviješten o prekidu tog smjera, neće odmah takav smjer staviti u svoju tablicu već će određeno vrijeme zadržavati promjenu.

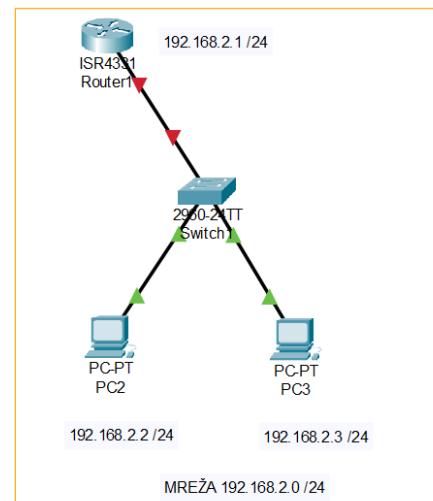
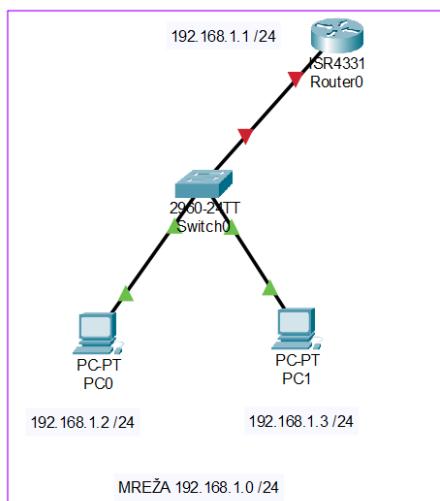
KREIRANJE MREŽNE TOPOLOGIJE

Napravite dvije lokalne mreže (prema donjoj slici), sa po dva računala spojena na svaki switch. Računala spojite na portove Fa0/2 i Fa0/3 na svakom switch-u, kako bi port Fa0/1 ostao slobodan radi jednostavnosti (IP adresa uređaja x.x.x.2 je na switch portu Fa0/2, a IP

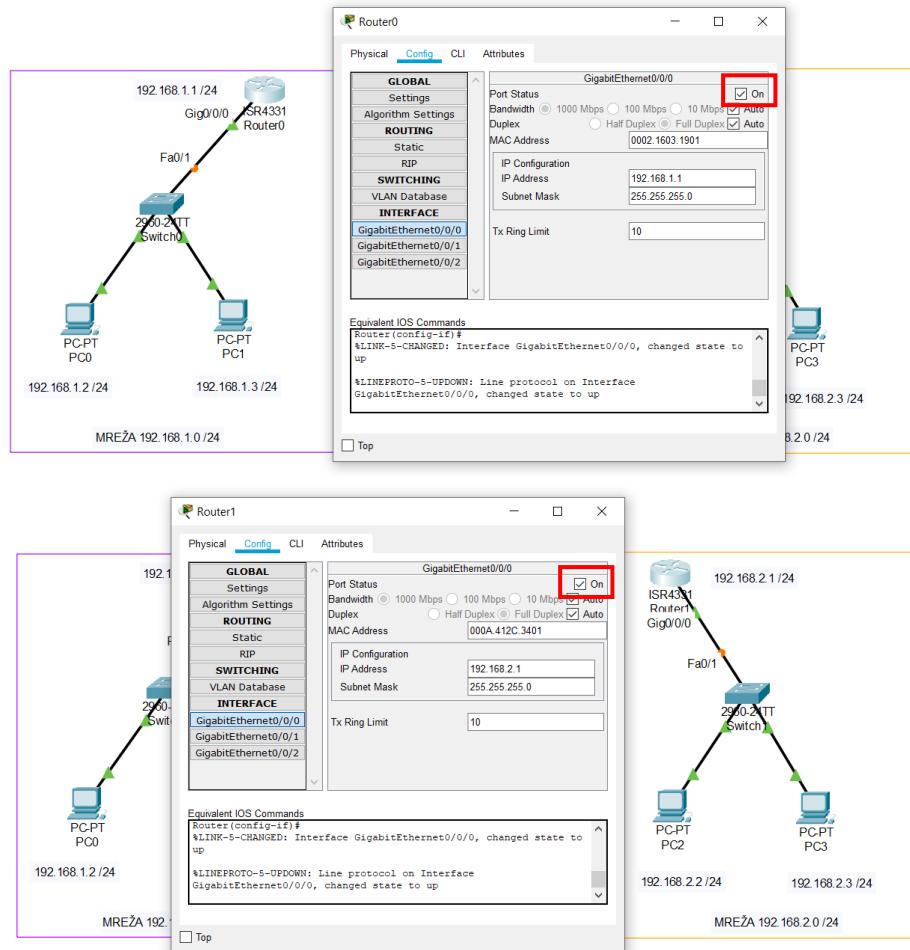
adresa uređaja x.x.x.3 je na switch portu Fa0/3). Dodajte računalima IP adrese i mrežnu masku prema slici.



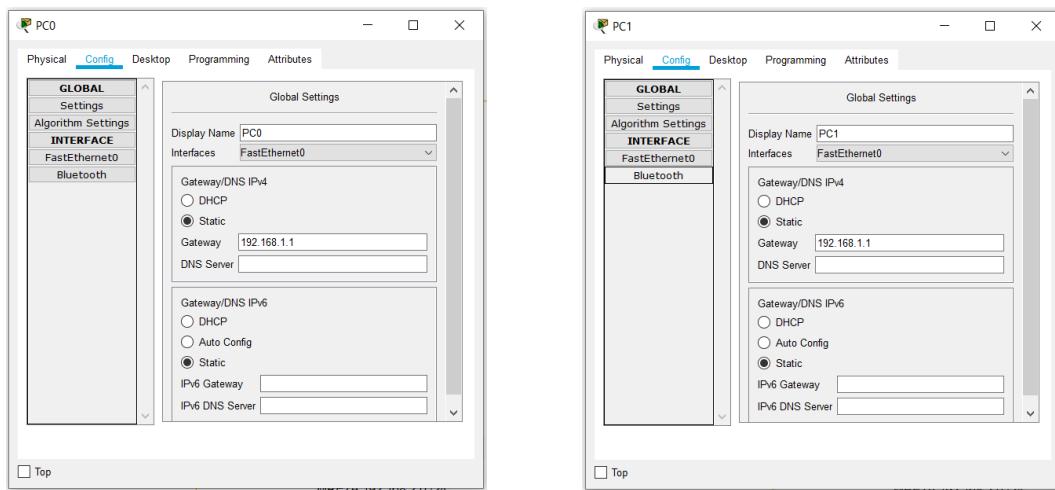
U vježbi 2 smo naučili da ove dvije mreže možemo povezati korištenjem samo jednog routera, ali za potrebe današnje vježbe i algoritama usmjeravanja smatrat ćemo da svaka mreža ima svoj router i dodijelit ćemo mu odgovarajuću IP adresu. Veza između routera i switcha se ostvaruje pomoću standardnog bakrenog straight-trough kabela (kao i kod spajanja računala na switch). Priključak lijevog switch-a Fa0/1 povežite na port Gig0/0/0 na lijevom routeru, a priključak desnog switch-a Fa0/1 povežite na port Gig0/0/0 na desnom routeru.

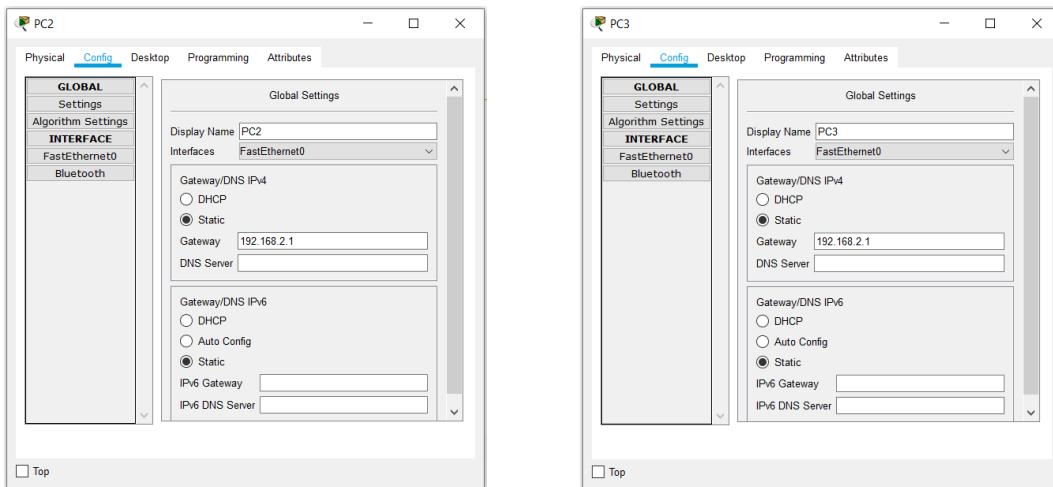


Kako je lijevi router zapravo default gateway za lijevu mrežu, on mora imati IP adresu koja odgovara lijevoj mreži, a kako je desni router default gateway za desnu mrežu, on mora imati IP adresu koja odgovara desnoj mreži. Nakon podešavanja IP adrese ne zaboravite aktivirati odgovarajući priključak router-a tako što ćete selektirati polje "On" u okviru grafičkog sučelja kao što je prikazano na donjim slikama.

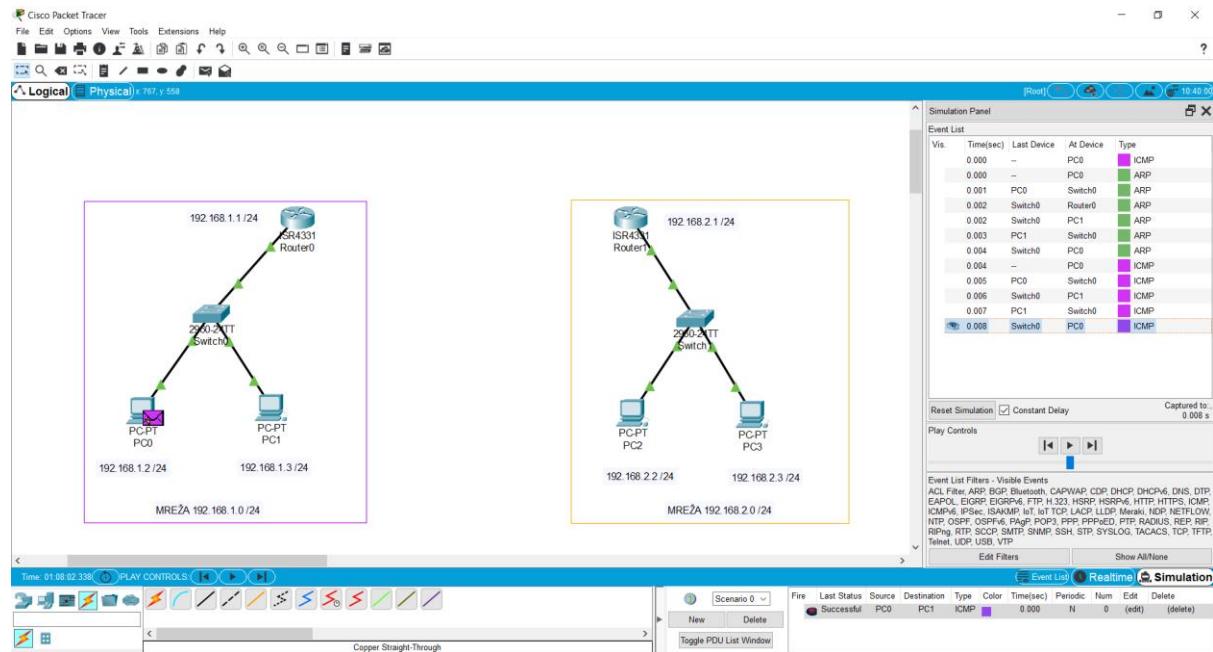


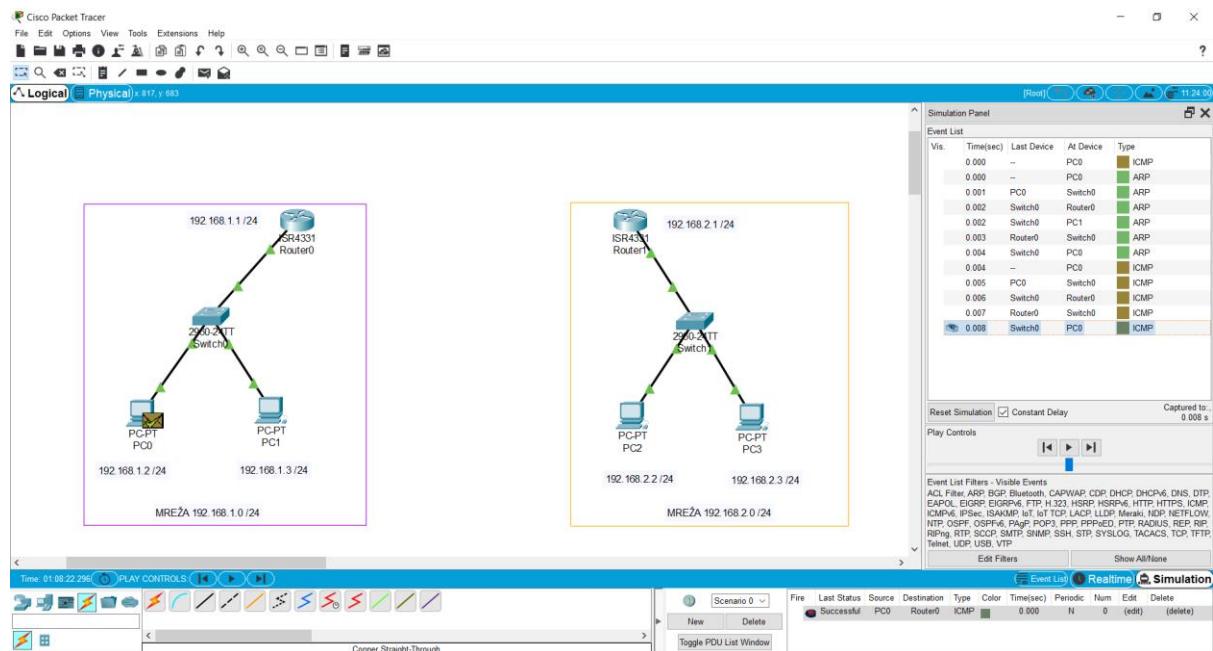
Kako smo već naučili, potrebno je napraviti još jedan korak - na računalima u svakoj od mreža treba podesiti adresu default gateway-a:





Korištenjem naredbe ping u simulacijskom načinu rada provjerite je li ostvarena komunikacija između računala u svakom LAN-u: od PC0 do PC1 i od PC2 do PC3. Također provjerite da svako računalo može pingati svoj default gateway. Primjer za PC0 je dan na idućim slikama.

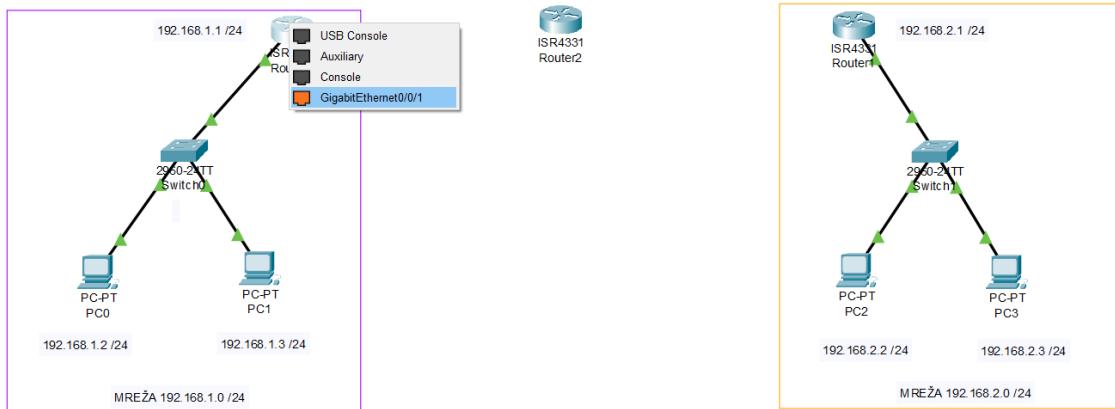


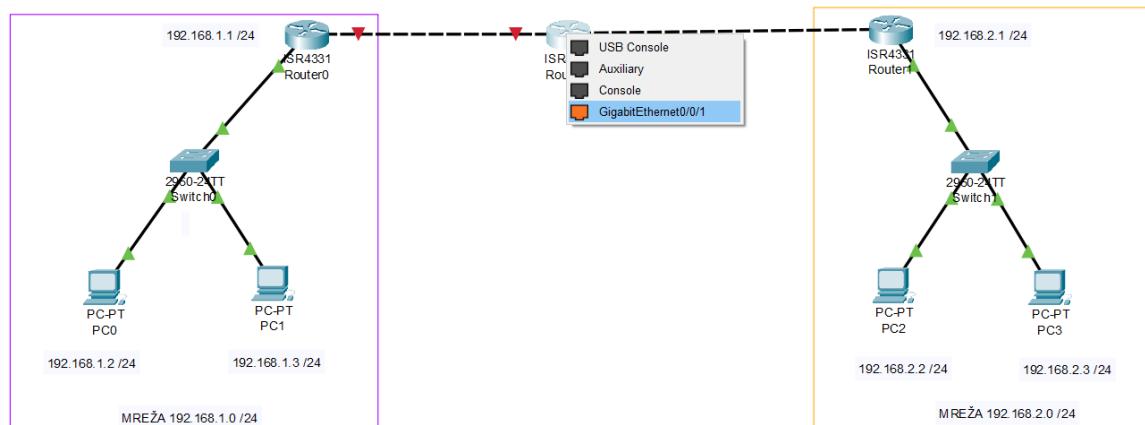
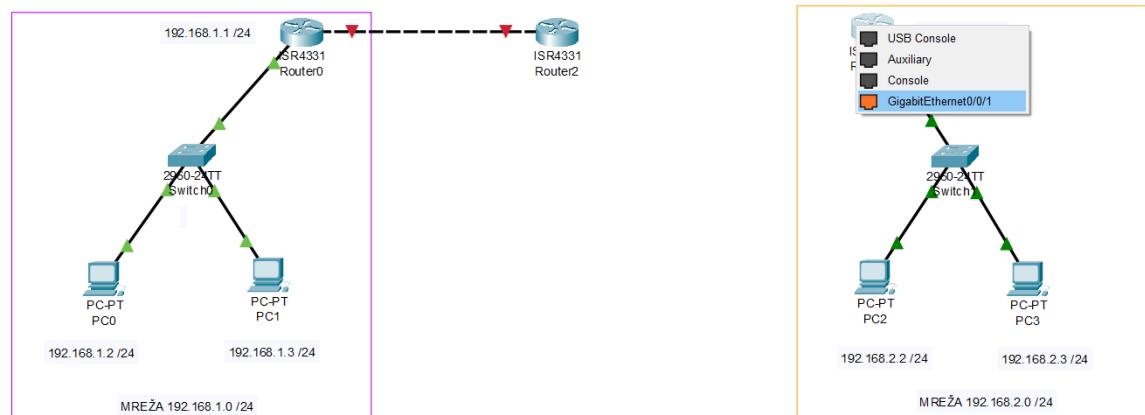
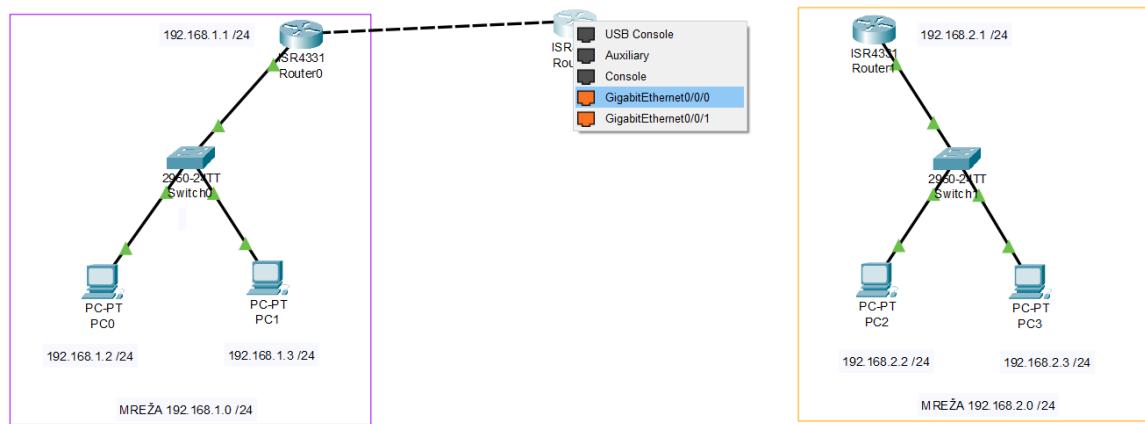


Spremite Packet Tracer topologiju pod nazivom **ime_prezime_zadatak1.pkt**.

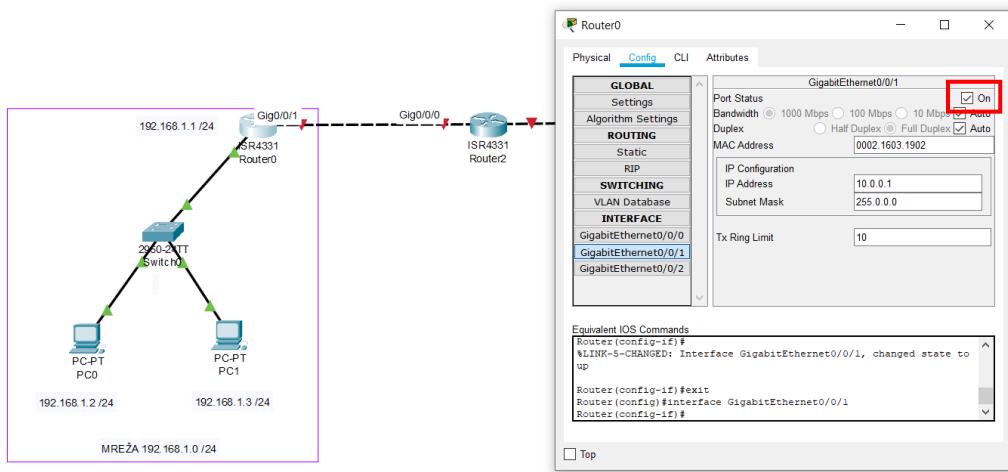
STVARANJE MREŽE SUSJEDNIH ROUTERA

Nećemo routere direktno povezati, nego ćemo ih povezati preko još jednog dodatnog routera. Routere međusobno spajamo korištenjem Copper Cross-Over kabela i to priključak Gig0/0/1 na lijevom routeru povežemo sa Gig0/0/0 na srednjem routeru, a port Gig0/0/1 srednjeg routera na port Gig0/0/1 na desnom routeru.

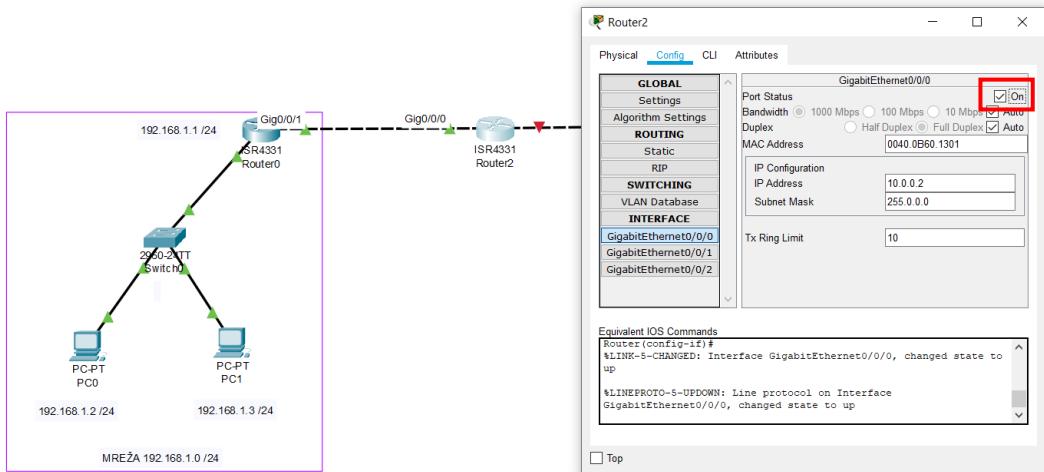




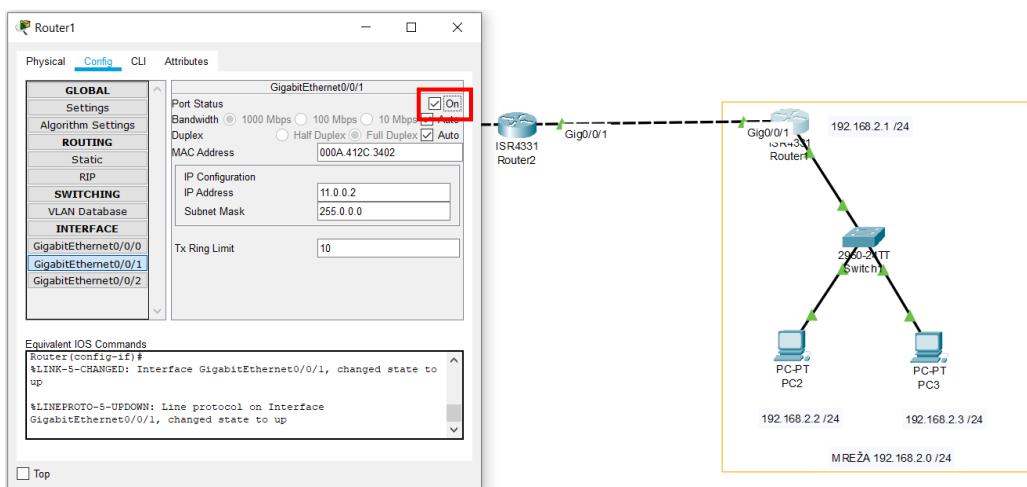
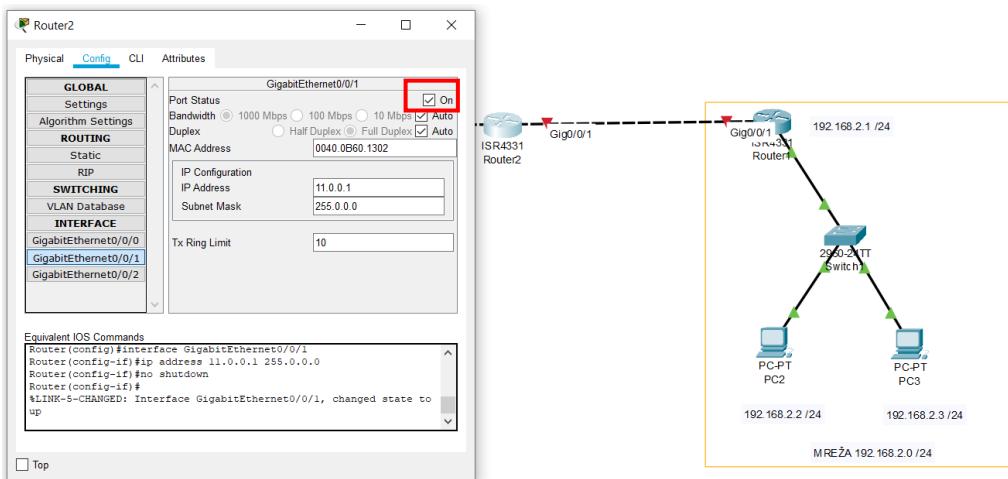
Lijevi router s lijeve strane ima adresu klase C i to je 192.168.1.1 (na portu prema switch-u od mreže 192.168.1.0), a s desne strane (na portu Gig0/0/1) ćemo mu staviti adresu klase A, na primjer 10.0.0.1. Naravno, možemo i ovdje odabratи adresu klase C, ali ovu smo odabrali radi jednostavnosti - da lakše možemo pratiti adresu mreža između routera. Važno je samo da bude druga adresa (sa drugačijim mrežnim dijelom) jer se radi o drugoj mreži. Ponovno ne zaboravite uključiti port na routeru uz pomoć opcije "On".



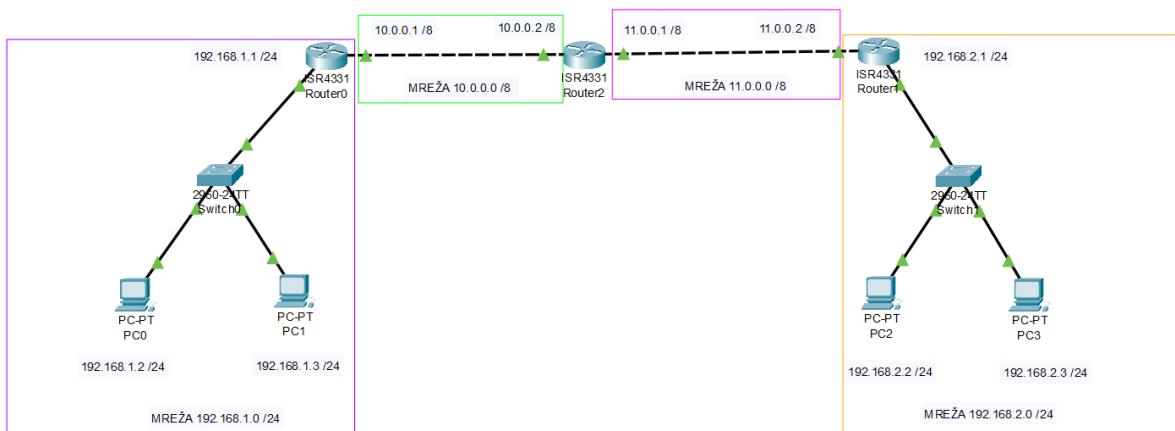
Sada srednjem routeru s lijeve strane moramo staviti adresu koja odgovara mreži 10.0.0.0 kako bi router0 i router2 bili u istoj mreži. Odabrali smo iduću dostupnu adresu hosta, a to je 10.0.0.2 i dodijelimo je portu Gig0/0/0 srednjeg routera i uključimo ga.



Istu stvar napravimo na desnoj strani srednjeg routera. Ovo je sada još jedna odvojena mreža pa moramo dodijeliti novu adresu s drugačijim mrežnim dijelom – odabrali smo 11.0.0.1 kojeg ćemo dodijeliti desnoj strani srednjeg routera (port Gig0/0/1). Desnom routeru na port Gig0/0/1 stavimo IP adresu sa istim mrežnim dijelom, ali sa drugom adresom hosta (prva dostupna iza prethodne je 11.0.0.2).



U našoj konfiguraciji sada imamo četiri lokalne mreže. U jednoj su dva računala s lijeve strane i lijeva strana lijevog routera, u drugoj su desna strana lijevog routera i lijeva strana srednjeg routera, u trećoj su desna strana srednjeg routera i lijeva strana desnog routera, a u četvrtom LAN-u su dva računala s desne strane i desna strana desnog routera.



Spremite Packet Tracer topologiju pod nazivom **ime_prezime_zadatak2.pkt**.

Provjerite komunikaciju između računala PC0 i PC2. Prije nego što pokrenete simulaciju, odgovorit ćemo na slijedeće pitanje:

Pitanje 1.

PC0 nema u svojoj ARP tablici MAC adresu od PC2. Hoće li se poslati ARP paket?

U ovom slučaju se NEĆE poslati ARP paket zato što smo u prethodnom zadatku provjeravali da li svako računalo u LAN-u može pingati svoj default gateway. Inače, da nismo u prethodnom zadatku već pingali router0 sa PC0, switch bi ARP pakete proslijedio na uređaje PC1 i router0 (default gateway), znači na sve uređaje u LAN-u od PC0.

Provjerite navedeno tako što ćete izbrisati ARP tablicu na PC0 uz pomoć naredbe arp -d u komandnoj liniji i ponovno pokrenuti simulaciju.

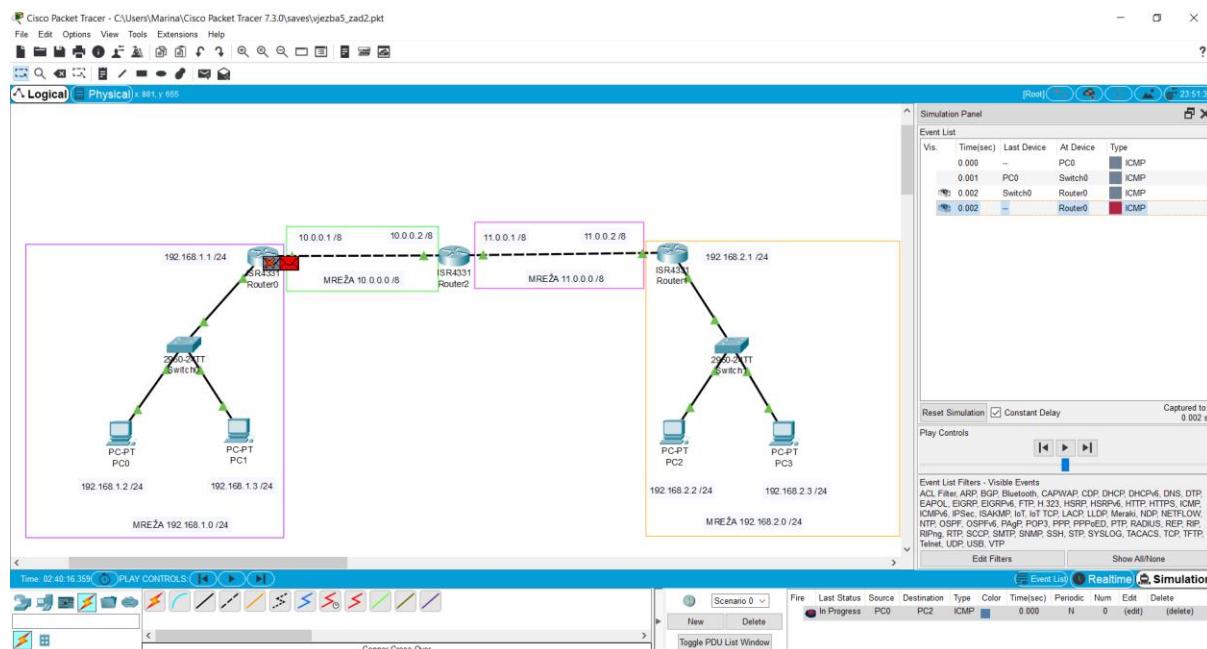
U našem slučaju, PC0 već zna MAC adresu default gateway-a i to je MAC adresa odredišta paketa koja se upisuje u ICMP poruci upućenoj na PC2.

Pokrenite simulaciju kojom pingamo računalo PC2 sa PC0. Pratite putanju paketa u simulacijskom načinu rada i odgovorimo na iduće pitanje:

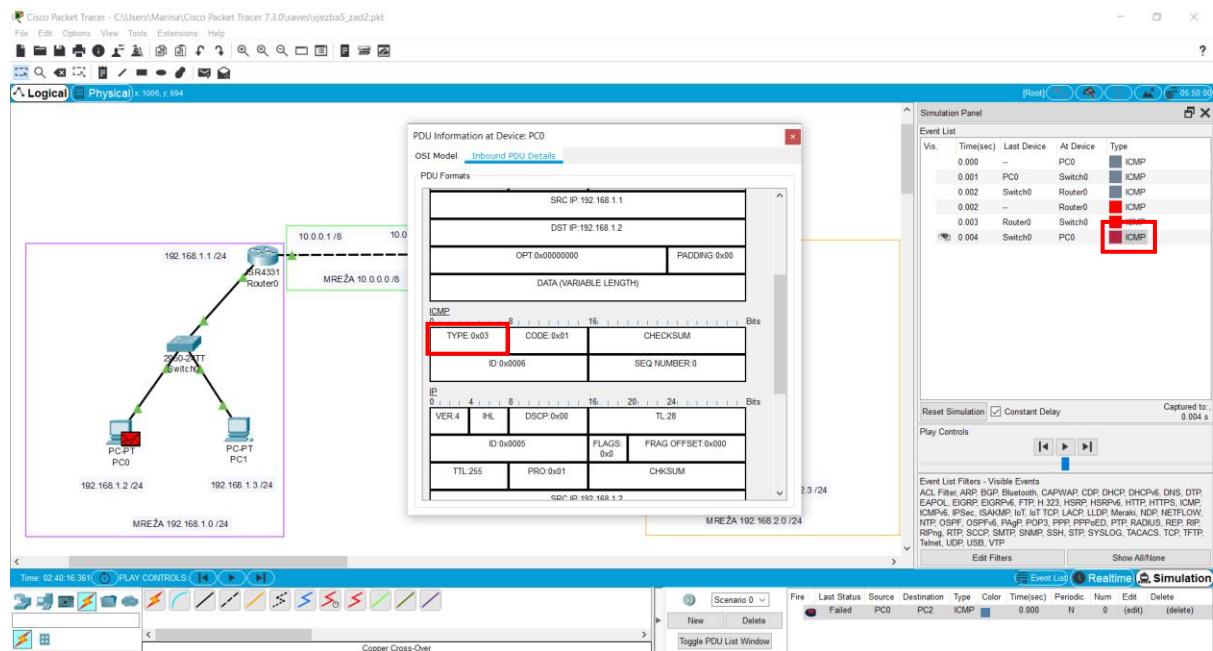
Pitanje 2.

Gdje nastaje prekid u vezi između mreže 192.168.1.0 i mreže 192.168.2.0.?

Prekid nastaje na uređaju router0, odnosno na default gateway-u od PC0 (slika dolje).



Naime, zadatak routera je na temelju IP adrese odredišta pronaći putanju do tog odredišta. Paket namijenjen nekom računalu mreže 192.168.2.0 koji polazi iz mreže 192.168.1.0 dolazi na router0 koji predstavlja default gateway. Router0 međutim nema podešenu tablicu usmjeravanja i ne može pronaći putanju do odredišta. Znači, on ne zna gdje treba proslijediti taj paket i zato dolazi do prekida veze. ICMP paket se vraća na PC0 kao tip poruke "Destination Unreachable", i to je kod 0x03 – odredište PC2 nije dostupno sa PC0.

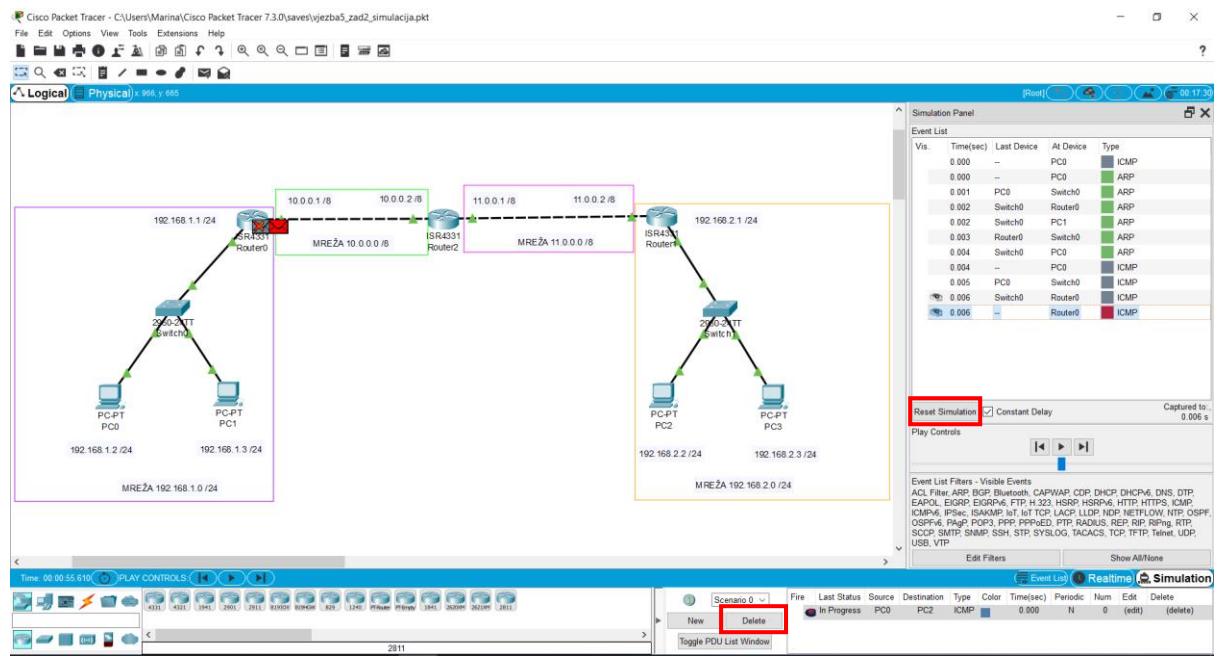


DINAMIČKO USMJERAVANJE (RIP PROTOKOL)

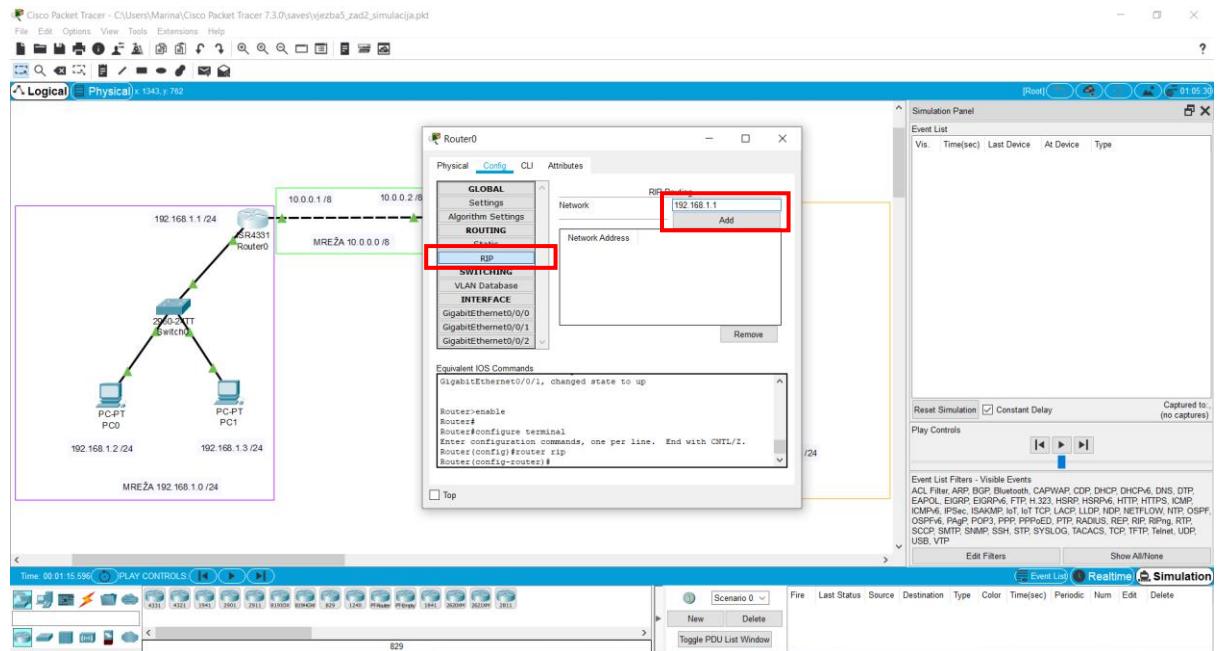
Kod dinamičkog usmjeravanja, ideja je da routeri sami pronađu adresu idućeg odredišta (next-hop) na kojeg će proslijediti paket (to je samo idući korak na putu do finalnog odredišta kojem je paket namijenjen). Znači, router će pronaći kojem susjedu treba proslijediti taj paket kako bi on došao (što prije) do svog finalnog odredišta. Za to se koriste tablice usmjeravanja i temelj za njihovo stvaranje kod RIP protokola su tzv. **RIP poruke**, na temelju kojih routeri pune svoje tablice i stvaraju sebi "sliku" ili "predodžbu" o tome kako izgleda mreža.

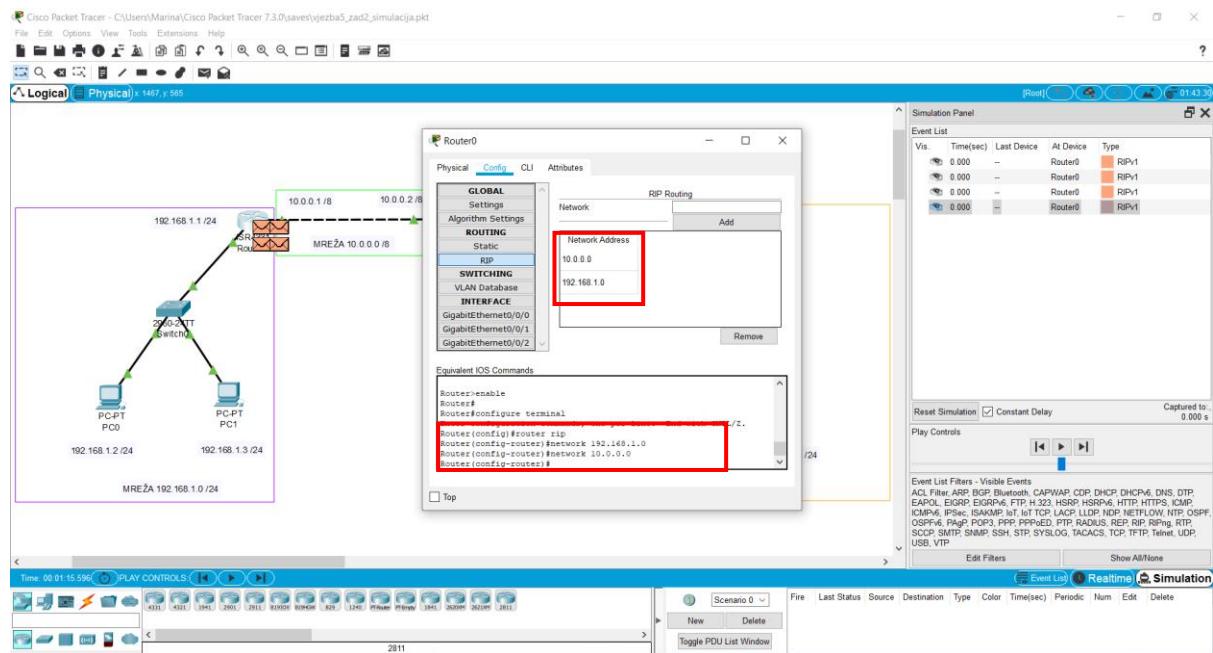
U drugom dijelu vježbe je potrebno obavezno biti u simulacijskom načinu rada, **kako biste mogli vidjeti RIP poruke u Packet Tracer-u**.

Resetirajte simulaciju iz prethodnog zadatka i izbrišite simulacijski scenarij pomoću opcije „Delete“:



Sada ćemo konfigurirati dinamičko usmjeravanje sa RIP protokolom. Kliknemo na lijevi router i u Config tabu odaberemo RIP. Potrebno je unijeti dvije adrese koje su njegove - prisjetimo se da na dva porta on ima adrese 192.168.1.1 i 10.0.0.1. Unosimo jednu po jednu i nakon svakog unosa odaberemo opciju „Add“. Obratite pažnju na ekvivalentne naredbe koje se pojavljuju u konzoli i služe za podešavanje RIP-a.

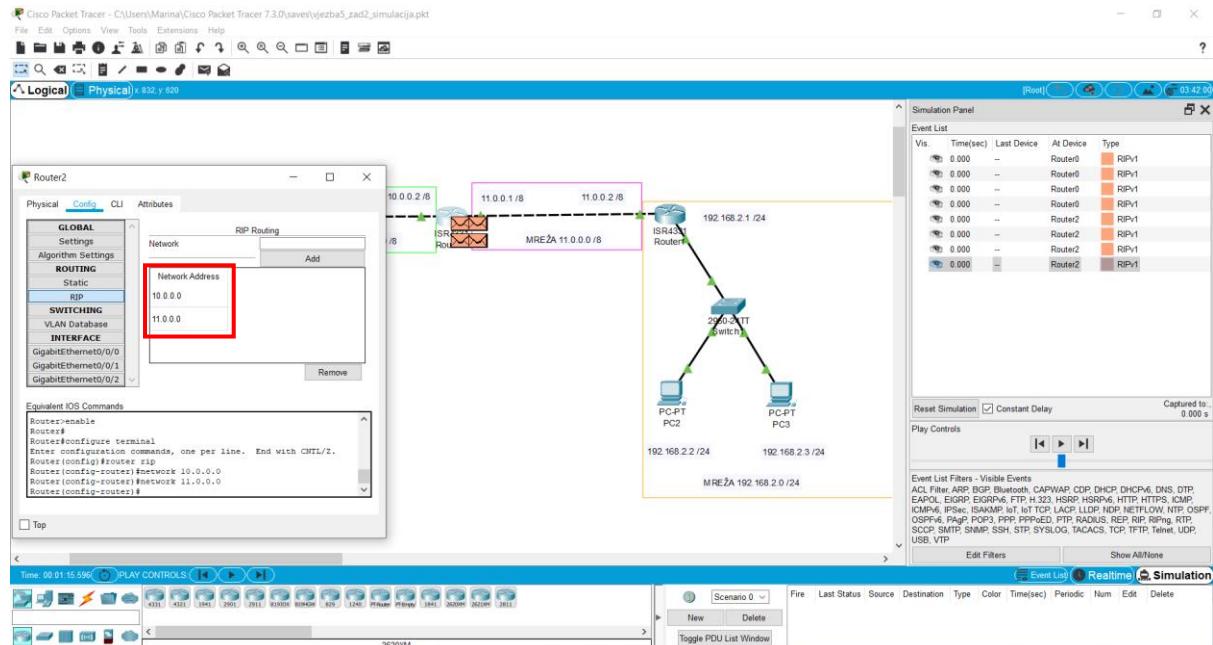


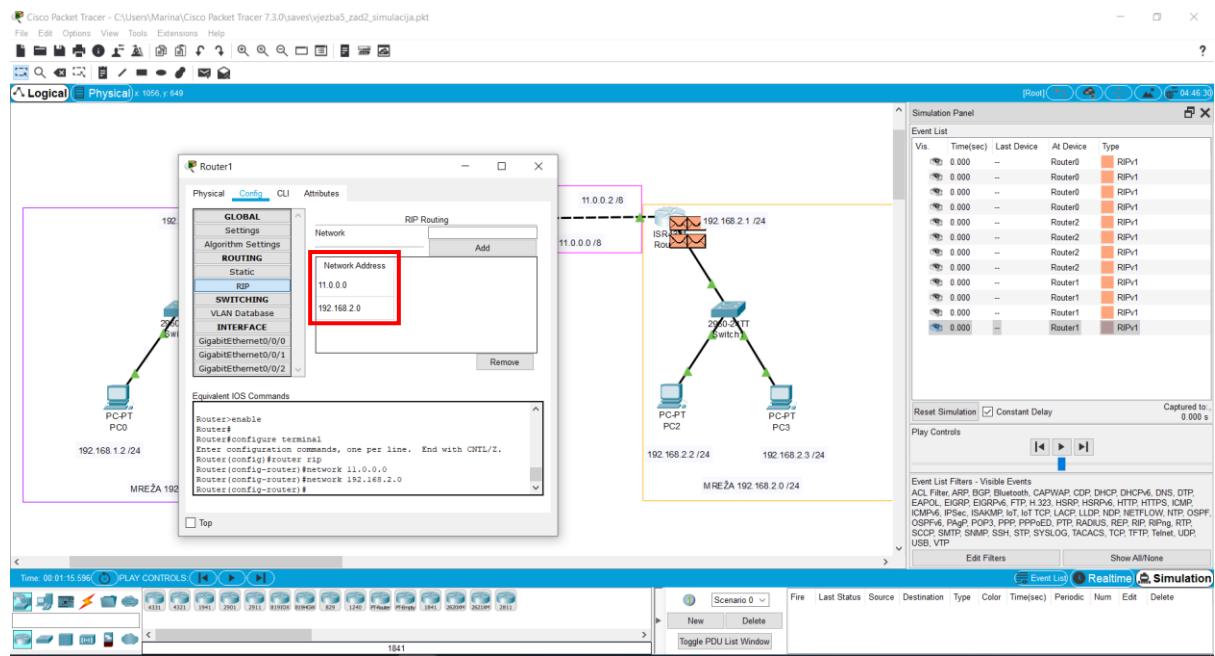


Primijetite kako će se automatski prilikom dodavanja pojedine adrese ona zapravo pretvoriti u adresu mreže. To je zato što, za razliku od statickog usmjeravanja, ovdje radimo dinamički pa ne trebamo zadati adresu idućeg koraka (next-hop), već je dovoljno zadati adresu mreže pa će router sam odrediti najbolju adresu idućeg koraka za proslijediti paket (na primjer na temelju drugih metrika kao što je udaljenost).

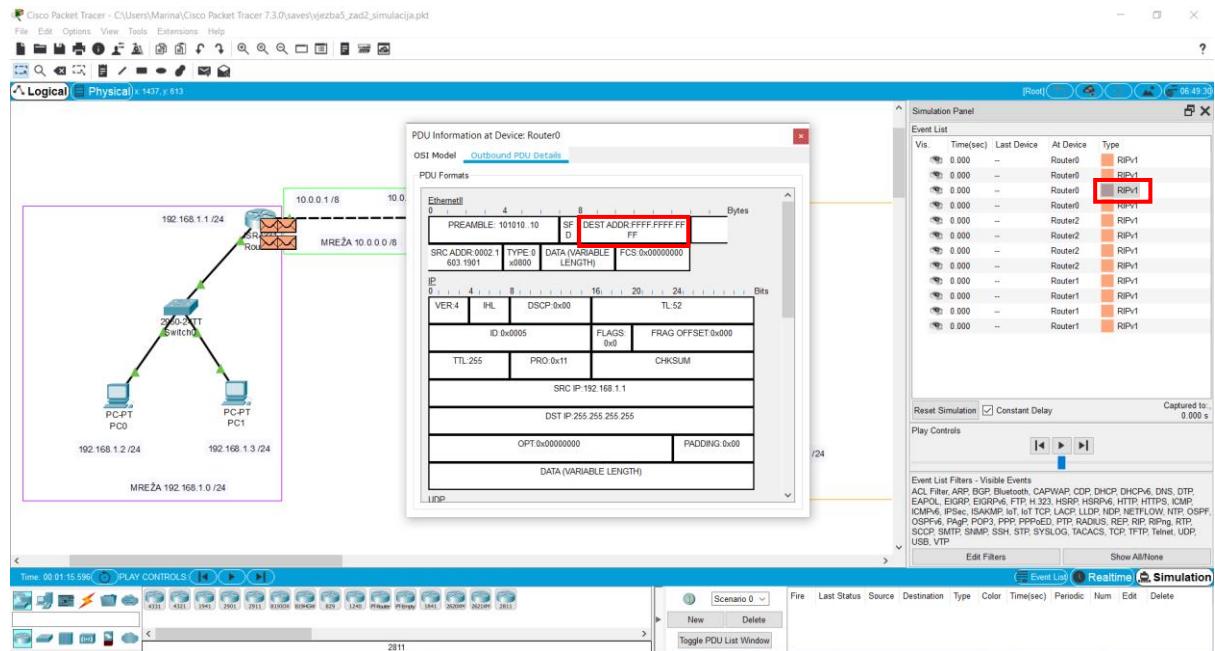
Također primijetite kako su se u Simulacijskom Panel-u već pojavile neke RIP poruke koje ćemo kasnije analizirati.

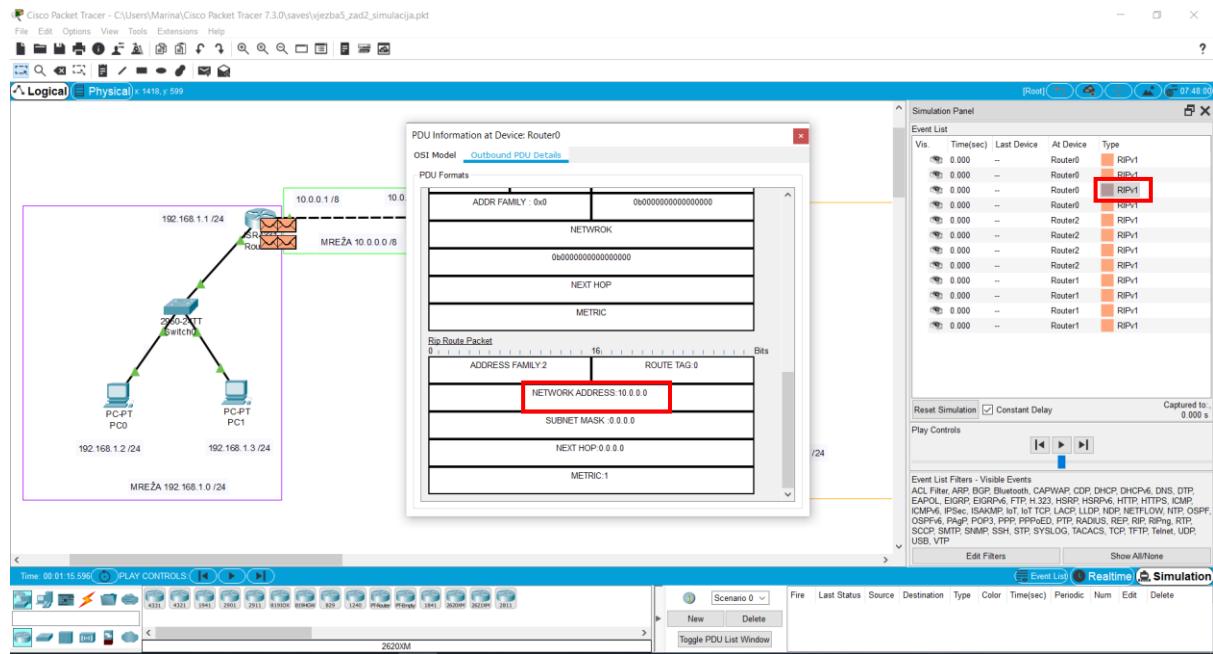
Za sada nastavimo dalje i unesemo adrese mreža na srednjem routeru koje on poznaje (to su 10.0.0.0 i 11.0.0.0), a zatim isto ponovimo za desni router i unesemo mreže koje su njemu dostupne (to su 11.0.0.0 i 192.168.2.0).





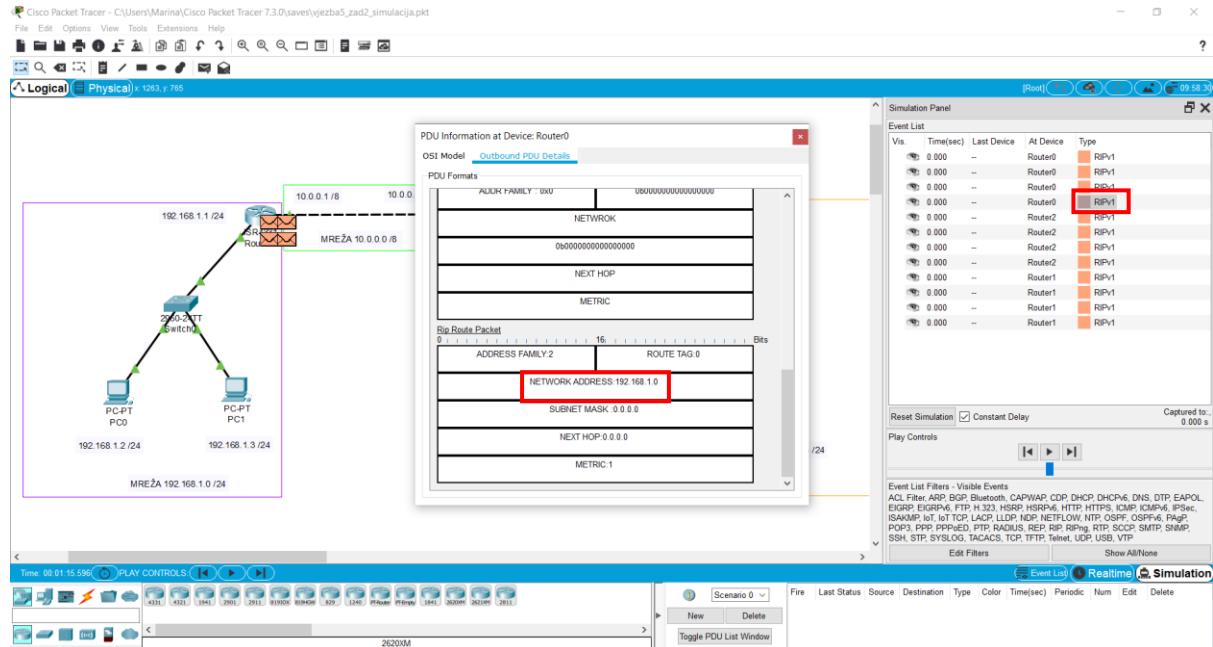
Analizirajmo sada RIP poruke koje su se pojavile u simulaciji u prvom koraku. To su poruke koje će razmjenjivati routeri i s kojima će se routeri javljati jedni drugima i govoriti na koje mreže su spojeni. Pogledajmo prvu RIP poruku koju je router0 pripremio za poslati svome susjedu (uređaju router2).



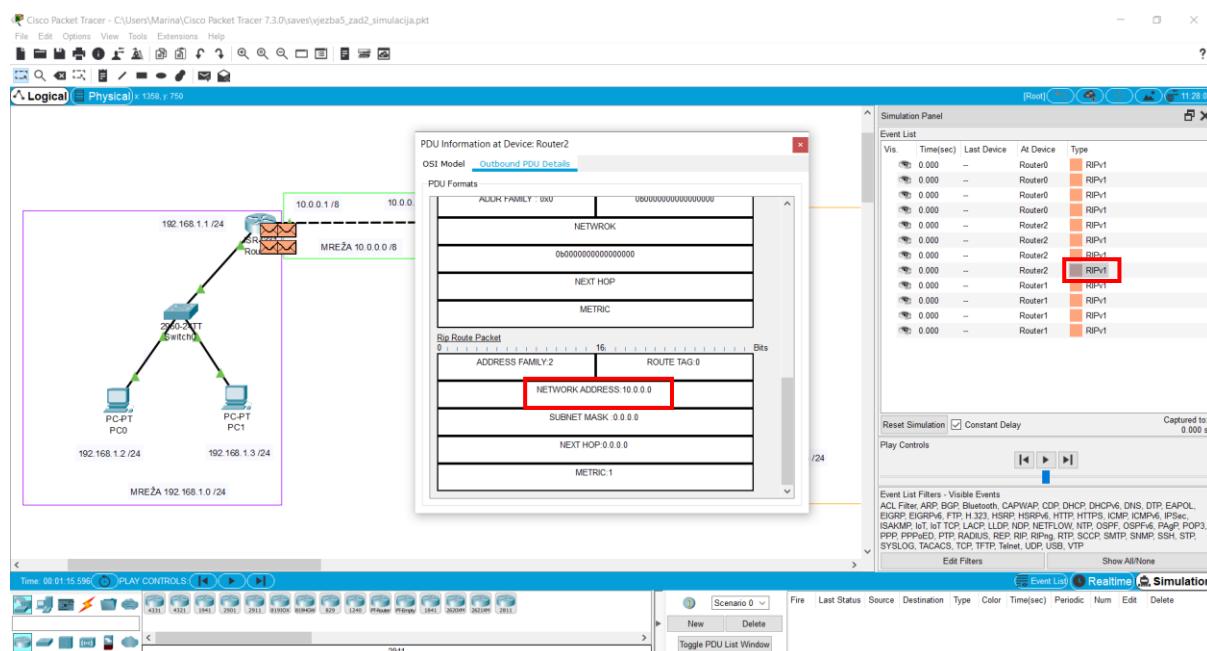
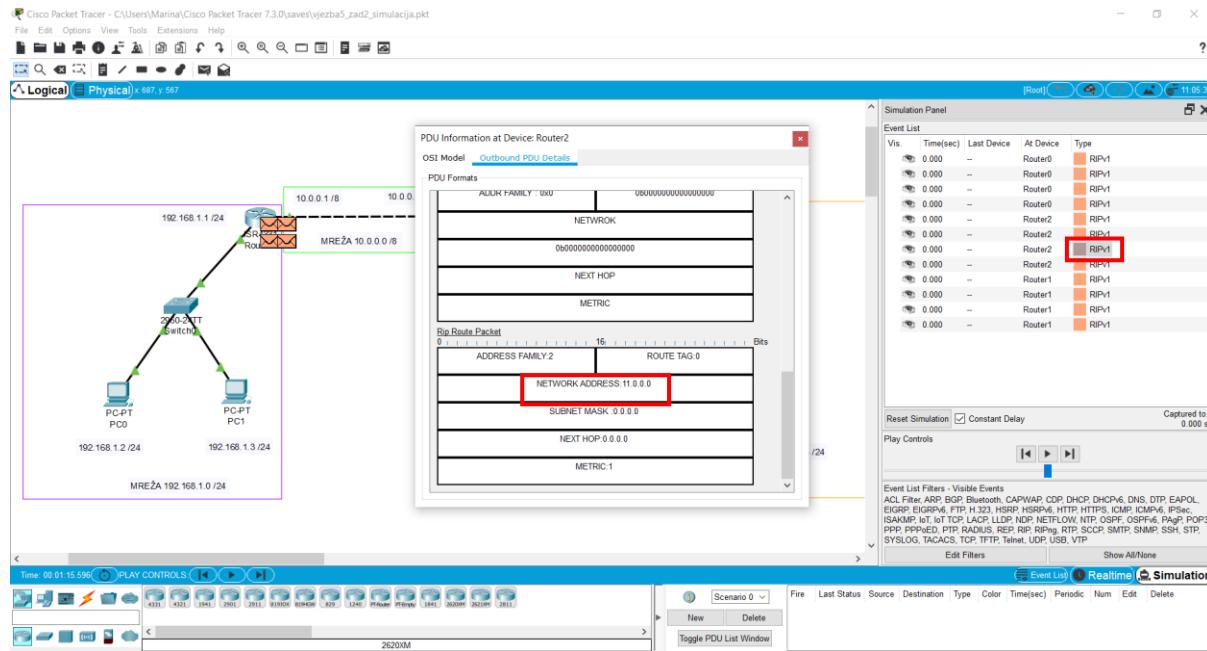


Primijetite kako se radi o porukama sa broadcast adresom zato što se one šalju svim susjedima. Dakle, router će svim svojim susjedima poslati na koje je mreže on spojen, a onda će taj susjed javiti svojim susjedima na koje mreže je on spojen (u prvom koraku), zatim na koje mreže je spojen njegov susjed (u nekom od narednih koraka RIP protokola) i tako routeri grade „sliku“ mreže.

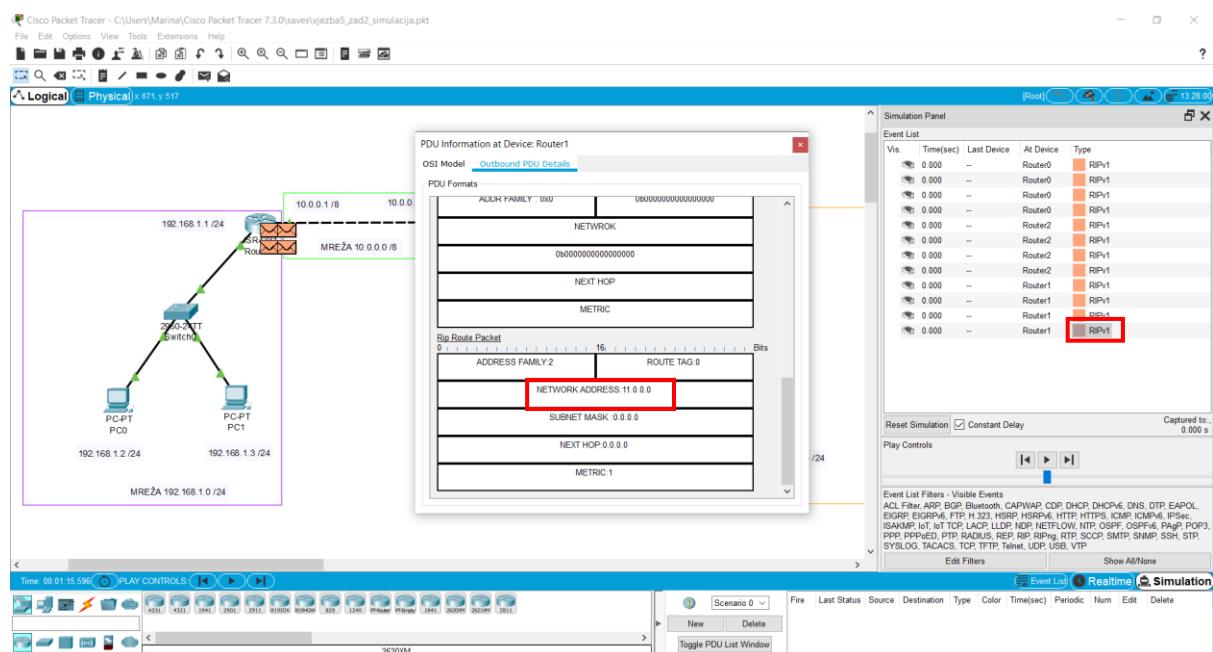
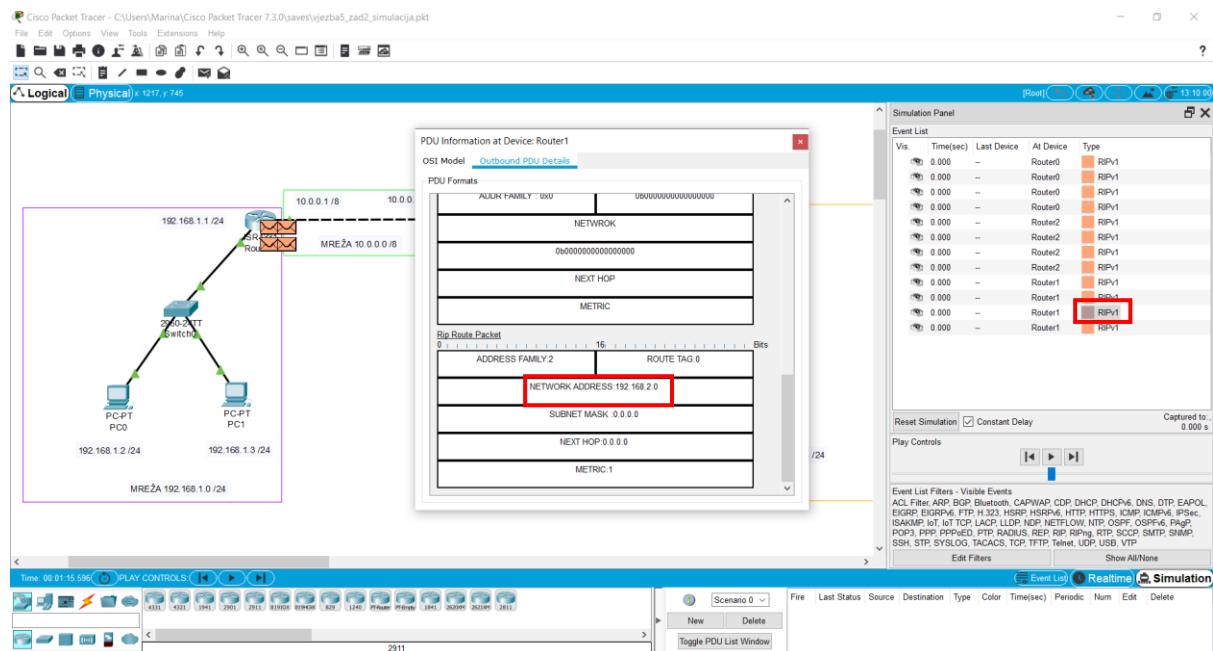
Na gornjoj slici vidimo da je router0 pripremio poruku u kojoj javlja svome susjedu routeru2 da je spojen na mrežu 10.0.0.0 i da je ona od njega (od routera2) udaljena za 1 hop (polje metric = 1). Otvorimo iduću poruku koju je pripremio router0 - da je spojen na mrežu 192.168.1.0 i da je ona također od susjeda udaljena 1 hop:



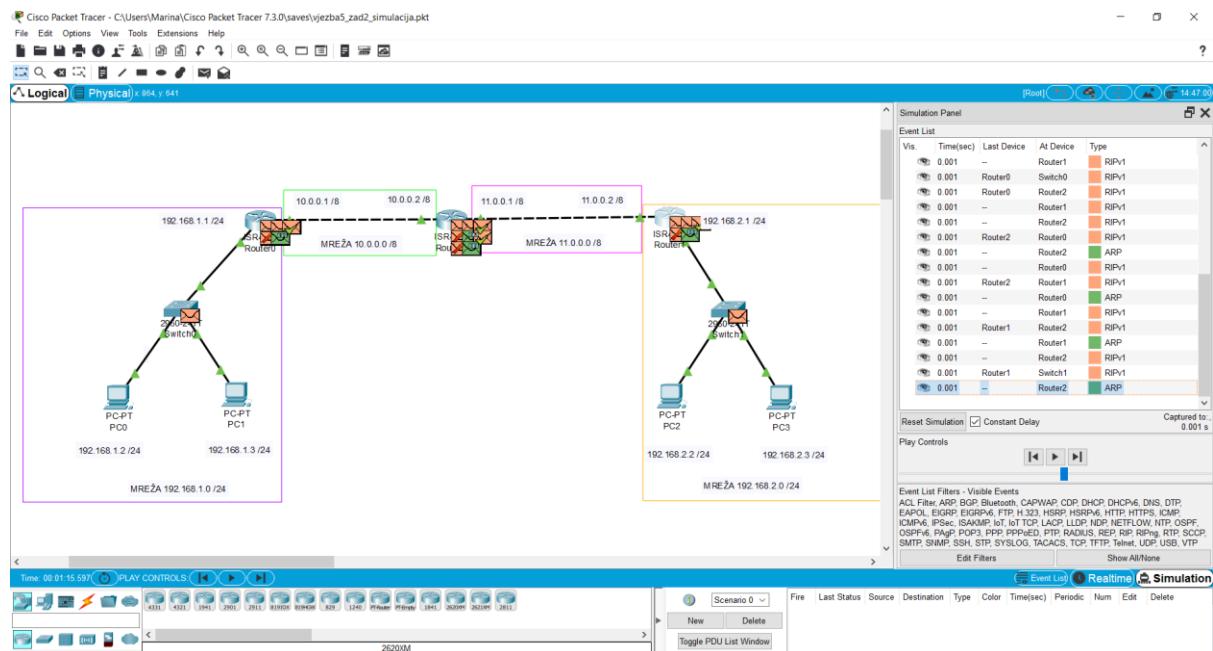
Pogledajmo RIP poruke koje je pripremio router2 kako bi dojavio na koje mreže je on spojen:



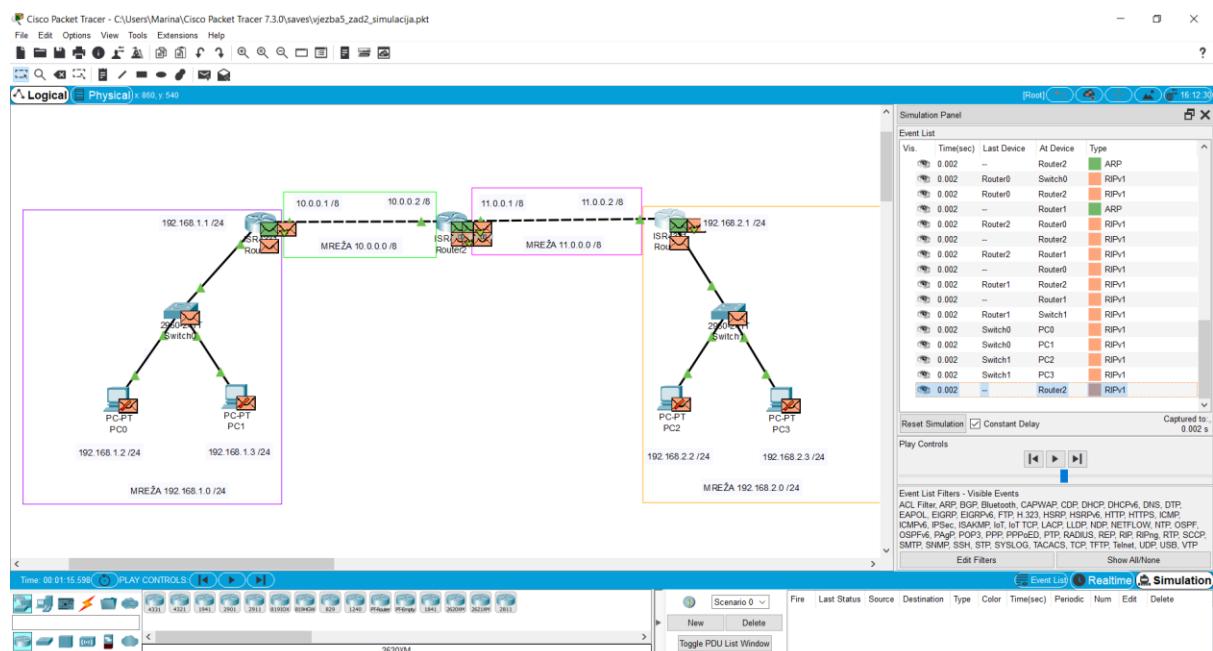
Pogledajmo RIP poruke koje je pripremio router1 kako bi dojavio na koje mreže je on spojen:



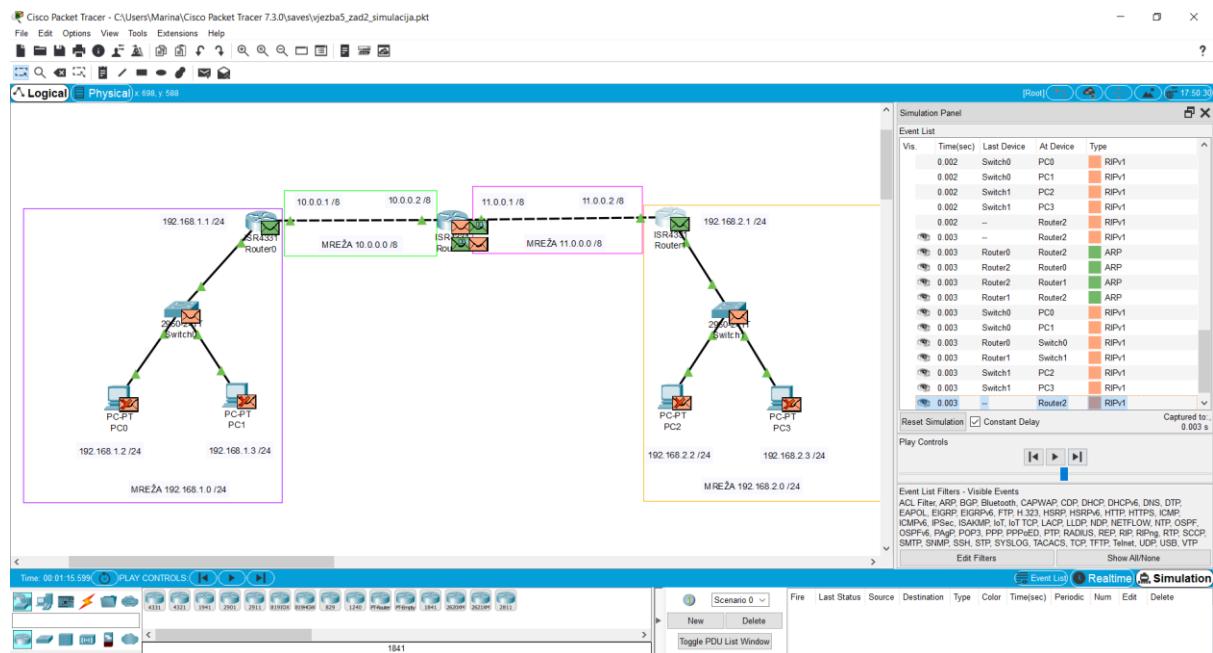
Pokrenite sada idući korak simulacije na Capture Forward i stvorite se situacija kao na slici:



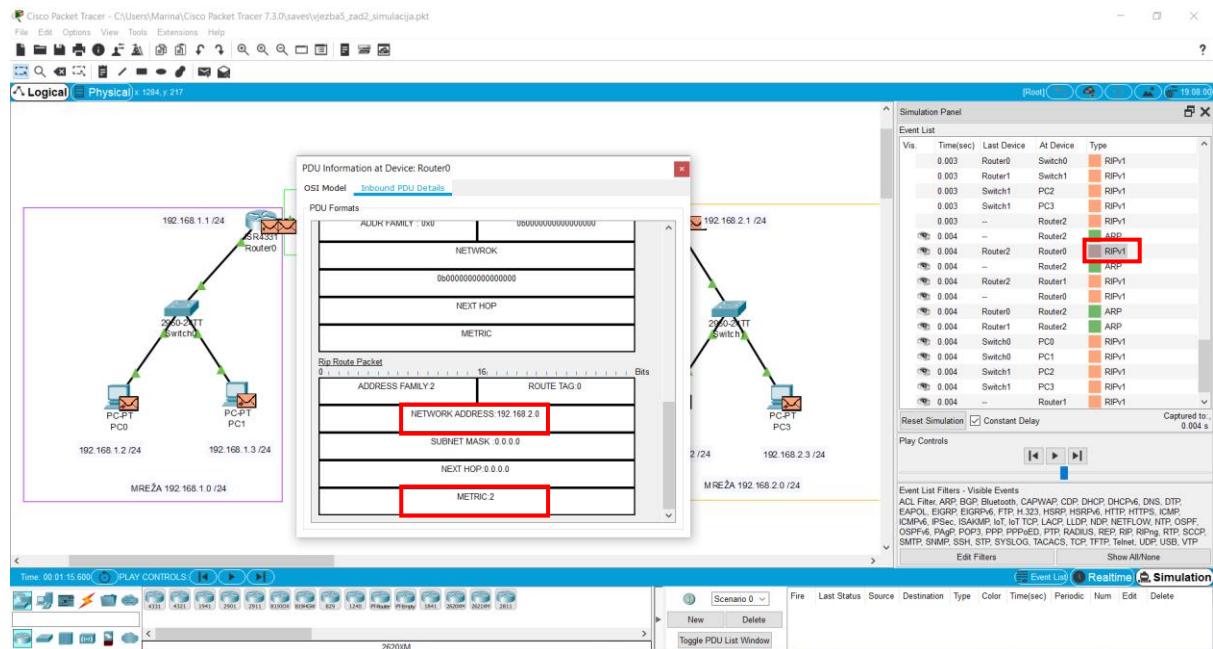
Routeri sada razmjenjuju RIP poruke, ali i svoje MAC adrese uz pomoć ARP protokola. Pokrenite idući korak simulacije sa Capture Forward i nastavlja se razmjena RIP poruka. Zapravo se šalju one poruke koje smo prethodno gledali kao "pripremljene za slanje" koje govore o mrežama na koje su ruteri direktno spojeni (metric je 1 hop). **Otvorite svaku poruku i pogledajte koji router i što točno javlja svome susjedu.**



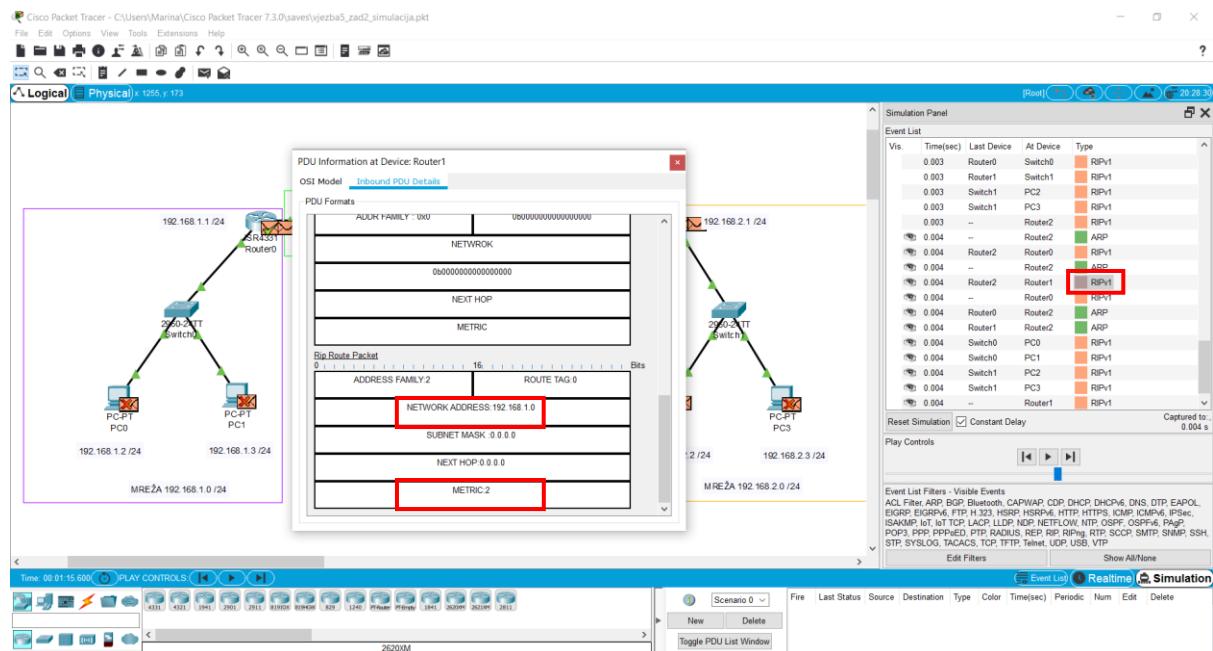
Pokrenite idući korak simulacije sa Capture Forward:



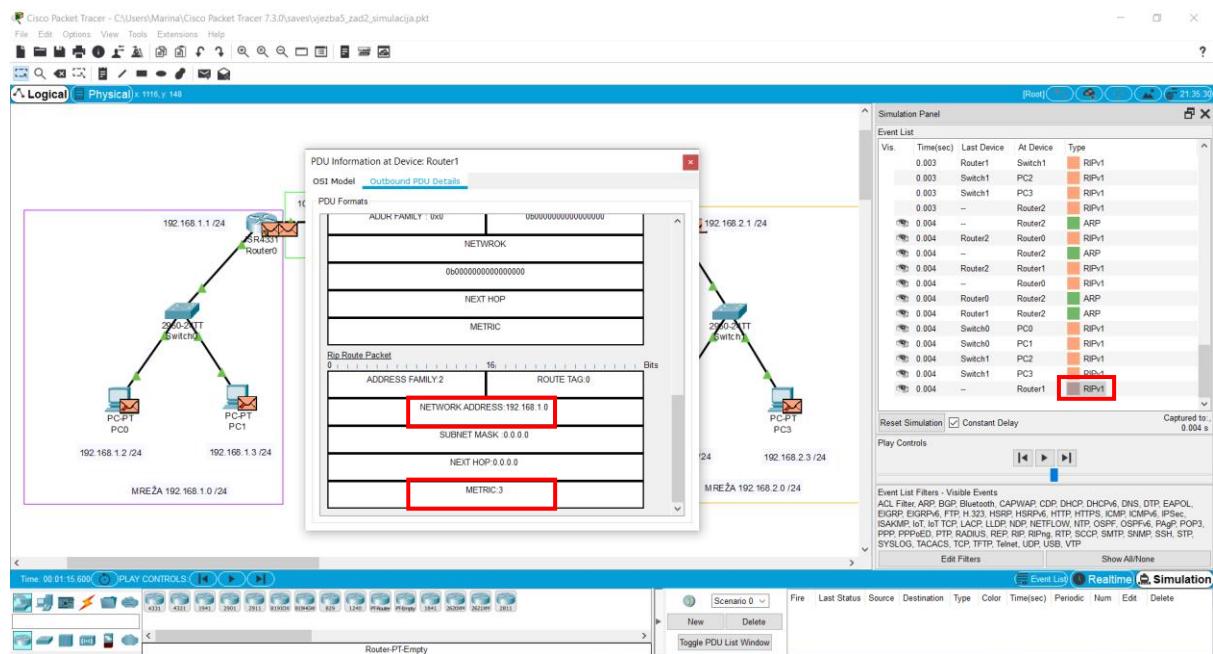
Odaberite idući korak simulacije sa Capture Forward da se dovrši ARP razmjena i pogledajte kako sada router2 javlja routeru0 da je i on spojen na mrežu 192.168.2.0 (iako ne direktno, nego preko routera1), znači ova poruka je složena na temelju poruke koju je router2 prethodno dobio od routera1. Vidimo da je u polju metric sada udaljenost postavljena na 2 koraka (2 hops), zato što router2 želi reći routeru0 da vidi tu mrežu, ali da je ona od njega (od routera0) udaljena 2 koraka.



Analogno, router2 javlja routeru1 da on vidi i mrežu 192.168.1.0 (jer je to doznao od routera0), ali opet ne direktno nego na udaljenosti od 2 koraka:

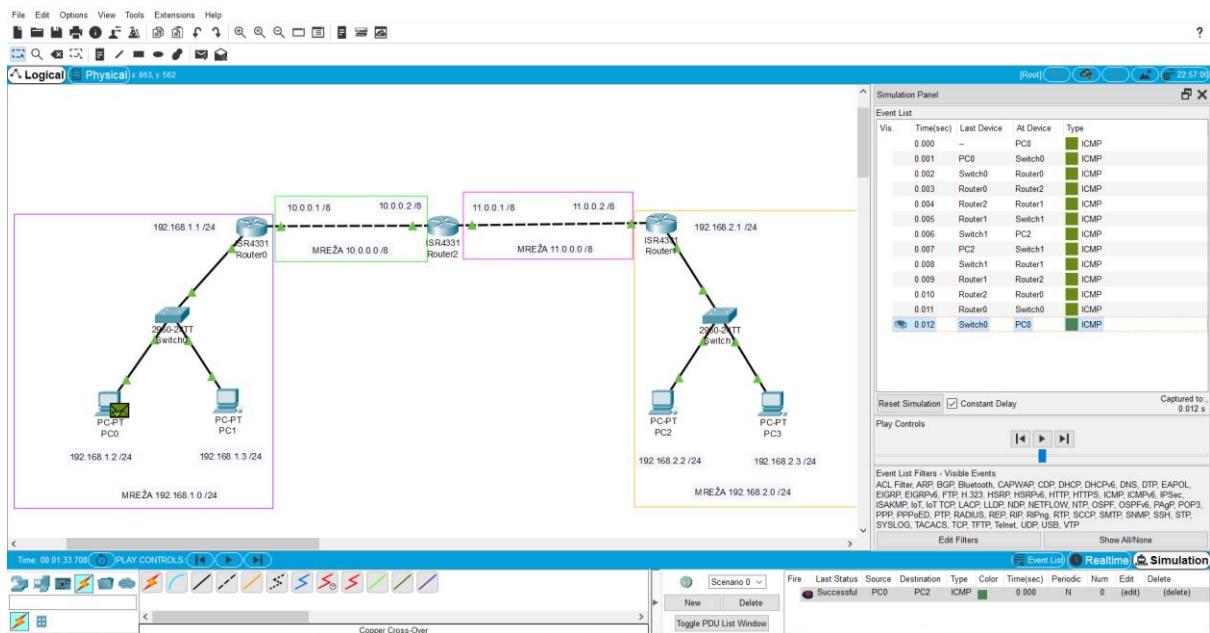


Pogledajte poruku koju je pripremio router1 – da vidi mrežu 192.168.1.0 ali na udaljenosti 3 koraka preko svojih susjeda. Ova metrika će se inače koristiti za izračun najboljeg puta kojim će se paket slati na odredište.



Na kraju razmjene RIP poruka routeri znaju kako izgleda mreža.

Resetirajmo simulaciju i ponovimo ping od PC0 do PC2 u simulacijskom načinu rada. Pogledajte kako ping sada prolazi i komunikacija od PC0 do PC2 je sada uspješna.



Spremite Packet Tracer topologiju pod nazivom **ime_prezime_zadatak3.pkt**.

RAZLIKA STATIČKOG I DINAMIČKOG USMJERAVANJA

U prethodnom primjeru smo prikazali dinamičko usmjerenje i pokazali smo kako svaki router kontinuirano uči o stanju mreže na temelju komuniciranja sa svojim susjedima. Promjene u mrežnoj topologiji se tako prenose kroz sve routere. Na osnovu raspoložive informacije, svaki router može odrediti najbolji put prema željenoj destinaciji [20].

Kod statičkog usmjerenja je razlika što se na temelju topologije mreže izračunavaju putanje za usmjerenje koje se zatim, uglavnom ručno, unose u tablice usmjerenja i ostaju fiksne za relativno dug vremenski period. Kod statičkog usmjerenja bismo morali ručno unijeti putanje paketa korak po korak i u slučaju da se neka veza prekine, potrebno je ručno ažurirati tablice usmjerenja. S druge strane, kod dinamičkog usmjerenja će routeri naučiti novi izgled mreže i pronaćiće alternativni put paketa do odredišta.

Glavna prednost statičkog usmjerenja je jednostavnost, dok mu je glavni nedostatak nefleksibilnost. Zato se statičko usmjerenje češće koristi kod manjih mreža, a za veće mreže je bolje koristiti dinamičko usmjerenje kako bi mreža mogla sama izaći na kraj s problemima.

ZADACI ZA VJEŽBU 4 (PREDAJA IZVJEŠTAJA):

Napraviti sve simulacije u alatu Packet Tracer kako je pokazano na vježbi i predati konfiguracije pod nazivom:

- **ime_prezime_zadatak1.pkt**
- **ime_prezime_zadatak2.pkt**
- **ime_prezime_zadatak3.pkt**.

VJEŽBA 5: TCP/IP WIRESHARK

CILJ VJEŽBE

Prijenosna razina TCP/IP skupa protokola koristi usluge IP razine za realizaciju protokola prijenosne razine. Dva najčešća protokola u upotrebi su TCP i UDP, a u okviru ove vježbe ćemo se koncentrirati na detalje TCP protokola. Na ovoj vježbi nećemo koristiti alat Packet Tracer nego alat za praćenje paketa koji se zove Wireshark.

Vježba je prilagođena sa [21], [22] i temelji se na knjizi „Computer Networking: A Top-Down Approach“ (J.F Kurose and K.W. Ross) [23].

Vježba se sastoji od dva dijela:

- Generiranje datoteke sa tragovima paketa (eng. packet traces) koji su poslati u TCP prijenosu od računala do servera (.pcap file koji se dobije u Wiresharku)
- Analiza .pcap datoteke

U vježbi ćemo analizirati tragove (eng. traces) TCP segmenata poslanih i primljenih u prijenosu .txt datoteke „alice.txt“ (koja sadrži tekst Alise u zemlji čudesa Lewisa Carrola) s vašeg računala na server. Proučit ćemo korištenje TCP-ovih rednih brojeva paketa (eng. sequence numbers) i primljenih potvrda (eng. acknowledgement numbers) za pružanje pouzdanog prijenosa podataka. Također ćemo ukratko razmotriti uspostavljanje TCP veze (three-way handshake).

TEORIJSKI PREDUVJETI

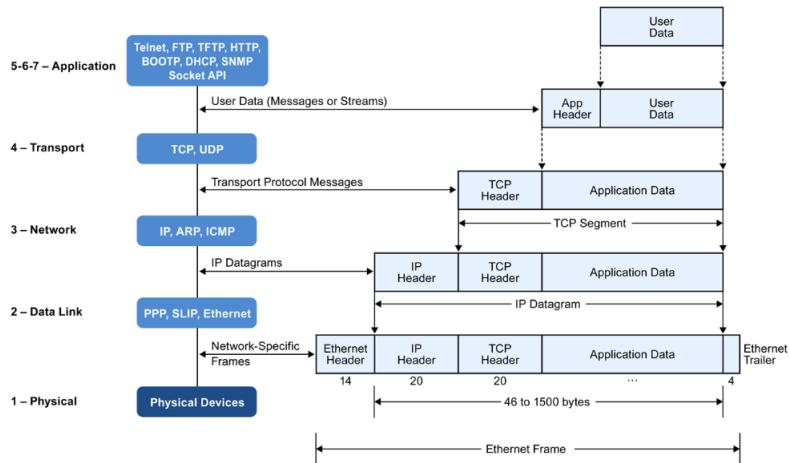
Teorijski dijelovi vježbe preuzeti su sa [5].

TCP PROTOKOL

TCP (Transmission Control Protocol) je spojevni protokol koji omogućuje pouzdanu komunikaciju Internet aplikacija korištenjem nepouzdanog (best-effort) IP protokola. TCP procesi na dva računala u Internet mreži komuniciraju razmjenom **segmenata**. Računalo koje šalje segment podataka formira segment određene veličine i prosljeđuje ga IP razini koji ga eventualno razdijeli na više IP **datagrama** i šalje ga odredištu. TCP proces na prijemnom računalu ima zadatak formirati originalni **segment** od jednog ili više primljenih IP **datagrama** i proslijediti ga aplikaciji.

Na idućoj slici je prikazana enkapsulacija podataka u TCP/IP mrežnom modelu kojeg nazivamo **TCP/IP network stack**. On sadrži više slojeva, uključujući aplikacijski sloj, transportni sloj, mrežni sloj i sloj veze podataka [24].

Aplikacijski sloj uključuje protokole koje koristi većina aplikacija za pružanje korisničkih usluga. Primjeri protokola aplikacijskog sloja su Hypertext Transfer Protocol (HTTP), Secure Shell (SSH), File Transfer Protocol (FTP) i Simple Mail Transfer Protocol (SMTP).



Transportni sloj uspostavlja povezanost između procesa te uvodi koncept porta. Primjeri protokola transportnog sloja su Transport Control Protocol (TCP) i User Datagram Protocol (UDP). TCP omogućuje kontrolu protoka, uspostavljanje veze i pouzdan prijenos podataka, dok je UDP model prijenosa bez uspostavljanja veze.

Mrežni sloj odgovoran je za slanje paketa preko različitih mreža. Ima dvije funkcije:

- 1) identifikacija uređaja pomoću sustava IP adresiranja (IPv4 i IPv6);
- 2) usmjeravanje paketa od izvora do odredišta na temelju IP adrese odredišta

Primjeri protokola mrežnog sloja su Internet Protocol (IP), Internet Control Message Protocol (ICMP) i Protocol Resolution Protocol (ARP).

Podatkovni sloj (naziva se još i sloj veze podataka, i sloj veze ili sloj pristupa mreži) definira metode umrežavanja na razini lokalne mreže. Koristi se za slanje paketa između dva hosta na istom linku. Uobičajeni primjer protokola ovog sloja je Ethernet.

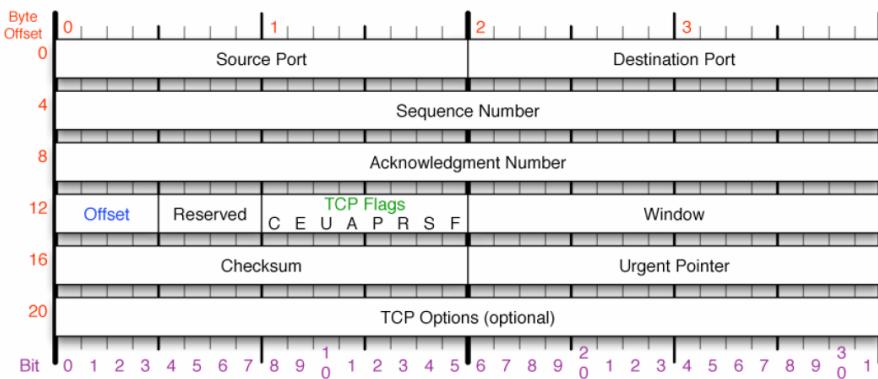
TCP veza između dva računala na Internetu uspostavlja se korištenjem krajnjih točaka na oba računala. Ove krajnje točke nazivamo **priklučnicama** (socket). Svaka priključnica jedinstveno je određena IP adresom računala i priključnom točkom (port). Priklučna točka identificira proces koji šalje ili prima podatke. Drugim riječima, port je adresa protokola aplikacijske razine za kojeg prijenosna razina prenosi podatke. Veza je jedinstveno određena parom priključnica

$$\text{IP_adresa_A} + \text{port_A} \leftrightarrow \text{IP_adresa_B} + \text{port_B}$$

Ukoliko s osobnog računala A otvorimo dvije veze prema istoj aplikaciji na istom serveru B (npr. prema http serveru Wikipedije), te dvije veze imat će različiti par priključnica. U oba slučaja će IP adresa servera i port na serveru biti isti, kao i IP adresa osobnog računala, ali te dvije veze imat će različite portove na strani računala:

$$\begin{aligned} \text{veza 1: } & \text{IP_adresa_PC} + \text{port_49321} \leftrightarrow \text{IP_adresa_wiki} + \text{port_80} \\ \text{veza 2: } & \text{IP_adresa_PC} + \text{port_50229} \leftrightarrow \text{IP_adresa_wiki} + \text{port_80} \end{aligned}$$

Na idućoj slici je prikazano TCP zaglavljje:



Polja **Source port** i **Destination Port** u TCP zaglavljiju su duljine 16 bita, dakle omogućuju 65k vrijednosti. Kao što je već rečeno, portovi služe za adresiranje protokola aplikacijske razine za kojega prijenosna razina (tj. TCP ili UDP) prenosi podatke.

Portovi 0-1023 su staticki (well-known) i pridruženi su najčešćim Internet uslugama; portovi 1024-49151 su registrirani (registered), a 49151-65535 su dinamički/privatni portovi.

Uzmimo za primjer WEB (HTTP) preglednik: operacijski sustav klijentskoj aplikaciji (web browseru) dodjeljuje dinamičku priključnu točku, koja zajedno s IP adresom klijenta određuje klijentovu priključnicu. DNS uslugom određuje se IP adresa poslužitelja iz dane web adrese (<http://www...>). Vrijednost priključne točke na poslužitelju (adresa procesa aplikacijske razine kojemu želimo pristupiti, u ovom primjeru http serverski proces) se zna jer serveri koriste staticke portove za najčešće korištene procese (port 80 za http). Time je određena i priključnica na strani poslužitelja. Dakle, u TCP zaglavljima segmenata koje klijent šalje poslužitelju nalazi se vrijednost Destination Port 80, a Source Port vrijednost dodijelio je operacijski sustav (dinamički port).

Primjeri portova za često korištene usluge su:

Port	Protokol	Usluga
21	FTP	Prijenos datoteka
22	SSH	Razmjenu podataka preko "sigurnog kanala"
23	Telnet	Rad na udaljenom računalu
25	SMTP	e-mail
80	HTTP	World Wide Web
110	POP3	udaljeni e-mail pristup

Polje **Sequence Number** (SEQ) označava poziciju segmenta u originalnom bloku podataka, a **Acknowledgement Number** (ACK) se koristi za potvrdu ispravnog prijema paketa u suprotnom smjeru. Ukoliko računalo 1 šalje računalu 2 segment od 100 bajta podataka sa SEQ = 0 (dakle, radi se o početnih 100 bajta podataka), računalo 2 će odgovoriti s ACK = 101, odnosno potvrđuje ispravan prijem segmenta s prvih 100 bajta podataka i očekuje od računala da slijedeći segment sadrži podatke od 101 bajta nadalje. Ako se pozitivna potvrda ne primi do isteka vremena retransmisije, podatak se automatski ponovo šalje.

Sequence number i Acknowledgement Number polja TCP-u omogućuju:

- detekciju i oporavak od gubitka u prijenosu,
- da ispravno poreda segmente kod poruka koje se prenose u više IP datagrama i mogu stići do odredišta redoslijedom različitim od redoslijeda kod slanja,
- eliminiranje duplicitarnih segmenata (koji nastaju kao posljedica Flooding algoritma usmjeravanja na nekoj od mreža preko kojih IP datagram prođe).

Polje **TCP flags** sadrži podatke o vrsti i sadržaju segmenta. Polje se sastoji od 8 zastavica (flag) - bitova koji kada su postavljeni u jedinicu označavaju:

- URG paket sadrži hitnu poruku, a polje Urgent Pointer pokazuje na kraj hitnih podataka
- ACK segment nosi potvrdu čiji se broj nalazi u polju Acknowledgement Number
- PSH predajnik zahtijeva trenutnu isporuku pristiglih podataka na prijemnoj strani
- RST resetiranje veze
- SYN sinkronizacija Sequence Number polja
- FIN pošiljatelj nema više podataka za slanje

Najčešće se TCP segment formira od 1460 bajta podataka kako bi stao unutar jednog Ethernet okvira standardne veličine 1500 bajta. 40 bajta razlike čine TCP i IP zaglavlj. Slanje manjih količina podatka moguće je postavljanjem URG (Urgent) bita. Veličina bloka podataka koji se šalje definirana je **Urgent Pointer** poljem.

TCP omogućava prijemniku upravljanje količinom podataka koje smije odaslati predajnik. Poljem **Window**, koje služi za kontrolu toka, određuje se količina podataka koju prijemnik može primiti bez gubitaka. Sa svakom potvrdom (ACK), prijemnik šalje i veličinu prozora (RWIN, receiver window). Najveći prozor je 65536 okteta (polje ima 16 bita).

Uspostava TCP veze zahtijeva razmjenu ukupno tri paketa između računala koja komuniciraju (**three way handshake**). Obično ovaj postupak pokreće jedno računalo, dok drugo odgovara na njega:

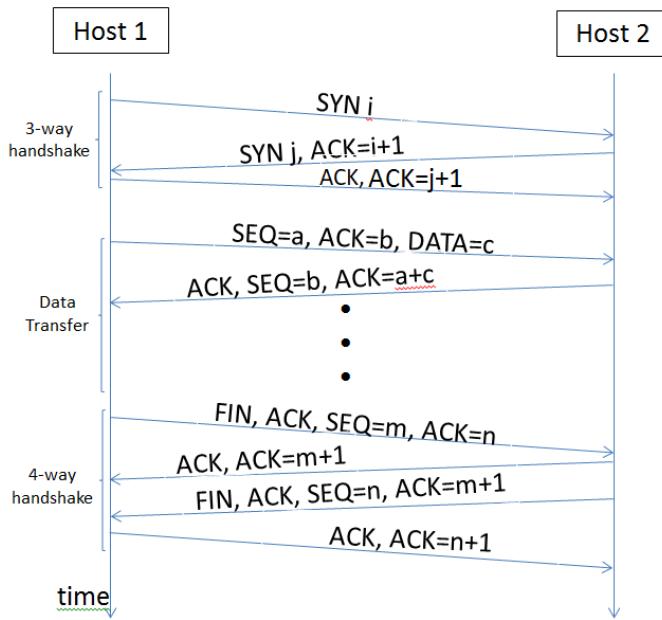
Računalo 1 koje inicira vezu šalje segment podataka sa postavljenim SYN bitom (zastavicom) i određenom vrijednošću SEQ=x polja.

- Računalo 2 odgovara slanjem segmenta s postavljenim SYN i ACK bitom, vlastitom vrijednošću SEQ = y i potvrdom prijema prethodnog segmenta ACK = x+1.
- Računalo 1 odgovara slanjem segmenta sa SEQ = x+1, i potvrđuje prijem prethodnog segmenta postavljenim ACK = y+1.

Nakon uspostave veze klijent i poslužitelj mogu razmjenjivati podatke, pri čemu obje strane i šalju i primaju podatke.

Po završetku slanja podataka, TCP veza se raskida razmjenom 3 ili 4 segmenta (slika dolje). Strana koja želi prekinuti vezu šalje segment s postavljenom FIN zastavicom. Uobičajena je situacija da klijent želi prekinuti vezu, a kasnije i poslužitelj prekida vezu. Nakon zatvaranja klijentske strane poslužitelj i dalje može slati podatke. U trenutku kada i poslužitelj želi zatvoriti vezu ponavlja istovjetan postupak, tj. šalje segment s postavljenom FIN zastavicom.

Uspostava, prijenos podataka i prekid veze TCP protokola prikazana je slikom koja je prilagođena sa [25]:



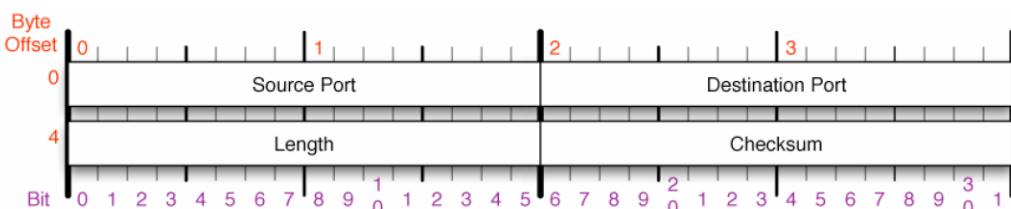
Poslužitelj (npr. HTTP poslužitelj) najčešće prihvata više klijenata odjednom. U tom slučaju pojedine klijente poslužitelj razlikuje po (IP adresi i) polju Source Port, čiju vrijednost na klijentskoj strani dodjeljuje operacijski sustav među vrijednostima >1023 (dinamičke priključne točke).

UDP PROTOKOL

UDP (User Datagram Protocol) je bespojni protokol, dakle omogućava slanje podataka bez uspostave logičke veze između dva računala koja komuniciraju i ne obavlja ispravak pogreški retransmisijom. Stoga se koristi za usluge kod kojih je bitnija jednostavnost rukovanja i brzina, od pouzdanosti prijenosa (npr. audio-video prijenos).

Također, UDP se koristi za prijenos podataka onih aplikacija kod kojih su svi podaci koji se šalju toliko mali da stanu u jedan UDP datagram koji se prenese jednim IP paketom, pa se za tako kratku komunikaciju ne isplati prolaziti cijelu proceduru uspostave i raskida veze koja bi bila potrebna da se podaci prenose preko TCP-a. Kod ovakvih kratkih poruka često je slučaj da pošiljatelj te podatke šalje periodički (npr. svakih 30 s), pa ako neka poruka i ne stigne do odredišta, sljedeće poruke će stići. Također, slanje kratkih poruka UDP-om koriste i aplikacije koje očekuju odgovor na takvu poruku (npr. DNS upiti), pa pošiljateljska aplikacija na temelju izostanka odgovora može sama zaključiti da se poslani upit treba retransmitirati (dakle, ovako se nadoknadi to što UDP ne obavlja retransmisijske prijenosnoj razini).

UDP zaglavljue duljine je 8 bajta i osim polja za izvorišni i odredišni port ima još samo polje duljine i zaštitne sume.



RAZVOJ KONTROLE TOKA TCP PROTOKOLA

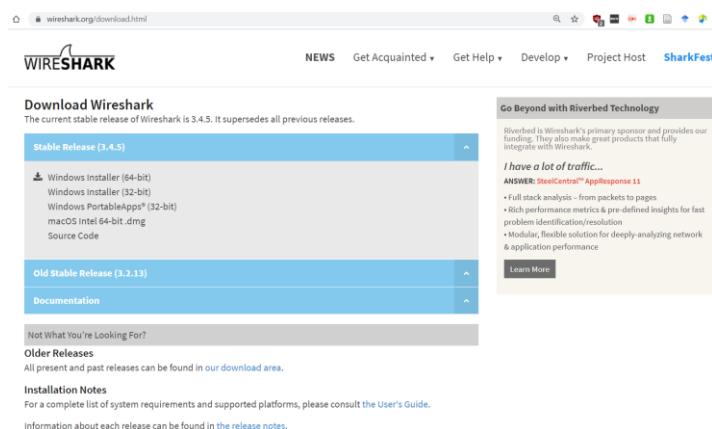
U stanju uspostavljene veze prijenos podataka se obavlja razmjenom podatkovnih segmenata. Usljed greške ili zagušenja na mreži može doći do gubitka segmenta. Stoga TCP koristi mehanizam **retransmisijske** kako bi osigurao dostavu svakog segmenta. Potvrde su kumulativne, što znači da potvrda x-tog okteta podrazumijeva i potvrdu svih prethodnih.

Ako u određenom vremenu (**RTO, Retransmission Timeout**) ne dobije potvrdu za poslani segment, TCP ponovno šalje taj segment, računajući da je izgubljen. Zbog raznolikosti mreža u sustavu i širokog raspona uporabe TCP veza, ovo vrijeme se računa dinamički. Kvalitetan proračun tog vremena od ključnog je značenja za učinkovitost TCP veze. Proračuni se zasnivaju na vremenu potrebnom da stigne potvrda za odaslan paket. To se vrijeme naziva vrijeme obilaska (**RTT, Round Trip Time**). RTT se stalno mijenja i ovisi o trenutnoj opterećenosti mreže.

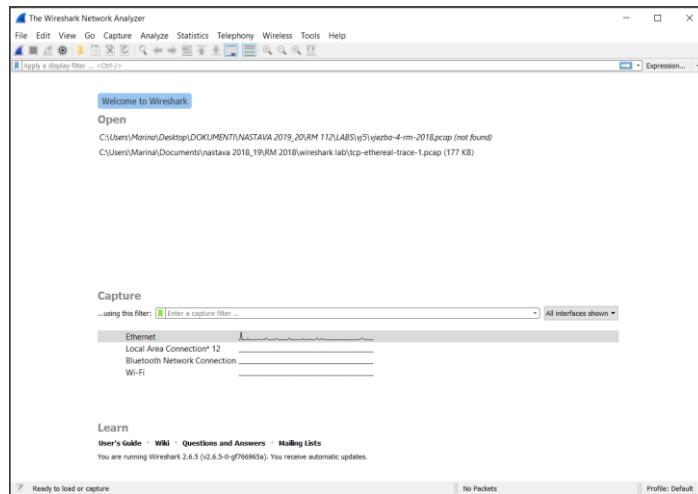
OSNOVE KORIŠTENJA ALATA WIRESHARK

Wireshark je alat koji se koristi za promatranje „protokola u akciji“, i služi za praćenje poruka koje se razmjenjuju između različitih entiteta [26]. Alat se još naziva i alat za praćenje paketa (packet sniffer) te je u svojoj osnovi pasivan program. To znači da prati poruke koje se šalju sa računala i na računalo, ali nikada ne generira ili šalje pakete sam. Osim što „hvata“ kopije poslanih i primljenih paketa u realnom vremenu, Wireshark ima mogućnost i analize poruka (prikazuje sadržaj polja u okviru poruke u formatu koji je razumljiv korisniku).

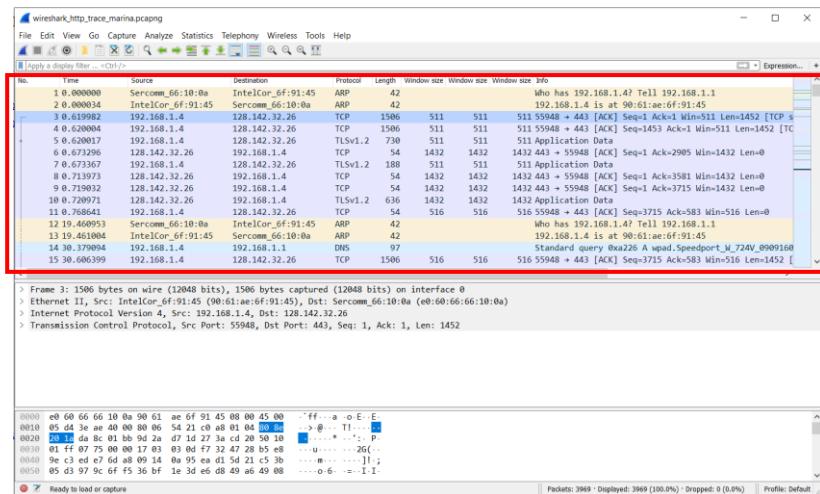
Dohvaćanje i instalacija besplatnog open-source alata Wireshark može se obaviti sa [27]. Ove upute se temelje na verziji Wiresharka 2.6.5.



Kada pokrenemo program Wireshark, njegovo sučelje izgleda slično kao na slici dolje:



Trenutno program ne hvata pakete. Potrebno je odabrati jedno mrežno sučelje ovisno o načinu kako ste spojeni na mrežu. U gornjem slučaju je autor spojen na Ethernet lokalnu mrežu i vidimo kako mrežni promet prolazi tim sučeljem (za ostala sučelja je ravna linija). Kako biste odabrali sučelje dvaput kliknite na njega i paketi će se automatski početi pratiti i vidjet ćete kako se popunjava lista poslanih i primljenih paketa na računalu.



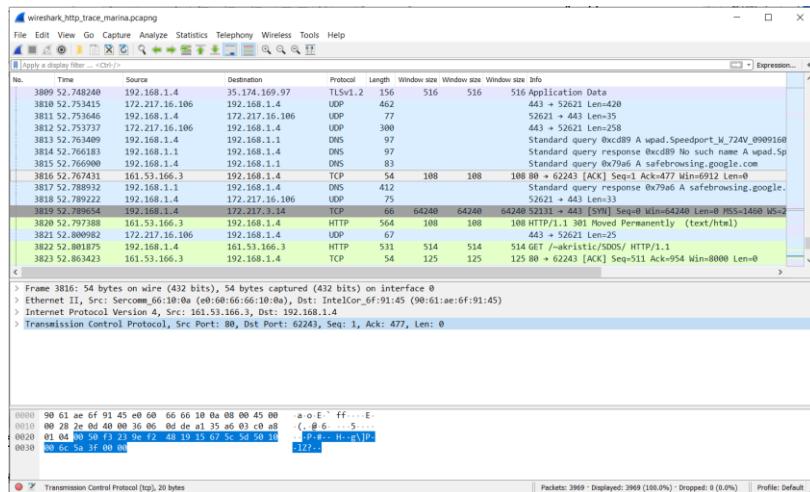
Ako praćenje paketa nije automatski, potrebno je odabrati opciju Capture → Start.

Za početak i upoznavanje s alatom, popratit ćemo pakete HTTP protokola. Znači, naše računalo će komunicirati sa web serverom (koji ima serverski http proces na portu 80) i pokušat će dobiti od njega web stranicu „<http://marjan.fesb.hr/~akristic/SDOS/>“.

Ostavite Wireshark da prati pakete u pozadini, a vi otvorite bilo koji web preglednik koji imate instaliran na vašim računalima i unesite „<http://marjan.fesb.hr/~akristic/SDOS/>“.

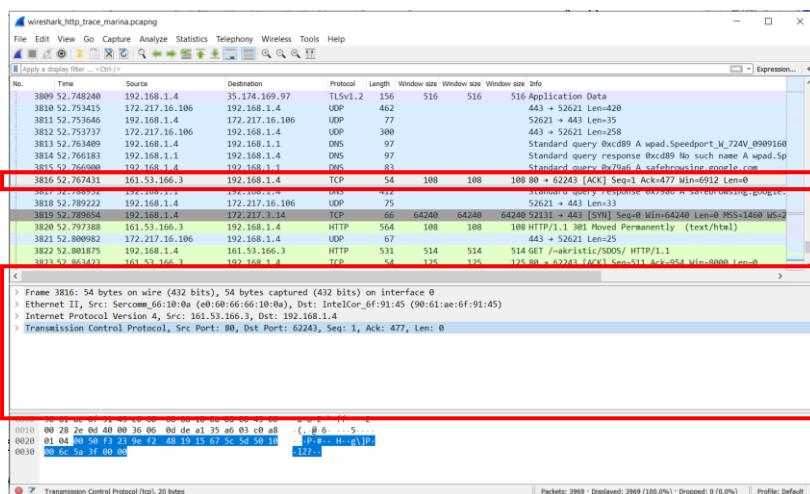
Nakon što vaš preglednik prikaže stranicu „<http://marjan.fesb.hr/~akristic/SDOS/>“, zatvorite web preglednik i zaustavite Wireshark hvatanje paketa odabirom opcije Capture → Stop.

Sada će se pojaviti prikaz svih uhvaćenih paketa od početka hvatanja paketa u Wireshark-u, slično kao na slici ispod:

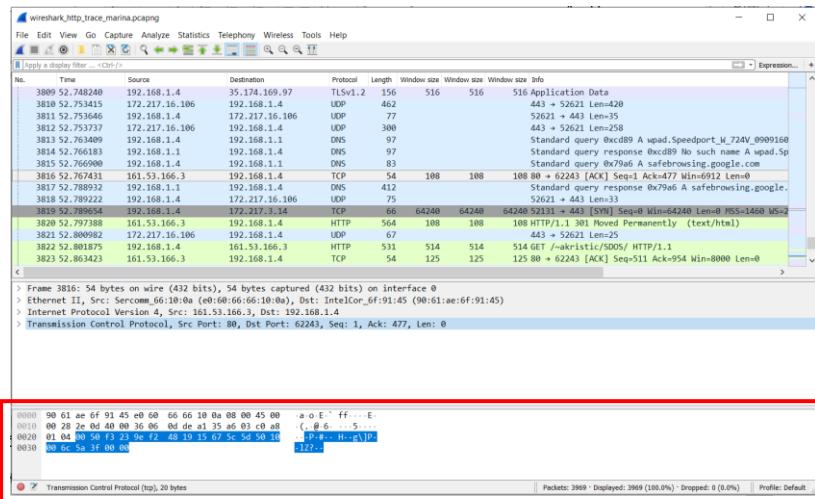


Na gornjoj slici možete vidjeti kako se prikazuje sažetak u jednom retku za svaki uhvaćeni paket, uključujući broj paketa (ovo je broj dodijeljen od strane Wireshark-a - napomenimo da ovo nije broj paketa sadržan u zaglavljiju protokola), zatim trenutak kada je paket uhvaćen, izvornu i odredišnu adresu paketa, vrstu protokola i informacije sadržane u paketu koje su specifične za protokol.

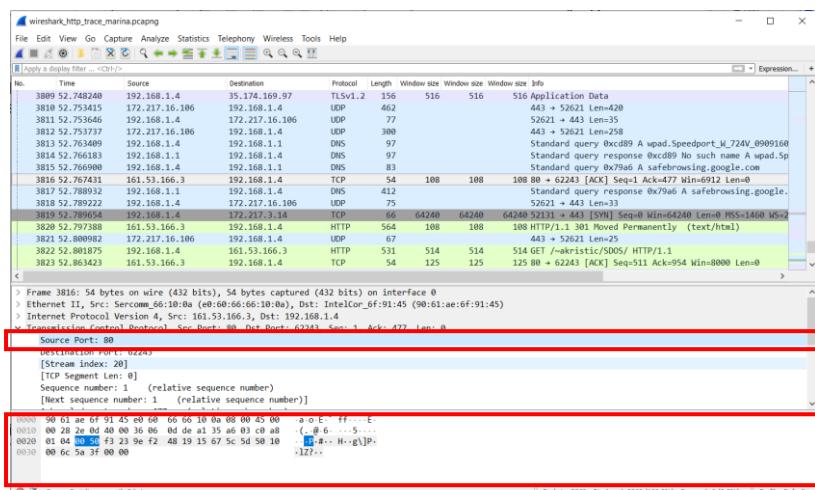
Kada kliknemo na redak, tj. neki paket (na donjoj slici je to slučajno odabrani paket broj 3816), možemo vidjeti detalje protokola kojim je taj paket prenesen. U ovom slučaju je to TCP protokol što znači da je on ovdje protokol „najviše“ razine, a možemo vidjeti i redom imena protokola nižih razina u slojevitoj mrežnoj strukturi (ispod TCP-a je IP protokol mrežne razine, pa je ispod njega Ethernet II protokol). Svaki od protokola dodaje svoje zaglavlje na paket, a detalji i sadržaj svakog pojedinog zaglavlja otvaraju se klikom na ime protokola. Vidimo da Ethernet okvir ukupno ima 432 bita (54 byta).



Na dnu na donjoj slici se može vidjeti sadržaj čitavog okvira u ASCII i heksadecimalnom formatu, a ako označimo TCP protokol, možemo vidjeti dio paketa kojeg čini TCP zaglavlje:



Detalji za svako pojedino polje u TCP zaglavju dobiju se klikom na strelicu kraj imena protokola, a zatim na polje koje nas zanima. Dolje je prikazan Source Port koji iznosi 80, odnosno 0x0050. **Zapišite u izvještaj detalje svakog pojedinačnog polja u TCP zaglavljtu (zapisati vrijednosti u decimalnom i heksadecimalnom obliku).**



U listi paketa možemo vidjeti sve razmijenjene poruke raznih protokola i možemo primijetiti da HTTP poruke nisu jasno prikazane jer postoje mnoge druge poruke dohvaćene u postupku hvatanja paketa. Iako niste napravili ništa drugo nego otvorili vaš Internet preglednik i zatražili jednu jedinu web stranicu, postoje mnogi drugi programi na vašem računalu koji komuniciraju putem mreže u pozadini.

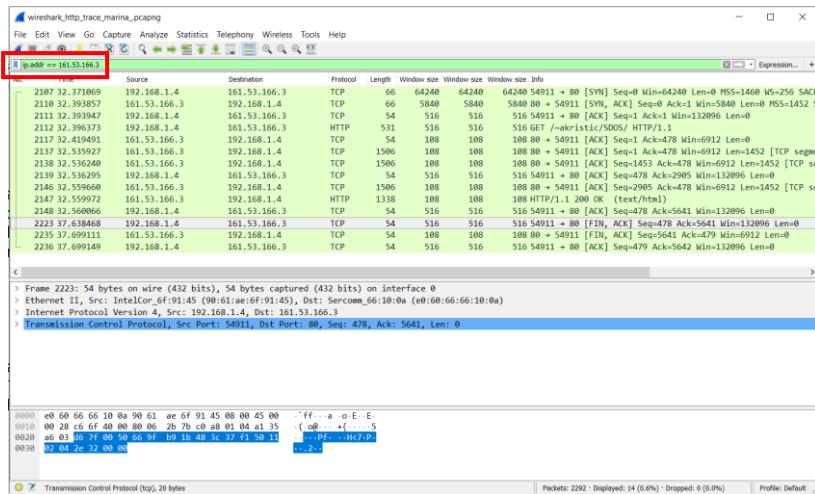
Otvorite Command Prompt na vašem računalu i napravite ping na server sa kojega dohvaćamo web stranicu, korištenjem naredbe:

```
ping marjan.fesb.hr
```

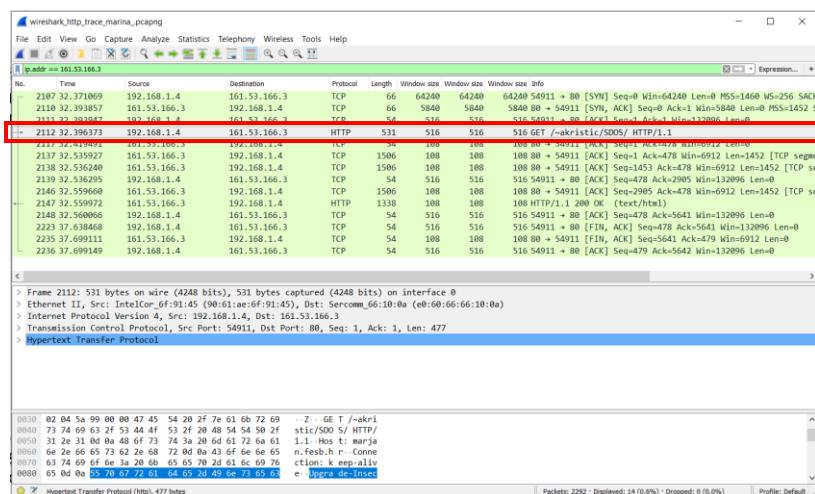
Zapišite u izvještaj koja je IP adresa od „marjan.fesb.hr“ i to je ujedno IP adresa koju očekujemo u Wireshark-u kao Destination IP s kojim naše računalo komunicira.

Saznajte IP adresu svoga računala i zapišite je u izvještaj. Ta adresa će nam u Wireshark-u biti Source IP, a naredba koju treba unijeti u Command Promptu je „ipconfig“.

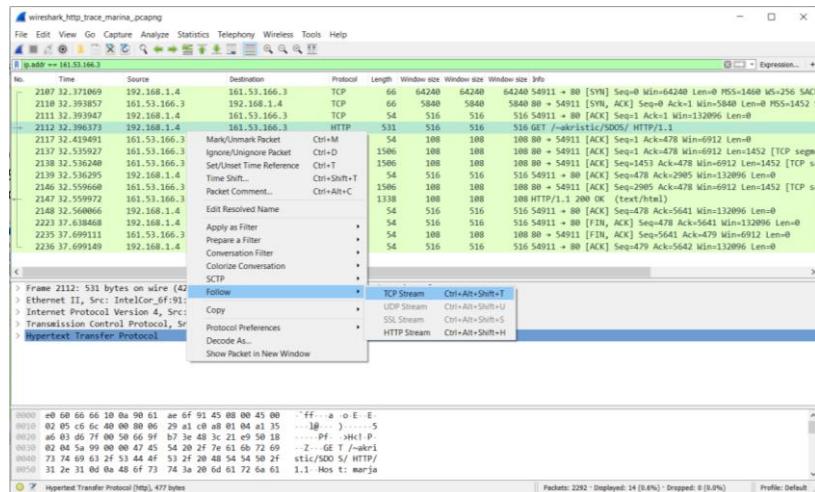
Sada kad smo saznali IP adresu odredišta, želimo analizirati samo promet odnosno pakete koji su razmijenjeni između našeg računala i baš tog odredišta. Zato ćemo iskoristiti funkciju filtriranja u Wireshark-u upisivanjem izraza "ip.addr==161.53.166.3" i nakon toga pritisnemo <enter>. Promet će se filtrirati slično kao na slici dolje:



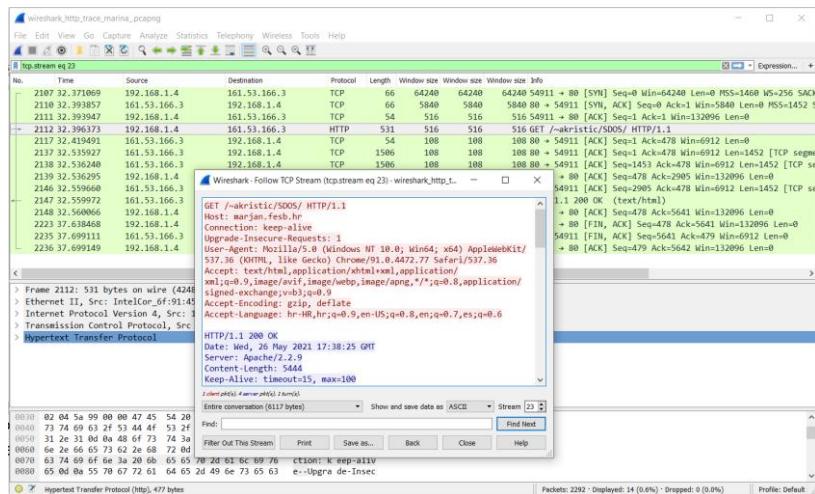
Označeni redak na donjoj slici je HTTP paket i vidimo da je adresa našeg računala 192.168.1.4, dok je adresa od „marjan.fesb.hr“ 161.53.166.3. Metodom GET zahtijeva se dohvaćanje web stranice od web servera.



Ako želimo vidjeti detalje uspostave TCP konekcije sa „marjan.fesb.hr“ na nižoj razini, moramo dodatno filtrirati pakete u Wireshark-u. Zato ćemo upotrijebiti precizniji filter praćenjem TCP paketa:

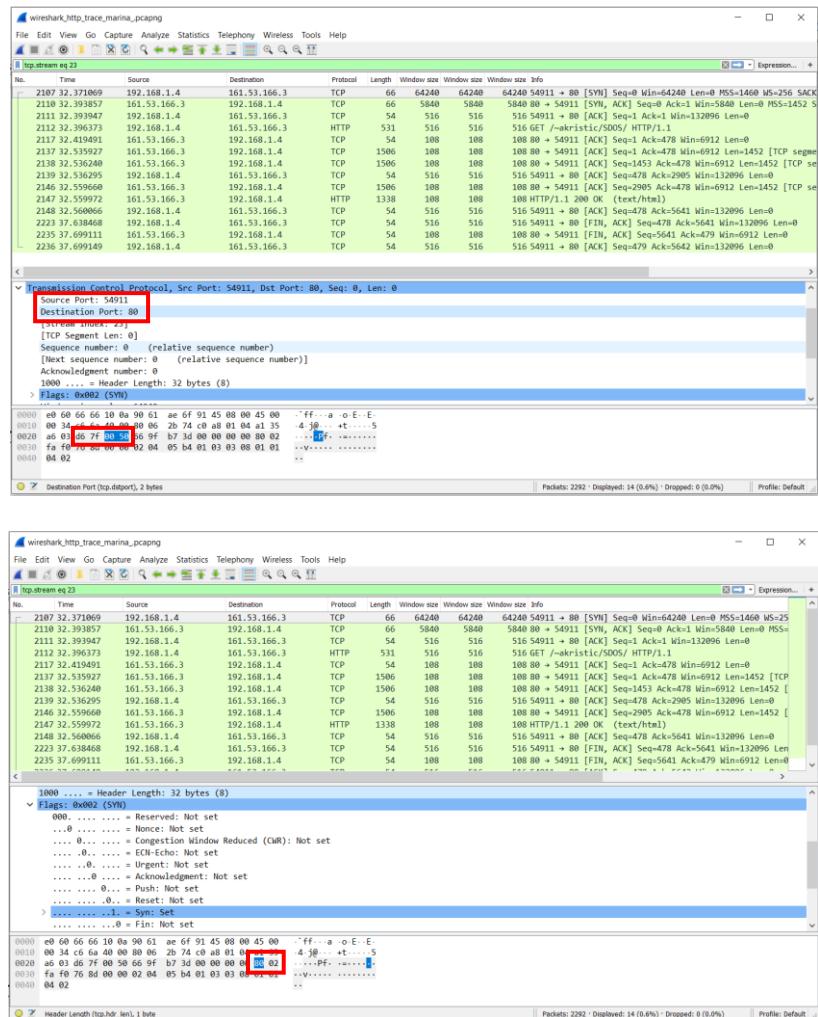


Ugasite mali prozor i pogledajte TCP poruke koje su uhvaćene. Prve tri poruke služe za three-way handshake, dakle uspostavu TCP konekcije klijenta i web servera. Vidimo da je port klijenta 54911, a web server zaprima zahtjev za konekcijom na portu 80.

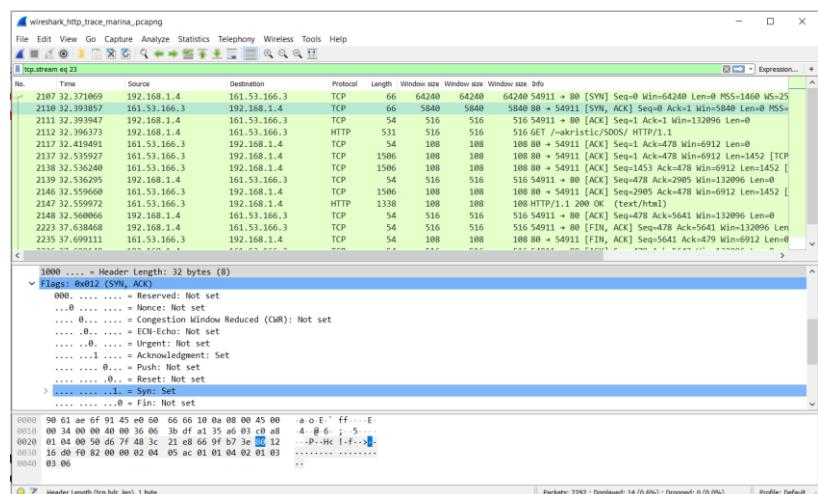


Odaberimo prvu poruku i pogledajmo njene detalje (slika dolje). Vidimo da računalo šalje zahtjev za konekciju serveru (source port=54911 i destination port=80) i to je SYN poruka (polje flags ima 8 zastavica od kojih su sve nula osim SYN flag-a koji je postavljen u jedinici). Zato polje flags iznosi 0x02 u heksadecimalnom zapisu (00000010₍₂₎). Redni broj paketa je SEQ=0, a definira se i Maximum Segment Size (MSS=1460), a to je parametar TCP zaglavja koji govori maksimalni broj bytova koji uređaj može primiti u TCP paketu.

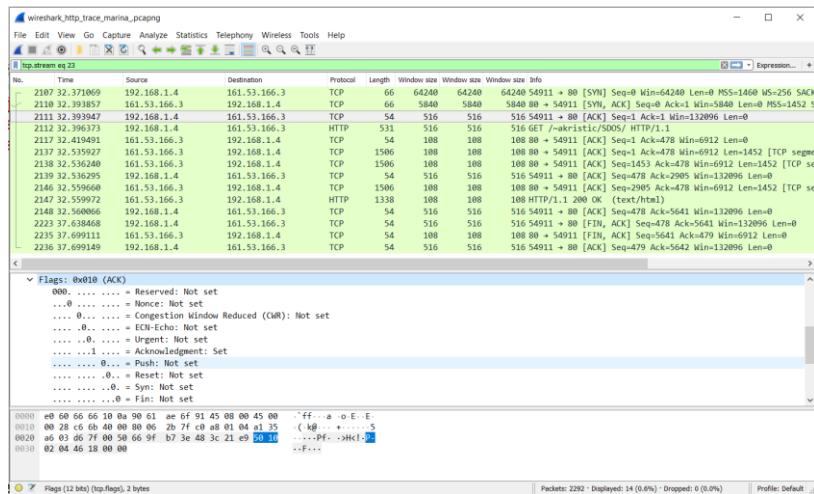
Jedan dio polja zastavica (prije 0x02) je rezerviran (Reserved) i tu je upisana 0, a prije toga je heksadecimalni broj 8 koji je potrebno pomnožiti sa 4 kako bi se dobio ukupan broj byteova u TCP zaglavju (u ovom slučaju je to 32 bytea).



U idućoj poruci (slika dolje) server odgovara klijentu da je primio njegovu poruku (zahtjev za konekcijom) – jer potvrđuje primitak uz pomoć polja ACK koji se postavlja na ACK=1. Time se potvrđuje primitak paketa sa rednim brojem SEQ=0, jer se postavlja ACK=SEQ+1. Ovo je sada SYNACK paket kojeg šalje server, u kojem su dvije zastavice (SYN i ACK) postavljene u jedinici, pa je iznos flags polja $00010010_{(2)}$ =0x12. Ovom porukom server kaže klijentu da je spremjan za uspostavu veze i očekuje od njega idući paket sa rednim brojem SEQ=0+1=1.

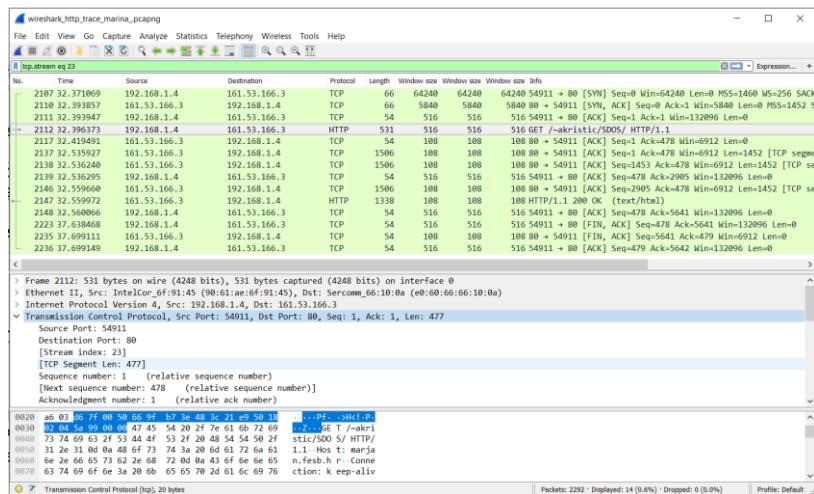


Klijent šalje treću poruku (slika dolje) kojom potvrđuje serveru da je dobio njegovu potvrdu da se veza može uspostaviti. Zato postavlja polje ACK=1, kako bi potvrdio primitak prethodnog paketa sa rednim brojem SEQ=0, jer je ACK=SEQ+1. Redni broj paketa kojeg šalje klijent je SEQ=1 jer je on jednak prethodnom ACK polju koji je primljen od servera. Ovo je ACK paket kojim klijent potvrđuje da je dobio poruku od servera da se veza može uspostaviti pa je ACK zastavica postavljen u jedinicu i nakon ovog trenutka veza je uspostavljena i počinje slanje podataka.



Pogledajte sliku ispod i primijetite kako u ovom primjeru u retku 2112 Wireshark-a klijent sada šalje zahtjev za dohvaćanje web stranice metodom GET.

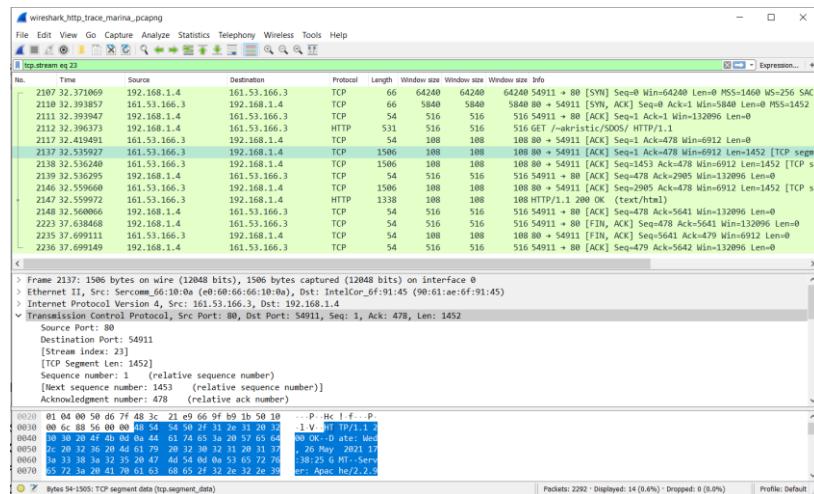
Kada TCP šalje potvrdu primitka nekih segmenata, postavi zastavicu ACK u 1, a u polje Acknowledgement number upiše redni broj prvog sljedećeg okteta kojeg očekuje. Kako segment kojeg računalo pošalje serveru u retku 2112 ima duljinu 477 okteta (TCP segment len), kada server primi taj segment on u retku 2117 generira potvrdu s postavljenom zastavicom ACK i brojem 478 u polju Acknowledgement number (jer je prvi sljedeći oktet kojeg očekuje 478). Primijetite da, pošto se radi samo o potvrdi paketa, duljina ove poruke je len=0. Takva poruka ne sadrži podatke.



Nakon toga, kako je prikazano u liniji 2137 na slici dolje, server počinje slati podatke klijentu. Duljina TCP segmenata koje server šalje klijentu u recima 2137 i 2138 je 1452 byteova.

TCP prilikom slanja podataka u polje Sequence number zapisuje redni broj (gledano od početka slanja svih podataka) prvog bytea u podacima koji se prenose tim segmentom. Stoga je za segment u retku 2137 postavljeno SEQ=1 (prvi byte podataka tog segmenta je ujedno i prvi byte podataka koje server šalje od početka veze). Za segment u retku 2138 je postavljeno SEQ=1453, jer se prvim segmentom (iz retka 2137) već poslalo 1452 byteova podataka tako da je prvi byte podataka u ovom segmentu 1453. byte od početka veze.

Polje ACK ostaje ACK=478 za oba paketa koja šalje server, jer nije u međuvremenu dobio niti jedan paket od klijenta (pa ne treba potvrđivati primitak nekih novih paketa).

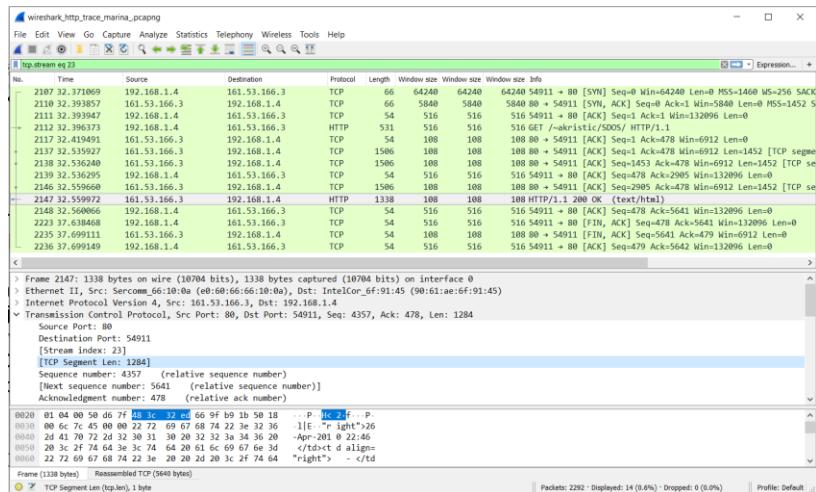


Klijent u retku 2139 šalje potvrdu kojom potvrđuje primitak prethodna dva paketa. Kako su ta dva segmenta prenijela 2904 bytea podataka ($1452 + 1452 = 2904$), prvi sljedeći byte kojeg klijent očekuje je 2905. byte od početka veze. Stoga u ovoj potvrdi klijent postavlja zastavicu ACK u 1, a u polje Acknowledgement number upisuje upravo broj 2905.

Kako je klijent do ove potvrde poslao 477 B podataka, u potvrdi u polje SEQ upisuje broj 478. Ipak, duljina podataka u potvrdi je len=0, što znači da tog 478. bytea podataka nema u ovoj potvrdi (nema nikakvih podataka).

U idućem retku (redak 2146) server šalje treću poruku klijentu, u kojoj je redni broj SEQ=2905 (jer je u prva dva segmenta poslao ukupno 2904 B podataka). Polje ACK je i dalje ACK=478 kao i za prethodna dva paketa koje je server poslao (jer i dalje očekuje primitak 478. B podataka od klijenta).

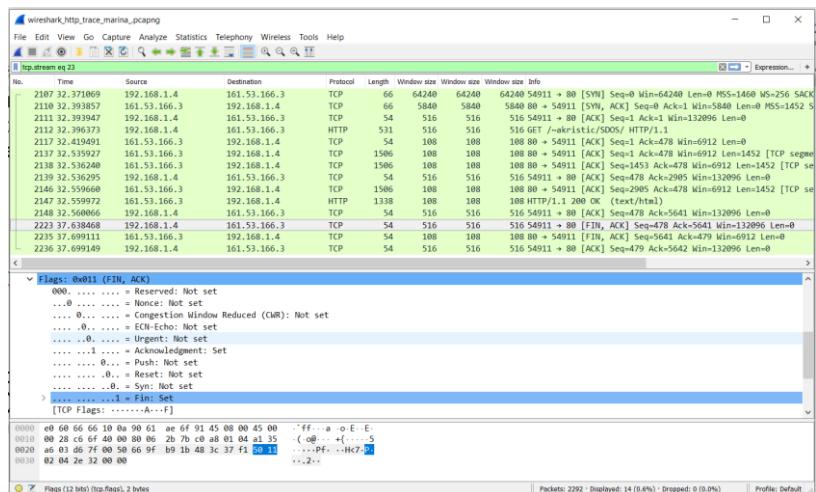
Nakon toga (redak 2147 na slici dolje) server šalje klijentu tekstualni html od web stranice koja će se klijentu prikazati u browser-u. Duljina poslanog TCP segmenta je 1284 byteova i njegov SEQ broj je SEQ=4357 (jer je do sada server poslao $3 \times 1452 = 4356$ B podataka).



Klijent u novom paketu (redak 2148) potvrđuje primitak i govori da je prvi sljedeći byte podataka kojeg očekuje ACK=5641 (jer je u prva tri segmenta primio 4356 B, a u ovome četvrtom je bilo 1284 B podataka, tj. ukupno je ispravno primio prvih 5640 B podataka).

SEQ polje u ovoj potvrđi je i dalje 478, a duljina je 0 (kao i u potvrđi iz retka 2139).

Klijent je sada primio sve od servera pa će poslati FINACK paket kojim će zahtijevati zatvaranje konekcije. Poruka je ista kao prethodna, samo ima još postavljenu FIN zastavicu u jedinici. Pogledajmo detalje te poruke (redak 2223):



U retku 2235, server potvrđuje da je primio klijentov zahtjev tako što postavi ACK zastavicu, a ACK polje uveća za jedan, iako u segmentu kojeg potvrđuje nije bilo podataka. Na ovaj način će klijent biti siguran da je server primio zahtjev za prekid. Također, postavljanjem zastavice FIN server javlja klijentu da je i on gotov sa slanjem podataka i traži prekid veze. Redni broj poruke je SEQ=5641, a len=0 (ne sadrži podatke).

U zadnjoj poruci (redak 2236) klijent postavljanjem zastavice ACK u jedinicu potvrđuje da je primio potvrdu za zatvaranje veze od strane servera. Redni broj ACK-a je uvećan za jedan (s 5641 na 5642) iako u segmentu kojeg potvrđuje nije bilo podataka. Tako će i server biti siguran da je klijent primio zahtjev za prekid. Sada je to kraj komunikacije.

PRAĆENJE PAKETA PRILIKOM UPLOADA DATOTEKE NA SERVER

Prvo ćemo upotrijebiti Wireshark za dobivanje fajla sa tragovima paketa za vrijeme prijenosa datoteke s računala na udaljeni server. To ćemo učiniti pristupanjem web stranici iz [22], koja će nam omogućiti da unesemo ime datoteke pohranjene na vašem računalu (koja sadrži ASCII tekst „Alise u zemlji čудesa“), a zatim da datoteku prebacimo na server. Naravno, za to ćemo vrijeme pokrenuti Wireshark kako bismo dobili trag TCP segmenata poslanih i primljenih sa našeg računala.

Učinite sljedeće:

1. Pokrenite svoj web preglednik. Idite na „<http://gaia.cs.umass.edu/wireshark-labs/alice.txt>“ i dohvate ASCII kopiju teksta „Alice u zemlji čudesa“. Spremite ovu datoteku negdje na računalu.
2. Sljedeće idite na „<http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>“.
3. Trebali biste vidjeti web stranicu iz knjige [22] koja izgleda ovako:

Upload page for TCP Wireshark Lab
Computer Networking: A Top Down Approach, 6th edition
Copyright 2012 J.F. Kurose and K.W. Ross, All Rights Reserved

If you have followed the instructions for the TCP Wireshark Lab, you have *already* downloaded an ASCII copy of Alice and Wonderland from <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> and you also *already* have the Wireshark packet sniffer running and capturing packets on your computer.

Click on the Browse button below to select the directory/file name for the copy of alice.txt that is stored on your computer.

No file chosen

Once you have selected the file, click on the "Upload alice.txt file" button below. This will cause your browser to send a copy of alice.txt over an HTTP connection (using TCP) to the web server at gaia.cs.umass.edu. After clicking on the button, wait until a short message is displayed indicating the the upload is complete. Then stop your Wireshark packet sniffer - you're ready to begin analyzing the TCP transfer of alice.txt from your computer to gaia.cs.umass.edu!!

4. Pomoću opcije „Choose File“ pronađite datoteku koja sadrži Alicu u zemlji čudesa i koju ste spremili na računalu. Još uvijek nemojte odabrati "Upload alice.txt file".
5. Sada pokrenite Wireshark i započnite hvatanje paketa (Capture→Start).
6. Vratite se u vaš web preglednik, i sada pritisnite gumb " Upload alice.txt file" da biste datoteku prenijeli na poslužitelj pod nazivom „gaia.cs.umass.edu“. Nakon što je datoteka prenesena, u prozoru preglednika prikazat će se kratka poruka.
7. Zaustavite hvatanje paketa u Wireshark-u i spremite .pcap file na računalo pod nazivom „**vjezba5_tcp_protokol.pcap**“.

Ako ne uspijete dobiti gornji .pcap fajl sa tragovima paketa, možete ga dobiti sa linka: <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> koji je također dodatak knjizi iz [23] i datoteka se zove „tcp-ethereal-trace-1“.

ANALIZA POSLANIH/PRIMLJENIH PAKETA

Sada ćemo analizirati prethodno spremljeni .pcap file. Prvo filtrirajte pakete prikazane u prozoru Wireshark unošenjem riječi "tcp".

Ono što biste trebali vidjeti je niz TCP i HTTP poruka između vašeg računala i servera „gaia.cs.umass.edu“. Trebali biste vidjeti početni three-way handshake koji sadrži SYN poruku kao i HTTP POST poruku. U ovom slučaju koristimo POST metodu jer šaljemo veće količine podataka na server, što je razlika od prethodno objašnjelog primjera gdje smo koristili GET.

Ovisno o verziji Wiresharka koju koristite, možda ćete vidjeti niz poruka "Nastavak HTTP-a (eng. HTTP Continuation)" koje se s vašeg računala šalju na „gaia.cs.umass.edu“. Podsjetimo da je ovo način na koji Wireshark pokazuje da se više TCP segmenata koristi za prijenos jedne HTTP poruke. U novijim verzijama Wiresharka, u stupcu Info na zaslonu Wireshark vidjet ćete "[TCP segment ponovno sastavljenog PDU-a (eng. TCP segment of a reassembled PDU)]" da bi se naznačilo da ovaj TCP segment sadrži podatke koji pripadaju većoj poruci protokola gornjeg sloja (u našem slučaju je to HTTP). Također biste trebali vidjeti da se TCP ACK segmenti vraćaju s „gaia.cs.umass.edu“ servera na vaše računalo.

Odgovorite na sljedeća pitanja na temelju analize Wireshark datoteke:

Pitanje 1. Koja je IP adresa i broj TCP porta koji koristi klijentsko računalo (source) koje prenosi datoteku na poslužitelj gaia.cs.umass.edu?

Klijentsko računalo (source) IP adresa: _____

Broj TCP porta: _____

Pitanje 2.

a) Koja je IP adresa gaia.cs.umass.edu?

b) Na kojem broju porta šalje i prima TCP segmente za ovu vezu?

IP adresa poslužitelja: _____

Broj TCP porta: _____

Pitanje 3.

Prepoznajte poruke koje sadrže početni three-way handshake.

a) Koji su brojevi redaka ovih poruka u Wireshark listi primljenih/poslanih paketa?

Odgovor: _____

b) Opišite vlastitim riječima koja je svrha three-way handshake mehanizma.

Odgovor: _____

Pitanje 4.

Odgovorite na iduća pitanja:

a) Koji je redni broj (sequence number, SEQ) od TCP SYN segmenta koji se koristi za pokretanje TCP veze između klijentskog računala i gaia.cs.umass.edu?

Redni broj TCP SYN segmenta: _____

b) Što segment ima što ga identificira kao SYN segment?

Odgovor: _____

c) Odaberite segment TCP SYN (u listi Wireshark paketa). Ispitajte koja je veličina i vrijednost zaglavlja IPv4 protokola?

Duljina zaglavlja IPv4: _____

IPv4 zaglavljje: _____

d) Koja je veličina i vrijednost TCP zaglavlja?

Duljina TCP zaglavlja: _____

TCP zaglavljje: _____

e) Koji bajt u TCP zaglavlju sadrži zastavicu SYN?

Vrijednost bajta zastavica (heksadecimalna): _____

Vrijednost bajta zastavica (binarna): _____

Pitanje 5.

Odgovorite na iduća pitanja:

a) Koji je redni broj segmenta SYNACK koji je gaia.cs.umass.edu poslao klijentskom računalu kao odgovor na SYN?

Redni broj segmenta TCP SYNACK: _____

b) Kolika je vrijednost polja potvrde (ACK) u segmentu SYNACK?

Vrijednost polja ACK: _____

c) Kako je gaia.cs.umass.edu odredio tu vrijednost za ACK?

Odgovor: _____

d) Što je to u segmentu što ga identificira kao SYNACK segment?

Odgovor: _____

Pitanje 6. Odaberite prvi segment u kojem se podaci šalju na poslužitelj.

a) Koji je broj retka (u listi Wireshark paketa) ove poruke?

Broj retka: _____

b) U novijim verzijama Wiresharka vidjet ćete "[TCP segment ponovno sastavljenog PDU-a]" pored segmenta za slanje podataka. Objasnite što to znači?

Odgovor: _____

Pitanje 7.

a) Pronađite prvi 5 segmenata koji služe za slanje podataka. Popunite tablicu sa njihovim rednim brojevima!

Data segment	Line No. in the trace	SEQ number
0		
1		
2		
3		
4		

b) Opišite kako klijent generira redne brojeve paketa?

Odgovor: _____

c) Pronađite ACK poruke koje šalje poslužitelj za prvi 5 segmenata koji služe za slanje podataka. Popunite tablicu sa odgovarajućim ACK vrijednostima!

Data segment ACK message	Line No. in the trace	ACK value
0		
1		
2		
3		
4		

d) Koja je razlika u duljini između segmenata podataka poslanih s računalna na poslužitelj i ACK segmenata poslanih s poslužitelja na računalo?

Odgovor: _____

e) Odaberite jedan segment podataka koji se šalje s računalna na poslužitelj. Ispitajte bajtove u TCP zaglavljju. Koliko bajtova postoji za SEQ broj i koliko on iznosi?

Odgovor: _____

f) Objasnite heksadecimalni prikaz rednog broja u TCP zaglavlju odabranog paketa! Kako se on dobije s obzirom da je relativan. Izračunajte ga.

Odgovor: _____

Pitanje 8. Vratite se na tablicu u Pitanju 7.

- a) Provjerite u koje je vrijeme poslan svaki od segmenata podataka. Popunite tablicu sa vremenom slanja paketa!
- b) Kada je primljena ACK potvrda za svaki segment?
- c) S obzirom na razliku između trenutka slanja svakog TCP segmenta i primanja potvrde, kolika je RTT vrijednost za svaki od 5 segmenata?

Tablica kojom ćete odgovoriti na pitanja:

Data segment	Sent time	ACK received time	RTT (seconds)
0			
1			
2			
3			
4			

Pitanje 9. Koja je minimalna i maksimalna veličina prozora prijamnika i predajnika?

Min. receiver window size: _____

Max. sender window size: _____

Pitanje 10. Koliki je protok (eng. throughput) za TCP vezu? S obzirom da su to bajtovi preneseni u jedinici vremena, napišite formulu pomoću koje ste izračunali ovu vrijednost.

ZADACI ZA VJEŽBU 5 (PREDAJA IZVJEŠTAJA):

Odgovoriti na pitanja koja su zadana u vježbi i predati izvještaj.

VJEŽBA 6: PRIVATNE MREŽE I VATROZID

CILJ VJEŽBE

U ovoj vježbi naučit ćešmo čemu služe privatne adrese i kako radi NAT-Network Address Translation protokol.

TEORIJSKI PREDUVJETI

Teorijski dijelovi vježbe preuzeti su sa [5].

PRIVATNE MREŽE (INTRANET)

Privatne mreže (Intranet) su mreže organizirane na TCP/IP tehnologiji, ali ne koriste javne, već privatne IP adrese. Za privatne mreže rezervirane su adrese 10.0.0.0/8, 172.16.0.0/16 i 192.168.0.0/16, dakle jedna A, jedna B i blok od 256 uzastopnih C klase. Usmjernici Interneta pakete s ovim IP adresama odbacuju bez pokušaja daljnog usmjeravanja.

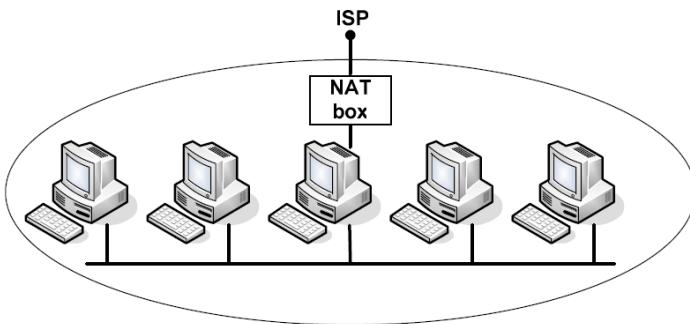
Postojanje Intranet mreža ima jedno od tri opravdanja:

- mreža nije povezana na Internet - **nepovezane podmreže** trebaju koristiti privatne adrese kako bi kod naknadnog povezivanja na Internet bili izbjegnuti poremećaji u usmjeravanju, mogući za slučaj duplicitiranja već iskorištenih adresa.
- mreža je povezana, ali zbog sigurnosti koristi privatne adrese - **sigurne podmreže** (Intranet) koriste privatne adrese, a povezane su na Internet preko jednog usmjernika koji prema Internetu djeluje kao krajnje računalo. Na taj način vanjskom učesniku komunikacije nije poznat broj ni nazivi računala unutar sigurne podmreže. Veze s javne mreže prenose se na privatnu (unutarnju) tehnikama maskarade i uslužnih veza, odnosno NAT-Network Address Translation i PAT-Port Address Translation protokolom (termin PAT se rješi koristi, radi jednostavnosti se pod NAT-om često podrazumijevaju oba protokola).
- mreža je povezana, ali zbog nedostatka/uštede IP adresa koristi privatne adrese.

Uobičajene lokalne mreže najčešće su preko usmjernika povezane na npr. zakupljeni vod odnosno njime na Internet. Usmjernik obavlja prevođenje s Ethernet na PPP protokol se koji koristi na zakupljenom vodu. IP datagram, njegovo zaglavje sa IP adresama i njegov podatkovni dio (TCP, HTTP, ...) prenose se transparentno, bez obrade, budući su razine Internet modela nezavisne. Ethernet zaglavje se odbacuje.

NAT protokol funkcioniра dosta drugačije. Unutar lokalne mreže koristi se adresiranje s IP adresama iz raspona za privatne mreže, a prema Internetu je mreža predstavljena samo usmjernikom, koji se sada ponekad naziva i NAT kutija (NAT box).

NAT protokol na lokalnoj mreži prikazan je na idućoj slici:



Kako smo vidjeli, većina aplikacija koristi TCP ili UDP na prijenosnoj razini te se svaka uspostavljena veza može identificirati priključnicom (socket) na dvije strane komunikacije (najčešće klijent i poslužitelj). Kada računalo iz Intranet lokalne mreže uspostavlja vezu prema poslužitelju izvan lokalne mreže, ono se spaja na priključnicu na poslužitelju, pri čemu odredišna priključna točka (Destination port) ovisi o usluzi na poslužitelju. Izvorišna priključna točka se dodjeljuje praktički nasumično iz raspona 1024 – 64k.

Ideja NAT protokola je jako jednostavna, ali nije "ISO/OSI kompatibilna". Kako je cijelokupna mreža predstavljena samo usmjernikom, izvorišna IP adresa paketa će pri prolasku kroz NAT kutiju biti zamijenjena IP adresom usmjernika. TCP ili UDP polje Source Port bit će također zamijenjeno vrijednošću po izboru NAT kutije, i ta će se vrijednost zapamtiti u memoriji NAT kutije, zajedno s Intranet IP adresom datagrama i originalnom vrijednošću polja Source port.

Dakle, NAT box radi mapiranje između para {internal address, internal port} i {external address, external port}. Zamjena vrijednosti Source Port TCP/UDP polja pri slanju je nužna jer je zbog slučajnog karaktera tog polja moguće da dva ili više Intranet računala pokušaju uspostaviti vezu s istom vrijednošću Source Port.

Kada dođe odgovor od poslužitelja kojem je datagram upućen, NAT kutija će pogledati TCP/UDP Destination Port, zatim u svojoj tablici pogledati kojoj Intranet IP adresi on odgovara, obaviti zamjene IP adrese i Destination porta i pustiti datagram na Intranet mrežu. Ovo rješenje funkcioniра dobro i masovno se koristi ali ima i mana. Neke od njih su:

- Prijenosna razina adresira računala, dakle radi posao mrežne razine;
- IP adresa više ne identificira jedinstveno računalo na Internet mreži, jer, mada prekriveno, može postojati više računala s istom IP adresom iz privatnog skupa adresa;
- Povećano je kašnjenje;
- Nemogućnost praćenja puta paketa s kraja na kraj; itd.

VATROZID (FIREWALL)

Vatrozid (firewall) je uređaj ili program koji nadzire mrežni promet na računalu ili mreži. Njegova uloga je kontroliranje prometa po kriteriju IP adrese, TCP/UDP porta, odredišne usluge, protokola, TTL vrijednosti, aplikacije i dr. Na taj je način moguće ograničiti različite zloupotrebe mreže i ograničiti djelovanje virusa preko mreže.

Koji promet se propušta, a koji blokira, definiraju pravila u tablicama filtriranja. Dvije su uobičajene politike filtriranja:

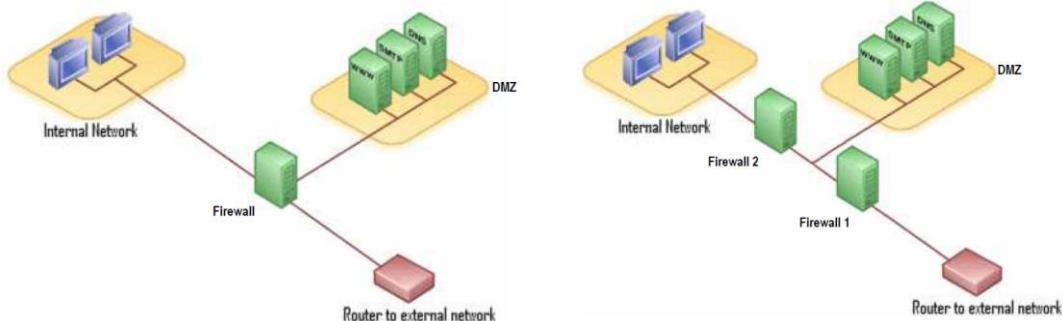
- blokira se sav promet koji nije eksplicitno dozvoljen - najsigurnija i najpreporučljivija politika kod koje administrator posebno dozvoljava ono što je potrebno.

- propušta se sav promet koji nije eksplizitno blokiran - manje sigurna, ali jednostavnija politika.

Vatrozidi često imaju ugrađenu NAT funkcionalnost, a računalima u lokalnoj mreži iza vatrozida uobičajeno su dodijeljene privatne mrežne adrese. Kako je osnovna namjena vatrozida reguliranje prometa među mrežama različitih nivoa sigurnosti uobičajeno se koriste za uspostavu **DMZ (demilitarizirajuće zone)** - fizičke ili logičke podmreže srednjeg nivoa sigurnosti, koja se nalazi između sigurne unutrašnje mreže (npr. privatne lokalne mreže) i nesigurne vanjske mreže (npr. Interneta). Svrha demilitarizirajuće zone je dodavanje još jednog sigurnosnog sloja nekoj lokalnoj mreži. Tipično DMZ sadrži uređaje koji trebaju biti dostupni Internet prometu, kao što su Web (HTTP) poslužitelji, FTP poslužitelji, SMTP (e-mail) poslužitelji i DNS poslužitelji.

Mreža sa demilitarizirajućom zonom može se uspostaviti na više načina. Dvije najčešće metode su s jednim i sa dva vatrozida. Ove jednostavne arhitekture mogu se proširiti u složenije, ovisno o zahtjevima mreže.

Kod arhitekture s jednim vatrozidom koristi se vatrozid s barem 3 mrežne kartice. Jedna mrežna kartica služi za vezu prema ISP-u, na drugoj se formira interna mreža, a na trećoj DMZ (slika dolje lijevo). Vatrozid mora nadzirati sav promet s Interneta i prema DMZ i prema Intranetu. Sigurnija i skuplja metoda je uspostava DMZ pomoću 2 vatrozida (slika dolje desno). Prvi mora biti konfiguriran tako da propušta i promet namijenjen DMZ i onaj namijenjen internoj mreži. Drugi vatrozid smije propuštati samo promet namijenjen internoj mreži, a koji ne potječe iz DMZ.



VPN (VIRTUAL PRIVATE NETWORK)

Tvrte koje se fizički rasprostiru na više fizički udaljenih lokacija mogu se povezati u jedinstvenu mrežu korištenjem zakupljenih vodova (fiksne cijene najma) između lokacija. Većini tvrtki to je preskupo i presloženo rješenje, a nije praktično niti kod umrežavanja novih lokacija kao niti kod umrežavanja privremenih korisnika (npr. kupaca).

Rješenje koje se danas koristi u takvim situacijama je virtualna privatna mreža (Virtual Private Network – VPN). VPN za umrežavanje pojedinih lokacija tvrtke koristi postojeću Internet infrastrukturu, koja je mnogo prikladnije rješenje od korištenja zakupljenih vodova.

Dva su problema kod korištenja Internet mreže za umrežavanje privatnih mreža: sigurnost i performanse. Stoga VPN mreža mora uključivati i sljedeće dodatke na protokole korištene u Internet mreži:

- Autentifikacija - potvrđuje autentičnost strana u komunikaciji;
- Kontrola pristupa - onemogućuje neautorizirani pristup mreži;

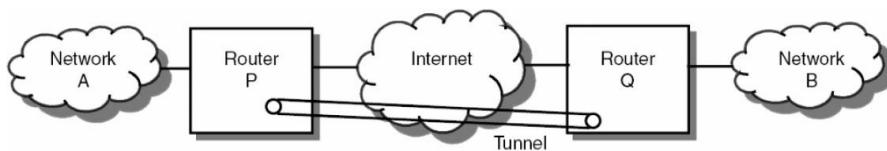
- Tajnost i integritet podataka - zaštićuje podatke od čitanja ili mijenjanja kod prijenosa kroz javnu mrežu.

Za autentifikaciju i kontrolu pristupa koristi se niz protokola (Challenge Handshake Authentication Protocol - CHAP, Remote Authentication Dial-in User Service - RADIUS, korištenje digitalnih certifikata, biometrijske provjere, itd). Tajnost i integritet podataka osigurani su enkripcijom.

VPN ARHITEKTURA I PROTOKOLI

Svaka lokacija tvrtke vezana je uobičajenim vodom na pružatelja Internet usluge (ISP). Veze između lokacija uspostavljaju se korištenjem tuneliranja, tj. enkapsuliranjem podataka u IP pakete, koje odvaja promet između lokacija (sa svojim rasponom IP adresa) od podataka predviđenih za usmjeravanje na Internet mreži.

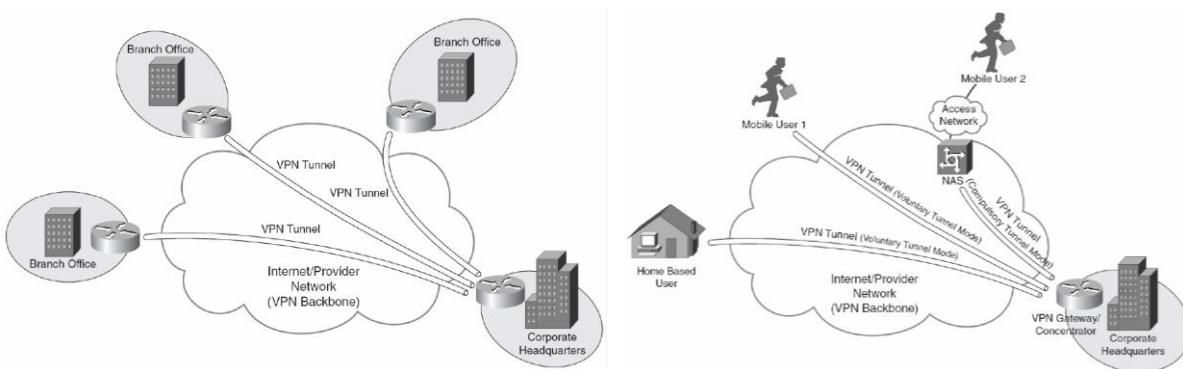
Tuneliranje između dvije VPN lokacije prikazano je na idućoj slici:



Proces tuneliranja između dvije VPN lokacije može se ukratko opisati kroz nekoliko faza (slika gore):

- Računalo iz mreže A komunicira s računalom iz mreže B; ono formira IP paket s IP adresom odredišnog računala iz mreže B, i prosljeđuje ga svojom lokalnom mrežom usmjerniku P.
- VPN usmjernik P formira IP paket koji u polju odredišne adrese sadrži adresu VPN usmjernika Q, a u podatkovnom dijelu kompletan paket primljen od računala iz mreže A.
- Internet mrežom taj se paket isporučuje VPN usmjerniku Q. On izdvaja iz podatkovnog dijela IP paketa originalni paket i isporučuje ga računalu iz mreže B.

Postoje dvije osnovne arhitekture VPN mreža: Site-to-Site (slika dolje lijevo) i Remote Access (slika dolje desno).



Site-to-Site VPN, odnosno VPN mreža od lokacije do lokacije, povezuje cijele podmreže u virtualnu privatnu mrežu. Računala u podmrežama nemaju podršku za VPN već se o enkripciji i enkapsuliranju/dekapsuliranju podataka brinu VPN pristupni uređaji (VPN gateway), obično usmjernici ili vratnizi preko kojih su podmreže spojene na javnu mrežu.

Najčešći protokoli koji se koriste u Site-to-Site VPN arhitekturi su:

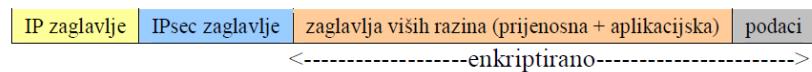
- IPsec – skup protokola za zaštitu IP prometa na javnoj mreži,
- L2TPv3 (Level 2 Transport Protocol version3) – koristi se najčešće za tuneliranje PPP okvira preko IP mreže, a moguće ga je koristiti i za Frame Relay i Ethernet.

Kod Remote Access VPN-a, tj. udaljenog VPN pristupa, pojedinačni nepokretni ili pokretni klijent se povezuje na podmrežu. U ovom slučaju taj klijent mora imati podršku za VPN. Najčešći protokoli koji se koriste u Remote Access VPN arhitekturi su:

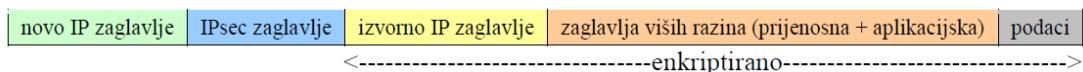
- PPTP (Point-to-Point Tunneling Protocol) – omogućuje tuneliranje klijentskih PPP okvira,
- L2TPv2/L2TPv3 (Layer 2 Tunneling Protocol versions 2 and 3) – IETF standard koji omogućava tuneliranje klijentskih PPP okvira, najčešće se zbog poboljšanja sigurnosti kombinira s IPsec protokolom na mrežnoj razini.
- IPsec - sam ili u kombinaciji s prethodnim protokolom
- SSL (Secure Sockets Layer) – protokol originalno razvijen u Netscape Communications, omogućava siguran pristup udaljenih ili čak mobilnih klijenata određenim aplikacijama.
- TLS (Transport Layer Security) – IETF standard, sličan SSLv3 standardu. Oba navedena standarda jako su prikladna i korištena jer ne zahtijevaju posebnu prilagodbu klijenata, s obzirom na to da se uglavnom koriste u web aplikacijama, a većina web preglednika ih podržava. Zbog toga se često koristi i termin web ili clientless VPN.

IPsec protokol je mrežni protokol, nastao kao rezultat rada na IPv6 protokolu, ali se koristi i na v4 protokolu i najčešći je izbor kod VPN mreža. Omogućuje klijentu ili usmjerniku autentifikaciju, provjeru integriteta i enkripciju IP paketa. Koriste se dva moguća načina rada:

- prijenosni način: enkriptiraju se samo podaci IP paketa (prijenosna razina i više), a iza IP zaglavljia se dodaje određeno IPsec zaglavlje (AH-Authentication Header ili ESP Encapsulating Security Payload) te se u IP zaglavljju mijenja oznaka protokola više razine u oznaku za IPsec umjesto npr. TCP.



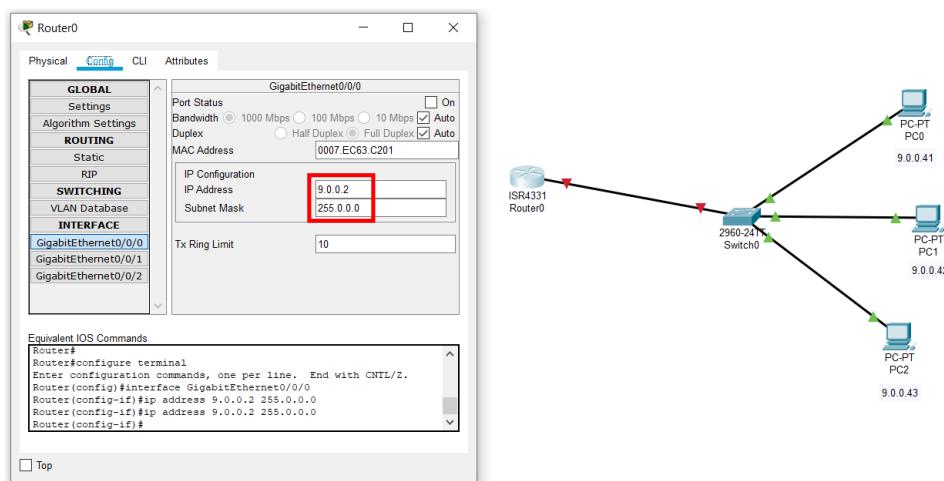
- tunelski način: kompletan IP paket, uključujući i zaglavlje, se enkriptira te mu se dodaje novo IP i IPsec zaglavlje (AH ili ESP).



PRIVATNE ADRESE

Svi mi u našim domovima koristimo privatne adrese (primjerice iz raspona 192.168.0.0 – 192.168.255.255) i te adrese se ne mogu koristiti na Internetu, već se koriste samo unutar naše privatne mreže. Kada se spojimo na Internet, naš kućni usmjernik ima ulogu NAT box-a, jer će on naše privatne adrese pretvoriti u javnu adresu. U prvom dijelu vježbe ćemo pokazati kako radi NAT protokol.

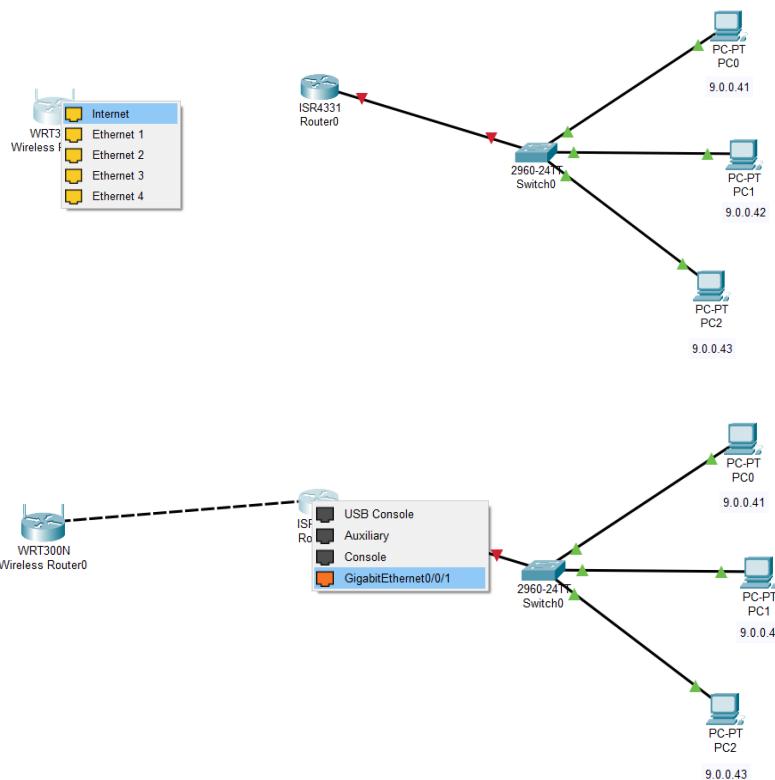
Za početak napravite jednu javnu mrežu gdje tri računala imaju javne IP adrese 9.0.0.41 do .43, a defaultni gateway im je svima 9.0.0.2 tj desna strana router-a. Postavite odgovarajuću IP adresu priključka na router-u, kako je prikazano na slici dolje:



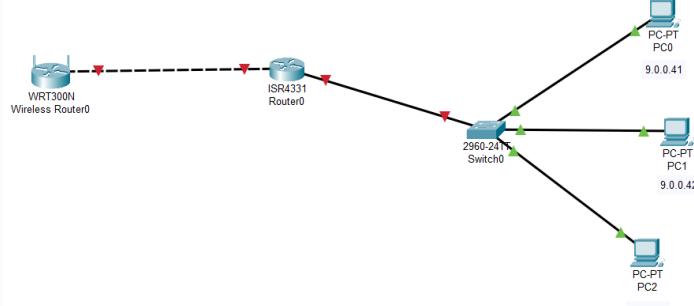
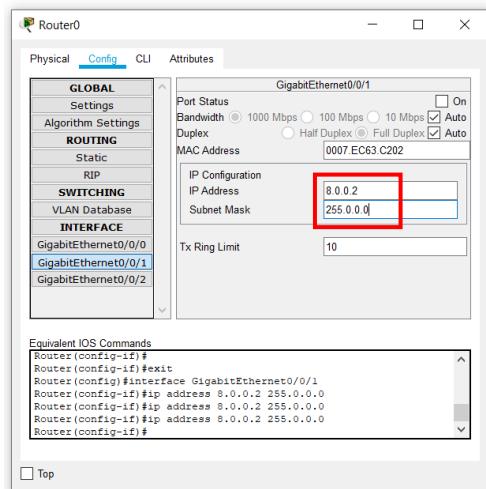
Kako bismo simulirali situaciju sličnu kao u našem domu, dodat ćemo jednu privatnu mrežu u našu mrežnu topologiju. Koristit ćemo Packet Tracer komponentu bežičnog routera Linksys WRT 300N iz grupe bežičnih uređaja (Wireless Devices) koja će predstavljati NAT box za našu privatnu mrežu.



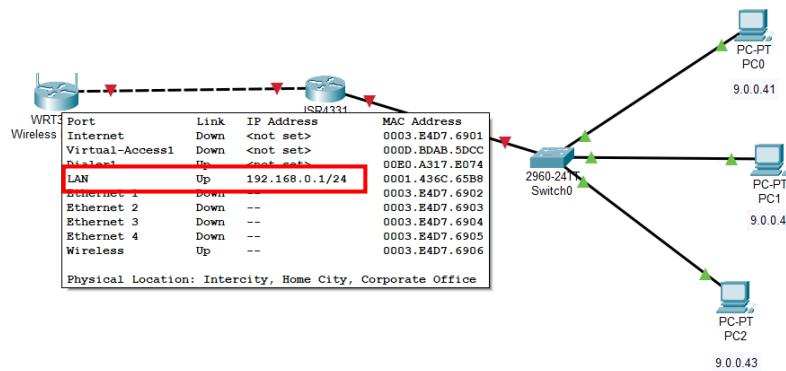
Potrebno je spojiti Internet (WAN) sučelje Linksys router-a sa dostupnim Gig0/0/1 sučeljem router-a Router0 (jer je na Gig0/0/0 već spojen switch). Postupak je prikazan na slikama dolje:



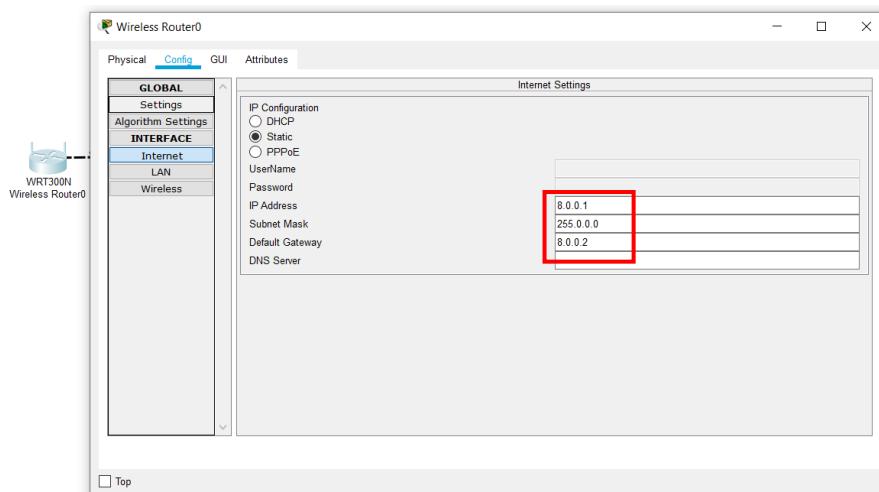
Postavimo javnu IP adresu sučelja Gig0/0/1 prema Linksys-u:



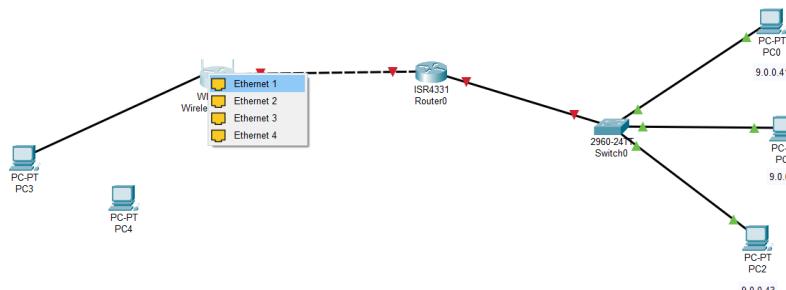
Konfigurirajmo Linksys router. Prvo, pogledajmo sučelja na Linksys-u (prođite mišem preko ikone uređaja):



Na gornjoj slici vidimo kako je sučelje prema privatnoj LAN mreži automatski postavljeno na IP adresu privatne mreže (192.168.0.1), dok IP adresa Internet sučelja prema javnoj mreži nije postavljena. Zato ćemo je postaviti na 8.0.0.1 (da desna strana Linksys-a bude u istoj mreži sa lijevom stranom uređaja Router0). Znači, na vanjskoj (desnoj) strani Linksys ima adresu 8.0.0.1, a njegov default gateway je 8.0.0.2 tj. lijeva strana od Router0. Dodavanje navedenih postavki prikazano je u nastavku. Kliknemo na Linksys i u Config tab-u odaberemo opciju staticke konfiguracije (ako već nije odabrana) i unesemo navedene podatke kao na slici:

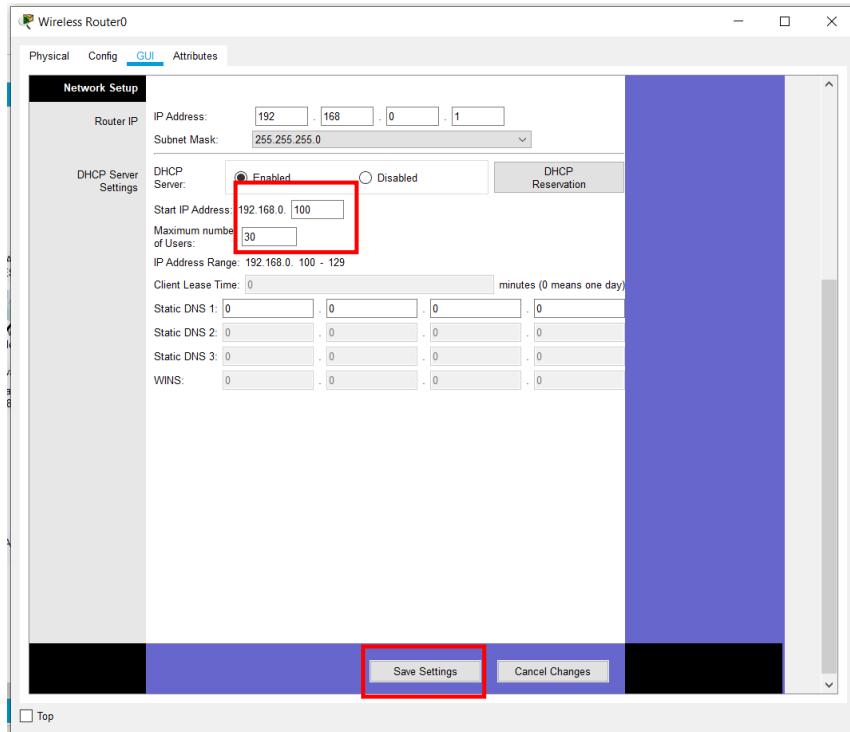


Dodajmo dva računala u mrežu i spojimo ih na Linksys router:

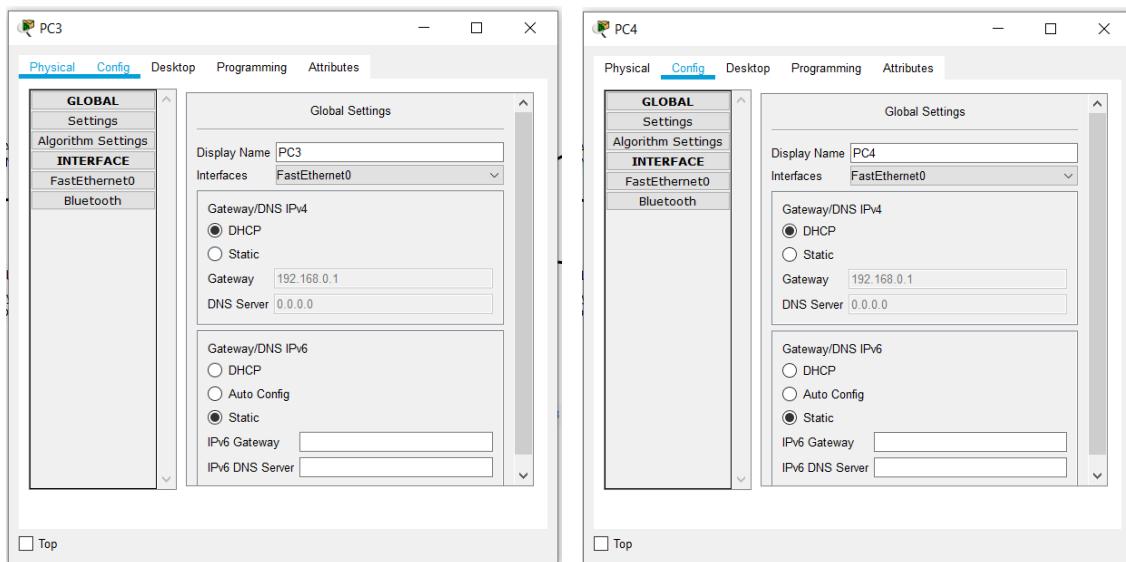


Postavimo DHCP protokol na računala PC3 i PC4 tako da računala automatski dobiju IP adresu kad se spoje u mrežu. Nije pravilo da se privatna IP adresa dodjeljuje automatski korištenjem DHCP protokola, nego se ona naravno može postaviti i staticki. Mi ćemo ovdje iskoristiti ovaj primjer da vidimo kako se postavlja DHCP. Također, default gateway na oba računala s lijeve strane Linksys-a je 192.168.0.1, a to je LAN strana Linksys-a (gdje je privatna mreža s privatnim adresama).

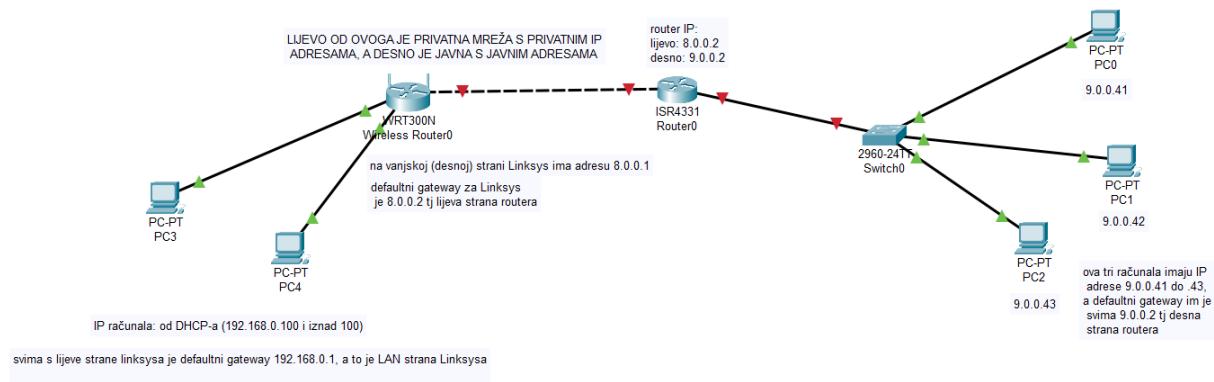
Postavimo DHCP na Linksys tako da računala automatski dobiju IP adresu (na primjer 192.168.0.100 i iznad 100). Kliknite na Linksys i u GUI tab-u pronađite i prilagodite DHCP postavke:



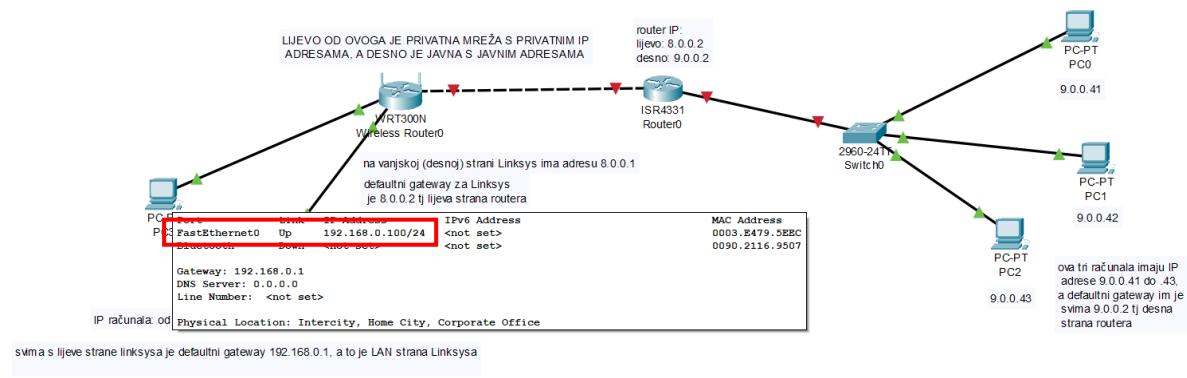
Postavimo DHCP na računala PC3 I PC4:



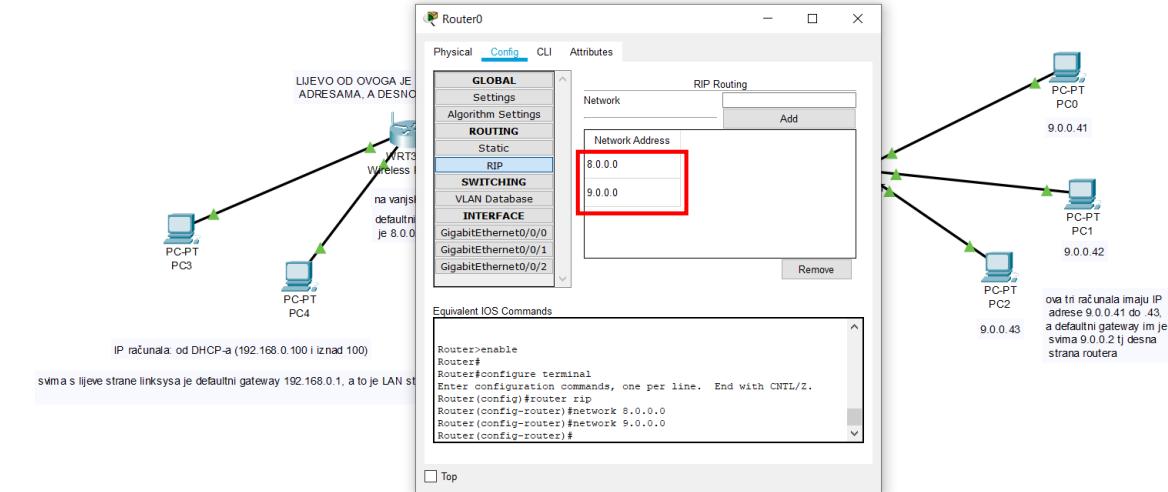
Naša mreža sada izgleda ovako:



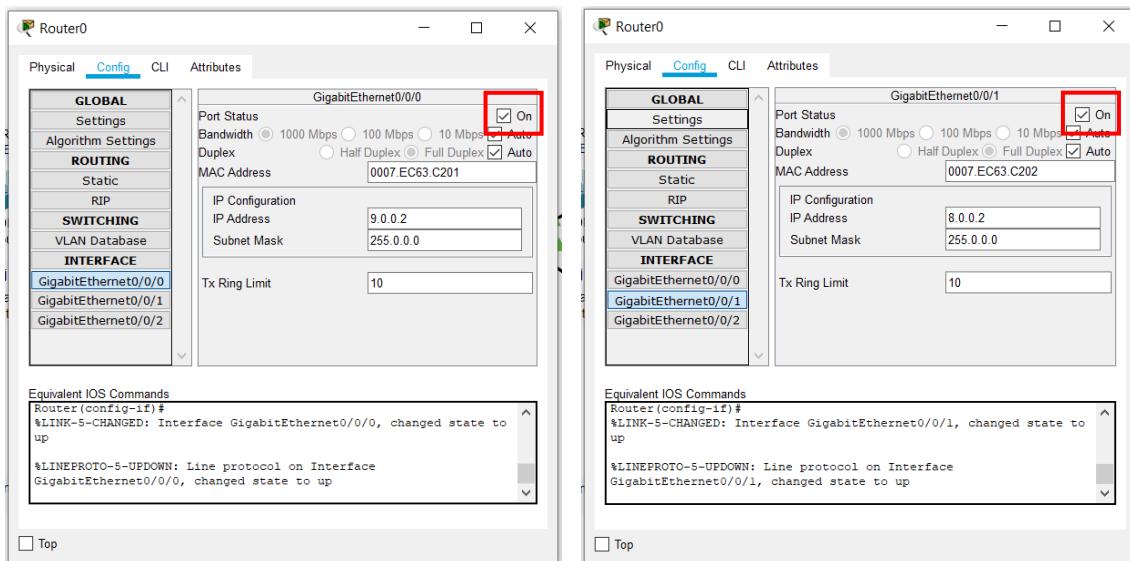
Prođite mišem preko oba računala PC3 i PC4 da vidimo jesu li računala stvarno dobila IP adresu preko DHCP-a. Primjer za PC3 je dan na slici:



Prije pinganja potrebno je uključiti RIP na uređaju Router0:



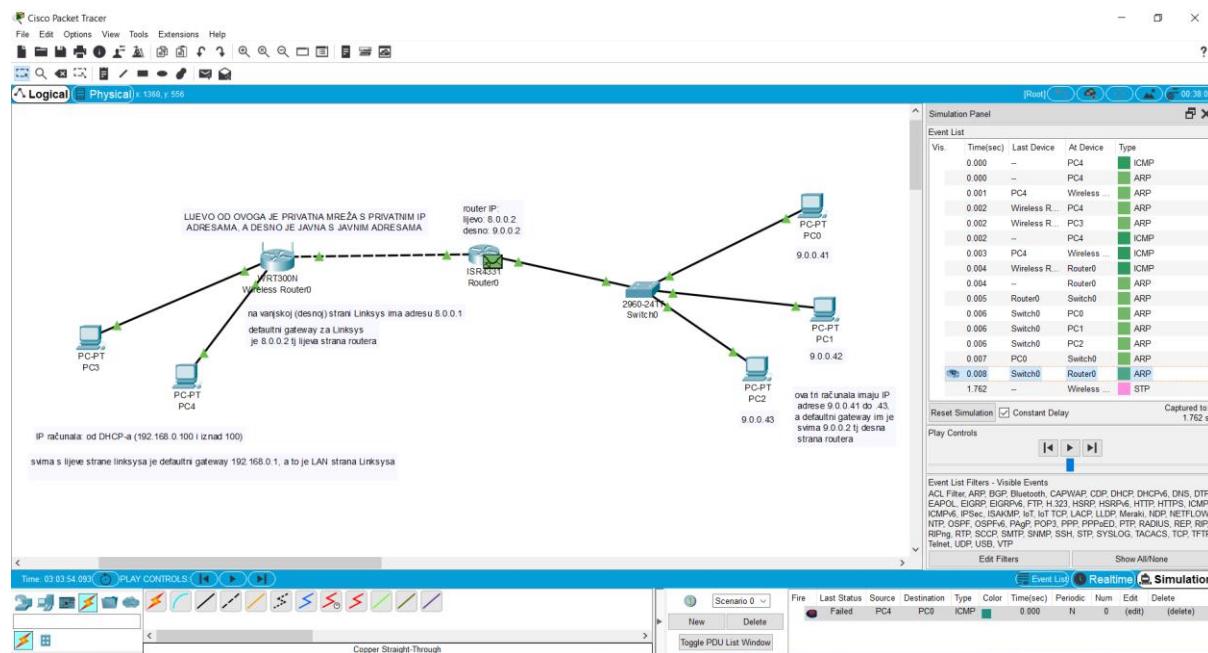
Ako su vam dijelovi mreže i dalje crveni, znači da još treba uključiti sučelja na uređaju Router0:



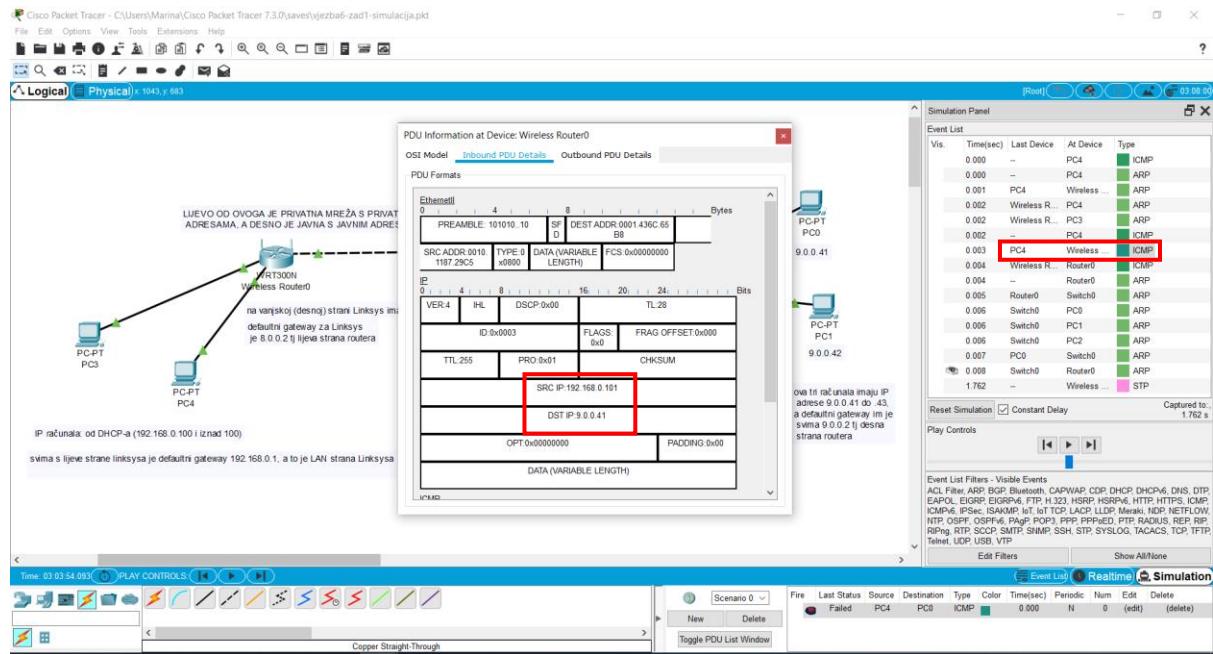
Mreža je sada spremna za pinganje. Provjerit ćemo komunikaciju od privatne prema javnoj mreži i od javne mreže prema privatnoj.

VERIFIKACIJA KOMUNIKACIJE (PRIVATNA MREŽA → JAVNA MREŽA)

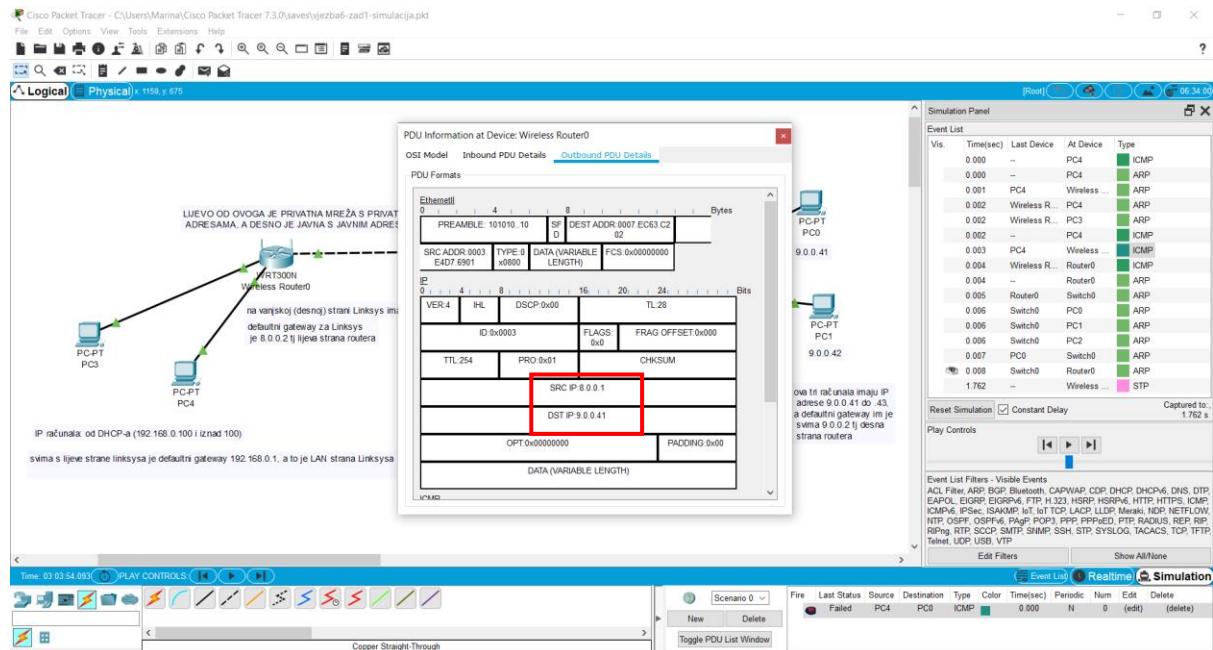
Pokušajmo pingati s nekoga od lijevih računala prema nekome od desnih računala u Simulacijskom načinu rada. Primjer pinganja sa PC4 na PC0 dan je na idućoj slici:



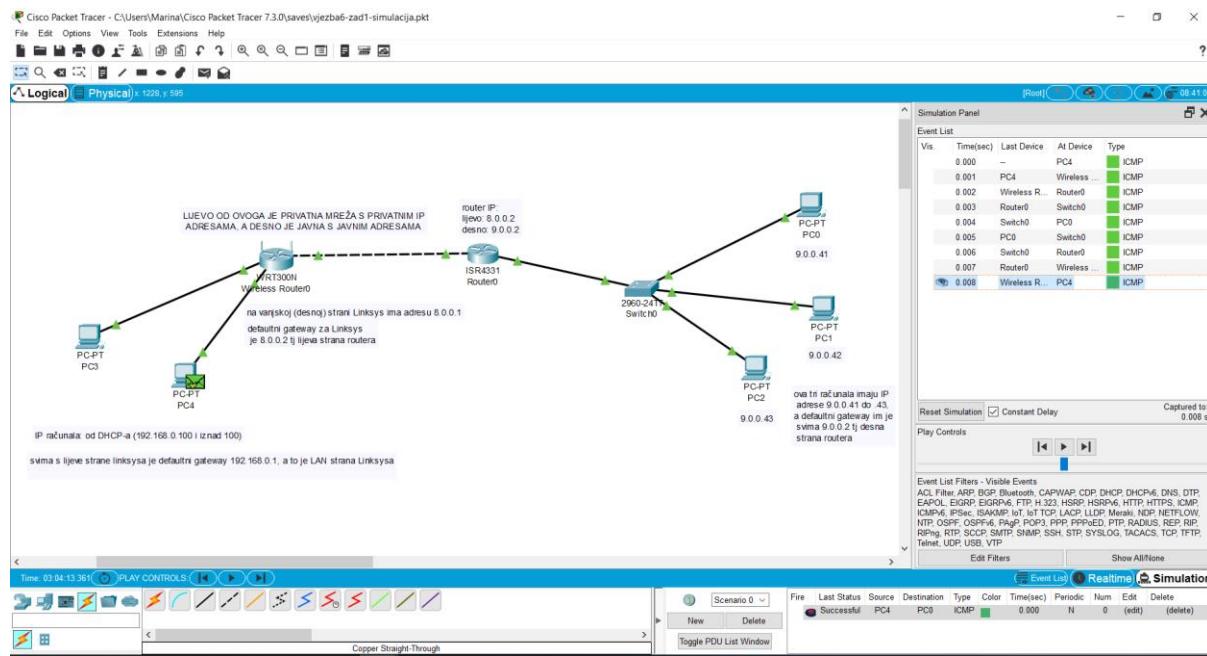
Pogledajte detalje prvog paketa kojeg PC4 šalje na Linksys i vidimo da paket ima privatnu adresu Source IP i javnu adresu Destination IP.



Pogledajte kako Linksys odradi NAT i kako se paket sada na izlazu iz privatne mreže predstavi vanjskom (desnom) adresom Linksys-a. Znači, zahvaljujući NAT protokolu, Linksys promjeni IP adresu paketa kad on izlazi iz privatne mreže.

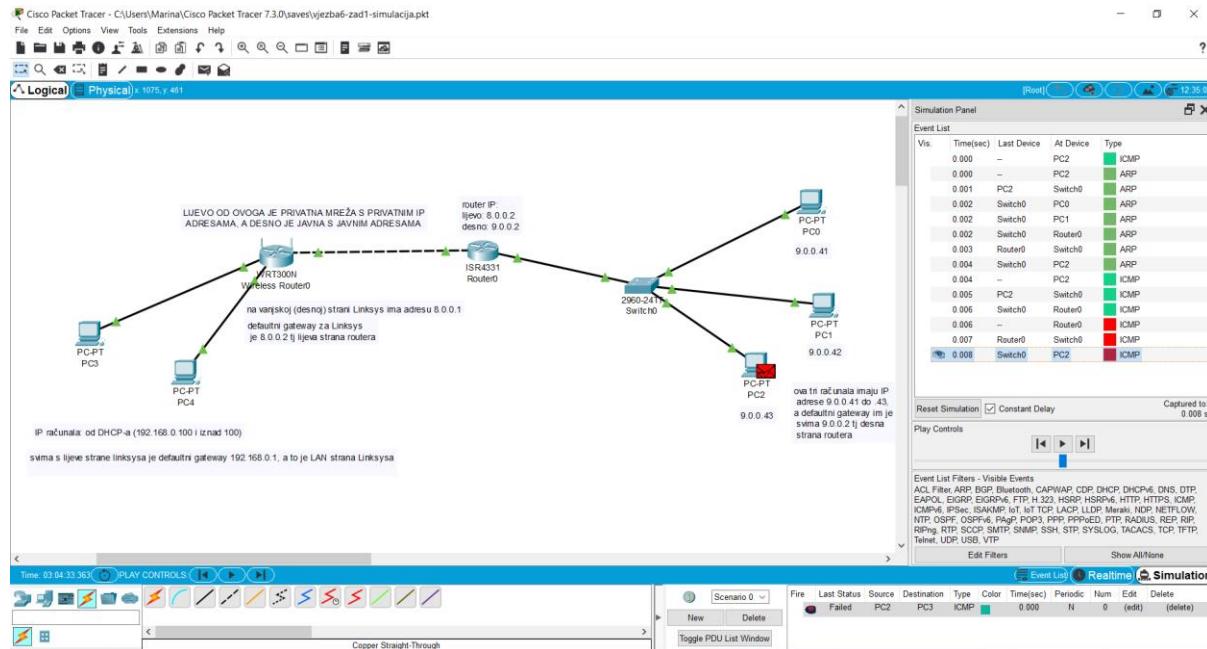


Komunikacija je „failed“ zato što je ovo tek dio u kojem Router0 doznaje preko ARP-a MAC adresu odredišta (računala PC0). Pošaljite novi ping od PC4 do PC0 kako bi prošao ICMP paket preko uređaja Router0:



VERIFIKACIJA KOMUNIKACIJE (JAVNA MREŽA → PRIVATNA MREŽA)

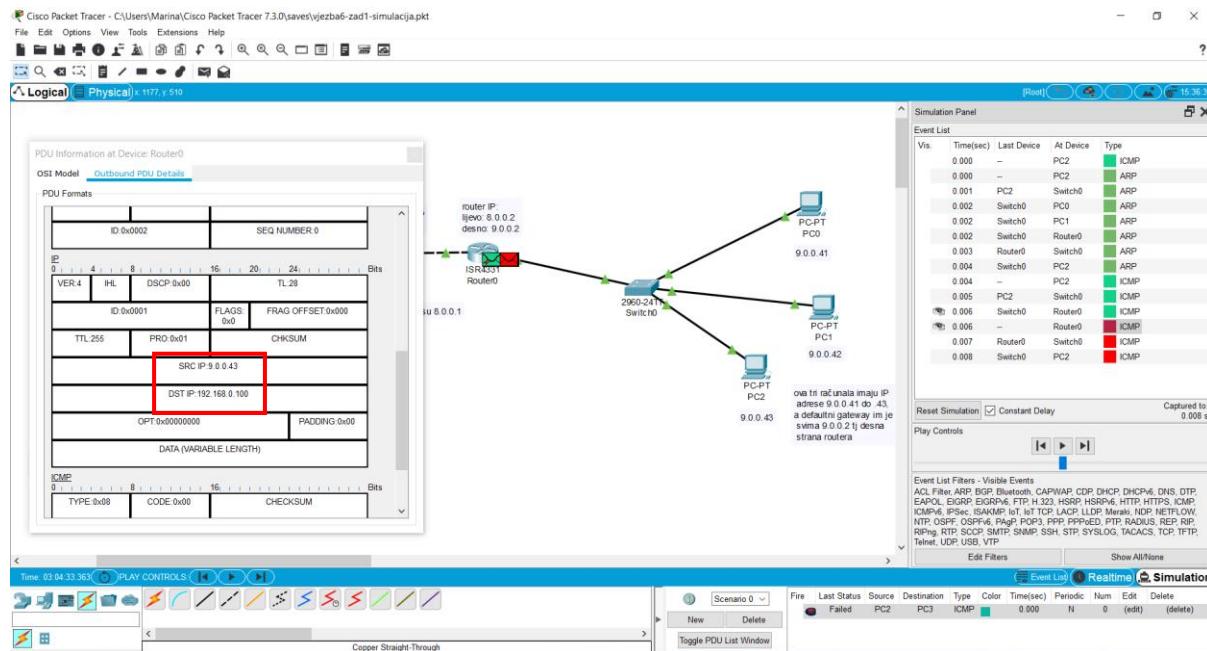
Vidjeli smo da je komunikacija uspješna jer je Linksys odradio NAT. Pokušajmo sada pingati u suprotnom smjeru, s nekoga od desnih računala na neko od lijevih. Primjer pinganja sa PC2 na PC3 je dan na slici:



Vidimo da komunikacija s javne na privatnu mrežu nije uspješna. Pratite putanju paketa u Simulacijskom načinu rada i odgovorite na pitanje:

Pitanje 1.
Gdje nastaje prekid u komunikaciji između javne i privatne mreže?

Prekid nastaje na uređaju Router0, jer će router vidjeti da odredište ima privatnu IP adresu i neće proslijedit takav paket (slika dolje).

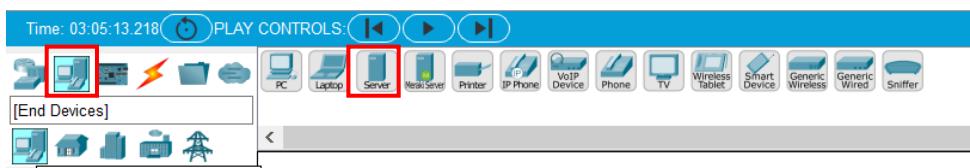


Spremite Packet Tracer topologiju pod nazivom **ime_prezime_zadatak1.pkt**.

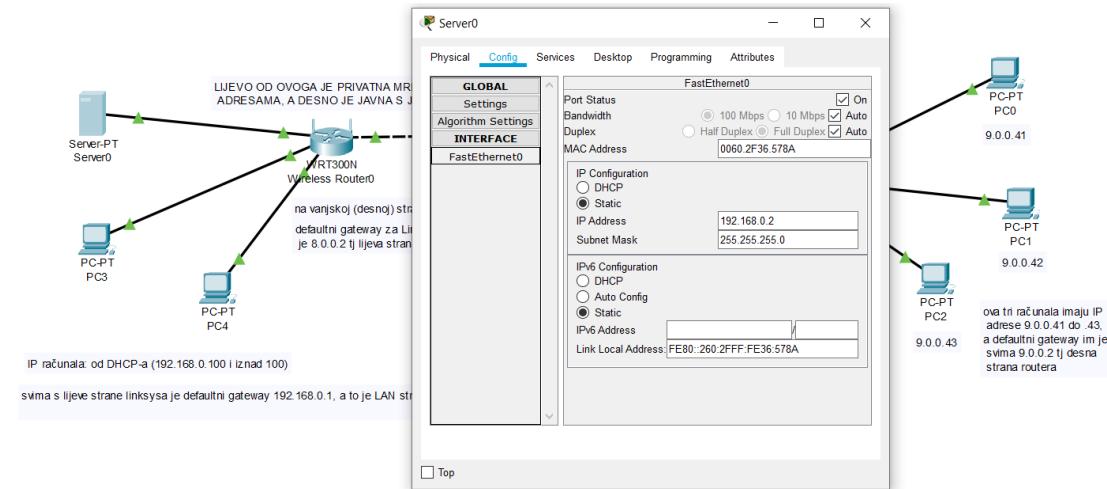
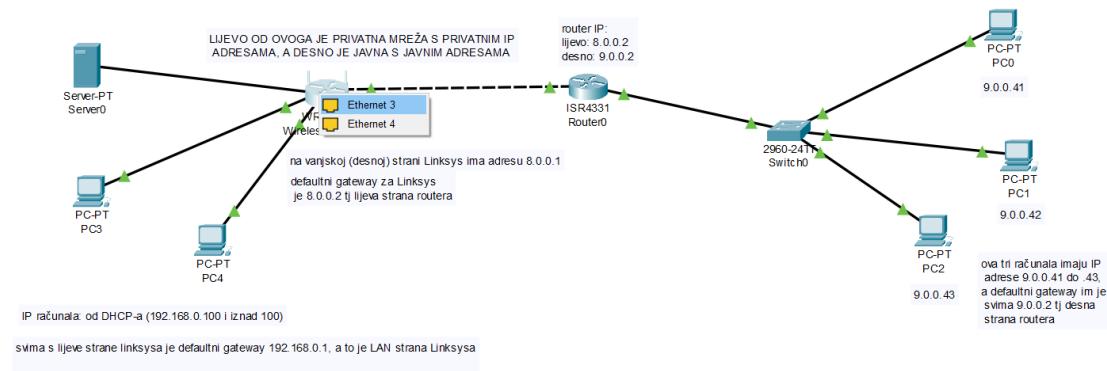
PORT MAPPING (PORT FORWARDING)

Port mapping je dio NAT-a koji preusmjerava komunikaciju s jedne kombinacije adrese i broja porta na drugu dok paketi prolaze kroz privatnu mrežu. Ova se tehnika najčešće koristi za omogućavanje usluga na host-u koji boravi u privatnoj (ili unutarnjoj) mreži host-ovima na suprotnoj strani (na vanjskoj ili javnoj mreži), preslikavanjem odredišne IP adrese i broja porta komunikacije na interni host [28]. Jedna od tipičnih primjena je pokretanje javnog HTTP servera unutar privatnog LAN-a i tu ćemo funkcionalnost pokazati u nastavku.

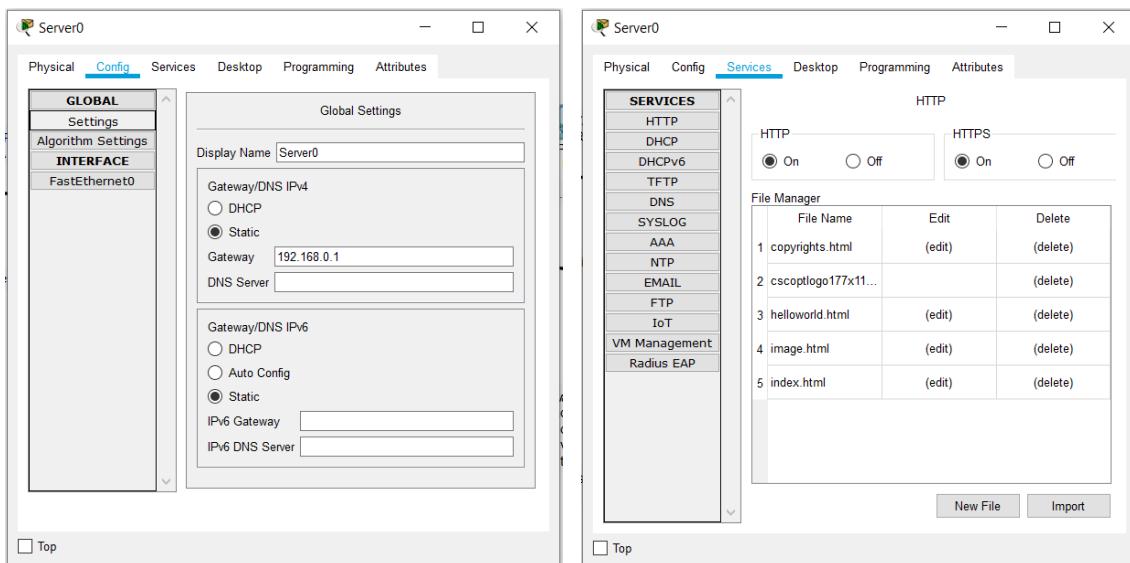
Odaberite server komponentu iz grupe krajnjih uređaja (End Devices):



Dodajte server u privatnu mrežu i dodijelite mu privatnu IP adresu (neka ona bude statička i to na primjer 192.168.0.2).



Default gateway za server je 192.168.0.1 (kao i za računala), a usluga neka ostane HTTP i HTTPS (to je po default-u tako u Packet Tracer-u):

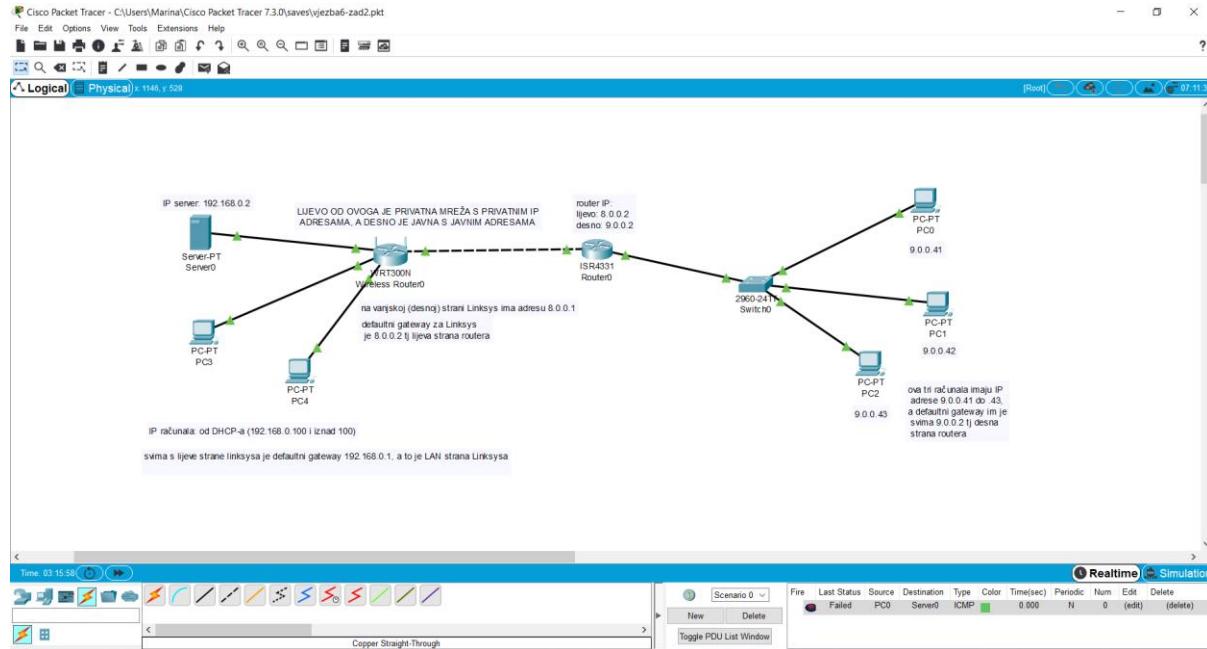


Sada imamo javni HTTP server na privatnoj mreži i pogledajmo da li mu računala sa desne (na javnoj mreži) mogu pristupiti.

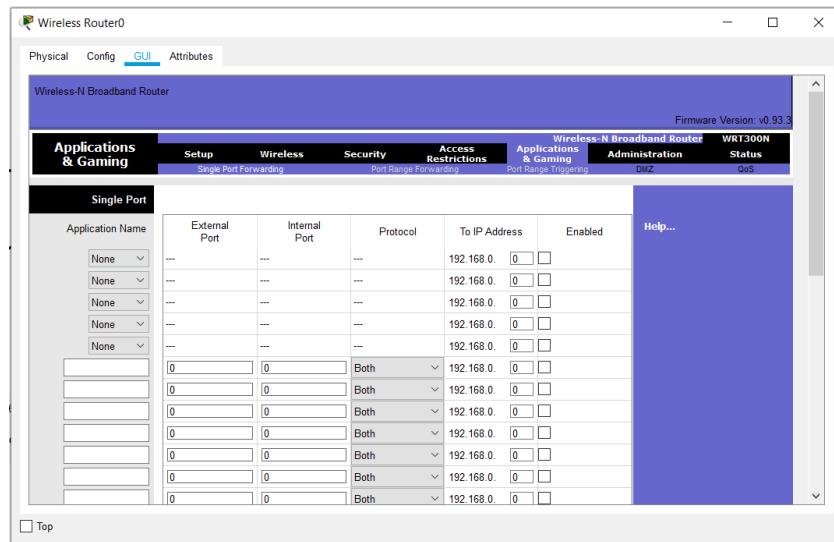
Pitanje 2.

Pokušajte pingati server sa računala PC0. Je li komunikacija uspješna?

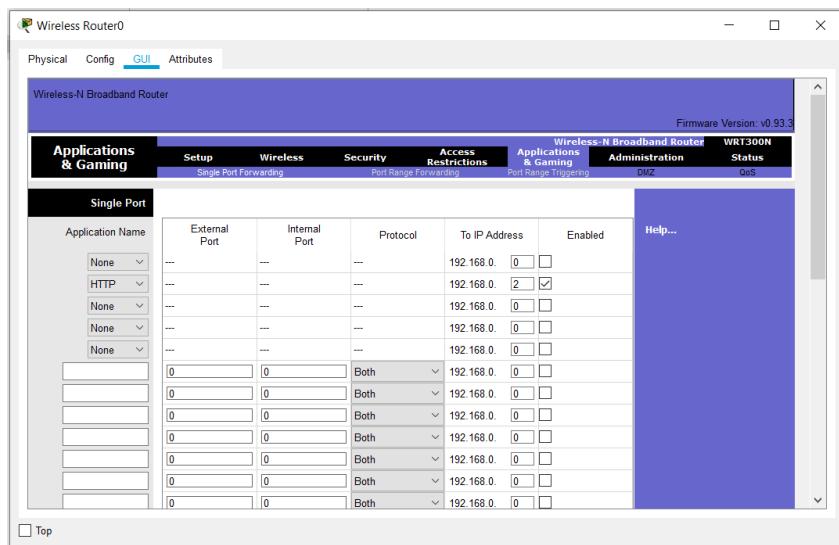
Ne, jer server (odredište) ima privatnu IP adresu (rezultat je na slici dolje).



Na Linksys-u je potrebno omogućiti port mapping → postaviti da se sav HTTP promet koji dođe na njegovu javnu adresu (8.0.0.1) proslijedi na privatnu adresu 192.168.0.2. Kliknite na Linksys i u GUI tab-u pod Applications pronađite opciju Single Port Forwarding:



Isključena su sva filtriranja po default-u, a mi ćemo uključiti samo filtriranje HTTP prometa, tako da radi samo ovaj port mapping i to na privatnu adresu servera:

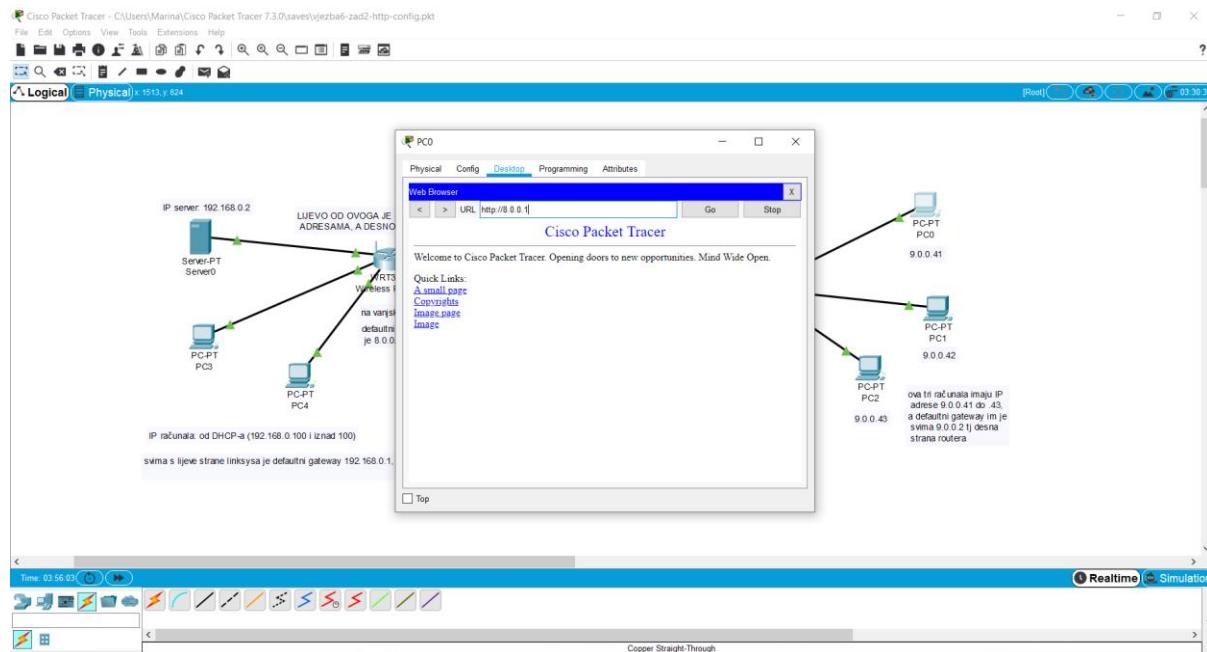


Ne zaboravite na dnu odabratи „Save Settings“ i zatvorite prozor.

Čak i ako i sada pokušamo izvanka sa nekog od desna tri računala pristupiti serveru preko njegove privatne IP adrese, to i dalje neće proći. **Provjerite navedeno pinganjem servera sa nekog od računala na javnoj mreži nakon što smo napravili port mapping!**

Međutim, port mapping nam omogućava da sada serveru možemo izvanka pristupiti preko aplikacije (preko web browser-a na računalu sa javne mreže).

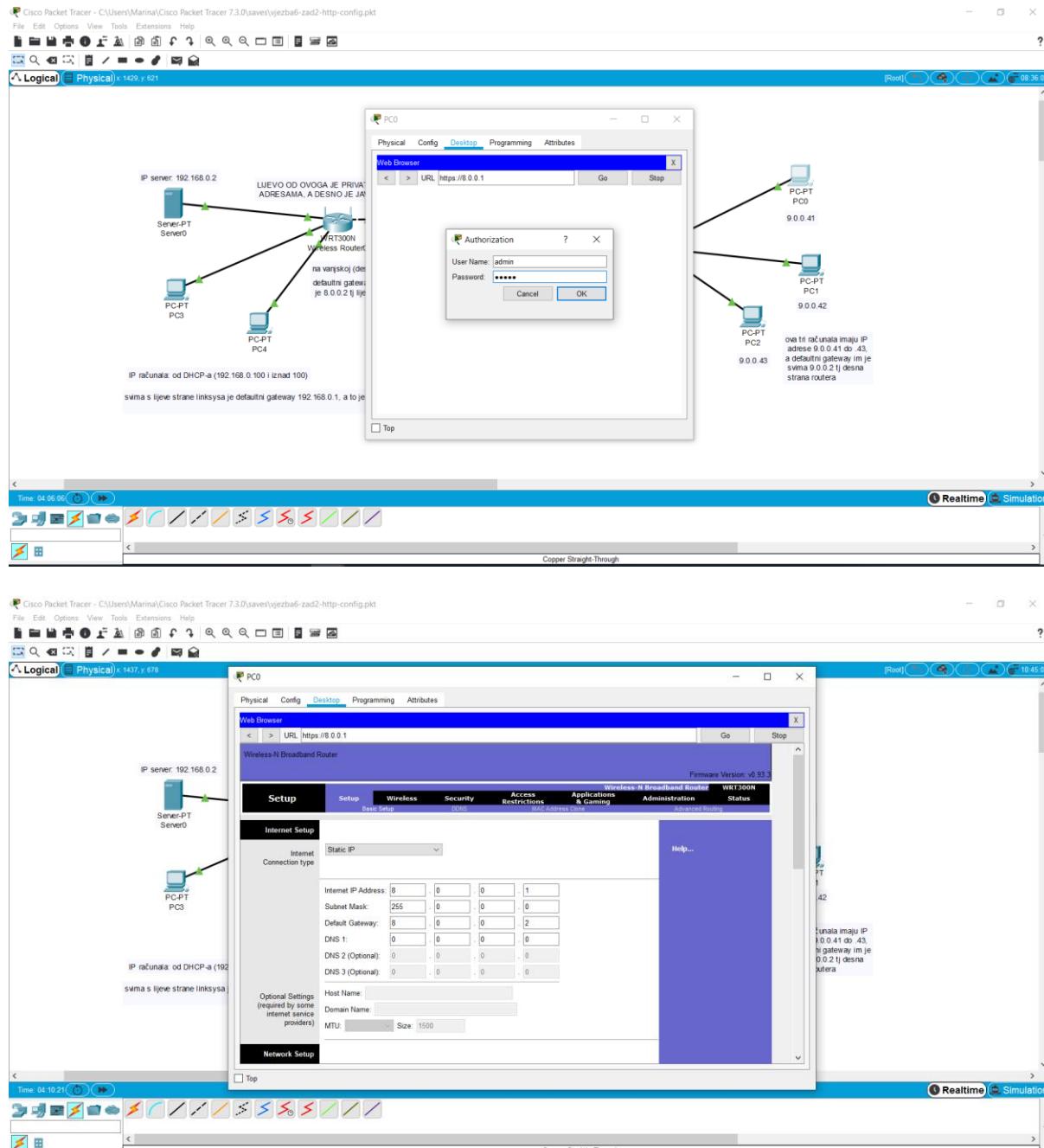
Recimo, nalazimo se na računalu PC0 i želimo dohvatiti web stranicu od HTTP servera koji je na privatnoj adresi. To možemo napraviti preko javne adrese od Linksys-a koju unesemo u web preglednik (unesite u pretraživač <http://8.0.0.1> i kliknite opciju „Go“):



Stranica je uspješno dohvaćena i to prolazi, iako server nije na toj adresi koju smo unijeli. Znači, kad s nekoga od desnih utipkamo u web browser <http://8.0.0.1>, onda će to doći do

servera iako je server na privatnoj IP adresi i uopće nema tu adresu koju smo utipkali u web browser (to je ustvari javna adresa Linksys-a). Ali, uspjelo je jer smo na Linksys-u postavili port mapping za HTTP promet.

Ako bi utipkali <https://8.0.0.1> onda ne idemo na web server, jer nije uključen port mapping za HTTPS, nego se u stvari spajamo na Linksys (npr. da bi ga remotely konfigurirali), pa nas pita username i password. Kada unesete default username i password od Packet Tracer-a (username: admin, password: admin), ulazimo u konfiguraciju na Linksys-u.



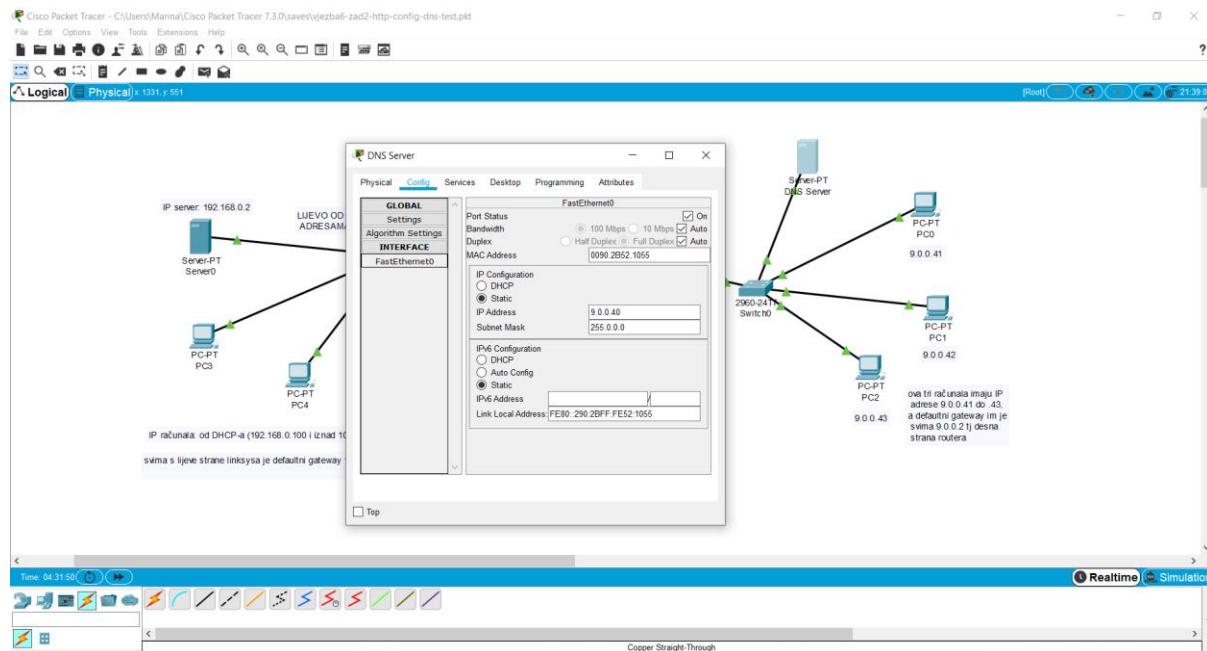
Pronađite gdje možemo promijeniti korisničko ime i lozinku za pristup na Linksys, i promijenite korisničko ime i password u „student“.

Spremite Packet Tracer topologiju pod nazivom **ime_prezime_zadatak2.pkt**.

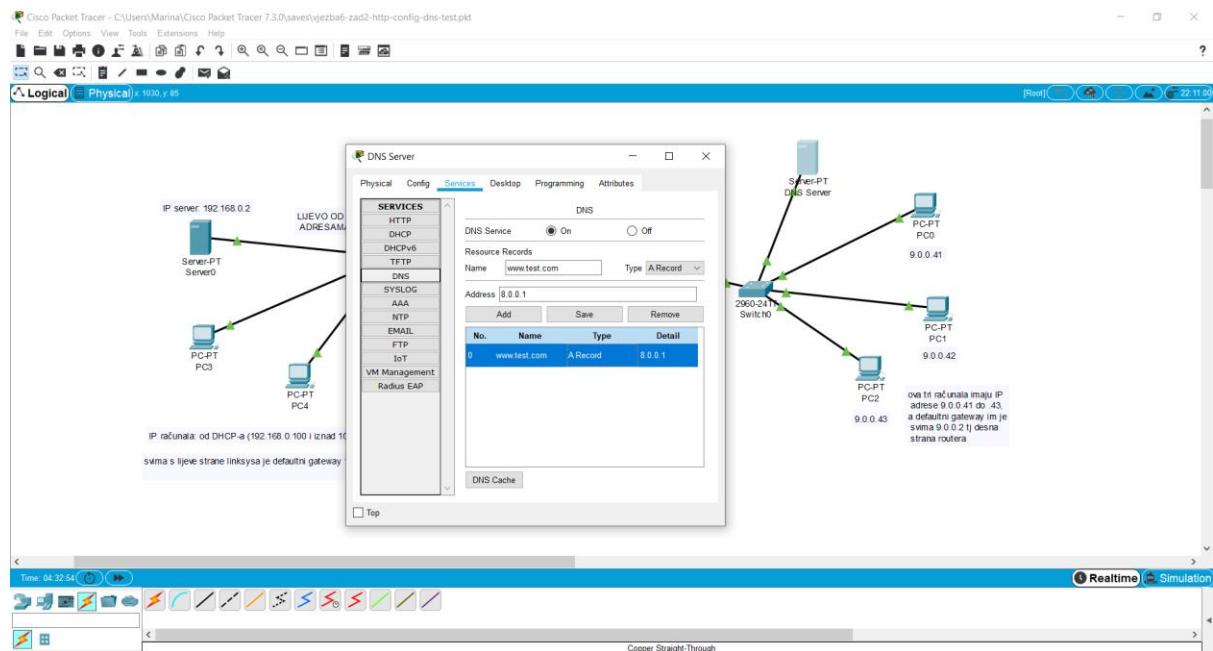
DNS SERVER

Iako nije direktno povezano sa današnjom vježbom, pokušajmo vidjeti kako možemo izbjegići direktno unošenje javne IP adrese u web preglednik, nego da se automatski dohvaća web stranica preko javne adrese kad unesemo „www.test.com“.

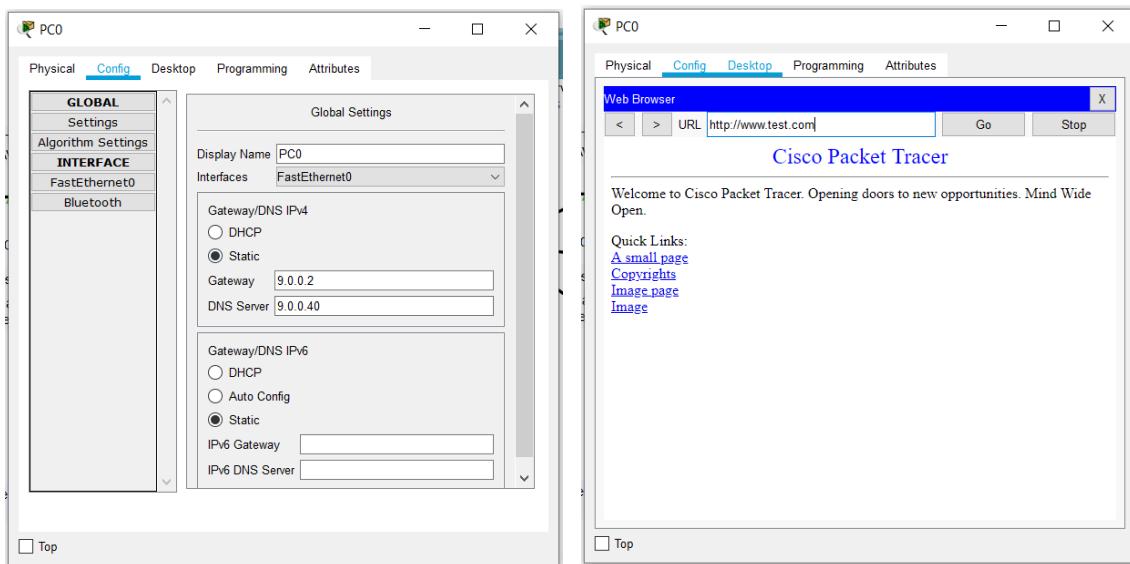
Naravno, potreban nam je DNS server kojem računalo PC0 treba pristupiti (radi jednostavnosti, postavimo DNS server na javnu mrežu). Zato, dodajte server i postavite mu IP adresu 9.0.0.40.



Pod tab-om Services odaberite DNS i uključite DNS uslugu odabirom opcije „On“. Pod name upišite naziv web stranice (www.test.com), a ispod javnu adresu servera (8.0.0.1). Nakon toga odaberite opciju „Add“. Sada će DNS automatski pronaći javnu adresu koju želimo dobiti (javna adresa od Linksys-a) čim unesemo u tražilicu bap tu web stranicu, a mi ne trebamo pamtiti adresu Linksys-a napamet.



Na računalu PC0 postavite DNS server i nakon toga pokušajte dohvatiti stranicu www.test.com sa računala PC0 u web pregledniku. Ona je uspješno dohvaćena.



Spremite Packet Tracer topologiju pod nazivom **ime_prezime_zadatak3.pkt**.

ZADACI ZA VJEŽBU 6 (PREDAJA IZVJEŠTAJA):

Kreirati sve tri mrežne topologije u alatu Packet Tracer kako je pokazano na vježbi. Predati sve konfiguracije pod nazivom:

- **ime_prezime_zadatak1.pkt**
- **ime_prezime_zadatak2.pkt**
- **ime_prezime_zadatak3.pkt**.

REFERENCE

- [1] C. NetAcademy. [Mrežno]. Available: <https://www.netacad.com/courses/packet-tracer/faq>.
- [2] C. NetAcademy, »Introduction to Packet Tracer,« [Mrežno]. Available: <https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer>.
- [3] »Download Packet Tracer,« [Mrežno]. Available: <https://www.computernetworkingnotes.com/ccna-study-guide/download-packet-tracer-for-windows-and-linux.html>.
- [4] R. Graziani, Cabrillo College, [Mrežno]. Available: http://calin.comm.pub.ro/Didactice/KN/Lab/KN_Lab_1.pdf. [Pokušaj pristupa 2 travanj 2021].
- [5] KDSM, Računalne mreže skripta sa e-learning portala, upute za laboratorijske vježbe, Split: Sveučilište u Splitu, FESB, 2010.
- [6] CISCO, »IP Addressing and Subnetting for New Users,« 10 August 2016. [Mrežno]. Available: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>. [Pokušaj pristupa 15 travanj 2021].
- [7] A. D. Costa, »How to Find the IP Address of Your Windows 10 PC,« 25 October 2019. [Mrežno]. Available: <https://www.groovypost.com/howto/find-windows-10-device-ip-address/>. [Pokušaj pristupa 14 travanj 2021].
- [8] Microsoft, »Dynamic Host Configuration Protocol (DHCP),« 8 July 2020. [Mrežno]. Available: <https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top>. [Pokušaj pristupa 14 travanj 2021].
- [9] M. Huc, »How to set a static IP address on Windows 10,« 18 January 2021. [Mrežno]. Available: <https://pureinfotech.com/set-static-ip-address-windows-10/>. [Pokušaj pristupa 14 travanj 2021].
- [10] D. El Mezeni, »Praktikum iz računara – 13E043PIR Osnovni načini povezivanja dva i više računara u jedinstveni komunikacioni sistem,« 2016. [Mrežno]. Available: http://tnt.etf.bg.ac.rs/~oe4pir/index_files/Vezbe/Materijali/Praktikum%20iz%20racunara%20-%20Lab1.pdf. [Pokušaj pristupa 15 travanj 2021].
- [11] »How to Connect two Networks using a router,« 17 May 2017. [Mrežno]. Available: https://www.youtube.com/watch?v=CiX30_JVyYQ. [Pokušaj pristupa 5 svibanj 2021].
- [12] M. Prvan, T. Kalinić i I. Andrun, »Virtualna lokalna mreža (VLAN) - Laboratorijska vježba za Praktikum iz računalnih mreža,« Prirodoslovno-matematički fakultet (PMF), Split, 2016.
- [13] T. Kalinić, »VLAN - seminarski rad za Praktikum iz računalnih mreža,« Prirodoslovno-matematički fakultet, Sveučilište u Splitu, Split, 2016.
- [14] CISCO, »Configuring VLAN Settings on the RV160 and RV260,« CISCO, 6 November 2019. [Mrežno]. Available: <https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv>

- series-small-business-routers/Configuring_VLAN_Settings_on_the_RV160_and_RV260.html. [Pokušaj pristupa 4 svibanj 2021].
- [15] CARNET, »Računalne mreže - Virtualna lokalna mreža (VLAN),« CARNET, 2017. [Mrežno]. Available: <https://sysportal.carnet.hr/node/671>. [Pokušaj pristupa 4 svibanj 2021].
- [16] E. Vallejo i E. Garcia, »Design of an introductory networking subject in advance of the European Higher Education Area: Challenges, experiences and open issues.,« *IEEE Conference: Education Engineering (EDUCON)*, svez. 10.1109/EDUCON.2010.5492354., pp. 1461 - 1468, 2010.
- [17] N. -. N. E. Info, »NEI Post 004 – A bit about 802.1q Trunk ports,« [Mrežno]. Available: <http://www.networkengineerinfo.com/2016/11/28/nei-post-004-a-bit-about-802-1q-trunk-ports/>. [Pokušaj pristupa 4 svibanj 2021].
- [18] N. Hope, »Virtual LAN (VLAN),« 2021. [Mrežno]. Available: <https://networkhope.in/virtual-lan/>. [Pokušaj pristupa 4 svibanj 2021].
- [19] E. & C. E. Project, »Dynamic routing | RIP version 1 (Routing information protocol) | Cisco Packet Tracer Tutorial 04,« 9 August 2019. [Mrežno]. Available: <https://www.youtube.com/watch?v=i83qrFq3BYQ>. [Pokušaj pristupa 9 svibanj 2021].
- [20] »Rutiranje,« [Mrežno]. Available: [http://es.elfak.ni.ac.rs/rmif/Prenos-podatak-februar-2011/Pre.-pod-%202010/Pdf-2010/Pogl-06-Rutiranje%20\(155-167\).pdf](http://es.elfak.ni.ac.rs/rmif/Prenos-podatak-februar-2011/Pre.-pod-%202010/Pdf-2010/Pogl-06-Rutiranje%20(155-167).pdf). [Pokušaj pristupa 9 svibanj 2021,].
- [21] J. Kurose i K. Ross, »Wireshark Lab: TCP,« u *Supplement to Computer Networking: A Top-Down Approach*, 6th ed., Upper Saddle River, NJ, Pearson Education, chrome-extension://oemmndcbldboiebfnladdacbfmadadm/http://mfatihas.it.student.pens.ac.id/Wireshark_TCP.pdf, 2013.
- [22] J. Kurose i K. Ross, »Computer Networking: A Top-Down Approach 8th Edition,« Pearson Education, 4 June 2020. [Mrežno]. Available: https://gaia.cs.umass.edu/kurose_ross/wireshark.htm. [Pokušaj pristupa 24 svibanj 2021].
- [23] J. F. Kurose i K. W. Ross, *Computer Networking: A Top-Down Approach*, 6th ed., UpperSaddle River, New Jersey: Pearson Education, 2013.
- [24] F. Zhang, »CSC 5991 Cyber Security Practice: Lab 1 - Packet Sniffing and Wireshark,« [Mrežno]. Available: <http://webpages.eng.wayne.edu/~fy8421/16sp-csc5991/labs/lab1-instruction.pdf>. [Pokušaj pristupa 25 svibanj 2021].
- [25] R. Deshpande, »TCP Proxies Chaining: Performance Implications,« 2013. [Mrežno]. Available: https://www.researchgate.net/publication/283497223_TCP_Proxies_Chaining_Performance_Implications/citations. [Pokušaj pristupa 27 svibanj 2021].
- [26] »Osnovi računarskih mreža 1 - Računarska tehnika i računarske komunikacije,« 2019/2020. [Mrežno]. Available: <https://www.rtrk.uns.ac.rs/sites/default/files/materijali/lab/Vezba%207.pdf>. [Pokušaj pristupa 25 svibanj 2021].

- [27] Wireshark, »Download Wireshark,« [Mrežno]. Available: <https://www.wireshark.org/download.html>. [Pokušaj pristupa 25 svibanj 2021].
- [28] Wikipedia, »Port forwarding,« 28 February 2021. [Mrežno]. Available: https://en.wikipedia.org/wiki/Port_forwarding. [Pokušaj pristupa 31 svibanj 2021].