Planiranje i izvedba lokalne mreže sa Cisco opremom

Čanađija, Marko

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni studij

PLANIRANJE I IZVEDBA LOKALNE MREŽE SA CISCO OPREMOM

Diplomski rad

Marko Čanađija

Osijek, 2019.

SADRŽAJ

1. UVOD 1

2. MREŽA 2

2.1. Tipovi mreža 2

2.2. Modeli Internetske infrastrukture 3

2.3. Internet Protokol (IP) 6

3. MREŽNA OPREMA 8

3.1. Preklopnik (*engl. Switch*) 8

3.2. Usmjerivač (*engl. Router*) 11

3.2.1. Usmjerivački protokoli 14

3.3. Višeslojni preklopnik (*engl. Multilayer Switch*) 17

3.4. Krajnji mrežni uređaji 18

4. KONFIGURACIJA CISCO MREŽNE OPREME 19

4.1. Cisco *Packet Tracer* 19

4.2. Osnovna konfiguracija uređaja 21

4.3. Konfiguracija preklopnika 24

4.4. Konfiguracija usmjerivača 26

5. REZULTATI I IZGLED MREŽE 33

5.1. Simulacija mreže u Packet Traceru 33

5.2. Lokalna mreža na stvarnoj Cisco opremi 40

5.3. Usporedba stvarne mreže i mreže u simulacijskom programu 45

6. ZAKLJUČAK 47

LITERATURA 49

SAŽETAK 52

ŽIVOTOPIS 54

PRILOZI 55

1. UVOD

Zahvaljujući napretku tehnologije, sve više uređaja radi preko Interneta, što je dovelo do kritične točke za proširenje i unaprjeđenje mogućnosti za komunikaciju tih uređaja. Globalizacija Interneta se dogodila toliko brzo koliko nitko nije mogao ni zamisliti i danas se koristi u svim granama društva - socijalnog, političkog, komercijalnog, kao i osobnog te je danas gotovo nezamislivo živjeti bez njega. Zbog naglog rasta korisnika i uređaja, potrebno je osigurati stabilnu i dovoljno brzu konekciju prema Internetu, ali i uređajima međusobno. To se može omogućiti konfiguracijom što većeg broja zasebnih lokalnih mreža koje se međusobno spajaju te imaju pristup Internetu jer, u slučaju da se nešto dogodi s jednom od tih mreža, ostale mreže mogu dalje normalno funkcionirati. Da bi se te lokalne mreže mogle konfigurirati, moraju postojati i globalne mreže i operateri koji omogućuju pristup Internetu, a tu na snagu stupa Cisco Systems koji je jedan od glavnih proizvođača mrežne opreme u svijetu - kako za korporacije, tako i za privatne korisnike.

U ovom radu se opisuju neke od fundamentalnih činjenica koje je nužno znati da bi se mogla konfigurirati funkcionalna mreža koja bi se mogla spojiti na Internet. U drugom poglavlju opisuju se neki od tipova mreža, modeli prema kojima se mreža kreira te IP (*engl. Internet Protocol*), u trećem poglavlju će se kratko opisati mrežna oprema koja je potrebna za realizaciju mreže. U četvrtom poglavlju upoznat će se *Packet Tracer,* računalni program u kojem se može napraviti simulacija mreže s Cisco opremom te će biti opisane osnovne konfiguracije preklopnika (*engl. Switch)* i usmjerivača (*engl. Router)*. Unutar petog poglavlja će biti analizirani rezultati mreže napravljene u simulaciji i konfiguracije stvarne mreže na Cisco opremi te mala usporedba tih dviju konfiguracija. Posljednje poglavlje sadrži zaključak ovog rada.

2. MREŽA

Kako bi se mogla realizirati jedna lokalna mreža, potrebno je poznavanje nekih temeljnih pojmova vezanih uz mrežu. Takvo znanje je neophodno kod planiranja mreže da bi se konfiguracija iste napravila što bolje, odnosno optimalnije za daljnji rad i održavanje. Računalna mreža je skup međusobno povezanih uređaja gdje je omogućena komunikacija jednih s drugima. Najjednostavnija mreža se sastoji od dvaju međusobno povezanih računala, dok je najveća mreža Internet.

2.1. Tipovi mreža

Mrežna infrastruktura može znatno varirati, ovisno o veličini područja koje pokriva, broju spojenih korisnika, broju i vrsti dostupnih usluga i prostoru gdje je mreža dostupna. Prema tome, postoje dvije najpoznatije vrste mrežne infrastrukture: lokalna mreža ili kraće LAN (*engl. Local Area Network*) i globalna mreža ili WAN (*engl. Wide Area Network*). Postoje ostale vrste koje nisu toliko rasprostranjene, a to su gradska mreža ili MAN (*engl. Metropolitan Area Network*), bežični LAN ili WLAN (*engl. Wireless LAN*) i mreža za pohranu ili SAN (*engl. Storage Area Network*). Posebna mrežna infrastruktura koja je zapravo skup ranije nabrojanih je Internet.

LAN je mrežna infrastruktura koja omogućava pristup korisnicima i krajnjim uređajima na malom geografskom području, kao što su organizacije, stambeni prostori (kuće, stanovi, zgrade) ili male poslovne mreže u vlasništvu pojedinca ili IT odjela. LAN-om najčešće upravlja pojedinac ili jedna organizacija koji vode kontrolu o sigurnosti i provode kontrolu na razini mreže. Kako se takve mreže nalaze na ograničenom području, gdje nije velik broj uređaja spojen, pružaju se prilično velike brzine prijenosa podataka.

WAN mreže su mrežne infrastrukture koje pokrivaju široka geografska područja, koje zapravo čine velik broj povezanih LAN mreža. Te mreže u većini slučajeva održavaju operateri tkz. SP (*engl. Service Providers*) i Internet operateri odnosno ISP (*engl. Internet Service Providers*). WAN međusobno povezuje LAN mreže preko širokog geografskog područja, kao što su gradovi, sela, države ili kontinenti. WAN-om većinom upravlja više operatera te su, zbog udaljenosti između LAN-ova, brzine prijenosa male u odnosu na udaljenosti između uređaja u LAN mreži.

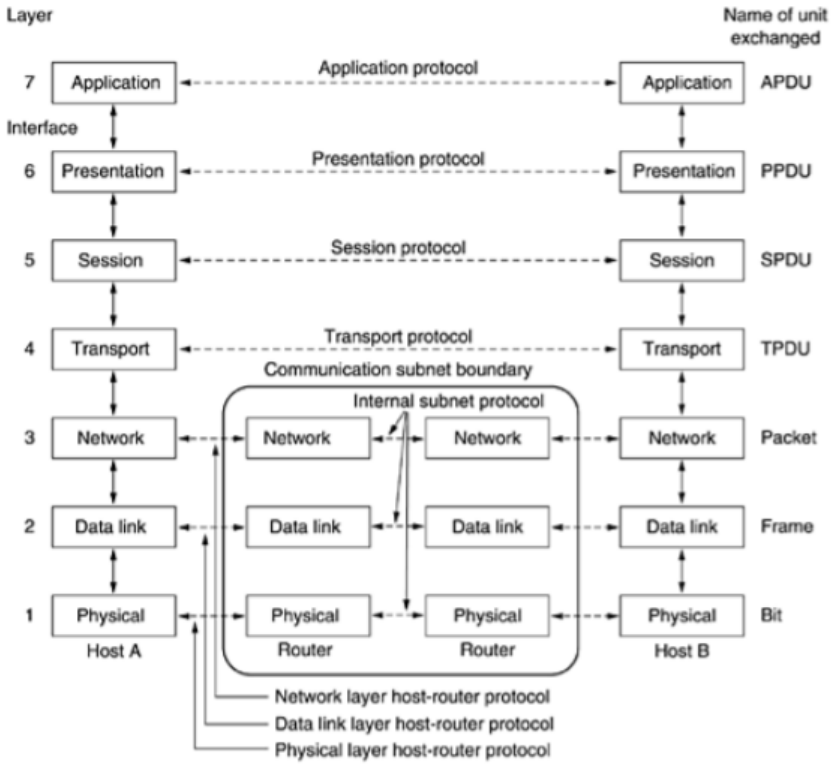
Internet je skup svih međusobno povezanih LAN i WAN mreža koje čine jednu globalnu mrežu koja nije ni u čijem vlasništvu. Da bi se osigurala efektivna komunikacija preko raznih infrastruktura, zahtijeva se primjena dosljednih i uobičajenih tehnologija i standarda, kao i

suradnja mnogih agencija za upravljanje mrežom. Postoje organizacije koje su razvijene s namjerom da pomažu održavanju strukture i standardizaciji procesa i Internet protokola. Neke od tih organizacija su IETF (*Internet Engineering Task Force*), ICANN (*Internet Corporation for Assigned Names and Numbers*) te IAB (*Internet Architecture Board*). O njima više na [1], [2] i [3].

2.2. Modeli Internetske infrastrukture

Razvojem računalne mreže, Interneta, zbog lakšeg razumijevanja, stručnjaci su razvili dva modela mrežne arhitekture koji slojevito opisuju princip rada Interneta i protokole koji se pojavljuju na svakom sloju. Prvi razvijeni model je OSI referentni model (*engl. Open Systems Interconnection Reference Model*) na kojem je kasnije razvijen TCP/IP model (*engl. Transmission Control Protocol/Internet Protocol*). Danas se na principu TCP/IP modela i protokola bazira Internet i skoro svaki veliki mrežni operativni sustav, dok se OSI model rijetko gdje koristi.

OSI referentni model je baziran na prijedlogu razvoja koji je predložen od ISO organizacije (*International Standards Organization*). To je prvi korak prema internacionalnoj standardizaciji protokola i različitih slojeva. OSI model sastoji se od sedam slojeva: fizičkog sloja, podatkovnog sloja, mrežnog sloja, transportnog sloja, sloja sesije, prezentacijskog sloja i aplikacijskog sloja, a svaki sloj ima svoju funkciju, usluge i protokole koje koristi u komunikaciji. Svih sedam slojeva radi kao cjelina te neki podatak ili informacija prolazi redom kroz svaki sloj, no razlika je u smjeru kojim ide, a to ovisi o tome prima li se podatak ili se šalje. To se može vidjeti na slici 2.1.

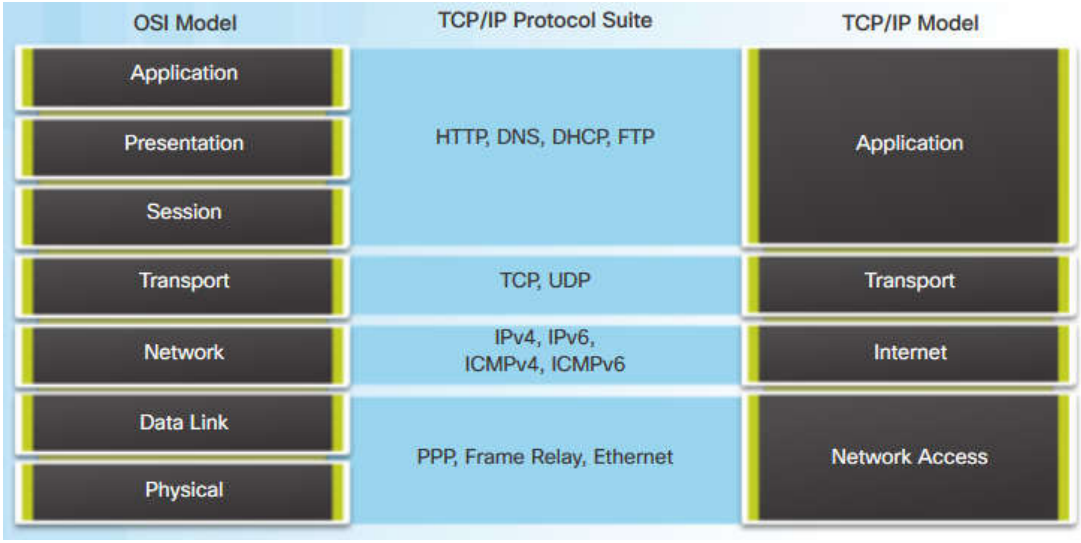


Sl.2.1. *Referentni OSI model, [4]*

Fizički sloj zadužen je za slanje i primanje bitova preko komunikacijskog kanala i u njega ubrajamo fizičke komponente kao što su konektori, naponske i strujne razine i mediji za prijenos. Glavni zadatak podatkovnog sloja je kontrolirati prijenos podataka između medija i pretvorba bitova koji se dijele u okvire koji moraju stići do mrežnog sloja bez ikakvih grešaka. U mrežnom sloju okviri se pretvaraju u pakete koji u sebi sadrže informacije o rutama, što i je zadaća mrežnog sloja, odnosno odabrati najbolju rutu za prijenos podatka kroz mrežu i pružiti uslugu povezanosti. Četvrti ili transportni sloj ima zadaću prenositi podatke na pouzdan način između uređaja, a ako dođe do pogreške - tu pogrešku otkriti i ako je moguće, ispraviti. Transportni sloj ima još jednu funkciju, a to je odabrati koji od dvaju tipova protokola koristiti za slanje podataka: TCP (*Transmission Control Protocol*) ili UDP (*User Datagram Protocol*). Glavne razlike između tih dvaju protokola su u važnosti redoslijeda dolaska paketa, veličini zaglavlja, pouzdanosti, sigurnost... Idući sloj je sloj sesije koji ima funkciju upravljanja, uspostavljanja i prekida veze između dvaju krajnjih uređaja te sinkronizacije prezentacijskih slojeva dvaju uređaja, kao i kontrolu kvalitete usluga. Prezentacijski sloj se bavi sintaksom i semantikom prenesenih informacija da bi se mogli izmjenjivati podatci između uređaja koji imaju različite reprezentacije podataka.

Struktura tih podataka za razmjenu može se definirati na apstraktni način, a zadaća prezentacijskog sloja je upravljati tim apstraktnim strukturama podataka. Posljednji, najviši sloj je aplikacijski, a sadrži različite protokole kojima se koriste korisnici - to je jedini sloj koji ne pruža usluge nižim slojevima, već aplikacijama koje nisu izričito povezane s modelima. Neki od tih protokola su POP *(Post Office Protocol*), FTP (*File Transfer Protocol*), SMTP (*Simple Mail Transfer Protoco*l), HTTP *(HyperText Transfer Protocol*), IMAP (*Internet Message Access Protocol*)… Detaljnije opisani slojevi i protokoli koji se koriste unutar njih mogu se pronaći u [5], [6] i [7].

TCP/IP model je ustvari unaprijeđeni OSI model, odnosno, kako i u većini stvari, tako se i ovdje teorija i praksa razlikuju, pa je TCP/IP zapravo prilagođeni OSI referentni model na kojem se bazira cijeli Internet. Ovaj model je dobio ime po dvama najbitnijim protokolima, a to su TCP i IP protokol. Kako je TCP/IP model isto slojeviti model, najveća razlika između OSI i TCP/IP je u broju slojeva. Dok je kod OSI sedam slojeva, TCP/IP se sastoji od četiriju slojeva, a to su aplikacijski sloj, transportni sloj, Internet sloj i sloj podatkovne mreže. Kako se u OSI modelu komunikacija mogla vršiti samo između dvaju susjednih slojeva, kod TCP/IP modela prvo su bili protokoli prema kojima je napravljen model, za razliku od OSI modela kod kojega su neki protokoli tek naknadno razvijeni.



Sl. 2.2. *Usporedba slojeva OSI i TCP/IP modela [8]*

Prvi sloj ili sloj podatkovne mreže služi za kontrolu uređaja i medija koji čine mrežu, a to se odnosi na sve potrebne procedure za pristup medijima i slanje podataka kroz mrežu. Za to su u OSI modelu bila zadužena prva dva sloja, odnosno fizički i podatkovni.

Drugi sloj je Internet sloj koji je izravno povezan s mrežnim slojem iz OSI modela koji određuje najbolju rutu koristeći protokole za adresiranje poruka za slanje kroz mrežu. Transportni sloj, odnosno treći sloj u TCP/IP modelu opisuje usluge i funkcije koje osiguravaju pouzdanu isporuku podataka između izvora i odredišta te omogućuje komunikaciju između raznih uređaja preko različitih vrsta mreža. Ovaj sloj ima isti naziv i funkciju kao četvrti sloj u OSI modelu. Najviši sloj kod TCP/IP modela je aplikacijski sloj koji obuhvaća zadnja tri sloja iz OSI modela, a sadrži velik broj protokola od kojih svaki ima neku specifičnu funkciju te razne računalne aplikacije kojima se služe krajnji korisnici, a koji su izravno povezani s transportnim slojem, za razliku od ISO modela. Detaljnije na [7], [8] i [9].

2.3. Internet Protokol (IP)

Internet protokol je glavni protokol na Internet sloju te jedan od najvažnijih protokola kod TCP/IP modela, a zadužen je za određivanje izvorišne i odredišne IP adrese za svaki paket. Postoje dvije vrste IP adresa, a to su IPv4 (Internet Protokol verzije 4) i IPv6 (Internet Protokol verzije 6). Najvažnija razlika je u duljini i načinu zapisa. IPv4 je 32 bitni broj koji se zapisuje u decimalnom obliku zbog jednostavnosti, dok je IPv6 128 bitni broj koji se zapisuje u heksadekadskom obliku. Glavni razlog zbog kojeg postoje dvije vrste je to što broj slobodnih adresa IPv4 postaje sve manji pa se zbog toga sve više koristi IPv6 koji ima još neke dodatne funkcije koje olakšavaju adresiranje i povećavaju sigurnost. Više o tome u [10]. Zbog još uvijek veće prisutnosti IPv4 u današnjici, u ovom radu će se više govoriti o IPv4.

Sl. 2.3. *Primjer IPv4 u decimalnom i binarnom obliku [11]*

Mrežni administrator pridjeljuje svakom hostu njegovu jedinstvenu IP adresu, bez obzira je li to fizička mrežna kartica ili mrežni uređaj, čime IP adresa predstavlja logičku adresu kojom se može pristupiti nekom hostu negdje u mreži. IP adresa se sastoji od mrežnog i računalnog dijela. Mrežni dio predstavlja broj bitova koji identificira IP adresu mreže, dok računalni dio predstavlja IP adresu računala ili nekog drugog uređaja. Postoji nekoliko klasa IP adresa (klase od A do E), a razlikuju se po tome koliko bitova predstavlja mrežni dio, a koliko bitova predstavlja računalni dio. To se odnosi na broj uređaja koji se mogu spojiti u jednoj mreži.

Broj koji predstavlja koliko bitova je mrežni dio, a koliko računalni dio naziva se maska podmreže (*engl. subnet mask*) te može biti zapisan u binarnom ili decimalnom broju, koji uvijek ide zajedno s IP adresom mreže, a može se vidjeti na sl. 2.4.

Class	*IP address range (1st Octet)*	*Network Mask*	*Prefix*	*Number of Networks*	*Number of Hosts*
A	1. - 127.	255.0.0.0	/8	125	16,777,214
B	128. - 191.	255.255.0.0	/16	16,382	65,534
C	192. - 223.	255.255.255.0	/24	2,097,150	254
D	224. - 239.	Multicast addresses			
E	240. - 254.	Restricted/Experimental			

Sl. 2.4. *Klase IP adresa, njihovi rasponi i mrežne maske [12]*

Postoje tri vrste IP adresa: IP adresa koja predstavlja mrežu i uvijek se piše zajedno s maskom, drugi tip je IP adresa hosta, koja predstavlja IP adresu točno jednog uređaja, a posljednja vrsta IP adresa je *broadcast* koju predstavlja zadnja IP adresa u mreži, a ima posebnu funkciju koja će biti razjašnjena u nastavku ovog rada. Svaka klasa IP adresa ima svoj raspon, unutar svake klase postoje dvije vrste adresa, a to su privatne i javne adrese, što znači da je unutar svake klase dio rezerviran za privatne adrese, a dio za javne adrese. Ovakav način podjele adresa uveden je zbog nedostatka IPv4 pa se s ovakvim načinom korištenja podmreža znatno povećao kapacitet adresa IPv4, npr. neko kućanstvo ili kompanija od operatera dobije jednu javnu IP adresu preko koje komunicira s vanjskim svijetom, a unutar te kompanije, koristeći privatne adrese, može se spojiti još mnogo uređaja ovisno o klasi, koji također komuniciraju s vanjskim svijetom preko javne IP adrese, ali da bi se komunikacija između te dvije vrste IP adresa mogla realizirati, mora postojati uređaj koji usmjerava pakete do željenog uređaja izvan te mreže. Taj uređaj naziva se *Router* koji će u nastavku biti detaljnije opisan.

	Private address range	
Class	start address	finish address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

	Public address range	
Class	start address	finish address
A	0.0.0.0	126.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	254.255.255.255

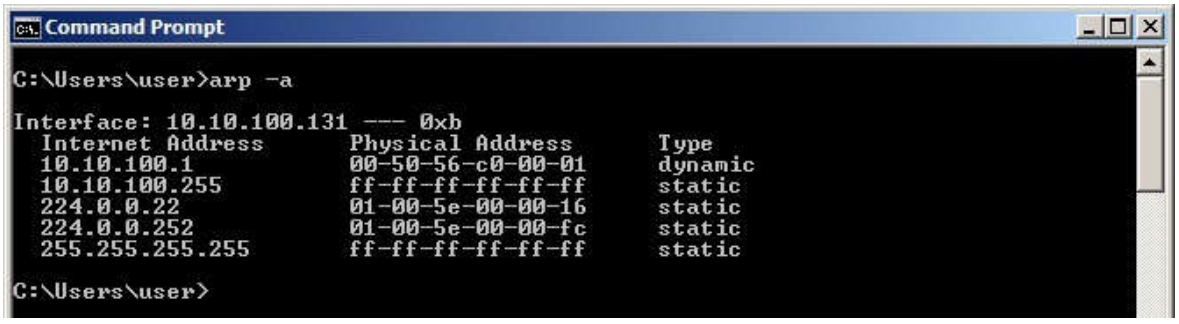
Sl. 2.5. *Privatne i javne adrese unutar različitih klasa [13]*

3. MREŽNA OPREMA

S ciljem razumijevanja principa rada mreža, odnosno kako dva računala komuniciraju, kojim principom su spojeni da bi se komunikacija mogla odvijati, potrebno je znati koji se uređaji koriste da bi se komunikacija mogla uspostaviti te po kojem oni principu rade i koje protokole koriste. Postoji veliki broj uređaja koji su se prije koristili, ali su zbog napretka tehnologije izbačeni iz svakodnevne upotrebe, uređaji koji se danas koriste mnogo su napredniji i svakim se danom sve više i više razvijaju da bi mogli zadovoljiti potrebe korisnika za sve većom brzinom prijenosa podataka. Zbog velike raznolikosti uređaja s njihovim različitim funkcijama, ovisno o potrebi, bit će objašnjeni samo najvažniji uređaji i njihove općenite funkcije i protokoli.

3.1. Preklopnik (*engl. Switch*)

Mrežni preklopnik je uređaj koji centralizira komunikaciju između više uređaja unutar jednog LAN-a, preklopnici jakih performansi u širokoj su upotrebi unutar većih korporacija, stambenih domova, centara za prikupljanje podataka… Mrežni uređaji kao što su računala, pisači ili neki drugi krajnji uređaji, na mrežu se spajaju preko preklopnika koji dalje komunicira s usmjerivačem da bi uređaj mogao pristupiti Internetu. Preklopnik je zadužen za komunikaciju uređaja unutar jedne LAN mreže koristeći MAC adresu (*engl. Media Access Control*). Ta adresa je zapravo identifikacijski broj svakog uređaja, zapisan u heksadecimalnom obliku, a sama MAC adresa dobiva se pomoću posebnog protokola koji prevodi IP adresu u MAC adresu i obrnuto. Taj protokol se naziva ARP *(engl. Address Resolution Protocol)* i pomoću njega podatak prelazi s drugog na treći OSI sloj i obratno, ali prvo, kad paket dođe, preklopnik provjerava unutar svoje ARP tablice postoji li IP adresa koja već odgovara nekoj MAC adresi. U slučaju da veza ne postoji u tablici, šalje upite svima u mreži i čeka odgovor traženog uređaja. Detaljniji opis pretvorbe može se naći u [14].



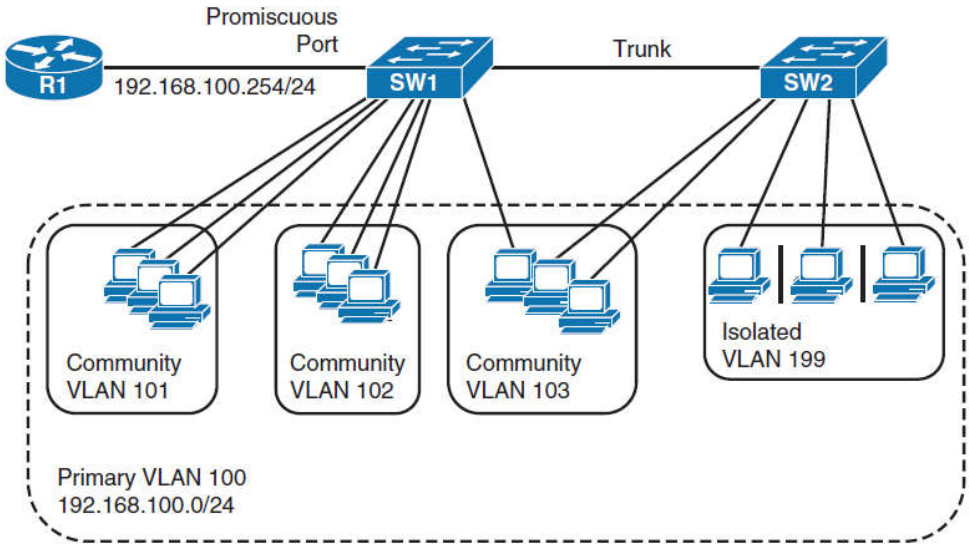
Sl. 3.1. *Primjer ARP tablice te povezivanje IP i MAC adrese*

S obzirom da je preklopnik u većini slučajeva uređaj na koji se spaja veći broj uređaja, posjeduje veći broj utora na koji se uređaji mogu spojiti. Od najčešće korištenih te ovisno o proizvođaču, to može biti 4, 8, 24 i 48 utora. Da se neki podatak ne bi slao svima u mreži, koristi se MAC adresa da bi se podatak dostavio željenom uređaju. Zbog toga se preklopnik smatra uređajem koji radi na drugom sloju OSI modela jer prima pakete s trećeg sloja i pakira ih u okvire (*engl. frames*) te ih priprema za slanje na prvi sloj. Ponekad se preklopnike u literaturi može naći pod nazivom *uređaji podatkovnog linka* ili *uređaji drugog sloja*. Budući da preklopnik u isto vrijeme može slati i primati informacije s više uređaja, a da mu se performanse ne smanje, zamijenio je korištenje mrežnih koncentratora (*engl. network hub*) koji su imali ograničen broj konektora te su brzine prijenosa ovisile o broju priključenih uređaja. Klasični preklopnici koji su predviđeni za kućnu upotrebu su uređaji koji ne zahtijevaju specijalnu konfiguraciju, osim spajanja s drugim uređajima. Ta vrsta preklopnika je unaprijed konfigurirana i koriste je privatni korisnici te za nju nije potrebno nikakvo stručno znanje. Druga vrsta preklopnika nije unaprijed konfigurirana i ta se vrsta, koju po potrebi konfiguriraju sistem administratori, koristi za veliki broj korisnika, a sama konfiguracija se vrši u komadnoj liniji i u njoj se, ovisno o potrebi, svaki protokol podešava zasebno. Svaki preklopnik koji nije unaprijed konfiguriran, pored svih priključaka za LAN kabel, sadrži još priključak za poseban kabel *(engl. console cable*) koji se koristi za spajanje preklopnika s računalom da bi se izvršila željena konfiguracija preklopnika.

Sl. 3.2. *Primjer preklopnika s 24 priključka [15]*

Kako se u praksi često međusobno povezuje više preklopnika, da bi se mogao veći broj uređaja spojit unutar jedne mreže, a da ne dođe do kruženja podataka između njih, koristi se STP (*engl. Spanning-Tree Protocol*) koji implementira algoritam koji izmjenjuje poruke s ostalim preklopnicima kako ne bi došlo do kruženja, a zatim se kruženje uklanja gašenjem određenog sučelja. Algoritam osigurava postojanje samo jednog aktivnog puta između dvaju mrežnih uređaja. Detaljnije o STP-u [16]. Jedna od bitnih stvari na preklopnicima su virtualne lokalne mreže ili kraće VLAN *(engl. Virtual Local Area Network)* koje služe da se jedna mreža segmentira na više manjih koje se mogu dinamički mijenjati.

Komunikacija među računalima unutar te jedne manje mreže se može izvršavati bez problema, dok se komunikacija računala iz tih dviju manjih mreža mora izvršavati preko usmjerivača jer, bez obzira na to što se nalaze na istom preklopniku, na LAN-ove se gleda kao na potpuno dva odvojena preklopnika od kojih svaki ima svoju kolizijsku domenu. VLAN-ovi se primjenjuju zbog financijske uštede jer se na jednom preklopniku može izvesti veliki broj zasebnih logičkih mreža. VLAN se može koristiti i zbog sigurnosti jer, budući da su priključci preklopnika podijeljeni u više mreža, ako je jedna izložena nekakvoj prijetnji, ostale mreže su sigurne. Postoji još jedna primjena VLAN mreža: u većini slučajeva se nekoliko priključaka ostavlja slobodnima kako bi se napravio VLAN rezerviran samo za administratore da bi mogli s tih priključaka održavati ili konfigurirati mrežu. U slučaju da postoje dva ili više preklopnika koji sadrže isti VLAN, potrebno je da na svakom bude omogućen promet između njih. Da bi se to olakšalo, koristi se VTP *(engl. VLAN Trunking Protocol)* koji osigurava da se promet prenosi preko jednog sučelja. Detaljnije o VLAN protokolu u [17] i [18].



Sl. 3.3. *Primjer nekoliko VLAN-ova na dvama preklopnicima [18]*

3.2. Usmjerivač (*engl. Router*)

Usmjerivač je jedan od najvažnijih uređaja u mrežama. Njegova glavna zadaća je povezivanje dviju ili više različitih mreža, žičano ili bežično. Usmjerivač je uređaj koji radi na trećem sloju OSI modela i koji prema odredišnoj IP adresi traži najbolji put za slanje paketa. Usmjerivač, kao hardverski uređaj, sadrži sve komponente kao računalo - od procesora, digitalne memorije, ulaznih i izlaznih sučelja, samo što ima posebnu funkciju pa mu nisu potrebni tipkovnica, displej i ostali dodatni dijelovi osobnog računala. Od priključaka, svaki standardni usmjerivač ima nekoliko *ethernet* i *gigabit* priključaka za povezivanje usmjerivača s ostatkom mreže, a po potrebi se mogu još ugraditi serijski, dodatni *ethernet* priključci te priključak za optički kabel. Postoji još nekoliko posebnih priključaka, ali ti su priključci slični onima na preklopniku, to su priključci za *aux* i *konzolni* kabel koji služe za prvo konfiguriranje usmjerivača dok nijedno drugo sučelje nije uključeno, a zadnji priključak je za USB.

Sl. 3.4. *Izgled Cisco usmjerivača s prednje i stražnje strane [19]*

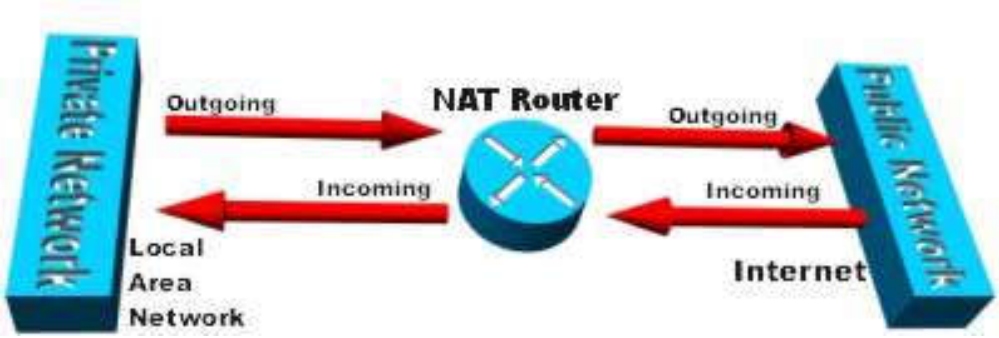
Svaki usmjerivač u svojoj memoriji sadrži tablicu usmjeravanja prema kojoj šalje pojedine pakete na pojedina sučelja. Te tablice usmjeravanja se popunjavaju i osvježavaju komunikacijom više usmjerivača. Da bi usmjerivač mogao proslijediti paket u željenu mrežu prema odredišnoj IP adresi, on prvo, unutar tablice usmjeravanja, mora provjeriti na koje sučelje poslati paket. Tablice usmjeravanja se mogu popunjavati statički ili dinamički, oba načina imaju svoje prednosti i mane. Statičke rute administrator mora sam ručno unositi - odredišnu mrežu, njezinu masku te sučelje ili IP adresu, ovisno o tome preko čega će usmjerivač naučiti rutu. Ova metoda je bolja kada administrator nema puno mreža jer statičke rute imaju administrativnu vrijednost 1, dok dinamičke rute imaju iste vrijednosti mnogo veće. Administrativne vrijednosti su bitne jer svaki paket ima svoj maksimalni TTL *(engl. Time To Live)* koji predstavlja broj skokova koji paket može napraviti između usmjerivača dok ne nestane. Najveća vrijednost TTL-a je 2^8-1 ili 255, što bi značilo da paket u početku ima TTL 255 i svakim skokom se ta vrijednost smanjuje.

Kod statičkih ruta to znači da se vrijednost smanjuje za 1, dok se kod dinamičkih ruta TTL smanjuje za veću vrijednost. Zbog toga se preporučuje korištenje statičkih ruta, ali ono oduzima mnogo vremena i ako dođe do neke promjene, sve se mora mijenjati ili ručno ponovo postavljati. Zbog toga je bolje koristiti dinamičke rute jer se na svakom usmjerivaču treba jednokratno postaviti jedan od protokola za dinamičko usmjeravanje preko kojeg se vrši komunikacija između više usmjerivača i ako dođe do bilo kakve promjene u mreži, usmjerivači će sami osvježiti tablicu usmjeravanja. TTL je uveden da ne bi došlo do zagušenja u mreži jer bi tada paketi beskonačno kružili mrežom. Ovako paket ima svoju vrijednost TTL-a koja se svakim skokom kroz mrežu smanji, a kad ta vrijednost dođe do 0, paket se uništava. Postoji nekoliko vrsta dinamičkog pronalaženja ruta. Svaka ta vrsta radi po nekim pravilima, odnosno protokolima pa se skup tih protokola naziva protokoli usmjeravanja. Svaki od tih protokola će biti u nastavku objašnjen.

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 2 subnets
D       10.5.10.0 [90/30720] via 192.168.0.1, 00:01:53, FastEthernet0/1
D       10.20.15.0 [90/284160] via 192.168.0.1, 00:00:18, FastEthernet0/1
C    192.168.0.0/24 is directly connected, FastEthernet0/1
```

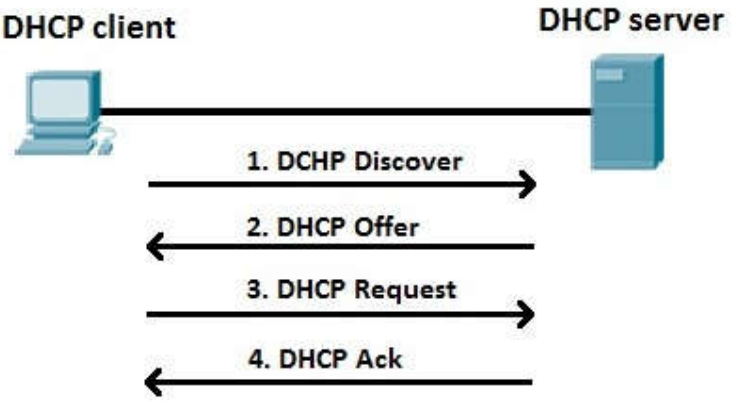
Sl. 3.5. *Primjer tablice usmjeravanja u memoriji usmjerivača*

Usmjerivač je uređaj koji odvaja različite mreže, a samim tim odvaja privatne IP adrese od javnih IP adresa i obrnuto. Budući da se od jedne javne IP adrese može dobiti veliki broj privatnih adresa, tu se koriste dva bitna protokola. Prvi protokol je NAT *(engl. Network Address Translation)* protokol koji služi da privatne IP adrese mogu pristupiti Internetu, odnosno zadužen je za prevođenje javnih IP adresa u privatne i obrnuto. NAT se postavlja na usmjerivač kako bi uređaji koji se nalaze unutar privatne mreže mogli komunicirati s drugim uređajima koji se nalaze unutar neke druge privatne mreže preko Interneta. Osim što je to alat koji omogućava veći broj IP adresa verzije 4, u isto vrijeme osigurava neku vrstu sigurnosti hosta budući da je puno teže saznati točnu IP adresu nekom uređaju izvan te privatne mreže jer on maskira cijelu privatnu mrežu jednom javnom IP adresom. NAT je sastavni dio svakog usmjerivača i danas se koristi masovno, a više o vrstama, prednostima i manama te detaljnijem principu rada može se naći u [20] i [21].



Sl. 3.6. *Principijelna shema NAT protokola [21]*

Drugi koristan protokol je DHCP *(engl. Dynamic Host Configuration Protocol)*. Kako postoji statičko i dinamičko pronalaženje rute, tako postoji statičko i dinamičko dodjeljivanje IP adresa različitim uređajima. Svaki uređaj mora imati svoju jedinstvenu IP adresu unutar nekog LAN-a, a ona se može dodijeliti na dva načina: prvi je da mrežni administrator svakom uređaju u mreži ručno dodijeli IP adresu, a da pritom ne napravi pogrešku pa istu IP adresu dodijeli dvama ili više uređaja te u slučaju da se naknadno nešto u mreži promijeni (neki uređaj se doda ili makne iz mreže, mijenja se maska mreže…). To je statički način dodijele IP adresa koji administratoru oduzima puno vremena i koncentracije. Drugi način je korištenje DHCP-a koji dinamički dodjeljuje svakom uređaju u mreži jedinstvenu IP adresu. Radi na principu klijent-poslužitelj, a jedina zadaća mrežnog administratora je da na usmjerivaču odnosno poslužitelju konfigurira DHCP koji za svakog klijenta unutar podmreže ili za svakog LAN-a dodijeli IP adresu iz određenog raspona IP adresa. Ovaj protokol radi na principu zahtjeva i odgovora, što se može vidjeti na sl.3.7., a ako se neka IP adresa za određeni uređaj ne koristi određeno razdoblje, njegova IP adresa se oslobađa i može se dodijeliti nekom drugom uređaju, odnosno klijentu. Više o principu rada, konfiguraciji i ostalim bitnim starima oko DHCP-a može se pronaći u [22],[23],[24].



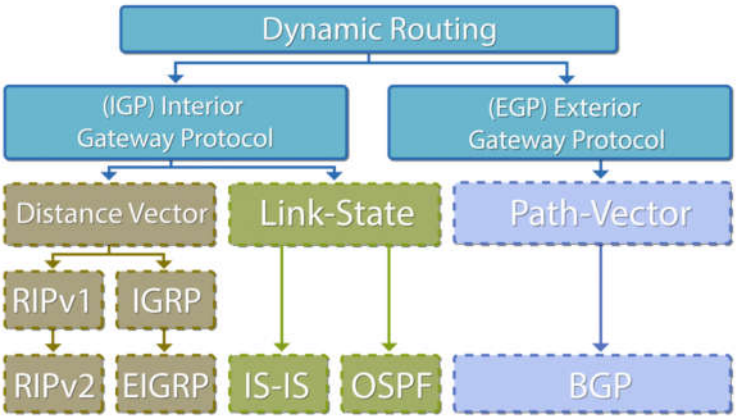
Sl. 3.7. *Princip rada klijent-poslužitelj DHCP-a [23]*

Usmjerivač ima još jednu vrlo važnu zadaću, a to je kontrola pristupa određenim uređajima ili uslugama, a to se provodi s ACL *(engl. Access Control List).* One su zadužene za kontrolu prometa kroz usmjerivač te mogu ograničiti ili totalno onemogućiti pristup nekim uslugama. ACL su jedna vrsta vatrozida *(engl. firewall)* koje poput filtera određene pakete propuštaju, a ostatak ne propuštaju ili obratno, ovisno kako su ACL koncipirane. ACL su liste naredaba usmjerivaču s uputama što smiju propuštati, a što ne. Postoje dvije vrste - standardne i proširene. Standardne liste su bazirane na trećem sloju - filtriraju samo na temelju IP adrese, što znači da uređaj s određenom IP adresom ne može pristupiti mreži ili komunicirati s nekim drugim uređajem. Nekoj IP adresi se nešto dopušta ili brani, ovisno o tome koja vrijednost joj se dodijeli. Druga vrsta su proširene ACL koje se odvijaju na trećem i četvrtom sloju OSI modela, gdje postoji više opcija konfiguriranja. Svakom uređaju u mreži se može zabraniti korištenje jednog ili više protokola, dok se određenim uređajima dopusti pristup, npr. konfiguriranju mreže. Primjeri standardne i proširene liste, kao i detaljnije objašnjenje, može se naći na [24]i[25].

3.2.1. Usmjerivački protokoli

Usmjerivački protokoli su mehanizmi koji koriste alate i algoritme za pronalaženje i određivanje optimalne rute za slanje podataka te komunikaciju između dviju točki u mreži. Usmjerivački protokoli omogućuju komunikaciju između bilo kojih dvaju usmjerivača, a imaju tri osnovne funkcije: pronalaženje ruta, upravljanje rutama (sadrže podatke o više mogućih ruta istodobno, s nekim bitnim informacijama) te odabir optimalne rute kuda će se informacija poslati. Osim već prije objašnjenih statičkih ruta, postoje dinamičke rute koje koriste usmjerivačke protokole, a dijele se na unutarnje ili IGP (*engl. Interior Gateway Protocol*) koje se još dijele prema načinu izračuna optimalnog puta: protokoli vektora udaljenosti *(engl. Distance Vector)* i protokoli stanja veze *(engl. Link State)* i vanjske ili EGP (*engl. Exterior Gateway Protocol*). Protokoli vektora udaljenosti u većini slučajeva šalju cijelu tablicu ruta svakom susjedu te najbolju rutu pomoću algoritma. Ova vrsta protokola jednostavna je za konfiguraciju, ali sporije pokriva mrežu od protokola stanja veze i zauzima veću propusnost mreže jer se šalje cijela tablica usmjerivanja. Drugi protokol je protokol stanja veze koji također ima zadatak pronaći najbolju putanju do destinacije, samo što koristi drukčiju metodu. Ovaj protokol ne šalje cijelu tablicu usmjeravanja, nego prosljeđuje informacije o mreži (izravno spojene linkove, susjedne usmjerivače i dr.) tako da svi usmjerivači imaju istu topologiju mreže. Ova metoda je mnogo brža jer šalje sve promjene kroz mrežu koristeći *multicast* adrese, ali je i teža za konfiguriranje od protokola vektora udaljenosti.

Na slici 3.8 se vidi daljnja podjela protokola usmjeravanja, od kojih će najčešće korišteni biti kratko opisani, dok se detaljnije opisani protokoli mogu pogledati u [26] i [27].



Sl. 3.8. *Podjela dinamičkih usmjerivačkih protokola [28]*

RIP *(engl. Routing Information Protocol)* je prvi usmjerivački protokol koji se koristi na malim i srednjim mrežama jer je sposoban za slanje usmjerivačkih poruka kroz mrežu od najviše 15 skokova. RIP istražuje mrežu tako što prvo šalje poruku sa zahtjevom za usmjerivačkim tablicama od susjednih usmjerivača, zatim susjedni usmjerivači odgovaraju na zahtjev tako što šalju cijelu usmjerivačku tablicu nazad. Prema nekom vremenskom rasporedu, RIP usmjerivači periodično šalje svoje usmjerivačke tablice svojim susjedima tako da se eventualne promjene prošire mrežom.

OSPF *(engl. Open Shortest Path First)* je osmišljen kako bi se nadopunili neki nedostatci RIP protokola, a to su 15 skokova, nemogućnost organizacije mreže prema usmjerivačkoj hijerarhiji važnoj za upravljanje i izvedbi velikih mreža i zadnje, povećanje mrežnog prometa stvorenog zbog stalnog slanja tablica upravljanja. Upravljači koji koriste OSPF protokol usmjeravanja istražuju mrežu tako što međusobno šalju identifikacijske poruke, a zatim šalju specifične usmjerivačke podatke, a ne cijelu tablicu usmjeravanja.

EIGRP *(engl. Enhanced IGRP) i* IGRP *(engl. Internet Gateway Routing Protocol)* su još jedna vrsta protokola kojom bi se unaprijedio RIP. EIGRP je samo unaprijeđena verzija IGRP koju je počela razvijati Cisco korporacija kako bi se primjenjivala na njihovim uređajima. EIGRP podržava bez klasne IP podmreže i poboljšava iskoristivost usmjerivačkih algoritama u usporedbi s prethodnom verzijom, odnosno IGRP, a ne podržava usmjerivačku hijerarhiju kao RIP. EIGRP je osmišljen s idejom lakšeg konfiguriranja, ali boljih performansi od OSPF.

IS-IS (*engl. Intermediate System to Intermediate System*) je protokol sličan OSPF-u. Budući da je OSPF postao češći odabir nego IS-IS, on je ostao u široj upotrebi kod pružatelja mrežnih usluga koji su imali koristi od protokola zato što se lakše može prilagoditi njihovim posebnim zahtjevima. Za razliku od ostalih protokola, IS-IS se ne pokreće preko IP protokola i koristi vlastitu sheme adresiranja.

BGP (*engl. Border Gateway Protocol*) je jedini protokol za vanjsko usmjeravanje koji detektira promjene na tablicama usmjeravanja i selektivno prosljeđuje te promjene ostalim usmjerivačima preko TCP/IP-a. Internet poslužitelji često koriste BGP kako bi se spojile mreže, ponekad i veće korporacije koriste BGP da bi se spojile njihove unutarnje mreže. Gledano s profesionalne strane, BGP se smatra najzahtjevnijim usmjerivačkim protokolom za konfiguraciju zbog svoje kompleksne složenosti. Detaljno opisan, svaki protokol se može naći na [30].

3.3. Višeslojni preklopnik (*engl. Multilayer Switch*)

Višeslojni preklopnik ili kraće MLS je preklopnik koji radi na drugom sloju OSI modela, ali ima dodatne funkcije s viših slojeva. MLS kombinira funkcije s drugog, trećeg i četvrtog sloja kako bi se osigurala velika brzina skalabilnosti s malim kašnjenjem. Višeslojni preklopnik se opisuje kao preklopnik koji ima mogućnost kreiranja tablica usmjeravanja te podržava nekoliko usmjerivačkih protokola i prosljeđuje IP pakete brzinom približnoj prosljeđivanju na drugom sloju. Budući da većina korporacija koristi usmjerivače i preklopnike, sve više se počinju koristiti višeslojni preklopnici kako bi ostvarili velike brzine prijenosa paketa koristeći preklopnike koji rade i na trećem sloju jer posjeduju usmjerivačka sučelja slična sučeljima koji se nalaze na usmjerivačima i virtualna sučelja preklopnika za kreiranje VLAN-ova kojima se mogu konfigurirati virtualne rute. Kada paket dolazi na usmjerivač na trećem sloju, provjeri se odredišna i izvorišna IP adresa da se definira kojim putem će paket ići, a zatim se, kao na normalnom preklopniku, otkriva odredišna i izvorišna MAC adresa paketa, a taj se proces odvija na drugom sloju [31].

Sl. 3.9. *Primjer višeslojnog preklopnika marke Cisco [32]*

3.4. Krajnji mrežni uređaji

Pojam krajnji mrežni uređaji odnosi se na sve uređaje koji imaju jedan ulaz odnosno izlaz. Postoje razni krajnji uređaji koji mogu predstavljati „početak“ mreže jer svaki takav uređaj može imati ulogu klijenta i poslužitelja, ovisno o tome nudi li ili zahtijeva uslugu zato što host u jednom slučaju može biti klijent, a u drugom poslužitelj. Klijent je uređaj koji zahtijeva neku uslugu, servis koji se nalazi na nekom drugom uređaju, a taj drugi uređaj je u tom slučaju poslužitelj koji ima instaliran takav servis i pruža uslugu klijentu. U drugom slučaju, ti uređaji mogu zamijeniti uloge. Danas veliki dio Interneta funkcionira na takvom sustavu klijent-poslužitelj jer mnogo internetskih aplikacija radi na ovom principu. U te takozvane krajnje uređaje ubrajamo računala, mrežne pisače, mobilne uređaje, nadzorne kamere… Jedino važno zajedničko obilježje tih uređaja je mrežna kartica (*engl. Network Interface Card- NIC*) koja je zadužena da pretvara nekakav podatak u oblik koji je prilagođen za prijenos ili taj preneseni oblik pretvara nazad u koristan podatak. Svaka mrežna kartica ima svoju MAC adresu prema kojoj se taj uređaj pronalazi u mreži. Bez nje nijedan uređaj ne bi mogao biti uključen u komunikaciju jer se ne bi prepoznao unutar mreže.

Sl. 3.10. *Princip rada klijent-poslužitelj [33]*

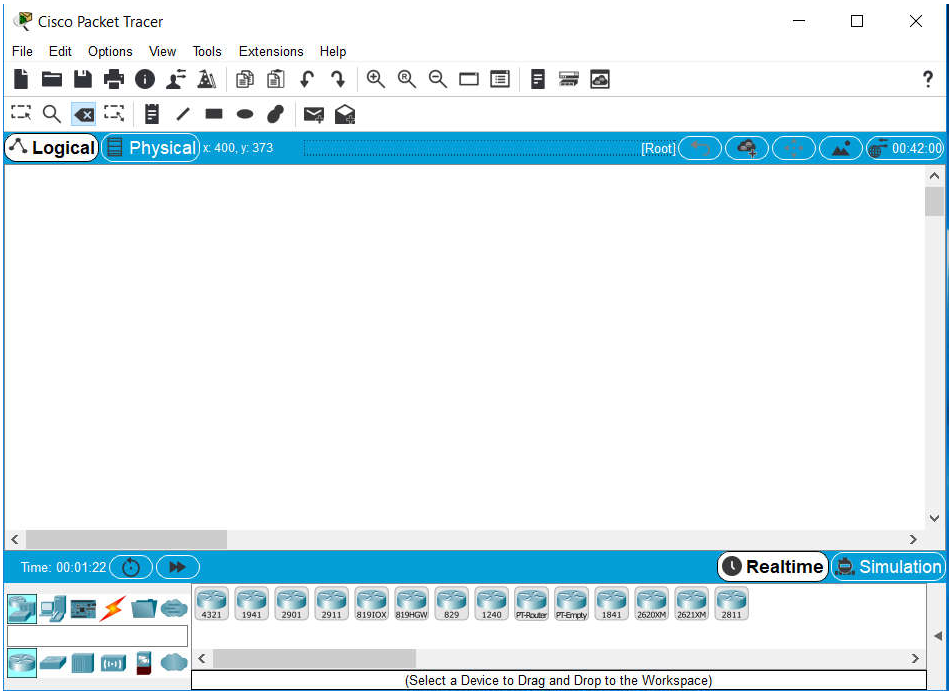
4. KONFIGURACIJA CISCO MREŽNE OPREME

Budući da se cijeli rad bazira na Cisco opremi koja ima vlastiti operacijski sustav na kojem se konfiguriraju uređaji, potrebno je poznavati sintaksu za svaki protokol, uslugu ili bilo što drugo što se može uključiti i postaviti na svakom uređaju. S obzirom da je oprema Cisco proizvođača poprilično skupa i za poslovne korisnike, rijetko tko će si moći priuštit Cisco opremu samo za učenje. Zbog toga je Cisco Systems dizajnirao mrežni simulator *Packet Tracer*. Cisco Systems omogućuje korisnicima besplatno preuzimanje i instaliranje tog programa na svakom operacijskom sustavu (*Linux, Mac OS i Windows*) te samostalno stvaranje vlastite mreže, njenu konfiguraciju i testiranje. Dakako, nijedan simulacijski program se ne može usporediti s realnim uvjetima pa se zato ovaj program koristi samo za učenje, no bez obzira na to, vrlo dobro opisuje rad Cisco mrežnih uređaja.

4.1. Cisco *Packet Tracer*

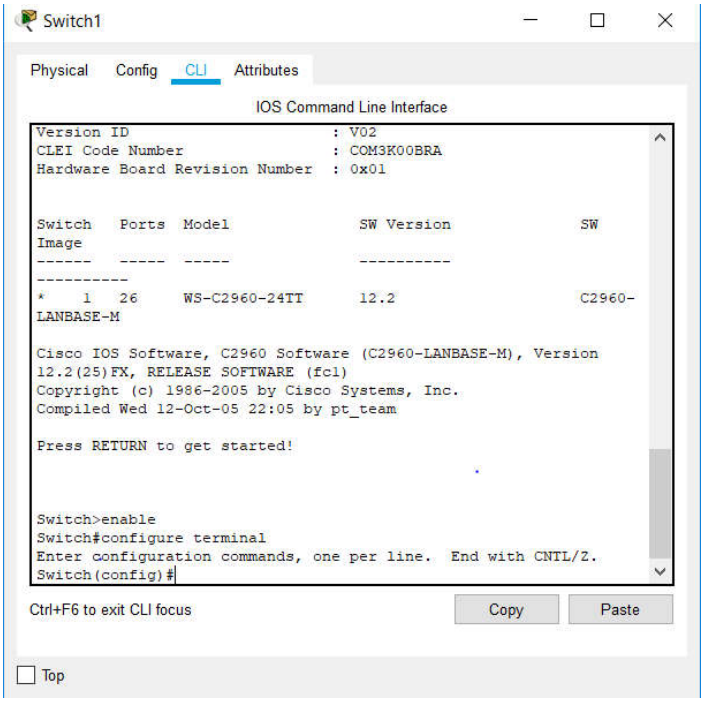
Već je spomenuto da je *Packet Tracer* mrežni simulator koji je napravila Cisco Systems korporacija, a služi za obrazovanje i upoznavanje s radom Cisco opreme. *Packet Tracer* je program koji vrlo dobro može simulirati stvarnu mrežu, ali, kako je već rečeno, ne može u potpunosti zamijeniti Cisco usmjerivače i preklopnike. Bez obzira na neka ograničenja koja se ne mogu napraviti u simulatoru, a na stvarnim uređajima mogu, program je iznimno koristan za obrazovanje. U njemu se mogu dizajnirati prilično velike, a ujedno i kompleksne mreže koje je zbog velike cijene teško realizirati na fizičkim uređajima, pogotovo za edukacijske svrhe. Program nudi još jednu mogućnost, a to je multi-korisnički sustav kojim veći broj korisnika može spojiti više različitih topologija u jednu veliku računalnu mrežu.

Packet Tracer je program koji omogućuje vizualne konfiguracije te konfiguraciju pomoću komandne linije. S obzirom da se konfiguriraju stvarni uređaji, program nudi mnogo mogućnosti kao što su: velik broj uređaja (mrežnih, krajnjih ili bilo kakvih uređaja koji se mogu pojaviti u stvarnom svijetu, a da imaju veze s računalnim mrežama), izmjena na tim uređajima, načini spajanja uređaja, rad uređaja u stvarnom vremenu kao i u simulaciji. Postoji još i mogućnost mijenjanja logičkog i topološkog prikaza mreže… Uređaji se u radni prostor dodaju metodom dovuci (*engl. drag*) i ostavi (*engl. drop*), a povezuju se odabirom željenog kabela te odabirom sučelja na koji se želi spojiti uređaj. Može se odabrati način konfiguracije kao u stvarnom svijetu - koristeći računalo i konzolni kabel ili samo pritiskom na uređaj… Zbog stvarno velikog broja mogućnosti *Packet Tracera,* više o njemu u [34][35][36].



Sl. 4.1. *Packet Tracer sučelje*

Cisco mrežni uređaji imaju nekoliko stupnjeva konfiguracije uređaja unutar sučelja komandne linije ili skraćeno CLI *(engl. Command Line Interface*), a razlog tomu je što svaki stupanj ima različite privilegije. Prvi stupanj je korisnički stupanj (*engl. User Exec Mode*) koji je prilično ograničen i ima pristup samo nekim osnovnim funkcijama, odnosno naredbama te se često još naziva i „stupanj samo za gledanje“, drugom stupnju se pristupa naredbom „*enable*“ koji je povlašteni konfiguracijski (*engl. Privileged EXEC Mode*) stupanj unutar kojeg se može pristupiti svim naredbama. Postoji još jedan stupanj, a to je globalni konfiguracijski stupanj (*engl. Global Configuration Mode*) kojemu se može pristupit samo putem povlaštenog stupnja upisivanjem naredbe „*configure terminal*“, a unutar njega se mogu izvršavaju konfiguracije koje utječu na cijeli uređaj. Unutar CLI-a, svaki od tih stupnjeva ima neku oznaku prema kojoj se oni mogu međusobno razlikovati, a stoji odmah iza imena uređaja kao što se može vidjeti na slici 4.2 gdje je preklopniku unaprijed postavljeno ime *Switch.* Postoje još dva podstupnja koji se nalaze na najvišem konfiguracijskom stupnju, a to su Linijski konfiguracijski mod (*engl. Line Configuration Mode*) i konfiguracijski mod sučelja (*engl. Interface Configuration Mode*) koji se koriste kad su potrebne neke posebne konfiguracije na uređajima.



Sl. 4.2. *Komandna linija za konfiguraciju usmjerivača unutar Packet Tracer-a*

4.2. Osnovna konfiguracija uređaja

Već prije u radu je spomenuto da postoje unaprijed konfigurirani uređaji i uređaji koji nisu unaprijed konfigurirani, kao i uređaji za manje, odnosno privatne korisnike te uređaji za korporacije s većim brojem mrežnih uređaja koji se moraju međusobno povezati. Zadnje spomenuti uređaji ne mogu biti unaprijed konfigurirani zato što se svaki uređaj mora konfigurirati kako bi izvršavao svoju zadaću u mreži. Većina Cisco uređaja mora se konfigurirati iz nule prema potrebama određene mreže, a izvršava se upisivanjem naredbi unutar sučelja komandne linije. Konfiguraciju bi se moglo podijelit u nekoliko skupina ovisno o tome što se konfigurira ili koji se protokoli konfiguriraju. Dakako, tu su i neke osnovne konfiguracije kao što su: naziv uređaja, vrijeme (podešava se prema potrebi ako nema NTP poslužitelja [27]), ulazne poruke, a mogu biti još i sigurnosne postavke, postavke za pristup uređajima preko mreže i naravno, ostale konfiguracije svakog protokola zasebno.

Na početku konfiguriranja, prvo se u praksi radi promjena imena koje se konfigurira koristeći naredbu „*hostname*“ zbog jednostavnog razloga - raspoznavanje uređaja kada je u mrežu spojeno više uređaja.

```
Switch(config)#hostname Preklopnik_primjer
Preklopnik primjer(config)#
```

Nakon toga se trebaju konfigurirati korisničko ime i šifra s kojima će se moći pristupiti nekim drugim uređajima u mreži koristeći jedan od protokola za upravljanje uređajima iz daleka.

```
Preklopnik_primjer(config)#username Primjer password 1234
```

Slijedi podešavanje sigurnosti samog uređaja kako ne bi bilo tko mogao pristupiti i mijenjati postavke uređaja, a to se može napraviti korištenjem naredbi „*enable password*“ ili „*enable secret*“, ovisno o razini sigurnosti koja se očekuje, a razlika je u tome što se naredbom „*secret*“ lozinka kodira i nije ju moguće vidjeti u postavkama uređaja.

```
Preklopnik_primjer(config)#enable secret 1234
```

Sljedeće postavke koje se mogu zaštiti su pristup uređaju konzolnim kabelom, kao i zaštita pristupa uređaju virtualnom linijom, odnosno preko mreže. Kada se postavi lozinka kojom će se moći pristupiti uređaju, mora se naredbom „*login*“ uključiti opcija da se prilikom svakog pristupa uređaju upiše lozinka. Da bi se te dvije zaštite mogle uključiti, mora se pristupiti linijskom konfiguracijskom modu za virtualnu i konzolnu liniju kao jednom od dvaju podstupnjeva u globalnom konfiguracijskom modu koristeći naredbe „*line console*“ i „*line vty*“.

```
Preklopnik_primjer(config)#line console 0
Preklopnik_primjer(config-line)#password 1234
Preklopnik_primjer(config-line)#login
Preklopnik_primjer(config-line)#line vty 0 4
Preklopnik_primjer(config-line)#password 1234
Preklopnik_primjer(config-line)#login
```

Da bi se povećala sigurnost, nakon tih svih naredbi unosi se naredba „*service password-encryption*“ kako bi se sve lozinke kriptirale i kako se ne bi mogle vidjeti u postavkama, nego bi se samo vidjelo postoji li lozinka ili ne. Samim tim, mogućnost neovlaštenog ulaza bi bila znatno manja. Dodatno se postavlja poruka da neovlaštene osobe nemaju pravo ulaska u konfiguraciju uređaja naredbom „*banner motd*[1]“.

```
Preklopnik_primjer(config)#banner motd "Security Enable Access!"
Preklopnik primjer(config)#service password-encryption
```

Postoje dva protokola kojima se uređajima preko mreže može pristupiti daljinski, a to su SSH (*engl. Secure Shell Command*) i Telnet. Razlikuju se tome što Telnet ne koristi nikakav oblik zaštite, a SSH koristi pa se zbog toga on više koristit. Prilikom konfiguracije SSH-a postavljaju se

[1] motd-message of the day

sljedeće postavke: verzija koja se koristi, vrijeme čekanja ako se pogrešno unese lozinka i broj pokušaja unošenja ispravne lozinke.

```
Preklopnik_primjer(config)#ip ssh version 2
Preklopnik_primjer(config)#ip ssh authentication-retries 3
Preklopnik_primjer(config)#ip ssh time-out 30
```

Naravno, da bi sve naredbe ostale spremljene kada se uređaj ugasi ili resetira, mora se unijeti naredba kojom će se trenutna konfiguracija kopirati i spremiti u memoriju prilikom pokretanja.

```
Preklopnik_primjer#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Sve prethodno unesene naredbe su konfigurirane na preklopniku, ali vrijede za svaki uređaj Cisco korporacije, kao i za usmjerivače, višeslojne preklopnike i druge mrežne uređaje. Ove naredbe su osnovna konfiguracija za svaki uređaj i konfiguriraju zasebno te nemaju utjecaj na druge uređaje. U slučaju da se nešto u mreži promijeni, ove naredbe se ne trebaju ponovo unositi ni mijenjati.

4.3. Konfiguracija preklopnika

Najčešće se na preklopniku konfiguriraju VLAN-ovi (*engl. Virtual Local Area Network*) koji su prethodno objašnjeni, a konfiguriraju se u nekoliko koraka. Prvo se kreira VLAN tako što mu se da neka vrijednost od 1 do 1005 (VLAN-ovi 1 te od 1002 do 1005 su tvornički stvoreni u memoriji preklopnika), zatim se, zbog lakšeg raspoznavanja te kasnijeg upravljanja, pridodaju nazivi.

```
Preklopnik_primjer(config)#vlan 55
Preklopnik_primjer(config-vlan)#name VLAN_Primjer
```

Nakon što je VLAN 10 napravljen, mora se postaviti u stanje „*up*“ odnosno naznačiti da je stvoren i da se može koristiti, ali to ništa ne znači dok god mu se ne dodijeli neka IP adresa jer tek tada on postaje virtualni uređaj koji se može koristiti.

```
Preklopnik_primjer(config)#interface vlan 55
Preklopnik_primjer(config-if)#
%LINK-5-CHANGED: Interface Vlan55, changed state to up

Preklopnik primjer(config-if)#ip address 192.168.0.1 255.255.255.0
```

Nakon što je VLAN stvoren, mora mu se pridijeliti određen broj sučelja na kojima će se on koristiti. Budući da u većini slučajeva preklopnici imaju 24 sučelja, ovisno o broju VLAN-ova i sučelja koja će za njih trebati, broj sučelja se mora pametno podijeliti te se ne smiju zaboraviti sučelja kojima se spaja s usmjerivačem. Administrator mreže mora svakom VLAN-u pridijeliti određen broj priključaka od kojih postoje dvije vrste: *Access* i *Trunk* veze. *Access* način rada se koristi kada je potrebna kontrola okvira jer se svaki okvir označava brojem VLAN-a i kada se pošalje, prema oznaci će se znati proslijediti na odgovarajući VLAN. Ovakav način se inače koristi na sučeljima kojima se povezuju računala ili krajnji uređaji.

```
Preklopnik_primjer(config)#interface range fastEthernet 0/1-15
Preklopnik_primjer(config-if-range)#switchport mode access
Preklopnik_primjer(config-if-range)#switchport access vlan 55
```

Ovdje se može vidjeti kako smo sučelja od 1 do 15 postavili u *Access* način rada i da se preko njih pristupa VLAN-u 55. Drugi način je *Trunk* veza koja se većinom koristi za komunikaciju između većeg broja preklopnika ili između usmjerivača i preklopnika kada se koriste i označeni i neoznačeni okviri. Ovakav način se koristi kada imamo više VLAN-ova jer bi inače trebalo koristiti minimalno jedno sučelje unutar jednog VLAN-a kojim bi povezao isti VLAN na drugom preklopniku.

```
Preklopnik_primjer(config)#interface range fastEthernet 0/20-24
Preklopnik_primjer(config-if-range)#switchport mode trunk
Preklopnik_primjer(config-if-range)#switchport access vlan 100
```

Sučelja od 20 do 24 su postavljena u *Trunk* način rada, a na njih će se spajati dugi preklopnici i usmjerivači. Oni pripadaju VLAN-u 100. Kada se sve navedeno konfigurira, upisivanjem naredbe „*show running-configuration*“ može se vidjeti sve što je u tom trenutku postavljeno na uređaju.

```
Sw1_Zg2#show running-config
Building configuration...

Current configuration : 4324 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw1_Zg2
!
enable secret 5 $1$mERr$0eGBzcy.X4Iywh9k0A29k/
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 50
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security violation protect
!
interface FastEthernet0/2
 switchport access vlan 50
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security violation protect
!
interface FastEthernet0/3
 switchport access vlan 50
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security violation protect
!
interface FastEthernet0/4
 switchport access vlan 50
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security violation protect
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode access
interface FastEthernet0/20
 switchport access vlan 60
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security violation protect
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
 switchport mode trunk
!
interface FastEthernet0/24
 switchport mode trunk
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan50
 mac-address 0060.477b.de01
 ip address 192.168.2.1 255.255.255.128
!
interface Vlan60
 mac-address 0060.477b.de02
 ip address 192.168.2.129 255.255.255.128
!
banner motd ^CSecurity Enable Access!^C
!
!
!
line con 0
 password 7 0825455E05
 login
!
line vty 0 4
 password 7 0825455E05
 login
line vty 5 15
 login
!
!
!
!
end
```

Sl. 4.3. *Primjer napravljene konfiguracije na preklopniku*

4.4. Konfiguracija usmjerivača

Osnovna konfiguracija, prethodno opisana i napravljena na preklopniku, može se identično napraviti i na usmjerivaču: naziv uređaja, sigurnost uređaja, *SSH* ili *Telnet*, ulazna poruka i drugo. Najvažnije što se na usmjerivaču mora napraviti jest uključiti i postaviti sučelja kako bi usmjerivač mogao raditi ono za što je namijenjen. Nijedno sučelje nije uključeno na novim, odnosno nekorištenim uređajima stoga, kada se nešto spoji, na sučelje u uređaju se mora postaviti stanje „*Up*“.

```
Usmjerivac_Primjer(config)#interface gigabitEthernet 0/0
Usmjerivac_Primjer(config-if)#no shutdown

Usmjerivac_Primjer(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
```

Nakon što je stanje sučelja promijenjeno u „*Up*“, mora mu se pridijeliti IP adresa, odnosno *gateway* zajedno s maskom da bi usmjerivač znao na koje sučelje koji paket mora usmjeravat te koliki je raspon IP adresa.

```
Usmjerivac_Primjer(config-if)#ip address 192.168.0.1 255.255.255.0
```

Ovakav princip se koristi kada nema VLAN-ova, nego je jedan preklopnik jedna mreža. U slučaju da se koriste VLAN-ovi, uključuje se podsučelje i koristi se naredba enkapsulacije s brojem VLAN-a.

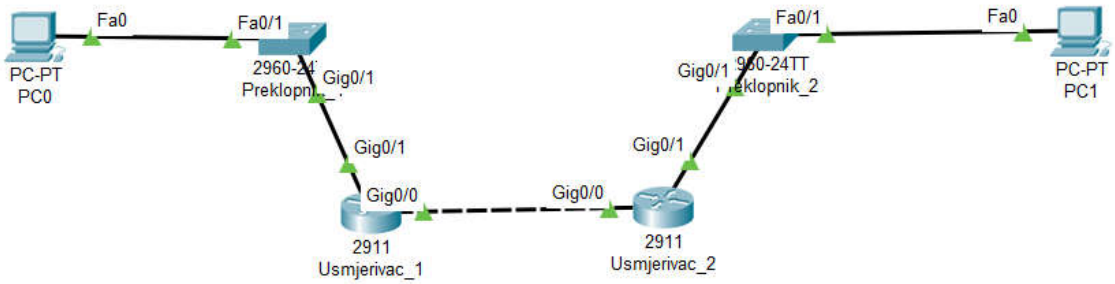
```
Usmjerivac_Primjer(config)#interface gigabitEthernet 0/0.55
Usmjerivac_Primjer(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.55, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.55,
changed state to up
Usmjerivac_Primjer(config-subif)#encapsulation dot1Q 55
Usmjerivac Primjer(config-subif)#ip address 192.168.1.1 255.255.255.0
```

Ovime je uključeno sučelje kojim je spojen preklopnik s kreiranim VLAN 55 i ovisno o broju VLAN-ova koji postoje na prekolopniku, trebaju se ponoviti ove naredbe, samo s drugim brojem VLAN-a, kako bi se mogla vršiti komunikacija među njima.

Na usmjerivaču se postavlja još jedan prethodno objašnjen protokol, a to je DHCP koji uvelike olakšava posao mrežnom administratoru. Bitna stvar je paziti na raspon IP adresa koje nalaze u mreži i na *gateway* mreže.

```
Usmjerivac_Primjer(config)#ip dhcp pool VLAN55
Usmjerivac_Primjer(dhcp-config)#default-router 192.168.1.1
Usmjerivac_Primjer(dhcp-config)#network 192.168.1.0 255.255.255.0
```

Nakon što se konfiguriraju sučelja, da bi usmjerivač izvršavao svoju zadaću, moraju se postaviti rute, statičke ili dinamičke. Obje vrste su prethodno objašnjene u radu. Na sl. 4.4 se vidi jednostavna mreža u kojoj je jednostavnije konfigurirati statičke rute jer se moraju postaviti rute samo za dva usmjerivača.



Sl. 4.4. *Primjer jednostavne mreže s dvama usmjerivačima*

Postavljanje statičke rute na Usmjerivaču_1 se radi tako da se upisuje IP adresa mreže s kojom želimo komunicirati, njena maska i IP adresa sučelja preko kojeg se dobiju podatci o mreži.

```
Usmjerivac_1(config)#ip route 192.168.2.0 255.255.255.0 192.168.0.2
```

To bi u ovom slučaju bilo sučelje *Gig 0/0* s IP adresom 192.168.0.2. Da bi se dovršilo postavljanje ruta i da bi se komunikacija između računala mogla uspostaviti, mora se postaviti ruta nazad, a to se radi na Usmjerivaču_2.

```
Usmjerivac_2(config)#ip route 192.168.1.0 255.255.255.0 192.168.0.1
```

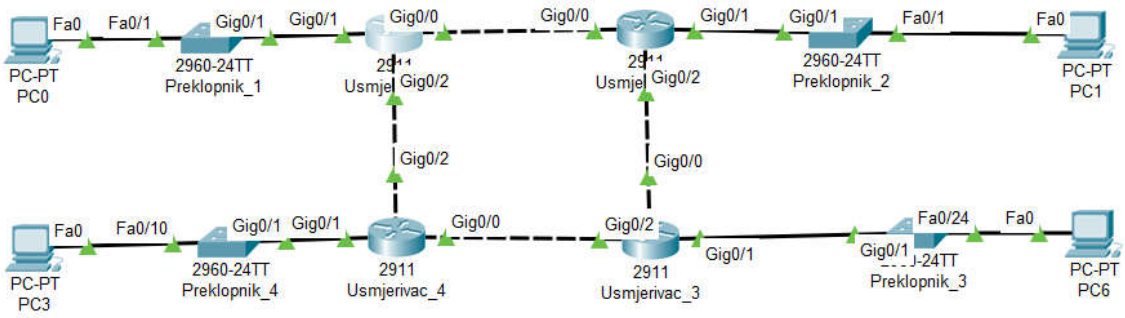
U slučaju da se pogriješi u bilo kojem od triju segmenata pri unosu statičkih ruta, ruta se može poništiti, odnosno obrisati naredbom negacije rute dodavanjem naredbe „*no*“ ispred svega.

```
Usmjerivac_2(config)#no ip route 192.168.1.0 255.255.255.0 192.168.0.1
```

Ovakvo, statičko postavljanje ruta radi se kada nije potreban veliki broj ruta jer statičke rute imaju manju vrijednost od dinamičkih. Međutim, ako mreža ima više usmjerivača i preklopnika kao na slici 4.5, potreban je veći broj statičkih ruta pa se u tom slučaju koriste dinamičke jer se broj ruta povećava četiri puta.

```
Usmjerivac_2(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.1
```

Ovakav način postavljanja ruta odnosno statičko postavljanje ruta se radi kada nije potreban veliki broj ruta, zbog toga što imaju manju vrijednost nego dinamičke rute, ali ako mreža ima više usmjerivača i više preklopnika kao na slici 4.5 potreban je veći broj statičkih ruta, pa se u tom slučaju koriste dinamičke rute jer broj ruta se povećava četiri puta.



Sl. 4.5. *Primjer malo kompliciranije mreže s četiri usmjerivača i četiri preklopnika*

Već je prije spomenuto i objašnjeno nekoliko vrsta dinamičkih protokola postavljanja ruta. Najjednostavniji i vjerojatno najčešće korišten je RIP protokol koji se treba samo aktivirati, postaviti verzija koja se želi koristiti, isključiti automatsko sažimanje te dodati mreže koje su na njega spojene jer usmjerivači komuniciraju sa susjednim usmjerivačima te oni međusobno izmjenjuju rute iz svojih tablica ruta.

```
Usmjerivac_1(config)#router rip
Usmjerivac_1(config-router)#no auto-summary
Usmjerivac_1(config-router)#version 2
Usmjerivac_1(config-router)#network 192.168.1.0
Usmjerivac_1(config-router)#network 192.168.0.0
Usmjerivac_1(config-router)#network 192.168.0.4
```

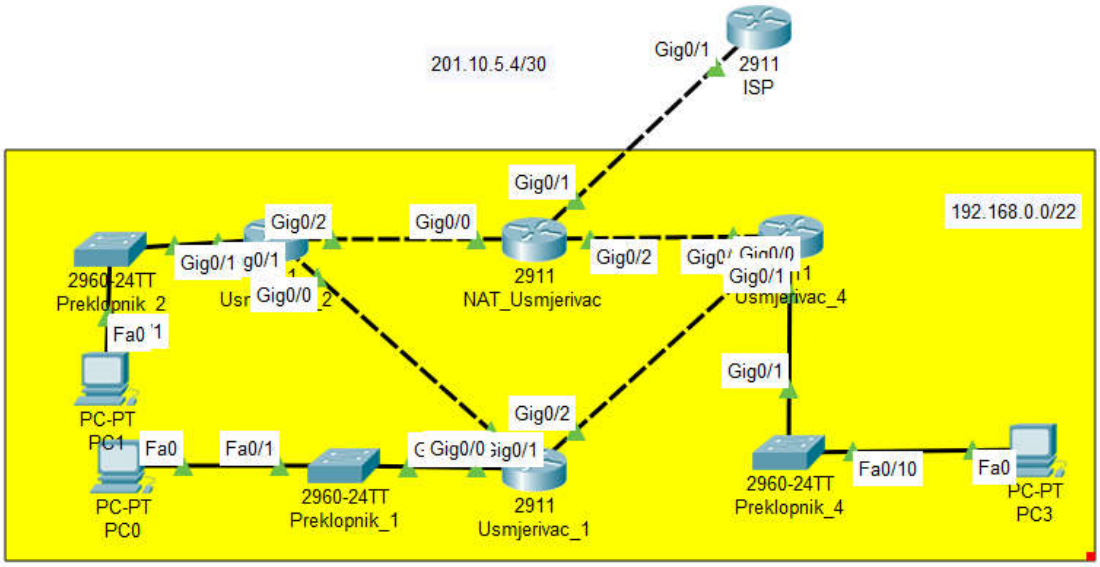
Ovom naredbom smo dodali sve mreže s kojima je Usmjerivač_1 spojen. Kada se na drugom usmjerivaču dodaju njegove susjedne mreže, ta dva usmjerivača međusobno izmijene rute iz svojih tablica pa je komunikacija između uređaja iz različitih mreža omogućena, a sve rute koje se nalaze u tablicama mogu se provjeriti naredbom „*show ip route*“.

```
Usmjerivac_1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.0.0/24 is variably subnetted, 6 subnets, 2 masks
C       192.168.0.0/30 is directly connected, GigabitEthernet0/0
L       192.168.0.1/32 is directly connected, GigabitEthernet0/0
C       192.168.0.4/30 is directly connected, GigabitEthernet0/2
L       192.168.0.6/32 is directly connected, GigabitEthernet0/2
R       192.168.0.8/30 [120/1] via 192.168.0.2, 00:00:19, GigabitEthernet0/0
R       192.168.0.12/30 [120/1] via 192.168.0.5, 00:00:00, GigabitEthernet0/2
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.253/32 is directly connected, GigabitEthernet0/1
S    192.168.2.0/24 [1/0] via 192.168.0.2
R    192.168.3.0/24 [120/1] via 192.168.0.5, 00:00:00, GigabitEthernet0/2
R    192.168.4.0/24 [120/2] via 192.168.0.5, 00:00:00, GigabitEthernet0/2
                    [120/2] via 192.168.0.2, 00:00:19, GigabitEthernet0/0
```

Unutar tablice ruta mogu se vidjeti sve mreže s kojima se može komunicirati, način na koji su rute dobivene i preko kojeg sučelja komuniciraju. Prilikom korištenja RIP protokola, u slučaju da u mreži postoji rute koje su dobivene korištenjem nekog drugog protokola ili statičke rute, informacije o njima mogu se dobiti korištenjem naredbe „*redistribute*“.

```
Usmjerivac_1(config-router)#redistribute static
```

Kada je mreža konfigurirana i svi uređaji u mreži mogu komunicirati, treba postaviti NAT koji će prevesti javnu IP adresu u privatne IP adrese koje se nalaze u kreiranoj mreži. U slučaju da se NAT ne konfigurira, uređaji u mreži se ne mogu spojiti na Internet i komunikacija bi se mogla vršiti samo između uređaja koji imaju isključivo privatnu IP adresu unutar mreže.



Sl. 4.6. *Kreirana mreža s privatnom IP adresom i ISP usmjerivač mrežnog operatera*

Prvo se moraju označiti sučelja koja su unutar naše mreže i ona koja su izvan mreže, odnosno koja su spojena na javnu IP adresu. IP adrese sučelja nije potrebno dodavati jer su ranije dodane pa ih nije potrebno ponovno unositi.

```
NAT_Usmjerivac(config-if)#int gig 0/0
NAT_Usmjerivac(config-if)#ip nat inside
NAT_Usmjerivac(config-if)#int gig 0/2
NAT_Usmjerivac(config-if)#ip nat inside
```

Nakon toga se na sučelje prema Internetu dodaje javna IP adresa i postavlja se naredba da je to izlaz iz mreže.

```
NAT_Usmjerivac(config)#int gig 0/1
NAT_Usmjerivac(config-if)#ip address 201.10.5.5 255.255.255.252
NAT_Usmjerivac(config-if)#ip nat outside
```

Da bi se NAT mogao do kraja konfigurirati, sljedeći korak je prethodno objašnjena ACL kojom će se navesti koje IP adrese mogu pristupiti Internetu, a koje ne mogu i kako će se one kasnije dodavati, odnosno detaljnije konfigurirati ACL. U ovom slučaju će se dopustiti svim IP adresama pristup Internetu.

```
NAT_Usmjerivac(config)#access-list 100 permit ip any any
```

Prema prikazu, dodana je ACL 100 koja dopušta pristup protokolu IP (u ovom slučaju, umjesto IP može biti bilo koji drugi protokol, npr. TCP, UDP, OSPF…).

Nakon toga se stavlja izvorišna adresa - u ovom slučaju, to je „*any*“, odnosno bilo koja IP adresa. Sljedeći korak je unošenje odredišne IP adrese koja je također postavljena tako da to može biti bilo koja adresa.

```
NAT_Usmjerivac(config)#ip nat inside source list 100 int gig 0/1 overload
```

Ovom naredbom je konfigurirano da sve IP adrese s ACL 100 mogu preko sučelja *gig 0/1* pristupiti javnoj IP adresi, a naredba „*overload*“ znači da istodobno veći broj IP adresa može koristiti NAT.

ACL liste mogu, kako je već spomenuto, nešto dopustiti ili zabraniti. Budući da se za najjednostavniju konfiguraciju NAT-a morala dodati ACL lista kako bi svi uređaji mogli pristupiti Internetu, tako se moglo konfigurirati da samo neki uređaji mogu pristupiti, dok drugi ne mogu ili se mogao postaviti raspon IP adresa koje imaju pristup, a ostale da nemaju.

Na principu ACL lista također se može konfigurirati da neki uređaji, odnosno IP adrese, mogu pristupiti Internetu, ali da pritom ne mogu pristupiti kompletnom sadržaju koji se nudi ili nekom protokolu. Važno je kod ACL lista znati da se ne koristi maska mreže, nego *wildcard* koja je zapravo zrcaljena maska mreže. Ako je maska mreže 255.255.255.0, *wildcard* bi bilo 0.0.0.255. Postoje dva načina unosa ACL tvrdnji. Prvi je da se cijela tvrdnja napiše u jednom redu.

```
Usmjerivac 2(config)#access-list 15 deny host 192.168.1.21
```

Drugi način je da se unutar ACL pišu sve tvrdnje koje želimo zabraniti ili dopustiti.

```
Usmjerivac_2(config)#ip access-list standard 50
Usmjerivac_2(config-std-nacl)#deny host 192.168.1.5
Usmjerivac_2(config-std-nacl)#deny host 192.168.1.55
```

Prilikom konfiguracije ACL liste važno je znati da je standardne ACL bolje unositi na usmjerivač što bliže izvoru, dok je za proširene bolje da budu konfigurirane na usmjerivač što bliže odredištu.

```
Usmjerivac_2(config)#ip access-list extended 150
Usmjerivac_2(config-ext-nacl)#deny tcp host 192.168.2.5 eq telnet host
192.168.2.253 eq telnet
```

Primjer zabrane uređaju s IP adresom 192.168.2.5 da preko telneta pristupi uređaju s IP adresom 192.168.2.253, odnosno preklopniku. Pri konfiguraciji ACL postoji velik broj mogućnosti i načina filtriranja paketa, no pritom se mora paziti na kojem usmjerivaču što zabraniti, odnosno dopustiti. Mora se paziti na redoslijed kojim se upisuju naredbe jer prije napisane naredbe imaju prioritet.

Drugim riječima, tvrdnje se gledaju redom i tvrdnje s manjim brojem imat će veću važnost od onih s većim brojem. Sve naredbe koje su konfigurirane za ACL mogu se pogledati unošenjem naredbe „*show access-lists*“ .

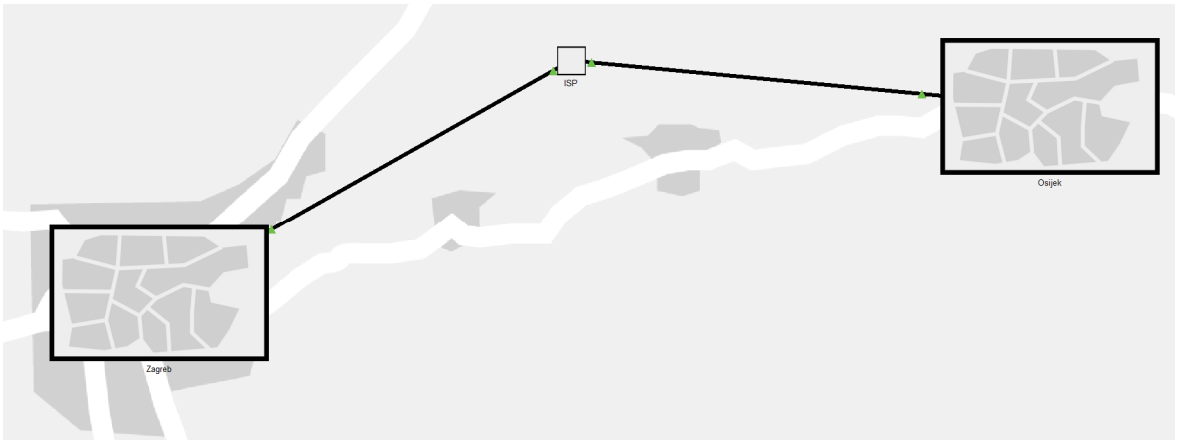
```
Usmjerivac_2#show access-lists
Standard IP access list 15
    10 deny host 192.168.1.21
Standard IP access list 50
    10 deny host 192.168.1.5
    20 deny host 192.168.1.55
Extended IP access list 150
    10 deny tcp host 192.168.2.5 eq telnet host 192.168.2.253 eq telnet
```

5. REZULTATI I IZGLED MREŽE

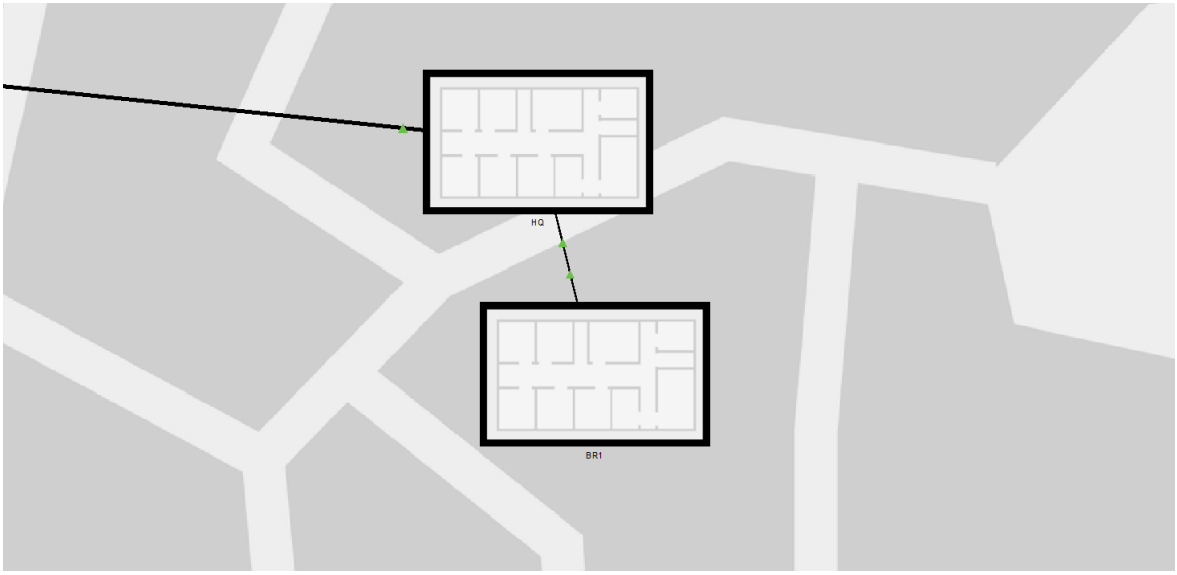
Unutar ovog poglavlja biti će napravljene i opisane dvije mreže, jedna će biti napravljena kao simulacija u računalnom programu *Packet Tracer,* dok će druga biti napravljena na stvarnim uređajima proizvođača *Cisco Systems.* Mreže će se razlikovati po tome što se, koristeći računalni program, može dodati velik broj uređaja koji se mogu posložiti kao da se nalaze na različitim lokacijama, dok će mreža napravljena na stvarnim uređajima zbog ograničenih resursa biti na istoj lokaciji predstavljena kao više mreža odnosno VLAN-ova na nekoliko uređaja.

5.1. Simulacija mreže u Packet Traceru

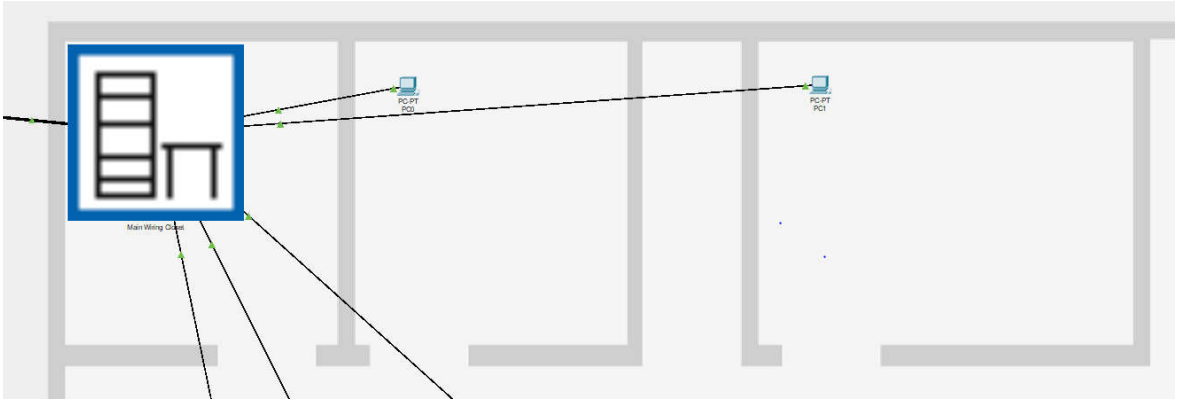
Mreža koja je napravljena u *Packet Traceru* sastoji se od nekoliko mreža konfiguriranih na nekoliko lokacija, komunikacija između njih je u prvom slučaju napravljena korištenjem kabela. U drugom slučaju udaljenost je prevelika pa je komunikacija realizirana preko mrežnog poslužitelja, odnosno komunikacija između uređaja na različitim lokacijama vršit će se preko Interneta. Zadatak je napraviti kompletan dizajn i konfiguraciju za tvrtku koja se nalazi na tri lokacije: glavnog ureda koji se nalazi u Osijeku, još jednog ureda također u Osijeku samo na drugoj lokaciji i trećeg ureda koji se nalazi u Zagrebu. S obzirom da se dva ureda nalaze unutar istog grada, mogu se povezati kabelom između njihovih usmjerivača, dok se treći ured mora povezati preko Interneta. Tvrtka je sastavljena od odjela za razvoj, administratore mreže i ostale korisnike koji se bave financijama, dizajnom, marketingom i drugim poslovima - te tri grane bave se zasebnim poslom, zato se svaki od računala na kojima oni rade postavlja u različite mreže kako bi imali različita prava u mreži i ne bi jedni drugima mogli smetati u poslu. Tako svaki uređaj koji se spaja u mrežu mora biti spojen u određenu LAN utičnicu koja se nalazi u određenom VLAN-u. Unutar glavnog ureda se nalaze serveri koji su maksimalno zaštićeni i kontroliraju pristup na resurse - DNS, FTP, SYSLOG. Infrastrukturnim uređajima može se pristupit preko mreže koristeći SSH protokol koji mogu koristit samo mrežni administratori jer je sva mrežna infrastruktura zaštićena. Bez obzira na zaštitu, svaki korisnički uređaj bi morao komunicirati s ostalim uređajima bez obzira na njegovu lokaciju i mrežu kojoj se nalazi.



Sl. 5.1. *Fizički prikaz dizajnirane mreže na različitim lokacijama u Packet Traceru*



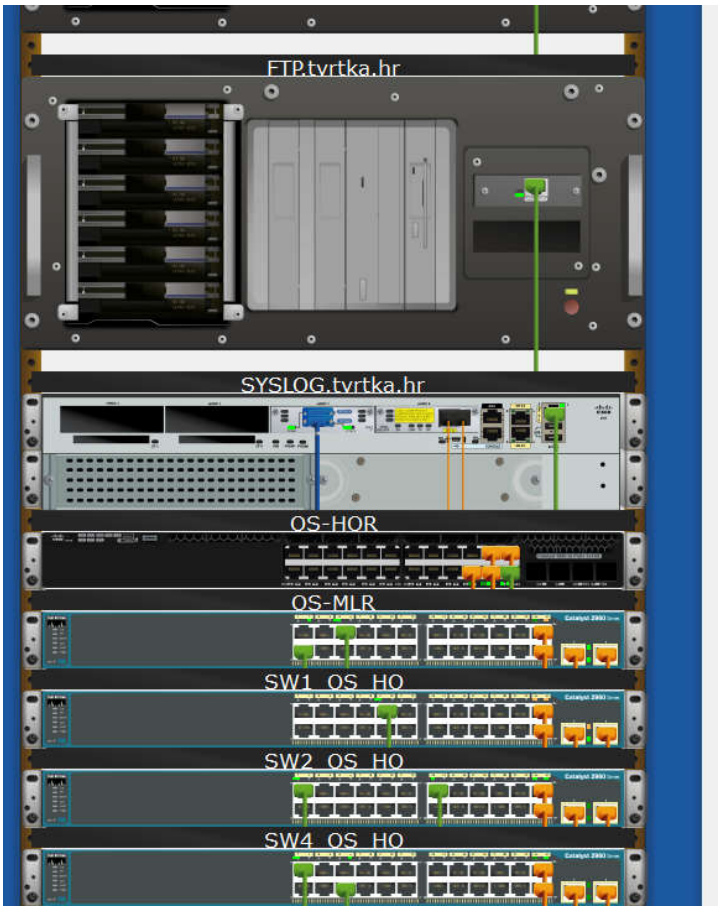
Sl. 5.2. *Fizički prikaz mreže u Osijeku na dvije lokacije odnosno zgrade u Packet Traceru*



Sl. 5.3. *Fizički prikaz mreže glavnog ureda u Osijeku*

Već je prije u radu spomenuto da se u *Packet Tracer*u može birati između fizičkog i logičkog prikaza mreže, što može uvelike olakšati posao dizajniranja mreže.

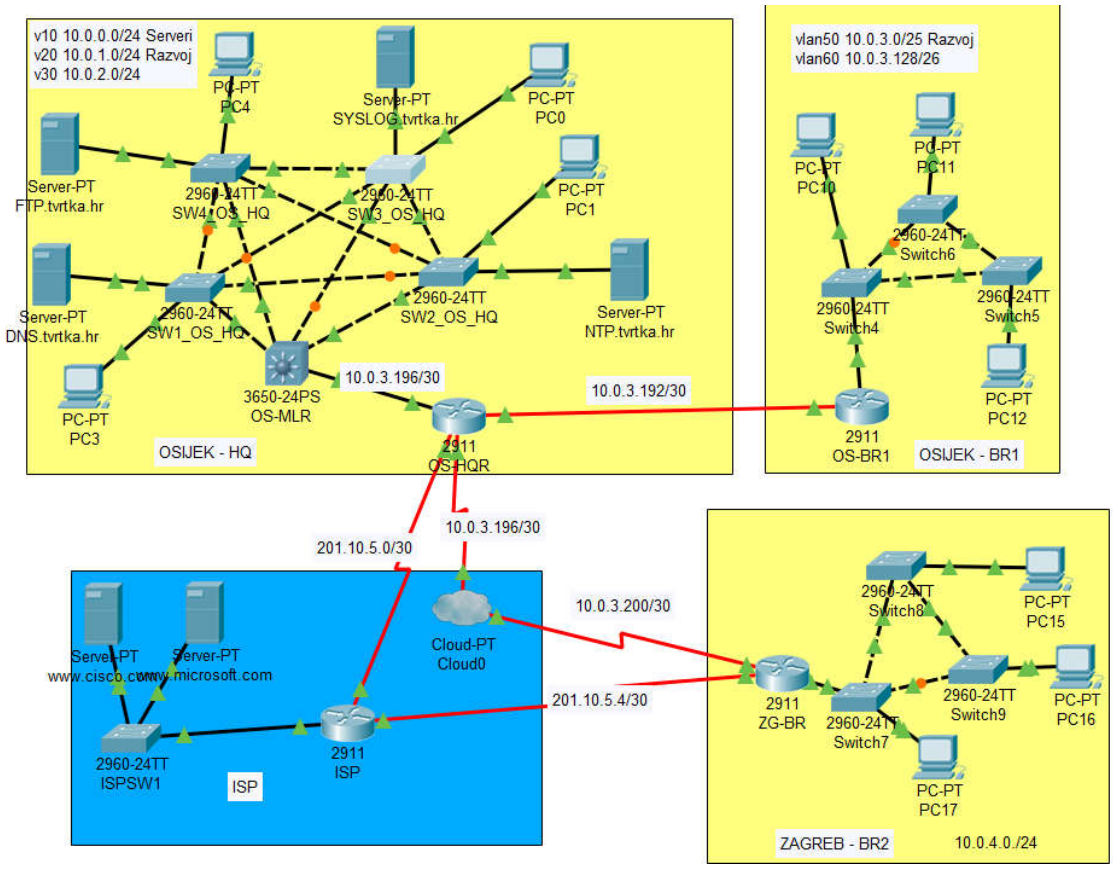
Kako se može vidjeti na slici 5.1., fizički je prikazana mreža na velikom prostoru, odnosno, u ovom slučaju, mreža između dvaju gradova. Slika 5.2 je zumiran prikaz slike 5.1 gdje se može vidjeti što je sve povezano unutar jednog grada (u ovom slučaju Osijeka) te kako se svaka ta zgrada može sastojati od više katova ili ureda od kojih svaki može biti neka zasebna podmreža. Daljnjim zumiranjem dobiva se slika kao se na slici 5.3 gdje je fizički prikazan raspored mrežnih uređaja i računala po katovima. Daljnjim zumiranjem se može vidjeti kako izgleda unutrašnjost jednog mrežnog ormara u kojemu se nalaze svi mrežni uređaji, od usmjerivača, preklopnika, servera i drugih uređaja te kako su oni spojeni, slika 5.4.



Sl. 5.4. *Fizički prikaz mrežnog ormara glavnog ureda u Osijeku uz simulacijski program*

U fizičkom prikazu lakše je predočiti kako će izgledati stvarna mreža, kako se bude što spojilo, ali koristeći simulacijski program *Packet Tracer,* puno je lakše dizajnirati mrežu u logičkom prikazu, gdje je najbitnije kako koncipirati mrežu na najbolji način.

U većini slučajeva mreža se prvo kreira u logičkom prikazu gdje se dodaju mrežni uređaji koji su nam potrebni za uspostavu komunikacije - koje vrste kablova koji će se koristiti, na koje portove spojiti koji kabel odnosno uređaj. Postoji mnogo stvari kojima se može poslužiti kako bi se kasnije lakše snalazilo u mreži, kao što su imena uređaja, koji rasponi IP adresa će se koristiti za pojedinu podmrežu ili VLAN, može se dodati napomena za pojedine uređaje koje IP adrese će koristit…



Sl.5.5. *Logički prikaz kompletne mreže rada u Packet Traceru*

Slika 5.5. prikazuje logički prikaz mreže koja se radila kao simulacijski dio ovog rada, na njemu se može vidjeti koji su se sve uređaji koristili, na koji način su spojeni te koje IP adrese su korištene. Cijela mreža se realizirala s 10.0.0.0/22 privatnim rasponom IP adresa, koji se zatim podijelio na nekoliko manjih podmreža s maskom 24. Za većinu mreža, odnosno VLAN-ova je korištena maska 24 sa slobodnih 252 IP adrese kako bi se ostavilo prostora u slučaju da se poveća broj uređaja koji se moraju dodati u mrežu. Za međusobno spajanje dvaju usmjerivača koristila se mreža s maskama 30, odnosno s dvije slobodne IP adresa kao bi se svakom usmjerivaču mogla dodijeliti jedna jer je nepotrebno koristit mrežu s većim rasponom IP adresa jer bi ostale IP adrese

ostale neiskorištene. Koristilo se pet VLAN-ova zbog toga što se koristi više preklopnika koji se mogu nalaziti na trima različitim mjestima, a uređaji koje korisnici spajaju koriste se za različite tipove posla koji se na njima obavljaju (administracija, razvoj..). Na svakom preklopniku postoji određeni broj portova na koje se spajaju korisnici koji rade na razvoju ili administratori koji upravljaju mrežom. Zbog toga se u glavnom uredu u Osijeku koriste tri VLAN-a. U drugom uredu, nema potrebe za VLAN-om na koji se spajaju serveri ili se upravlja s mrežom, nego samo za razvoj i ostale administrativne poslove pa su tamo kreirana samo dva VLAN-a. U trećem uredu koji se nalazi u Zagrebu radi se samo na razvoju, tako da tamo nije bilo potrebno kreirati više VLAN-ova, nego samo jednu podmrežu u kojoj će se spajati uređaji koji se koriste za razvoj, kako se može vidjeti u tablici 5.1.

Tablica 5.1. *Korišteni VLAN-ovi*

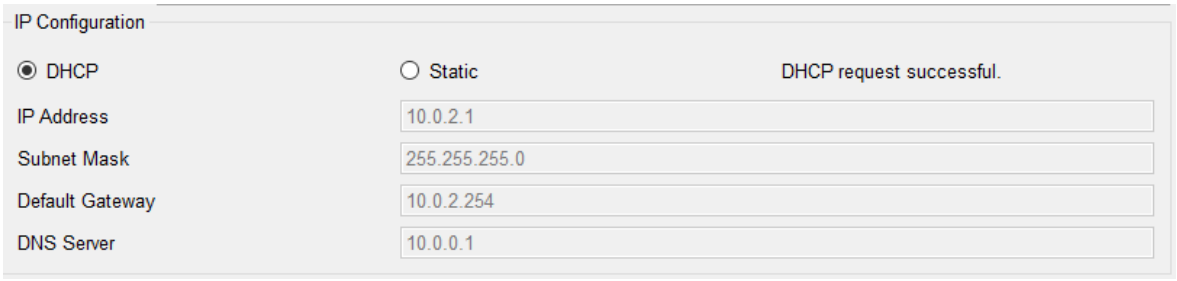
Lokacija	Oznaka	VLAN	Naziv	Podmreža	Raspon IP adresa
Osijek	OS-HQ	VLAN10	Serveri	10.0.0.0/24	10.0.0.1-10.0.0.253
		VLAN 20	Razvoj	10.0.1.0/24	10.0.1.1-10.0.1.253
		VLAN 30	Ostali	10.0.2.0/24	10.0.2.1-10.0.2.253
	OS-BR1	VLAN 40	Razvoj	10.0.3.0/25	10.0.3.1-10.0.3.126
		VLAN 50	Ostali	10.0.3.128/26	10.0.3.129-10.0.3.190
Zagreb	ZG-BR		Razvoj	10.0.4.0/24	10.0.4.1-10.0.4.253

Unutar glavnog ureda ili OS-HQ, kako je označeno, nalazi se jedan usmjerivač OS-HQR koji je zadužen za povezivanje svih dijelova mreže, preko njega su povezani i OS-BR1 koristeći kabel i ZG-BR preko ISP-a. Da bi se OS-HQ i ZG-BR mogli povezati preko ISP ili jednostavnije Interneta, na usmjerivaču OS-HQR mora se postaviti NAT protokol kojim će se javna IP adresa s poslužitelja odnosno ISP-a prevoditi u privatnu. Kako je usmjerivač OS-HQR najbliže ISP-u, kada se na njemu postavi NAT, svi uređaji koji se nalaze iza njega i imaju postavljene usmjerivačke rute moći će pristupiti Internetu preko njega. Cijela konfiguracija usmjerivača OS-HQR se nalazi u prilogu P.5.1. U radu je korišten višeslojni preklopnik za koji je unaprijed rečeno da može raditi i na drugom i na trećem sloju, zbog toga on ovdje izvršava zadaću usmjerivača preko kojega je omogućena komunikacija između svih uređaja koji se nalaze u OS-HQ, kao i onih koji se nalaze u drugim uredima. Razlog korištenja višeslojnog preklopnika, a ne usmjerivača, je taj što na njemu postoji veći broj portova na koji se mogu spojiti obični preklopnici i usmjerivač, kako je i napravljeno. Kako on izvršava zadaću usmjerivača, u ovom slučaju na njemu su konfigurirani VLAN-ovi koji se koriste u OS-HQ.

Također je konfiguriran DHCP kako bi se dinamički dodijelile IP adrese uređajima u OS-HQ te kako je on najbliži „usmjerivač“ serverima, na njemu se konfiguriraju proširene kontrolne liste kojima se dopušta pristup samo određenim IP adresama prema serverima, cijela konfiguracija OS-MLR se nalazi u prilogu P.5.2

```
access-list 100 permit udp any host 10.0.0.1 eq domain
access-list 100 permit tcp 10.0.1.0 0.0.0.255 host 10.0.0.2 eq ftp
access-list 100 permit tcp 10.0.3.0 0.0.0.127 host 10.0.0.2 eq ftp
access-list 100 permit udp host 10.0.3.194 host 10.0.0.3 eq 514
```

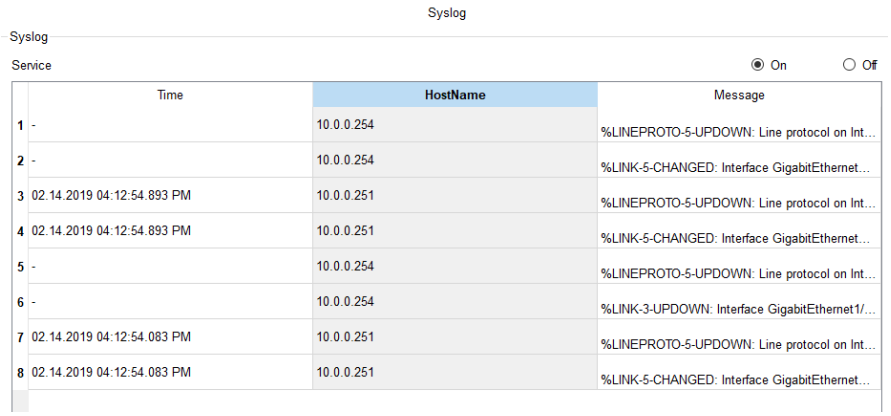
Na svakom standardnom preklopniku napravljene su standardne konfiguracije - konfiguracija SSH protokola kako bi se moglo pristupiti uređajima preko mreže, ali to mogu samo administratori, VLAN te koji port pripada kojem VLAN-u i koji način rada je postavljen za koji port. Sva četiri preklopnika imaju gotovo istu konfiguraciji, jedina razlika je u IP adresama, a cijela konfiguracija se nalazi u prilogu P.5.3. Za svako računalo koje se naknadno priključi u mrežu, mora se paziti na koji port preklopnika će se spojiti, da se ne bi spojilo u krivi VLAN, a zahvaljujući DHCP-u OS-MLR će mu dodijeliti prvu slobodnu IP adresu, slika 5.6.



Sl. 5.6. *Dinamičko dodjeljivanje IP adrese*

Kako je OS-HQ središte tvrtke, tako je i sjedište svih lokalnih mreža koji su dio tvrtke te se zbog toga tu nalaze serveri, preciznije, četiri servera od kojih svaki ima svoju zadaću. Prvi server je FTP server koji se koristi za prijenos podataka i njemu se moralo IP adresu dodati statički jer se u cijeloj mreži mora znati koju on ima IP adresu, a da je i dobio IP adresu preko DHCP, drugi put možda ne bi dobio istu adresu i došlo bi do problema u mreži. Drugi server je DNS server koji služi za prevođenje njegove IP adrese u neku internetsku domenu, kod nas je to: dns.tvrtka.hr te kao i kod prvog servera, njemu se mora dodati IP adresa statički zbog istog razloga. Treći server je NTP server na kojem je postavljeno vrijeme i preko kojega svi uređaji u mreži mogu sinkronizirati svoje vrijeme te kao i na prethodnim serverima, njemu se mora postaviti statička IP adresa. Četvrti server je SYSLOG koji bilježi sve promjene u mreži, ovisno o tome što se postavi da bilježi, bilo to da se dodao novi uređaj ili neki izbacio, da je došlo do pogreške ili drugo.

SYSLOG server će zabilježiti i spremiti što se dogodilo i u kojemu se točno trenutku dogodilo te za njega isto vrijedi kao i za ostale servere - da mora imati jedinstvenu statičku IP adresu. Zabilježene stvari se mogu vidjeti na slici 5.7.



	Time	HostName	Message
1	-	10.0.0.254	%LINEPROTO-5-UPDOWN: Line protocol on Int…
2	-	10.0.0.254	%LINK-5-CHANGED: Interface GigabitEthernet…
3	02.14.2019 04:12:54.893 PM	10.0.0.251	%LINEPROTO-5-UPDOWN: Line protocol on Int…
4	02.14.2019 04:12:54.893 PM	10.0.0.251	%LINK-5-CHANGED: Interface GigabitEthernet…
5	-	10.0.0.254	%LINEPROTO-5-UPDOWN: Line protocol on Int…
6	-	10.0.0.254	%LINK-3-UPDOWN: Interface GigabitEthernet1/…
7	02.14.2019 04:12:54.083 PM	10.0.0.251	%LINEPROTO-5-UPDOWN: Line protocol on Int…
8	02.14.2019 04:12:54.083 PM	10.0.0.251	%LINK-5-CHANGED: Interface GigabitEthernet…

Sl. 5.7. *Bilješke na SYSLOG serveru*

Ured koji se još nalazi u Osijeku je OS-BR1 koji nije na istoj lokaciji, ali nije predaleko smješten tako da se može povezati kabelom. Taj dio tvrtke zadužen je za razvoj i ostale poslove za koje su potrebna računala, ali nema servera ili uređaja kojima moraju upravljati administratori pa su samo dva VLAN-a. U OS-BR1 nalazi se jedan usmjerivač i nekoliko preklopnika zbog većeg broja uređaja koji se mogu spojiti. Usmjerivač OS-BR1 koristi se kako bi računala iz VLAN-ova 50 i 60 mogli komunicirati međusobno, kao i s ostalim uređajima na drugim lokacijama. Na tom usmjerivaču bilo je potrebno napraviti osnovnu konfiguraciju, postaviti sučelje i DHCP protokol za VLAN-ove i jednu *default*-nu statičku rutu pri ISP-u. Treći ured koji se nalazi u sklopu tvrtke je u Zagrebu. Budući da je on predaleko smješten i izravno spajanje bi bilo preskupo, koristi se usluga internetskog poslužitelja kako bi se svi uredi mogli povezati. Konfiguracija usmjerivača ZG-BR je gotovo identična kao i usmjerivača OS-BR1, razlika je što nema VLAN-ova nego je jedna podmreža te su IP adrese i usmjerivačke rute malo drukčije, a druga razlika je što se na njemu isto morao podesiti NAT jer ne bi imao pristup ISP-u pa samim time ne bi mogao komunicirati s ostalim uredima. U svakom uredu su korištena barem tri preklopnika, a razlog tome nije samo veći broj portova, nego da se svi mogu međusobno povezati. U slučaju da dođe do prestanka rada jednog od njih, ostali mogu normalno raditi i međusobno komunicirati bez njega. Kako su konfiguracije gotovo svih usmjerivača skoro iste, s jedinom razlikom u IP adresama, u prilogu P 5.4 nalazit će se konfiguracija samo jednog od njih.

5.2. Lokalna mreža na stvarnoj Cisco opremi

Cisco Systems je jedan od najvećih i najpoznatijih proizvođača mrežne opreme, a kako se oni većinom bave proizvodnjom opreme za velika poduzeća, a ne toliko za krajnje korisnike, Cisco proizvodi su vrlo skupi. Zbog skupoće Cisco opreme, ovaj dio rada je napravljen korištenjem ograničene količine opreme, odnosno: usmjerivačem i dvama preklopnicima. Oba preklopnika su Cisco Catalyst serije 2950, no nisu potpuno isti, jedan je WS-C2950-24 koji sadrži 24 porta s brzinom prijenosa 10/100Mbps, dok je drugi WS-C2950T-24 koji sadrži isto 24 porta 10/100Mbps i dodatna dva porta 10/100/1000 Mbps.

Sl. 5.8. *Cisco usmjerivač WS-C2950T-24 (iznad) i Cisco usmjerivač WS-C2950-24 (ispod)*

Broj portova i njihova brzina nisu jedina razlika, postoji još mnogo opcija i stvari po kojima se ta dva preklopnika razlikuju, no te razlike i dodatne opcije u ovom radu, odnosno osobnoj upotrebi, ne mogu se primijetiti. Detaljne karakteristike svakog od njih se mogu pronaći u [38] za WS-C2950-24 i [39] za WS-C2950T-24 Cisco Catalyst preklopnik. Usmjerivač je jedan od starijih modela, a to je Cisco 1760 koji tvornički ima samo jedan ulaz za spajanje konzolnog kabela, AUX kabela i Ethernet kabela, čime od početka postoji ograničenje.

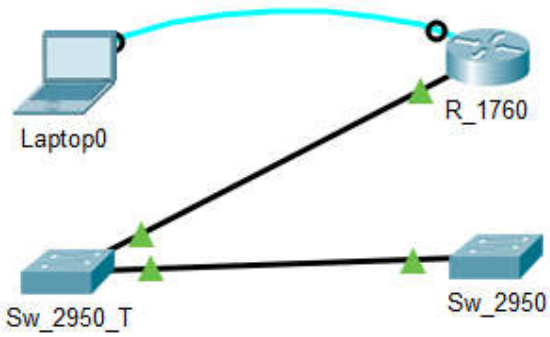
Sl. 5.9. *Cisco 1760 usmjerivač*

Ovaj model ima četiri otvora unutar kojeg se mogu ugraditi dvije WIC (engl. *WAN Interface Card*) kartice i dvije VIC (engl. *Virtual Interface Card*) kartice koje se moraju nabaviti i ugraditi posebno. Detaljnije specifikacije usmjerivača Cisco 1760 na [40].

Od dodatne opreme, potrebni su nam normalni Ethernet kabel za povezivanje uređaja međusobno i krajnjih uređaja odnosno računala i konzolni kabel preko kojeg je jedino moguće napraviti početnu konfiguraciju. Zbog toga što danas sve manje novih računala ima utor da se izravno može uključiti kabel za serijsku komunikaciju (RS-232), potreban je još i adapter sa serijskog utora na USB utor.

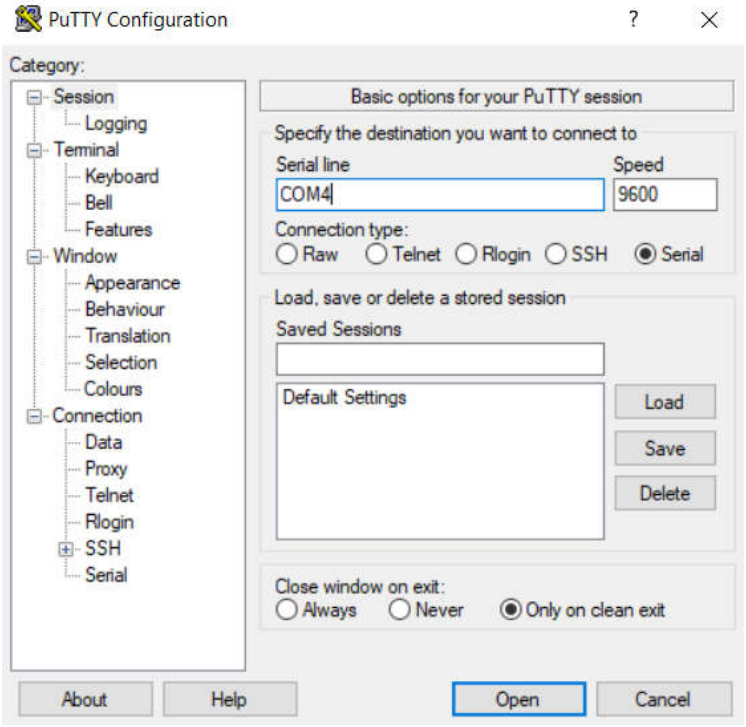
Sl. 5.10. *Konzolni kabel (desno) i adapter na USB (lijevo)*

Kako je već prije rečeno, zbog vrijednosti opreme, na raspolaganju je ograničena količina uređaja kojom bi se mogla realizirati prava lokalna mreže. Na svakom od uređaja je potrebna osnovna konfiguracija, VLAN-ovi na preklopnicima i konfiguracija da se postavkama uređaja može pristupiti preko mreže. Mreža je izrađena prema shemi sa slike 5.11 koja je napravljena u *Packet Traceru*.



Sl. 5.11. *Shema lokalne mreže na stvarnoj opremi*

Svaki uređaj se prvo posebno mora povezati s računalom koristeći konzolni kabel preko kojeg će se raditi konfiguracija, a da bi se moglo spojiti, mora se koristit jedan kod program za pristup uređaju serijski. Program preko kojeg će to biti realizirano je *Putty* unutar kojeg se mora odabrati serijski pristup i preko kojeg od portova na računalu će se pristupiti uređaju. Koristeći *Putty,* moguće je pristupiti uređajima preko mreže koristeći SSH ili Telnet, ali to je moguće tek kad se preko konzolnog kabela napravi konfiguracija uređaja i zna se IP adresa svakog uređaja.



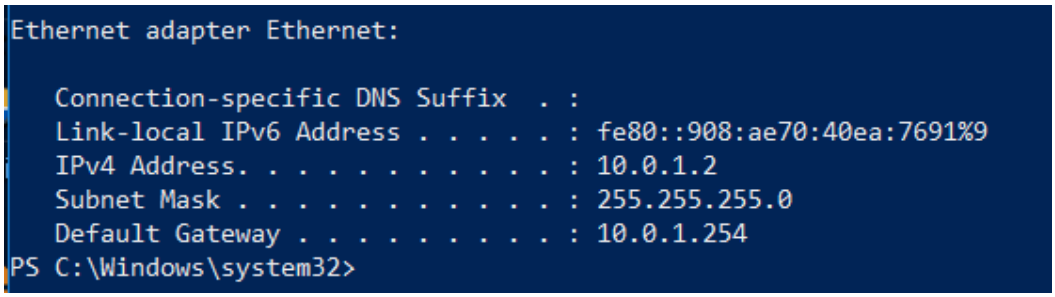
Sl. 5.12. *Računalni program Putty za računalo preko kojeg se pristupa mrežnim uređajima*

Zbog toga što koristeći stvarne uređaje nemamo tako lijep prikaz gdje se što nalazi, kao kad se radi u simulacijskom programu, dobro je napraviti shemu i bilješke za sljedeće: koji uređaj se gdje nalazi, gdje se i s čim spaja, koje IP adrese se koriste... Kako postoje ograničenja zbog opreme koja je zastarjela, mnogo stvari, kao i u simulaciji, nije moguće napraviti. Na usmjerivaču je konfigurirana osnovna konfiguracija i zaštitna konfiguracija dok je od protokola konfiguriran DHCP i podmreže za svaki VLAN. Konfiguracija na stvarnim uređajima mnogo se sporije obavlja nego u simulacijskom programu te postoji puno više opcija nego što je ponuđeno na uređajima u *Packet Traceru.* Prilikom konfiguracije preklopnika, došlo je od nekoliko prepreka jer, kako je već prije rečeno, oprema je zastarjela pa neke od opcija koja su inače moguće na ovakvim uređajima nisu bile dostupne. Uređaji su konfigurirani prema tablici 5.2 te su navedena sučelja koja su korištena i IP adrese koje su korištene.

Tablica 5.2. *Korištena sučelja i IP adrese*

Uređaj	Oznaka	Sučelja	VLAN	Mreža	IP Adresa *(default getway)*	Raspon Adresa
Usmjerivač	R_1760	FastEthernet 0/1				
1. Preklopnik	Sw_2560_T	FastEthernet 0/1-5	VLAN 10	10.0.0.0/24	10.0.0.254	10.0.0.1-10.0.0.253
		FastEthernet 0/6-10	VLAN 20	10.0.1.0/24	10.0.1.254	10.0.1.1-10.0.1.253
		FastEthernet 0/11-15	VLAN 30	10.0.2.0/24	10.0.2.254	10.0.2.1-10.0.2.253
		FastEthernet 0/16-20	VLAN 40	10.0.3.0/24	10.0.3.254	10.0.3.1-10.0.3.253
2. Preklopnik	Sw_2560	FastEthernet 0/1-5	VLAN 10	10.0.0.0/24	10.0.0.253	10.0.0.1-10.0.0.252
		FastEthernet 0/6-10	VLAN 20	10.0.1.0/24	10.0.1.253	10.0.1.1-10.0.1.252
		FastEthernet 0/11-15	VLAN 30	10.0.2.0/24	10.0.2.253	10.0.2.1-10.0.2.252
		FastEthernet 0/16-20	VLAN 40	10.0.3.0/24	10.0.3.253	10.0.3.1-10.0.3.252

Da bi se mogao provjeriti rad mreže, spojeno je računalo preko kojeg bi se moglo provjerit radi li mreža. Da bi se mogao vidjeti i provjeriti rad mreže, mora se provjeriti je li računalo dobilo IP adresu VLAN-a u kojem se nalazi, a to se može vidjeti upisivanjem naredbe *IPconfig* u CMD (eng. *Command Prompt*).



Sl. 5.13. *Provjera dobivene adrese korištenjem DHCP na prvom računalu.*

```
C:\Users\Sutko>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::78d4:d06e:8cea:f465%10
   IPv4 Address. . . . . . . . . . . : 10.0.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.254
```

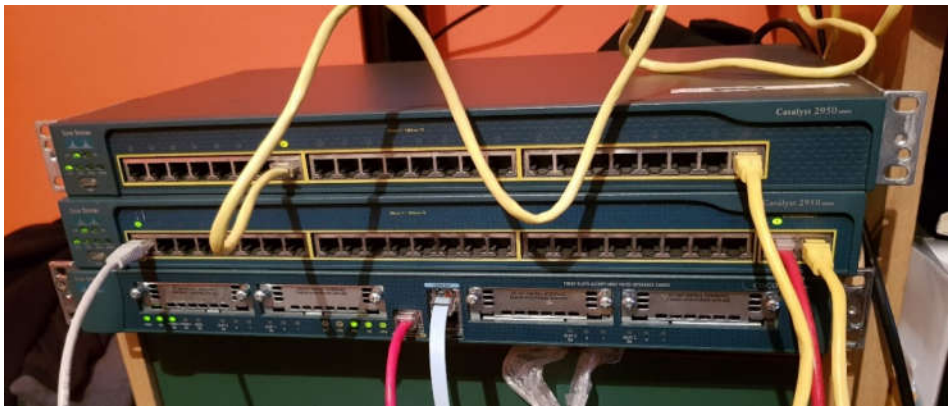
Sl. 5.14. *Provjera dobivene adrese korištenjem DHCP na prvom računalu.*

S obzirom da se na slikama 5.13 i 5.14 može vidjeti da su oba računala uspješno dobila IP adrese, može se zaključiti da DHCP radi, a kako bi se provjerila komunikacija između njih, koristi se naredba *ping* i IP adresa računala kojima se želi provjeriti komunikacija.

```
PS C:\Windows\system32> ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time=1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Sl. 5.15. *Provjera komunikacije između dvaju uređaja iz dvaju VLAN-ova korištenjem naredbe PING*

Prema slici 5.15 moguće je vidjeti kako je komunikacija između prvog računala koji se nalazi u VLAN-u 20 i drugog računala koji se nalazi u VLAN-u 10 uspostavljena i provjerena naredbom *ping* unutar CMD prozora.



Sl. 5.16. *Konačan izgled mreže*

5.3. Usporedba stvarne mreže i mreže u simulacijskom programu

Prilikom izrade ovog rada, susrelo se s dizajniranjem i konfiguracijom mreže u Ciscovom simulacijskom programu *Packet Tracer* koji je napravljen kako bi korisnici koji nisu u mogućnosti raditi na pravoj Cisco opremi mogli istraživati i učiti raditi na Cisco mrežnoj opremi. Unutar programa se može dodavati mnoštvo uređaja - bilo to mrežnih uređaja, servera, računala, IoT uređaja i drugih stvari na kojima se može konfigurirati jako puno stvari i samim time napraviti mrežu koju se konstantno može nadograđivati. Budući da je program napravljen za učenje i vježbanje, uvelike je prilagođen za početnike, stoga, ako dođe do neke pogreške, u programu je puno lakše naći rješenje ili u krajnjem slučaju - obrisati uređaj i konfigurirati novi. S druge strane, prilikom korištenjem stvarne opreme, stvari nisu tako jednostavne. Stvarni uređaji imaju neke svoje procese koji se u simulaciji mogu ubrzati ili preskočiti, dok prilikom korištenja stvarnog uređaja takvo nešto nije moguće. Prilikom najjednostavnije konfiguracije zaštite uređaja, može se slučajno dogoditi da se lozinka krivo postavi, a bez nje se uređaju više ne može pristupiti. Koristeći simulaciju, jednostavno bi se uređaj obrisao i konfigurirao bi se drugi, dok se prilikom takve pogreške na stvarnom uređaju ne može tako lako problem riješiti. Korištenjem stvarne opreme na raspolaganju je puno više opcija koje je moguće uključiti, dok s druge strane - ako se koristi starija oprema, neke od opcija na takvim uređajima nisu dostupne. Prilikom izrade ovog rada došlo je do nekoliko problema s konfiguracijom stvarnih uređaja. Neki od njih su se mogli riješiti na dulji način, dok je neke od njih bilo nemoguće riješiti jer uređaji ne posjeduju takve opcije ili usluge. Jedan od problema je bio da na preklopnicima ne postoji opcija postavljanja SSH protokola za pristupanje uređajima preko mreže, dok u *Packet Traceru* svaki uređaj posjeduje tu opciju. Većina novih uređaja posjeduje opciju AUTO MDI-X (engl. *AUTO medium dependent interface*) koja omogućuje korištenje bilo kakvog mrežnog kabela (*crossover i straight-through*) prilikom spajanja uređaja iste vrste. U slučaju da uređaj nema tu opciju, ako se koristi pogrešan kabel, uređaji neće moći komunicirati. Teško je raditi usporedbe mreža u ovom radu jer uređaji nisu isti. Uređaji koji su korišteni u izradi stvarne mreže, u simulacijskom programu više ne postoje jer se rijetko gdje u praksi koriste. Drugi razlog je ograničenost opreme jer je gotovo nemoguće konfigurirati mnogo osnovnih stvari koje su u simuliranoj mreži napravljene, kao što su rute ili NAT i već spomenuti SSH. Korištenje stvarne opreme ima mnogo razlika koje na kraju rezultiraju korištenjem nekih opcija koje se u simulaciji ne koriste često jer se na shemi mogu vidjeti ili provjeriti prelaskom miša preko uređaja, a na stvarnim uređajima tako nešto nije moguće. Neke od tih opcija su provjera susjednih sučelja korištenjem naredbe „*show ip interface brief*“ koja je korisna u slučaju da se u nekim poduzećima koristi puno opreme koja nije na istom mjestu.

```
OS-HQ1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     10.0.3.198      YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
GigabitEthernet0/0/0   10.0.3.193      YES manual up                    up
Serial0/1/0            201.10.5.2      YES manual up                    up
Serial0/1/1            10.0.3.201      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Sl. 5.17. *Ispis prilikom korištenje naredbe „show ip interface brief*“

Naredba koja se često koristi u praksi je i „*show cdp neighbors*“, a služi za provjeru koji uređaj je spojen na koje sučelje, no ova naredba jedino ima smisla kada su uređajima dodana imena.

```
OS-HQ1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
M-SW-OS      Gig 0/0          160                     3650        Gig 1/0/24
ISP          Ser 0/1/0        160            R        C2900       Ser 0/0/0
```

Sl. 5.18. *Ispis prilikom korištenje naredbe „show cdp neighbors“*

Navika koju treba usvojiti je redovno spremanje napravljene konfiguracije, a može biti problem ako se radi samo u simulacijskom programu jer se kod njega konfiguracija spremi na izlasku iz programa, kada se ponudi spremanje napravljenog. Svaki stvarni uređaj može raditi na napravljenoj konfiguraciji sve dok se uređaj ne ugasi, a ako konfiguracija nije spremljena, uređaj se vraća na zadnju spremljenu konfiguraciju.

6. ZAKLJUČAK

Komunikacija postoji u svakom segmentu društva, a napretkom tehnologije, razvila se komunikacija preko raznih uređaja. Da bi se računalna komunikacija mogla održati, postoje uređaji koji se moraju pravilno spojiti i konfigurirati. Više tih uređaja čini nekakvu mrežu. Ovisno o veličini, uređaji se mogu podijeliti u nekoliko vrsta. Cijeli razvoj mreža je krenuo od referentnog OSI modela na kojem se razvio današnji Internet, samo je s vremenom taj model unaprijeđen i danas je TCP/IP model na kojem se bazira rad mrežnih uređaja i sam Internet.

Postoje razni mrežni uređaji, ali dva su temeljna uređaja bez kojih računalna mreža ne bi mogla funkcionirati. To su usmjerivač i preklopnik koji su vremenom unaprjeđivani i danas postoje uređaji koji mogu izvršavati funkcije obaju uređaja odjednom. Postoje prethodno konfigurirani uređaji koji su prilagođeni za krajnje korisnike i uređaji koji se koriste u velikim poduzećima te se ti uređaji moraju specijalno konfigurirati da bi izvršavali svoje zadaće u mreži. Neke od postavki, kao što su: naziv uređaja, zaštita uređaja, vrijeme na uređajima i druge, rade se jednako na većini uređaja, dok primjerice, konfiguracija usmjerivačkih protokola ili NAT protokola se može raditi samo na usmjerivačima. Da bi se konfiguracije uređaja mogle naučiti, Cisco Systems je napravio besplatni simulacijski program *Packet Tracer* koji omogućuje dizajniranje, spajanje te konfiguracije velikog broja Cisco mrežnih uređaja. Dizajniranje i konfiguriranje mreže je olakšano zbog toga što je program napravljen za učenje, postoje simulacije gdje se može vidjeti kako se izvršavaju, korak po korak, neki procesi u mreži. Cilj je pokazati kako bi se nešto lakše razumjelo, a samim time i naučilo.

Kada bi se neku od tih mreža željelo napraviti na stvarnoj opremi, bili bi potrebni veliki resursi jer je Cisco oprema poprilično skupa s obzirom da se nalazi na samom vrhu najboljih mrežnih oprema. Prilikom izrade takve mreže, poželjno je napraviti shemu i voditi bilješke jer u stvarnosti pogled na mrežu nije tako jednostavan kao u simulacijskom programu te su potrebne neke opcije koje se u simulaciji ne moraju koristiti, a bez njih bi u stvarnosti konfiguracija bila jako teška. Razvojem tehnologije također se razvijala i mrežna oprema pa sad postoje naredbe i opcije koje na starim uređajima nisu postojale, a kako je simulacijski program prilagođen novijim tehnologijama, prilikom izrade ovog rada su neki dijelovi bili ili otežani ili neizvedivi jer na toj opremi ta opcija nije postojala. Gledajući s druge strane, na stvarnoj opremi postoji mnogo drugih opcija koje u *Packet Traceru* ne postoje pa se ne može osloniti samo na znanje rada u simulacijskom programu jer rad na stvarnoj opremi nudi neke nove izazove.

Dizajn i izgled mreže u simulacijskom programu uvelike se razlikuju od onih na stvarnoj opremi jer su za stvarnu mrežu postojala ograničenja opreme koja je zastarjela i količinski ograničena pa je teško uspoređivati i dati konkretan zaključak o razlici između stvarne lokane mreže i mreže napravljene u *Packet Tracer*u.

LITERATURA

[1] Organizacija za razvoj interneta: http://www.ietf.org/

[2] Internetska organizacija za dodjeljivanje naziva i brojeva: https://www.icann.org/

[3] Organizacija za definiranje cjelovite arhitekture interneta: https://www.iab.org/

[4] OSI referentni model: https://comptutorkg2pg.blogspot.com/2010/12/network-architectures-osi-reference.html [24.6.2018]

[5] Debbra Wetteroth: OSI Reference Model for Telecommunications; 2001.

[6] Andrew S. Tanenbaum: The Iso-osi Reference Model, Wiskundig Seminarium, 1981.

[7] Andrew G. Blank: TCP/IP Foundations; 2004.

[8] CCNA R&S: Introduction to Network, Poglavlje 3.2.4; Reference Models

[9] Libor Dostálek, Alena Kabelová: Understanding TCP/IP: A Clear and Comprehensive Guide to TCP/IP Protocol

[10] Julie C. Gaffin: Internet Protocol 6, 2007.

[11] IP adrese: https://www.digitalcitizen.life/what-ip-address-how-change-it-windows-7-windows-81 [28.6.2018]

[12] Klase IP adresa: http://www.telecomworld101.com/Classes.html [30.6.2018]

[13] Privatne i javne IP adrese: https://www.routerinstructions.com/192-168-0-1/ [2.7.2018]

[14] Noite.pl; ARP Protocol- Address Resolution Protocol: Network Basic. AL0-012

[15] Preklopnik Cisco 2960: https://www.cisco.com/c/en/us/support/switches/catalyst-2960-48tc-s-switch/model.html [3.7.2018]

[16] STP protokol: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10556-16.html [5.7.2018]

[17] Specifikacija IEEE 802.1Q “Standard for Virtual Bridged Local Area Networks“ , CCERT-PUBDOC-2006-03-153

[18] VLAN protokol: https://bethepacketsite.wordpress.com/2016/02/16/ethernet-private-vlans/ [15.11.2018]

[19] Usmjerivač Cisco 2901: https://produto.mercadolivre.com.br/MLB-1081303630-router-cisco-2901-uck9-_JM?quantity=1 [16.11.2018]

[20] Alan B. Johnston; SIP: Understanding of Session Initiation Protocol, Fourth Edition. Str. 247-277.

[21] NAT protokol: https://computer.howstuffworks.com/nat.htm/printable [19.11.2018]

[22] S. Goswami; Internet Protocols: Advanced, Technologies and Applications

[23] DHCP i DNS protokoli: https://study-ccna.com/dhcp-dns/ [19.11.2018]

[24] Konfiguracija DHCP protokola: https://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfdhcp.html [19.11.2018]

[25] Vrste ACL listi: http://etutorials.org/Networking/Router+firewall+security/Part+III+Nonstateful+Filtering+Technologies/Chapter+7.+Basic+Access+Lists/Types+of+ACLs/ ,veljača 2008.

[26] Filtriranje prometa usmjerivačima; https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-02-220.pdf

[27] D. Medhi, K. Ramasamy : Network Routing: Algorithms, Protocols, and Architectures, drugo izdanje

[28] Ruting protokoli: https://www.talari.com/glossary_faq/what-are-router-protocols/ [20.11.2018]

[29] Ruting protokoli: https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/network/3-8/reference/guide/routpro.html#wp1043046 [20.11.2018]

[30] Uyless D. Black: IP Routing Protocols: RIP, OSPF, BGP, PNNI, and Cisco Routing Protocols

[31] V.Theoharakis, D. Serpanos; Enterprise Networking: Multilayer Switching and Applications: Multilayer switching application

[32] Višeslojni usmjerivač: https://www.ibm.com/us-en/marketplace/mds9396s [11.12.2018]

[33] M. Korać, D. Car; Uvod u računalne mreže; Algebra otvoreno učilište, Zagreb, 2014.

[34] *Sheikh Raashid Javid: "Role of Packet Tracer in learning Computer Networks" . International Journal of Advanced Research in Computer and Communication Engineering.* [Kolovoz 2018.]

[35] Packet Tracer sadržaj: *https://www.cisco.com/c/dam/en_us/training-events/netacad/course_catalog/docs/Cisco_PacketTracer_DS.pdf ,Cisco Networking Academy.* [Kolovoz 2018.]

[36] Yongbin Zhang. *"Teaching Innovation in Computer Network Course for Undergraduate Students with Packet Tracer"*. [Kolovoz 2018.]

[37] NTP protokol: https://en.wikipedia.org/wiki/Network_Time_Protocol [25.11.2018.]

[38] Cisco 2950 preklopnik specifikacije: https://www.cnet.com/products/cisco-catalyst-2950-24-24-port-switch/ [3.2.2018]

[39] Cisco 2950T preklopnik specifikacije: https://www.cnet.com/products/cisco-catalyst-2950t-24-switch-24-ports-managed-desktop-series/ [3.2.2018]

[40] Cisco 1760 usmjerivač specifikacije : https://www.cnet.com/products/cisco-1760-vpn-bundle-router-rack-mountable/ [3.2.2018]

SAŽETAK

U ovom radu su objašnjene osnove kako bi se mogao razumjeti princip rada mreža, odnosno Interneta. Kratko su opisana dva modela mrežne infrastrukture na kojima je Internet razvijen: OSI referentni model koji se sastoji od sedam slojeva i TCP/IP model razvijen prema praksi, a temelji se na OSI modelu. Kratko su opisani uređaji bez kojih mrežna komunikacija ne bi bila moguća, a to su preklopnici koji rade na drugom sloju OSI modela i usmjerivači koji rade na trećem sloju te noviji uređaji koji rade i na drugom i trećem sloju paralelno, a to su višeslojni preklopnici. Objašnjen je simulacijski program Packet Tracer koji je napravio Cisco Systems, jedan od glavnih i najvećih proizvođača mrežne opreme. Dizajnirana je i konfigurirana mreža u simulacijskom programu koja povezuje tri lokacije koje imaju potpunu funkcionalnu mrežu u kojoj je svakom uređaju omogućen pristup Internetu. Napravljena je još jedna manja lokalna mreža koja zbog ograničenja opreme nije mogla imati karakteristike mreže u simulacijskom programu te kratka analiza između rada na stvarnoj opremi i u simulacijskom programu.

Ključne riječi: Internet, OSI referentni model, TCP/IP, Cisco, usmjerivač, preklopnik

PLANNING AND CREATING LOCAL NETWORK ON CISCO EQUIPMENT

ABSTRACT

This paper explains the basics of the Internet and network operation. Two models of network infrastructure on the basis of which the Internet was developed have been described: the OSI reference model consisting of seven layers and TCP/IP model which has been developed in practice and it is based on the OSI model. Devices without which network communication would be impossible have also been shortly described. One of these devices are switches that work on the second layer of OSI models, and routers working on the third layer. Also, there are new devices that work on both the second and third layers at the same time. These devices are called multilayer switches. Furthermore, Packet Tracer simulation program has been explained briefly. The program is created by Cisco Systems, one of the major and largest network equipment manufacturers. This network is designed and configured in a simulation program that connects three locations that have a completely functional network where each device can access the Internet. Another smaller local network was created which, due to the limitations of the equipment, could not operate at the same level as in the simulation program. Finally, a short analysis between the network on the actual equipment and in the simulation program has been made.

Keywords: Internet, OSI reference model, TCP/IP, Cisco, switch, router

ŽIVOTOPIS

Marko Čanađija rođen je 04. siječnja 1995. godine u Bjelovaru. Školovanje je započeo 2001. godine u III. osnovnoj školi Bjelovar. Godine 2009. upisuje srednju tehničku školu u Bjelovaru, a tijekom srednjoškolskog obrazovanja sudjeluje na natjecanju iz „Osnova elektrotehnike“. Srednju školu uspješno završava 2013. godine. Iste godine upisuje preddiplomski studij elektrotehnike na Elektrotehničkom fakultetu pri Sveučilištu J. J. Strossmayera u Osijeku, koji 2016. godine uspješno završava. Iste godine upisuje diplomski studij komunikacije i informatike, smjer komunikacijske tehnologije na Fakultetu Elektrotehnike, Računarstva i Informacijskih tehnologija u Osijeku.

U Osijeku, veljača 2019.

Marko Čanađija

_____

potpis

PRILOZI

Prilog 5.1. Konfiguracija usmjerivača OS-HQR

```
OS-HQ1#show run
Building configuration...

Current configuration : 1374 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname OS-HQ1
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2911/K9 sn FTX1524TZ48
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 10.0.3.198 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/0/0
 ip address 10.0.3.193 255.255.255.252
 ip nat inside
!
interface Serial0/1/0
 ip address 201.10.5.2 255.255.255.252
 ip nat outside
!
interface Serial0/1/1
 ip address 10.0.3.201 255.255.255.252
 encapsulation frame-relay
 frame-relay interface-dlci 100
!
interface Vlan1
 no ip address
 shutdown
!
ip nat inside source list 1 interface Serial0/1/0 overload
ip nat inside source static tcp 10.0.0.1 80 201.10.5.2 80
ip classless
ip route 10.0.0.0 255.255.252.0 10.0.3.197
ip route 10.0.3.0 255.255.255.0 10.0.3.194
ip route 10.0.4.0 255.255.252.0 10.0.3.202
ip route 0.0.0.0 0.0.0.0 201.10.5.1
!
ip flow-export version 9
!
!
access-list 1 permit 10.0.0.0 0.0.3.255
!
!
!
!
!
!
logging trap debugging
logging 10.0.0.3
line con 0
!
line aux 0
!
line vty 0 4
 login
!
```

Prilog 5.2. Konfiguracija višeslojnog preklopnika OS-MLR

```
M-SW-OS#show run
Building configuration...

Current configuration : 2718 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname M-SW-OS
!
!
!
!
ip dhcp pool v10
 network 10.0.0.0 255.255.255.0
 default-router 10.0.0.254
 dns-server 10.0.0.1
ip dhcp pool v20
 network 10.0.1.0 255.255.255.0
 default-router 10.0.1.254
 dns-server 10.0.0.1
ip dhcp pool v30
 network 10.0.2.0 255.255.255.0
 default-router 10.0.2.254
 dns-server 10.0.0.1
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet1/0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet1/0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet1/0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet1/0/24
 no switchport
 ip address 10.0.3.197 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
```

```
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 mac-address 000a.41cc.7801
 ip address 10.0.0.254 255.255.255.0
 ip access-group 100 in
 ip access-group 100 out
!
interface Vlan20
 mac-address 000a.41cc.7802
 ip address 10.0.1.254 255.255.255.0
!
interface Vlan30
 mac-address 000a.41cc.7803
 ip address 10.0.2.254 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.3.198
!
ip flow-export version 9
!
!
access-list 100 permit udp any host 10.0.0.1 eq domain
access-list 100 permit tcp 10.0.1.0 0.0.0.255 host 10.0.0.2 eq ftp
access-list 100 permit tcp 10.0.3.0 0.0.0.127 host 10.0.0.2 eq ftp
access-list 100 permit udp host 10.0.3.194 host 10.0.0.3 eq 514
!
!
!
!
!
!
logging trap debugging
logging 10.0.0.3
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
ntp server 10.0.0.4
!
end
```

Prilog 5.3. Konfiguracija preklopnika

```
SW1_OS_BR1(config)#do show run
Building configuration...

Current configuration : 2250 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW1_OS_BR1
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

Prilog 5.4. Konfiguracija preklopnika SW3_OS_HQ

```
SW3_OS_HQ#Show run
Building configuration...

Current configuration : 2697 bytes
!
version 12.2
service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SW3_OS_HQ
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
ip ssh version 2
ip ssh time-out 30
ip domain-name tvrtka.hr
!
username root privilege 1 password 7 0822455D0A16
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/23
 switchport mode trunk
!
interface FastEthernet0/24
 switchport mode trunk
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 mac-address 0004.9a26.5201
 ip address 10.0.0.251 255.255.255.0
!
ip default-gateway 10.0.0.254
!
logging trap debugging
logging 10.0.0.3
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login
!
!
!
ntp server 10.0.0.4
ntp master
!
end
```