Simulacija WLAN mreže primjenom GNS3 aplikacije

Smiljanić, Luka

Undergraduate thesis / Završni rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:752669

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-19**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Luka Smiljanić

SIMULACIJA WLAN MREŽE PRIMJENOM GNS3 APLIKACIJE

ZAVRŠNI RAD

Zagreb, Rujan 2018.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 5. travnja 2018.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Računalne mreže**

ZAVRŠNI ZADATAK br. 4645

Pristupnik: **Luka Smiljanić (0135237557)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Simulacija WLAN mreže primjenom GNS3 aplikacije**

Opis zadatka:

Na primjeru zadane arhitekture WLAN mreže primjenom programske podrške GNS3 istražiti performanse mreže.

Mentor:

prof. dr. sc. Zvonko Kavran

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

SIMULACIJA WLAN MREŽE PRIMJENOM GNS3 APLIKACIJE

SIMULATION OF WLAN NETWORK USING GNS3

Mentor: prof.dr.sc. Zvonko Kavran

Student:Luka Smiljanić
JMBAG:0135237557

Zagreb, Rujan 2018.

Sadržaj

1. Uvod 1
2. Bežične mreže 1
2.1. Povezivanje bežičnih mreža 1
2.2 Vrste mreža prema prostoru kojeg obuhvaćaju 2
2.2.1. Osobna mreža(PAN) 3
2.2.2.Lokalne mreže (LAN) 3
2.2.3. Gradske mreže (MAN) 5
2.2.4. Regionalne računalne mreže (WAN) 6
2.3.Prednosti i mane bežičnih mreža 6
2.3.1 Prednosti bežičnih mreža 6
2.3.2. Nedostaci bežičnih mreža 7
3. Arhitektura bežične mreže 9
3.1. Arhitektura 802.11 mreže 9
3.2. OSI referentni model 10
3.2.1. Fizički sloj OSI referentnog modela 13
3.2.2. Tehnika proširenog spektra (Spread Spectrum) 13
3.2.3.Podatkovni sloj OSI referentnog modela 18
3.3. Topologije WLAN mreža 21
3.3.1. Ad-hoc mreže 21
3.3.2. Infrastukturni WLAN 22
3.4. Sigurnost bežičnih mreža 23
3.4.1. WEP 24
3.4.2. WPA 25
3.4.3. WPA2 25
4. Simulacija WLAN mreže primjenom GNS3 aplikacije 27
4.1. Implementacija GNS3 aplikacije 27
4.2. Kreiranje LAN mreže 30
4.3. Pokretanje LAN mreže 32
4.4. Praćenje prometa putem aplikacije Wireshark 34
5. Zaključak 37
Literatura 39

Popis slika 41

Simulacija WLAN mreže primjenom GNS3 aplikacije.

Sažetak

U završnom radu obrađeno je...objašnjen je princip rada neke općenite mreže. Opisane su osnovne značajke bežičnih računalnih mreža, načini povezivanja mreža, prednosti i mane, te podjele mreža prema različitim kriterijima. Dodatno se opisuje arhitektura bežičnih mreža, protokol 802.11, OSI referentni model, slojevi, sigurnosni aspekt bežičnih mreža, te načini kako se zaštite mreža, mreža. Provedena je simulacija rada mreže primjenom aplikacije GNS3. Opisana je aplikacija, topologija simulirane mreže, te rezultati koji su dobiveni simulacijom rada mreže..

Ključne riječi: računalne mreže, bežične mreže, WLAN, GNS3, OSI referentni model, sigurnost bežičnih mreža.

Summary

In this final paper, the principle of some general networks has been explained. The final paper begins with introductory presentation of basic features of wireless computer networks, their development. After that, the ways of connecting the network, their advantages and disadvantages, and network divisions according to different criteria are described. The architecture of wireless networks is described in the following and includes architecture according to the 802.11 protocol, the OSI reference model, its layers, the security aspect of the wireless networks, and the methods of network protection, the techniques used in the network operation, more fully explained the OSI reference model layers are used in wireless networks. The

simulation of network operation is described in the GNS3 application. The application itself, the network topology that is compiled is described, the data presented by the simulation of the network is presented. At the end, it is part of the work where conclusions are drawn that are the result of the whole work.

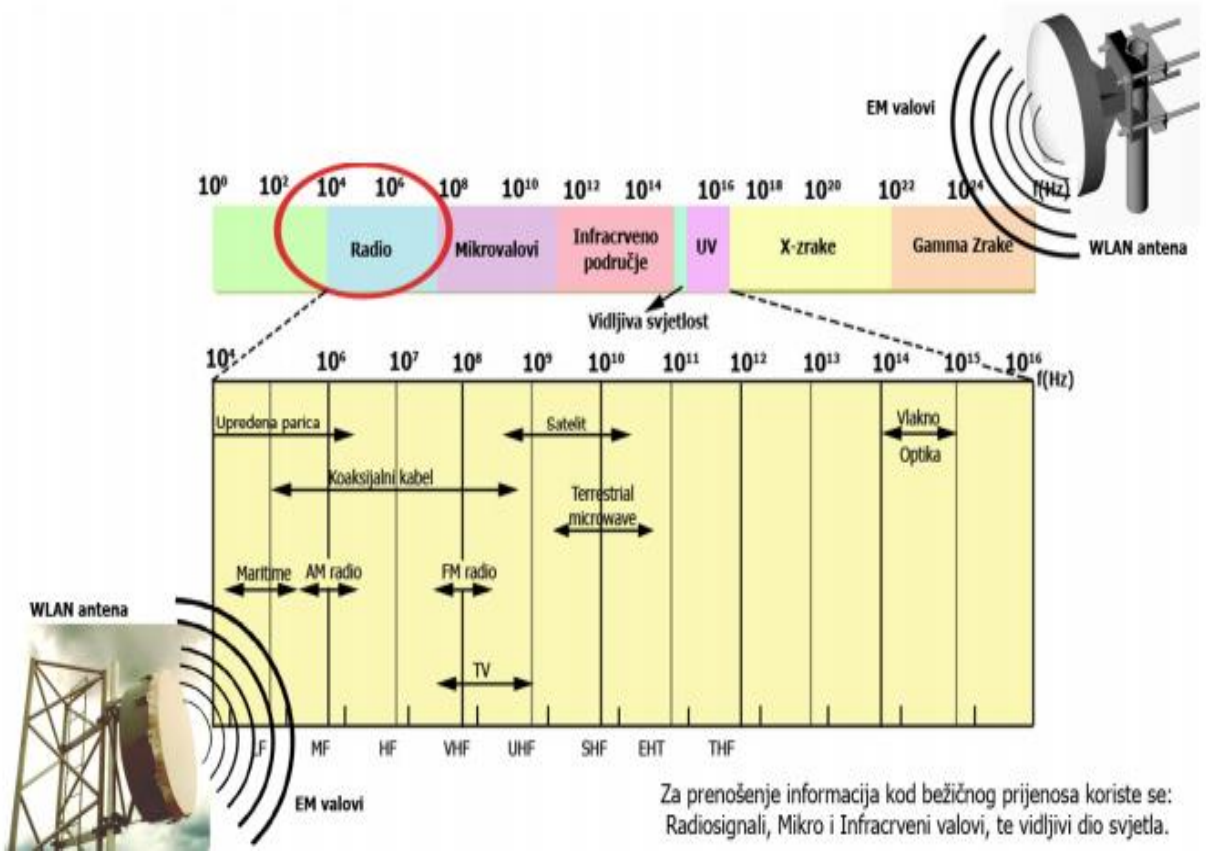
Key words: computer networks, wirelless networks, WLAN, GNS3, OSI reference model, wirelles network safety.

1. Uvod

2. Bežične mreže

2.1. Povezivanje bežičnih mreža

Bežične mreže koriste elektromagnetske valove (EM) za komunikaciju između dvije točke u prostoru. Za prenošenje informacija bežičnim putem koriste se radiosignali, mikro i infracrveni signali i vidljivi dio svjetla. Količina informacija koju elektromagnetski val može prenijeti, ovisi o rasponu frekvencija. Raspon frekvencija prikazan je na slici 1. (1)



Slika 1. Elektromagnetski spektar.

Izvor: (1)

Radio valovi se zovu i radiofrekvencijski nosioci jer prenose energiju signala do prijemnika. Podaci koji se prenose se moduliraju, odnosno pretvaraju u oblik pogodan za prijenos preko nosioca radio signala. Na istom prostoru mogu postojati više nosioca bez međusobne interferencije(kolebanja) ako se valovi prenose na drugim radio frekvencijama. Radioprijemnik demodulira prijemni signal na način da se podešava na određenu radio frekvenciju.

Infracrvene mreže imaju velika ograničenja, jer je potrebna neometana vidljiva linija od jednog infracrvenog primopredajnika (kombinacija odašiljača i prijemnika) do drugog. U velikim prostorijama to je teško ostvariti jer se primopredajnik ne može postaviti dovoljno visoko da bi se premostile sve prepreke, te da korisnici u prolazu ne blokiraju mrežni signal.

Problem optičke vodljivosti kod bežičnih mreža rješava se prelaskom na drugi opseg EM spektra. Moderne bežične mreže rade većinom na 2,4 ili 5 GHz, daleko ispod vidljivog spektra. (1)

2.2 Vrste mreža prema prostoru kojeg obuhvaćaju

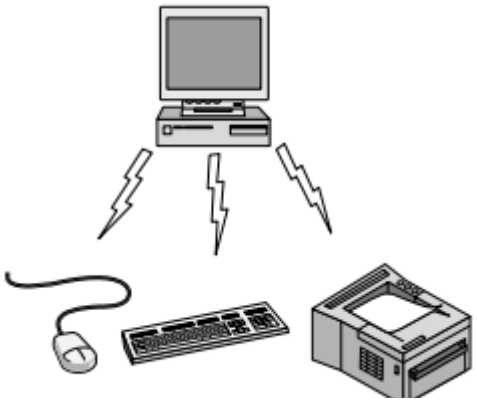
Bežične mreže se dijele prema geografskom kriteriju i broju uređaja od kojih može biti načinjena. Takve vrste mreža su:

- **Osobne računalne mreže** (eng. Personal area network (PAN))
- **Lokalne računalne mreže** (eng. Local area network (LAN))
- **Gradske računalne mreže** (eng. Metropolitan area network (MAN))
- **Regionalne računalne mreže** (eng. Wide area network (WAN)) (2)

2.2.1. Osobna mreža(PAN)

Osobna mreža (PAN) je mreža za povezivanje uređaja na računalo koje obično služe jednom korisniku. Doseg joj je najviše unutar nekoliko metara, a primjer PAN mreže prikazan je na slici 2. (3)

Ovakva mreža pruža veliku fleksibilnost. Omogućuje prijenos podataka na malim udaljenostima, npr. s mobitela na mobitel, s računala na računalo, s računala na printer i sl.



Slika 2. PAN mreža

Izvor: (5)

2.2.2.Lokalne mreže (LAN)

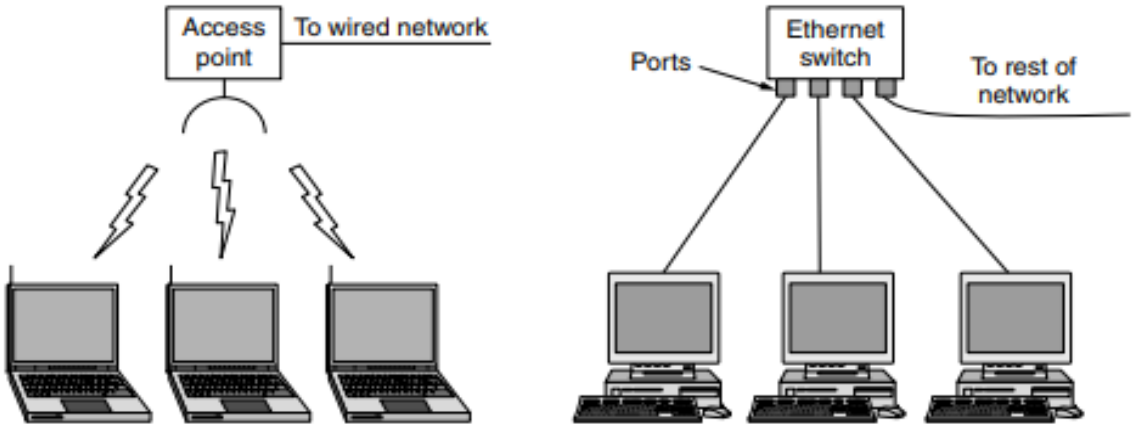
Lokalne mreže su uglavnom privatne mreže koje obuhvaćaju manji prostor, unutar jedne zgrade ili jednog užeg organizacijskog područja. LAN mreža nastaje povezivanjem ograničenog broja stanica (krajnjih uređaja/sustava, najčešće računala) na ograničenom prostoru unutar zgrade ili skupine susjednih zgrada, u pravilu uz dobre uvjete komuniciranja (malo kašnjenje, mala vjerojatnost pogreške. Koriste se i velike prijenosne brzine u rasponu do 10 Gbit/s. (4)

Obilježja LAN mreže su malo kašnjenje, mala vjerojatnost nastupa pogreške na simbolima (eng. BER – Bit Error Rate). Krajnji uređaji nalaze se u ravnopravnom odnosu. Svi okviri u LAN-u moraju sadržavati adresu primatelja (odredišta) i adresu

pošiljatelja (izvora). Podatkovne jedinice na protokolnoj razini lokalnih mreža su okviri, dok je Ethernet dominantna LAN tehnologija. (4)

Ethernet je prva široko korištena LAN tehnologija. Brzine prijenosa kod Etherneta su između 10 Mb i 10 Gb. Bus tehnologija je bila popularna sredinom 90-tih godina, svi čvorovi su u istoj domeni kolizije. Danas je najčešće korištena zvjezdasta topologija, kod koje je aktivni switch u centru, te tako ne dolazi do kolizije među čvorovima. (4)

Obično se koriste u vlasništvu su neke tvrtke, institucije koja njome i upravlja zato da bi njihovi korisnici mogli lakše dijeliti resurse i imati pristup potrebnim datotekama preko središnjeg poslužitelja. U današnje vrijeme se LAN mreže koriste kao bežične zbog pristupačnosti i lakoće korištenja. Primjer lokalne mreže (bežične i žične) prikazan je na slici 3. (2)



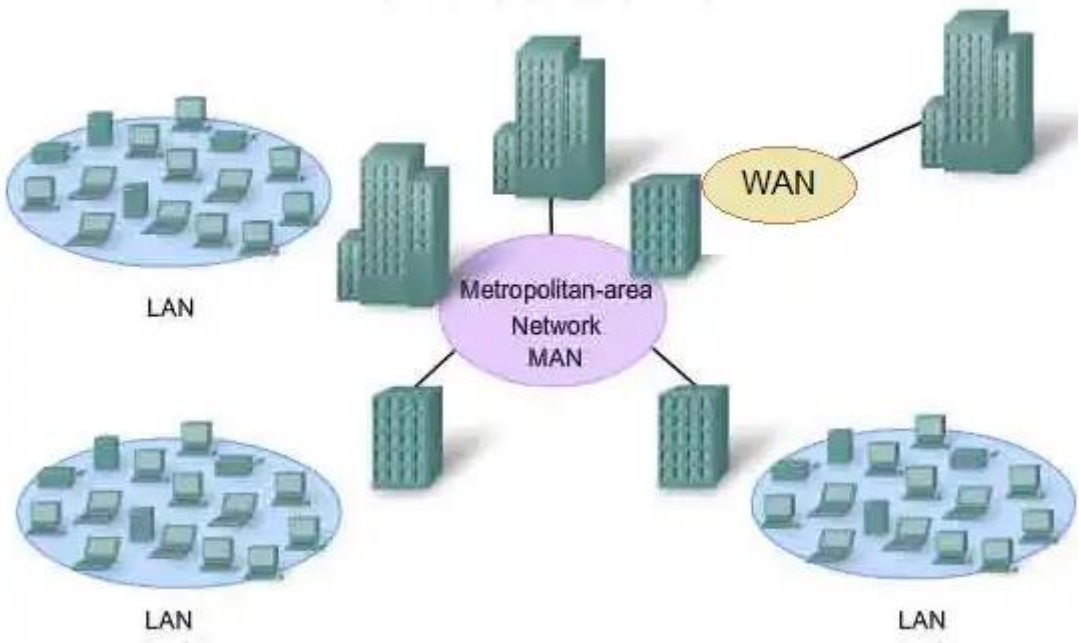
Slika 3. Prikaz bežične(lijevo) i žične(desno) lokalne mreže.

Izvor: (5)

2.2.3. Gradske mreže (MAN)

Gradska mreža (MAN) je mreža koja pokriva područje diljem grada, sveučilišnog kampusa ili manje regije. Ovisno o konfiguraciji, ova vrsta mreže može pokriti područje od nekoliko kilometara do nekoliko desetaka kilometara. Uglavnom se koristi da bi se povezalo više LAN mreža kako bi se formirala veća mreža, a primjer MAN mreže prikazan je na slici 4. Ova vrsta mreže je posebno dizajnirana za sveučilišne kampuse, pa se često i naziva CAN (Campus area network). (2)

Brzine MAN mreža su obično manje nego što su brzine kod lokalnih mreža. Najpoznatiji primjer takvih mreža su kabelske televizijske mreže dostupne u mnogim gradovima. Takvi sustavi su razvijeni iz ranijih komunikacijskih antenskih sustava koji se koriste u područjima u kojima je loš televizijski prijem. Kabelska televizija nije jedini MAN sustav. Nedavnim razvojem visoko brzinskog bežičnog Internet pristupa rezultirano je novim MAN mrežnim sustavima koji su standardizirani kao IEEE 802.16, popularno zvanim kao WIMAX. (5)



Slika 4. Prikaz MAN mreže.

Izvor: (14)

2.2.4. Regionalne računalne mreže (WAN)

Regionalne mreže (WAN) su mreže koje zauzimaju prostor veći od grada, regije ili države. Za povezivanje se koriste usmjerivači (ruteri) i javne komunikacijske veze. Značajka WAN mreže je da nisu u vlasništvu osoba ili organizacija koje ih koriste i prijenos podataka preko njih je ograničen prema brzini, količini i cijeni kao npr. lokalne ili gradske mreže. Potrebno je platiti za korištenje komunikacijskih veza. U odnosu na lokalne mreže, brzine kod WAN mreža su dosta ograničene. Najpoznatiji primjer javne WAN mreže je Internet, a prikaz WAN mreže prikazan je na slici 5. (3)

Uz prethodno nabrojene mreže, postoje i **mobilne mreže**. Danas se najviše koriste tehnologije kao što su 4G(LTE), 3G(HSPDA), EDGE, Bluetooth, Wi-Fi, GPRS, te se trenutno razvija peta generacija mobilnih mreža, poznata kao 5G koja bi trebala biti komercijalno dostupna na tržištu 2020. godine.

2.3.Prednosti i mane bežičnih mreža

2.3.1 Prednosti bežičnih mreža

Jedna od prednosti bežičnih mreža, je da nije potrebna fizička veza da bi se spojili uređaji u mrežu. Time su mreže jeftinije za instalaciju, jer nisu potrebni građevinski radovi da bi se provukla instalacija. Prednost bežične mreže je i mobilnost. To bi značilo da se može nesmetano kretati unutar dometa do kojeg mreža može slati signale uređaju i tako obavljati svoje funkcije, što kod žičnih mreža nije slučaj jer tamo gdje žica prestaje, prestaje i pristup mreži.

2.3.2. Nedostaci bežičnih mreža

Jedni od nedostataka bežičnih mreža u odnosu na žične su brzine prijenosa podataka, sigurnost bežičnih mreža, pokrivenost područja, te pouzdanost. (6)

Bežične mreže nažalost ne dosežu onolike brzine kao što dosežu žične brzine, pa pri tome treba više vremena da se podaci prenesu s jednog uređaja na drugi. Ovisno o standardu bežične LAN tehnologije koji koristimo, brzine se kreću između 11 Mbps i 54 Mbps, te u novije vrijeme do 100 Mbps i više. Te brzine su u redu za korisnike koji koriste osnovne funkcije, dok veće organizacije i dalje koriste žično LAN umrežavanje jer njihove funkcije zahtijevaju puno veće brzine.

Sigurnost je sigurno i veći problem od manjih brzina na bežičnim mrežama. Najveći je problem što se korisnici spajaju na više bežičnih mreža ili se netko drugi može spojiti na vlastitu mrežu ukoliko nije dovoljno zaštićena. Stoga je važno odabrati jedno od tehnologija zaštite podataka (enkripciju). Međutim, neke od najčešće korištenih metoda enkripcije pokazuju slabosti, a te slabosti koriste „hakeri“, koji neovlašteno ulaze u mrežu i koriste privatne podatke u vlastite svrhe.

Raspon pokrivanja područja sa standardnom opremom iznosi do 30 metara, što je dovoljno u okviru doma, zgrade, ali ne i za neke veće organizacije. Da bi se povećala pokrivenost, instaliraju se dodatne pristupne točke ili pojačivači signala, te se tako automatski povećavaju i troškovi.

Problem je i kod pouzdanosti jer je signal bežičnog umrežavanja podložan smetnjama zbog svog prijenosnog medija, kao i složenim propagacijskim efektima koji su izvan kontrole mrežnog admina. (6)

Kriptografija je proces sigurnog prijenosa podataka preko mreže na takav način ako netko od strane neovlaštenih korisnika dođe do tih podataka, ne zna dešifrirati što oni znače. Kriptografija uključuje dva procesa, a oni su enkripcija ili šifriranje i dekripcija ili dešifriranje. (7)

Enkripcija je proces preuzimanja podataka i njihovo modificiranje tako da ih nepoželjni korisnici ne mogu čitati, pa tako ni koristiti.Dekripcija je proces obrnut od enkripcija, tj. proces preuzimanja šifriranih podataka i pretvaranje u oblik pogodan za čitanje pouzdanim korisnicima.

Moderne kriptografije koriste proces šifriranja javnog ključa koji koristi dvije različite vrste ključeva. Koriste javni i privatni ključ. Javni ključ se distribuira svakom korisniku koji ga potražuje, dok privatni ključ je poznat samo vlasniku. Da bi šifrirana poruka bila poslana, pošiljatelj koristi svoj privatni ključ za šifriranje podataka, a primatelj koristi javni ključ pošiljatelja za dekriptiranje. Slično tome može primatelj poruke šifrirati poruku s javnim ključem, pa izvorni pošiljatelj koristi svoj privatni ključ kako bi dekriptirao poruku koja mu je poslana. (7)

3. Arhitektura bežične mreže

3.1. Arhitektura 802.11 mreže

Arhitekturu bežične mreže možemo opisati kao skup međusobno povezanih elemenata koje zajedno funkcioniraju kao cjelina. Osnovni standard po kojem su definirane bežične mreže je 802.11.

Standardi 802.11. su nadograđivani kao npr. 802.11a, 802.11b, 802.11g i dr., a oni se međusobno razlikuju prema brzinama prijenosa (max. Brzine: 54, 11, 54 Mbps), modulacijama signala(FHSS, DSSS, OFDM, PBCC) i broju kanala. WLAN-ovi koriste ISM opseg frekvencija na 2.4 i 5 GHz. ISM je u svijetu i Hrvatskoj prihvaćen kao FTA – free to air spektar, za koji nije potrebna dozvola. (1)

Standard definira najniža dva sloja OSI referentnog modela, a oni su fizički (physical layer) i podatkovni (data link layer) na kojem je kompatibilan s IEEE 802.3. standardom (Ethernet).

WLAN-ovi se izgrađuju pomoću dva elementa:

- Bežične mrežne kartice u korisničkom računalu
- Pristupne centralne točke (AP = Wireless Access Point)

AP ostale korisnike povezuje u lokalnu mrežu. Postoje dvije različite topologije bežičnih mreža:

- infrastrukturni WLAN
- neovisni (ad hoc) WLAN

Kod pristupa mediju, definiran je protokol višestrukog pristupa mediju s izbjegavanjem sudara okvira – MACA(Multiple Access with Collision Avoidance) ili CSMA/CA(Carries Sense With Multiple Access with Collision Avoidance) protokol. (1)

3.2. OSI referentni model

OSI referentni model (Open System Interconnection Model) je model za povezivanje otvorenih sustava. Uvođenjem računalskih komunikacija putem javne mreže, te razvojem paketnih i integriranih višeuslužnih mreža, postalo je nužno razraditi drukčiji pristup i koncept ustrojavanja telekomunikacijske mreže, tj. funkcija i procesa koji se u njoj obavljaju. OSI model je teoretski model koji pokazuje kako dva različita sustava mogu komunicirati jedan s drugim. Pokazuje funkcije i veze između sustava i omogućava različitim sustavima da komuniciraju neovisno o njihovoj temeljnoj arhitekturi (WLAN, ATM, Ethernet, GPRS i dr.). (8)

OSI referentni model se sastoji od sedam slojeva, a svaki od tih slojeva opisuje određenu funkciju. A ti slojevi su:

- Aplikacijski sloj (Application Layer)
- Prezentacijski sloj (Presentation Layer)
- Sjednički sloj (Session Layer)
- Prijenosni sloj (Transport Layer)
- Mrežni sloj (Network Layer)
- Podatkovni sloj (Data Layer)
- Fizički sloj (Physical Layer)

Aplikacijski sloj je sloj koji je najbliži korisniku. On dostavlja mrežne usluge/servise aplikacijama krajnjeg korisnika. Za razliku od svih ostalih slojeva, ne dostavlja usluge ni jednom drugom OSI sloju, nego isključivo aplikacijama koje se nalaze van OSI modela. Aplikacijski sloj uspostavlja dostupnost između komunikacijskih partnera i sinkronizira i uspostavlja dogovore o procedurama oporavka u slučaju greški i kontrolira integritet podataka. (4)

Prezentacijski sloj brine o tome da informacija koju pošalje aplikacijski sloj jednog sustava bude čitljiva od strane aplikacijskog sloja drugog sustava. Ako je potrebno, prezentacijski sloj prevodi između višestrukih podatkovnih formata, koristeći zajednički format. Česti grafički standardi prezentacijskog sloja su npr. GIF; TIFF, JPEG i sl. Primjeri Layer 6 standarda za zvuk i filmove su npr. MIDI, MPEG i sl. (4)

Sjednički sloj ima zadaću da uspostavi, upravlja i prekine vezu između dva računala koja međusobno komuniciraju. Usluge sjedničkog sloja se dostavljaju prezentacijskom sloju. Također, dodatna mu je zadaća sinkronizacija dijaloga između prezentacijskih sloja dvaju računala i upravljanje razmjenom podataka između njih. Osim upravljanja kontrolom veze, sjednički sloj nudi osiguranje efikasnog transfera podataka, kakvoću usluge i obavještavanje o problemima unutar aplikacijskog, prezentacijskog i sjedničkog sloja. Primjeri protokola sjedničkog sloja su: NFS (Network File System), SQL (Structured Query Language). X-Window sustav, ASP (AppleTalk sjednički protokol) i sl. (4)

Prijenosni sloj segmentira podatke koji dolaze od strane pošiljatelja i ponovo ih spaja u cjeloviti tok podataka na strani primatelja. Dok se aplikacijski, prezentacijski i sjednički sloj bave problematikom samih aplikacija, ostala četiri sloja bave se problematikom prijenosa podataka. Prijenosni sloj pokušava osigurati uslugu prijenosa podataka koja štiti gornje slojeve od implementacije samog prijenosa podataka. Npr. pouzdanost prijenosa podataka između dva računala je upravo briga prijenosnog sloja. Pružajući komunikacijske usluge, prijenosni sloj ostvaruje, održava i pravilno prekida virtualne krugove. Detekcija grešaka prilikom prijenosa, kao i otklanjanje istih, kontrola protoka informacija koriste se kako bi se ostvarila pouzdana usluga. Najznačajniji protokoli prijenosnog sloja su TCP (Transfer Control Protocol) i UDP (User Datagram Protocol). (4)

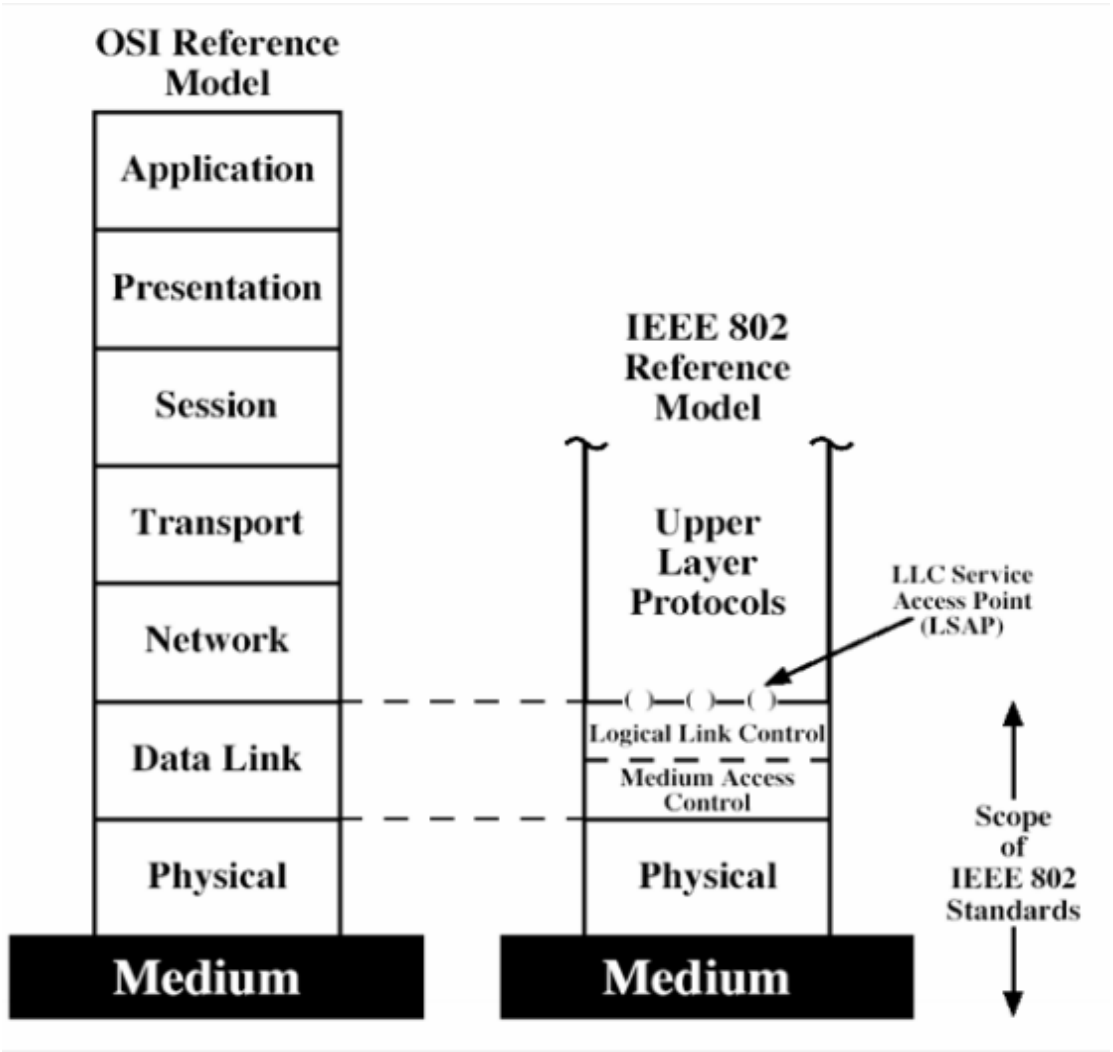
Mrežni sloj je vrlo kompleksan sloj koji omogućava povezivost i odabir puta između dva mrežna sustava koji mogu biti geografsko dislocirani. Zadužen je i za logičko adresiranje. Primjeri protokola mrežnog sloja su IP (Internet Protocol), IPX (Internetwork Packet Exchange) i AppleTalk. (4)

Podatkovni sloj omogućava pouzdan tranzit podataka preko fizičkog linka (poveznice). Upravo zato se podatkovni sloj bavi pitanjima fizičkog adresiranja, mrežne topologije, mrežnog pristupa, obavještavanju o greškama, uređene dostave okvira i kontrole protoka. (4) Sloj podatkovne veze dijeli se na dva sloja, a to su: kontrola logičke veze (LLC-Logical Link Layer) i kontrola pristupa mediju (MAC-Medium Access Control),

Fizički sloj definira električne, mehaničke, proceduralne i funkcionalne specifikacije za aktivaciju, održavanje i deaktivaciju fizičkog linka (poveznica) između krajnjih

sustava. Karakteristike kao što su voltaža, vremenska promjena voltaže, maksimalne udaljenosti za prijenos podataka, konektori i sl. su definirane sa specifikacijama fizičkog sloja. (4)

Na OSI referentni model temelje se IEEE 802.11 mreže koju definirane na posljednja dva sloja, podatkovnom i fizičkom sloju, kao što je prikazano na slici 5.



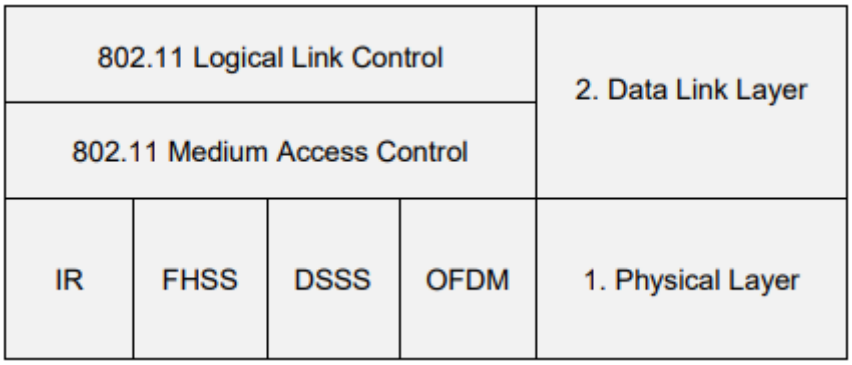
Slika 5. IEEE mreža u odnosu na OSI model.

Izvor: (15)

3.2.1. Fizički sloj OSI referentnog modela

802.11 standard definira podsloj MAC, MAC servise i protokole te četiri fizička sloja koja su prikazana na slici 6. Četiri fizička sloja unutra 802.11 standarda uključuju:

- Prošireni spektar skakanja frekvencija (FHSS – Frequency Hopping Spread Spectrum)
- Prošireni spektar izravnim širenjem spektra (DSSS – Direct Sequence Spread Spectrum)
- Tehniku frekvencijskog multipleksa ortogonalnih podnositelja (OFDM – Orthogonal Frequency Division Multiplexing)
- Infracrveni frekvencijski pojas (IR- InfraRed) (9)



Slika 6. Područje interesa 802.11 standarda

Izvor: (9)

3.2.2. Tehnika proširenog spektra (Spread Spectrum)

Tehnika proširenog spektra ostvaruje se korištenjem pseudo slučajnog niza (PN-pseudo noise) koji je najčešće binarni niz i ima valni oblik sličan šumu. Množenje korisnog signala s pseudo slučajnim nizom uzrokovat će:

- Proširenje spektra snage signala na šire frekvencijsko područje od njegovog osnovnog frekvencijskog pojasa (engl. Baseband),
- Signal će poprimiti valni oblik šuma.

Korisni signal se na taj način tijekom prijenosa skriva unutar šuma komunikacijskog kanala, a na prijemnoj strani se „sažima“ i dekodira pomoću poznatog PN signala.

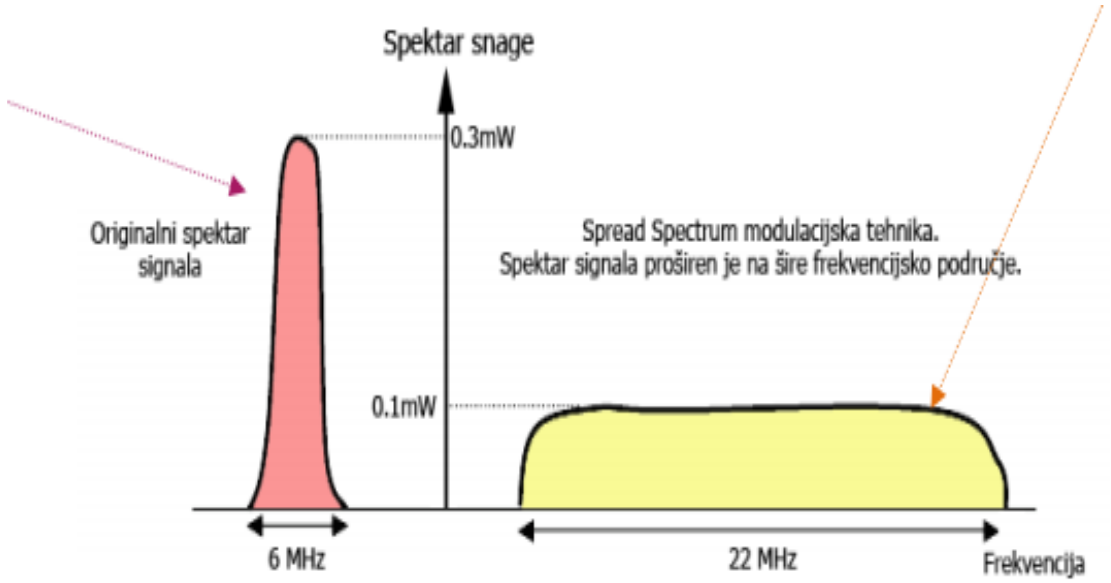
Zbog male gustoće *spread spectrum* signala, više korisnika istovremeno može koristiti isti medij za prijenos podataka, a da se međusobno ne ometaju. Sustavi s proširenim spektrom signala mogu se realizirati pomoću tri tehnike:

1. DSSS tehnike,
2. FHSS (FH) tehnike,
3. *Hybrid System* (DS/FFH) je kombinacija prve dvije tehnike.

Prve dvije tehnike koriste se kod bežičnog Etherneta. (1)

DSSS tehnika

Signal koji se prenosi prvo se množi s pseudo slučajnim signalom (PN) veće frekvencije (ima veći *bit rate*) i na taj način mu se spektar snage „proširuje“ na šire frekvencijsko područje, kao što je prikazano na slici 7.



Slika 7. Proširivanje spektra signala „Spread Spectrum“ tehnikom

Izvor: (1)

DSSS ili *Direct Sequence Spread Spectrum* je modulacijska tehnika poznata i pod nazivom DS-CDMA (engl. *Direct Sequence code division multiple access*). Tehnika je prihvaćena kod standarda IEEE 802.11g i 802.11b i koristi se kod WLAN, CSMA i GPS sustava. (1)

Kod IEEE 802.11 standarda, pseudo slučajni kod se zove *chip* ili *chipping code*. Podaci se šalju ISM frekvencijskim pojasom od 2.4 do 2.4835 GHz. ISM pojas se dijeli na 13 kanala od kojih se kod DSSS-a koristi svaki peti kanal, jer kanali moraju biti međusobno udaljeni za 25 MHz kako se ne bi preklapali. Tako je unutar cijelo pojasa moguće imati 3 korisnika, odnosno koristiti prvi, šesti i jedanaesti kanal ili drugi, sedmi i dvanaesti, itd kao što možete vidjeti na slici 8.. Kod DSSS-a su moguće brzine prijenosa do 1, 2, 5.5 i 11 Mbps. (1)

Slika 8. Primjer korištenja ISM pojasa pomoću DSSS tehnike.

Izvor: (1)

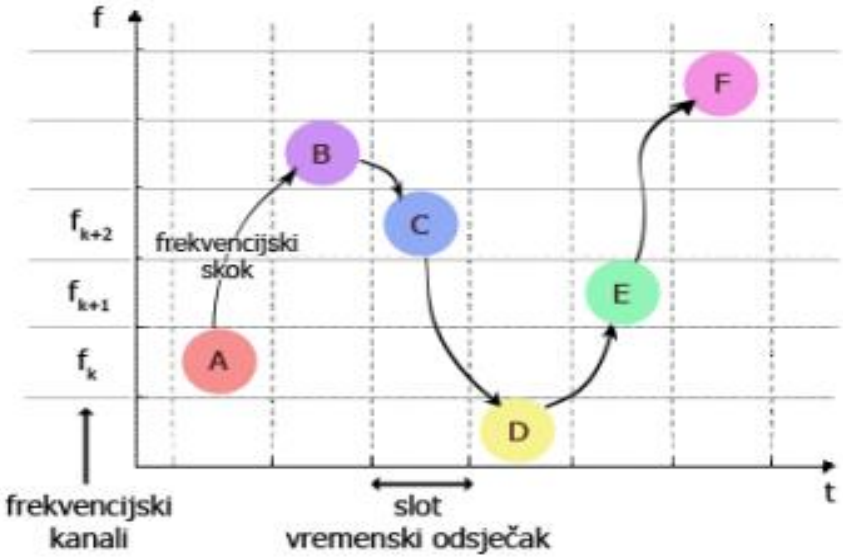
FHSS (FH) tehnika

FHSS ili *Frequency Hopping Spread Spectrum* je modulacijska tehnika koja je poznata i pod nazivom *Frequency-Hopping Code Division Multiple Access (FH-CDMA).*

Kod FHSS modulacije se definiraju frekvencijski skokovi unutar spektra, a misli se na ekstremno brze promjene frekvencija na kojima se prenose podaci. Odašiljač šalje kratke nizove podataka na jednoj frekvenciji neko vrijeme, a potom se prebacuje na

drugu frekvenciju. Odašiljač i prijemnik moraju biti sinkronizirani prema slijedu preskakivanja kako bi održali logički kanal, jer u suprotnom dolazi do gubitka podataka.

Ako se pojavi interferencija na jednoj frekvenciji, podaci se ponovo šalju prelaženjem na drugu frekvenciju. Stalnim mijenjanjem frekvencije FHSS sustav je otporan na preslušavanje, a postiže se i visoki stupanj sigurnosti prijenosa. Time je omogućen rad više različitih bežičnih mreža unutar istog područja, ali bez nepoželjnih međudjelovanja. Primjer frekvencijskih skokova kod FHSS modulacije je prikazan na slici 9.



Slika 9. FHSS modulacija

Izvor: (1)

Kod FHSS-a se najčešće koristi GFSK modulacija signala, a brzine koje postiže su između 1-2 Mbps.

Neke prednosti FHSS tehnike su:

- smanjenje uskopojasne smetnje (engl. *Narowband interference*),
- povećan kapacitet signala.

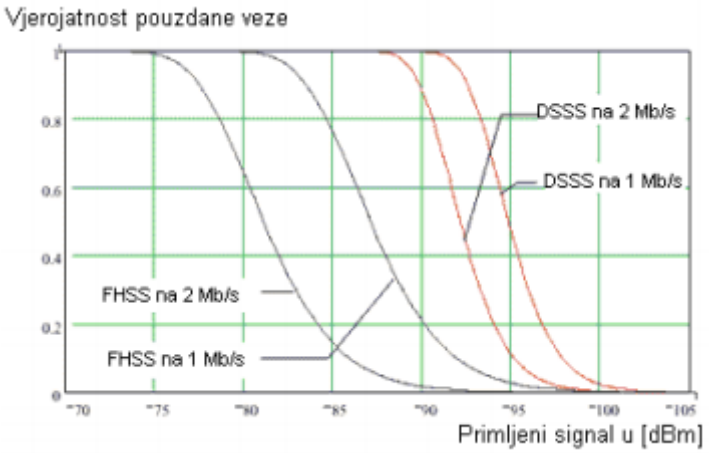
Spread spectrum modulacijske tehnike:

- omogućuju da više korisnika istovremeno dijeli isti frekvencijski opseg bez međusobne interferencije,
- koriste širi frekvencijski pojas za prijenos signala, ali i manje snage nego što to rade tradicionalne modulacijske tehnike(FDM, TDM...),
- trebaju manju potrebnu snagu za prijenos signala,
- pružaju otpornost na smetnje od drugih izvora,
- pružaju otpornost na višestazno prostiranje i iščezavanje signala

Usporedba FHSS I DSSS tehnike

Kada se usporede ove dvije modulacijske tehnike, mogu se vidjeti prednosti DSSS-a. DSSS modulacija je mnogo robusnija, ima puno veći doseg pokrivenosti, čak i kada radi s pola izlazne snage u odnosu na FHSS modulaciju. Skakanje s jednog kanala na drugi koje koristi FHSS modulacija nudi više iskoristivih frekvencija, postoji povećana mogućnost smetnji ukoliko koristimo više uređaja na nekom prostoru, a da već oni koriste ovu modulacijsku tehniku. Unatoč tome kako FHSS modulacija nije toliko raspršena, možemo je koristiti u uvjetima u kojima postoji puno smetnji u komunikacijskom kanalu.

Snaga FHSS moduliranog signala koncentrirana je u užem frekvencijskom području, što znači da je amplituda signala veća, a samim time je i mogućnost probijanja kroz smetnje veća. Još jedna prednost FHSS modulacije je u njenoj naturi, a ona je da je mogućnost kolizije manja. Ipak, te prednosti bivaju umanjene činjenicom da DSSS može raditi na puno većim udaljenostima kao što je prikazano na slici 10. (10)



Slika 10. Usporedba DSSS i FHSS modulacijske tehnike.

Izvor: (10)

3.2.3.Podatkovni sloj OSI referentnog modela

Sloj podatkovne veze (engl. *Data-Link Layer*) zadužen je da podatke, okvire koji su u ovom slučaju nastali enkapsulacijom podataka kroz slojeve mrežnog modela, pošalje prema fizičkom sloju. Podaci koje šalje sadrže podatke:

- Oznaku odredišta koja je najčešće izvedena kao MAC adresa (Media Access Control – fizička adresa mrežne kartice),
- Oznaku pošiljatelja (engl. *Sender ID*). Ta oznaka je najčešće MAC adresa odredišnog računala,
- Upravljačke informacije, a to su informacije o tipu okvira, usmjeravanja te informacije vezane za segmentaciju. (8)

U ovom sloju obavlja se kontrola greške, odnosno osiguranje detekcije i korekcije greške, te se provjerava integritet paketa prispjelog na odredište.

Podijeljen je na dva sloja:

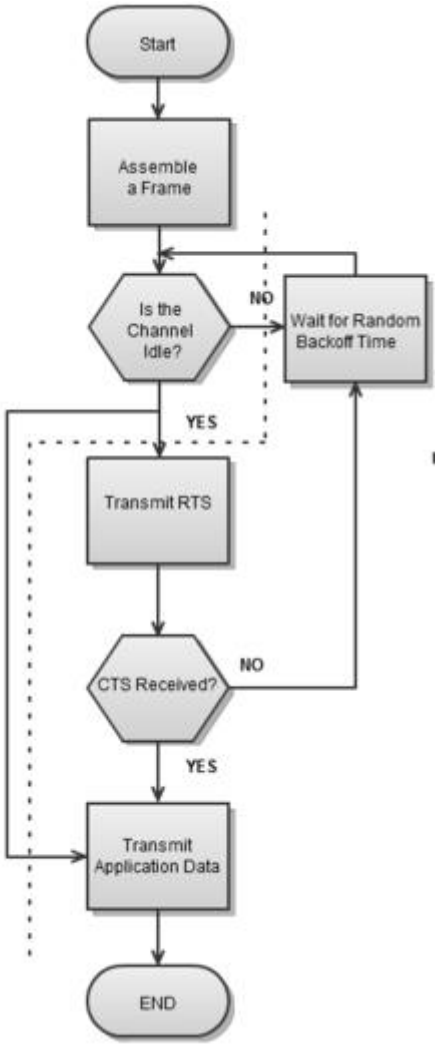
- **Kontrola logičke veze** (engl. *Logical Link Control* – LCC) osigurava kontrolu greške i primarno komunicira s mrežnim slojem radi osiguranja konekcijske i bezkonekcijske veze,
- **Kontrola pristupa mediju** (engl. *Media Access Contol* – MAC) pruža pristup LAN mediju i primarno komunicira s fizičkim slojem.

Sloj podatkovne veze predstavlja takozvana „vrata između svjetova“ i povezuje fizičke aspekte (kablove i digitalne impulse) s apstraktnim svijetom softvera i tokova podataka.

Mostovi i komutatori se smatraju uređajima podatkovnog sloja zbog toga što su u stanju kontrolirati promet na osnovu adresnih informacija. (8)

CSMA/CA mehanizam

CSMA/CA mehanizam je osnovni pristupni mehanizam za standard IEEE 802.11 mreže. Sličan je CSMA/CD mehanizmu koji se koristi kod žičnih LAN mreža (IEEE 802.3.) Za razliku od IEEE 802. Mreža koje šalju signale dok god ne detektira neki drugi paket, CSMA/CA neće početi s odašiljanjem dok bilo koja druga stanica emitira signal i dok se ne dobije povratna informacija da odredišna stanica sluša. Prije emitiranja signala, bežični uređaj oslušava komunikacijski kanal kako bi ustanovio emitira li ga neki drugi uređaj. Ako postoji neki drugi uređaj, pričekat će slučajno generirani vremenski odsječak i ponovo slušati komunikacijski kanal, ako nitko drugi ne koristi kanal, uređaj počinje s emitiranjem. (9) Princip po kojem radi CSMA/CA mehanizam prikazan je dijagramom toka na slici 11.

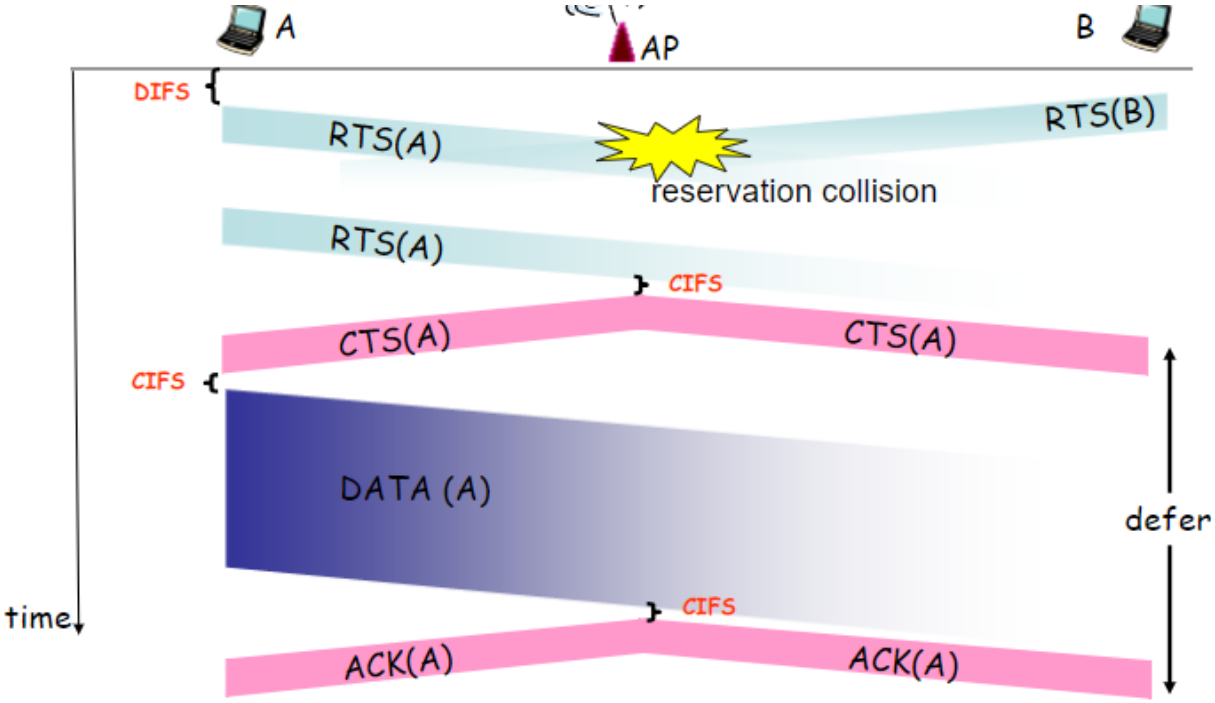


Slika 11. Princip rada mehanizma CSMA/CA

Izvor: (16)

RTS/CTS mehanizam

RTS/CTS mehanizam se može koristiti za zaštitu prijenosa, tj. da bi se spriječila kolizija koja nastaje emitiranjem signala dvaju uređaja. On rezervira medij unaprijed stvarnog prijenosa okvira. Primjer komunikacije tog mehanizma je sljedeći, ako je neki bežični klijent poslao adresni podatak na neku pristupnu točku (AP), AP će poslati RTS okvir tom klijentu, te tražiti vrijeme predaje tog podatka. Bežični klijent odgovara CTS okvirom, u kojem govori AP-u da je spreman primiti njegovu transmisiju i da neće održavati komunikaciju s nikim drugim dok AP ne završi prijenos. (11) Prikaz rada RTS/CTS mehanizma je prikazan na slici 12.



Slika 12. RTS/CTS mehanizam

Izvor: (17)

U isto vrijeme i drugi bežični klijenti mogu „vidjeti“ dogovor, ali se ne priključuju komunikaciji. Ovaj način omogućava prijenos podataka s minimalnom mogućnošću dolaska do kolizije, te rješava problem „skrivenog klijenta“. Skriveni klijent javlja se kada imamo dva ili više klijenata koji su u dosegu AP-a, ali ne i međusobno. Za razliku od žičnih LAN mreža gdje svaki klijent može „vidjeti“ sve sudionike u mreži, udaljenost kod bežičnih LAN mreža uzrokuje pojavu skrivenog klijenta, tako da klijenti mogu komunicirati isključivo posredstvom AP-a. (9)

3.3. Topologije WLAN mreža

Prema načinu spajanja WLAN mreža, postoje dvije različite topologije:

- **Infrastrukturni WLAN,**
- **Neovisni (ad hoc) WLAN.**

3.3.1. Ad-hoc mreže

Neovisna ili ad-hoc topologija omogućuje međusobno povezivanje stanica gdje pokretni čvorovi izravno komuniciraju jedni s drugima koristeći bežične adaptere koji su prikazani na slici 13. Ta topologiji je pogodna za brzu i jednostavnu implementaciju prema potrebni.

WLAN korisnik će koristiti *ad-hoc* topologije je to što svi sudionici moraju biti međusobno u dometu radio signala. Ako se želi povećati domet radio signal, tada se koristi infrastrukturna topologija sa središnjom pristupnom točkom (AP) koja može udvostručiti domet prijenosa između bilo koja dva pokretna čvora. (1)

Slika 13. Prikaz neovisnog (Ad-hoc) povezivanja računala.

Izvor: (1)

3.3.2. Infrastrukturni WLAN

WLAN mreže se izgrađuju pomoću dvaju elemenata, a oni su bežična mrežna kartica i središnja pristupna točka (AP). AP je uređaj koji ostale uređaje za bežično komuniciranje povezuje u lokalnu mrežu i karakteristična je za infrastrukturne WLAN-ove kao što je prikazano na slici 14. Pristupna točka je najčešće kabelom povezana s klasičnom LAN mrežom i služi za prijenos podataka između „žičnih“ i „bežičnih“ uređaja, pa se na takav način ostvaruje povezivanje bežičnih uređaja na Internet mrežu. Znači, infrastrukturna topologija pomoću pristupnih točaka omogućuje integraciju pokretnih čvorova u ožičeni LAN. (1)

Pristupna točka može raditi kao bežični *hub.* Na njega se spajaju bežični klijenti, radi kao *repeater* za povećanje dometa ili kao *bridge* za spajanje dva segmenta mreže. AP može istovremeno komunicirati s 30-tak klijenata koji su smješteni u krugu od 100 m.

Kvaliteta signala koji se prenosi ovisi o:

- smještaju uređaju,
- snazi emitiranja,
- mogućim smetnjama izazvanim blizinom drugih uređaja koji interferiraju sa signalom emitirajući na istoj frekvenciji. (1)

Slika 14. Prikaz infrastrukturne WLAN mreže

Izvor: (1)

Postoji nekoliko načina rada bežičnih krajnjih stanica ovisnih o proizvođaču mrežne opreme:

- „Master“ način rada jest standardni način rada gdje klijent komunicira s pristupnom točkom ili usmjerivačem,
- „Bridge“ način rada djeluje kao „most“ između dvije pristupne točke ili usmjerivača
- Repetitorski način rada dozvoljava premošćivanje poput „brigde“ način rada, ali uz mogućnost istovremenog spajanja klijenata na svaku pojedinu pristupnu točku ili usmjerivač
- Wireless Distribution System – WDS način rada, a označava tehniku povezivanja više pristupnih točaka (AP-ova). WDS je prisutan u obliku raznih Point-to-Point/Multipoint Bridge implementacija, kao i obliku nadogradnji standardnih pristupnih točaka. (12)

3.4. Sigurnost bežičnih mreža

Bežične mreže su sigurnosno mnogo ugroženije od onih u kojima se podaci prenose žično, zato što se podaci nekontrolirano prenose u cijelom radijusu dometa pristupne mreže, te svatko tko se nalazi u njemu može ih pokušati preuzeti. Napadi na bežično povezane dijelove sustava mogu se iskoristiti i za posredni napad na računala u unutrašnjem, žičano povezanom dijelu mreže.

Ključnu ulogu u zaštiti podataka koji se bežično prenose ima kriptografija zato jer se njome onemogućuju otkrivanje i mijenjanje podataka, lažiranje identiteta, poricanje slanja poruka i slični napadi. Iako su dostupne metode za zaštitu bežičnih mreža, najveći problem zapravo predstavljaju korisnici i vlasnici mreže ne primjenjuju te metode zaštite. (13)

Značajke sigurne komunikacije su:

- **Tajnost podataka** koji se prenose,
- **integritet podataka** – sigurnost da nisu mijenjani u prijenosu,
- **autentičnost pošiljatelja** – onaj koji je naveden kao pošiljatelj to doista i jest,
- **neporecivost** – ako je netko poslao poruku ne može to kasnije poreći.

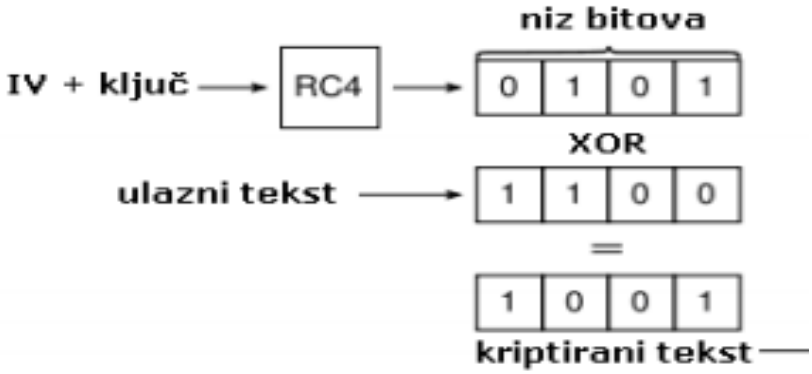
Najveći problem za bežične sustave predstavlja tajnost podataka koji se prenose i neovlašteno spaja na bežičnu mrežu. Ukoliko se napadač uspješno spoji na nezaštićeni WLAN, može izvoditi različite štetne radnje na računalima u njoj ili čak u LAN mreži na koju je ranjivi WLAN spojen preko pristupne točke. (13)

Potpuna i prava zaštita bežične mreže postiže se korištenjem posebno oblikovanih protokola kao što su WEP, WPA i WPA2.

3.4.1. WEP

WEP (eng. *Wireless Encryption Protocol*) je protokol za zaštitu bežičnih mreža, opisan IEEE standardnom 802.11b. WEP zaštita odnosi se na fizički sloj i sloj podatkovne poveznice (OSI referentnog modela) u računalnoj mreži, a temelji se na enkripciji podataka između krajnjih točaka. WEP koristi kriptografske ključeve standardnih duljina od 64, 128 i 256 bita. Optimalna duljina ključa je ona koja onemogućuje njegovo otkrivanje, a da se enkripcija istovremeno može obaviti što brže. Kriptiranje i dekriptiranje podataka obavlja se tajnim ključem u krajnjim točkama, a protokol uključuje provjeru integriteta poruke i provjeru identiteta korisnika, odnosno metode kojima se može utvrditi je li poruka bila mijenjana između izvorišta i odredišta.

WEP enkripcija koristi RC4 sustav za kriptiranje podatkovnih tokova, prikazan je na slici 15., koji na temelju ključa stvara pseudo nasumičan niz kojim se pomoću XOR funkcije kriptira ulazna poruka. Poznavanjem ključa moguće je upotrebom iste funkcije niz dekriptirati na odredištu. (13)



Slika 15. RC sustav za kriptiranje

Izvor: (13)

3.4.2. WPA

WPA (eng. *Wi-Fi Protected Access*) je sustav zaštite bežičnih mreža, opisan u okviru IEEE 802.11i standarda, koji omogućuje enkripciju podataka i provjeru identiteta korisnika. Isto kao i WEP, WPA također koristi RC4 sustav za kriptiranje podataka i to uz 128-bitni ključ i 48-bitni inicijalizacijski vektor (IV).Prednost nad WEP standardom je u korištenju TKIP protokola (eng. *Temporal Key Integrity Protocol*), koji dinamički mijenja ključeve za vrijeme korištenja sustava. Kombinacijom dugačkog inicijalizacijskog vektora(IV) i TKIP protokola sustav se lako može obraniti od napada kakvi se koriste za otkrivanje ključa kod primjene WEP protokola. Naime, slabosti prethodnih sustava ležale su u premalom broju mogućih inicijalizacijskih vektora koji su uz isti tajni ključ davali nesigurne nizove podataka. Analizom takvih nizova je bilo moguće otkriti vrijednosti ključa.

Uz spomenuta unaprjeđenja, WPA protokol također donosi i sigurniji sustav provjere besprijekornosti poruke u odnosu na CRC (eng. *Cyclic Redundancy Check*) sustav koji se koristi kod WEP protokola. Kod CRC provjere, napadač može promijeniti sastav poruke koja se šalje i vratiti vrijednost CRC-a na izvornu, čak i bez poznavanja ključa kojim je poruka kriptirana. Sigurniji način provjere je korištenje MIC-a (eng. *Message Integrity Code*) koji u WPA uključuje brojač okvira čime se isključuje mogućnost promjene sastava poruka u komunikacijskom kanalu. MIC ili tzv. „Michael“ algoritam izveden je tako da bude dovoljno siguran, a da ga je ipak moguće koristiti na starijim mrežnim karticama. (13)

3.4.3. WPA2

WPA2 je najrašireniji sustav zaštite bežičnih lokalnih mreža, a razvijen je u okviru Wi-Fi Alliance udruženja 2004. godine. Riječ je o poboljšanoj inačici WPA protokola nastalog u okviru iste generacije. Spomenuto je u odlomku gdje spominjemo WPA, kako je glavno poboljšanje WPA i WPA2 tehnologija u odnosu na WEP uvođenje TKIP protokola. Osim sigurnije provjere besprijekornosti poruke, TKIP koristi složenije funkcije za stvaranje niza bitova kojima se kriptira tekst. Na taj način napadaču otežava otkrivanje tajnog ključa prisluškivanjem mrežnog prometa. Uz to, TKIP jamči da je svaki paket u mreži kriptiran drukčijim ključem.

Otkrivena je i ranjivost TKIP protokola koju napadač može iskoristiti za otkrivanje niza bitova kojima je kriptiran određeni paket. Napad je pritom moguće izvesti samo na kratkim porukama većinom poznatog sadržaja, kao što su ARP (eng. *Address Resolution Protocol*) poruke za otkrivanje sklopovske adrese na temelju mrežne adrese uređaja. Posljedice uspješne zlouporabe mogu biti podmetanje lažnih ARP paketa ranjivom klijentu. Ta se ranjivost odnosi samo na WPA, ne i na WPA2 protokol.

WPA i WPA2 protokoli se mogu koristiti na dva načina:

- PSK (eng. *Pre-Shared Key*) – podrazumijeva prethodnu razmjenu između ključeva između pristupne točke i svih klijenata.
- Enterprise – podrazumijeva zaseban ključ između pristupne točke i svakog klijenta.

PSK način rada još se naziva i privatni, namijenjen je privatnim mrežama ili manjim poslovnim mrežama. Bitno je jednostavniji za izvedbu od Enterprise sustava jer ne zahtijeva autentifikacijski poslužitelj, već se definira jednostavni 256 bitni ključ koji se koristi za svu komunikaciju u mreži. Taj ključ se može unijeti kao 64 heksadecimalne znamenke ili niz od 8 do 63 ASCII znakova na temelju kojeg se računa ključ.

Enterprise način pak nudi bolju zaštitu jer se svaki uređaj u mreži mora autentificirati (identificirati i ovjeriti identitet lozinkom), no uvođenje i održavanje takvog sustava zahtijeva znatno više posla. WPA Enterprise autentifikacija temelji se na IEEE 802.11x standardu, dok WPA2 Enterprise autentifikacijski poslužitelji koriste RADIUS (eng. *Remote Authentication Dial In User Service*) mrežni protokol za centraliziranu autentifikaciju. (13)

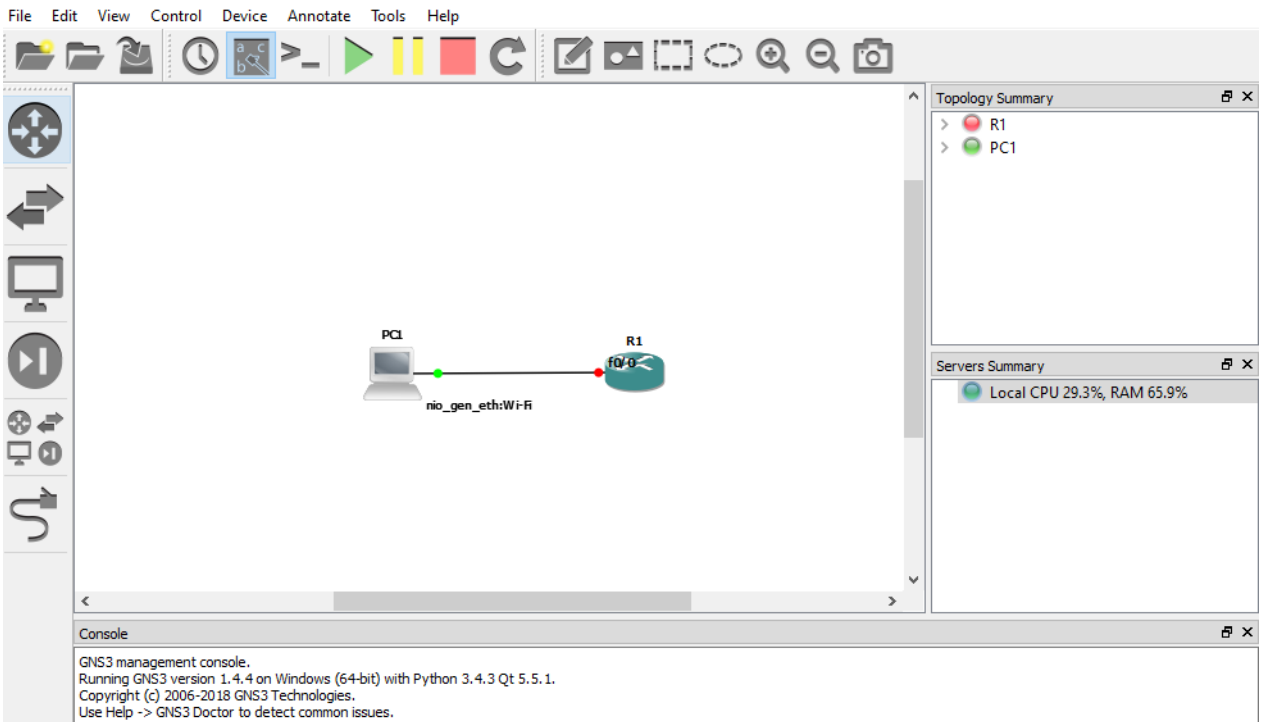
4. Simulacija WLAN mreže primjenom GNS3 aplikacije

Za simulaciju rada bežične mreže u ovom slučaju se koristi programska podrška GNS3 (Graphic Network Simulator), verzije 1.4.4., koji radi u operacijskom sustavu Windows 10. Cijeli program je napisan u programskom jeziku Python. Koristi „Dynamips“ emulatorski softver koji pokreće Cisco-ve elemente (usmjerivače, prespojnike).

Ova programska podrška se koristi kao alat za kreiranje mreža, od jednostavnijih pa sve do složenih. Dopušta kombiniranje realnih i virtualnih uređaja kod mrežnog komuniciranja pri simulaciji rada mreže. Praćenje prometa koji se generira kroz simulaciju u mreži prati se preko nekih drugih alata, ali najčešće se koristi alat za praćenje prometa Wireshark.

4.1. Implementacija GNS3 aplikacije

Aplikacija GNS3 se sastoji od glavnog prozora. Na njemu psotoji alatna traka na kojoj se može pokretati ili zaustavljati rad mreže, može se konfigurirati uređaje iz mreže, može uključiti konzulu kako bi bile npr. dodane IP (eng. *Internet Protocol*) adrese uređajima kako bi mogli međusobno komunicirati, koristiti naredbu ping i sl. S lijeve strane su uređaji koji su dostupni za korištenje ovisno po potrebama mreže. Na vrhu te alatne trake s uređajima su usmjerivači (eng. *Router*). Ispod njih stoje prespojnici (eng. *Switch*), a nakon njih krajnji uređaji (računala, virtualna računala i sl.), te na kraju sigurnosni uređaji. U središnjici aplikacije se nalazi radna pozadina koja služi za kreiranje mreže i tamo stoji cijelo vrijeme prikaz mreže i uređaja u njoj. Ispod radne površine nalazi se „konzola“ koja izbacuje informacije ukoliko se dogodi neka greška u radu ili slično. S desne strane se nalaze još dva prozora. Gornji prozor prikazuje sažetu topologiju mreže, tj. prikazuje popis svih uređaja koje koristimo u mreži, dok se ispod tog prozora nalazi prozor koji pokazuje servere koji se mogu koristiti u simulaciji mreže. Prikaz aplikacije se nalazi na slici 16.



Slika 16. Prikaz radne površine aplikacije GNS3 1.4.4.

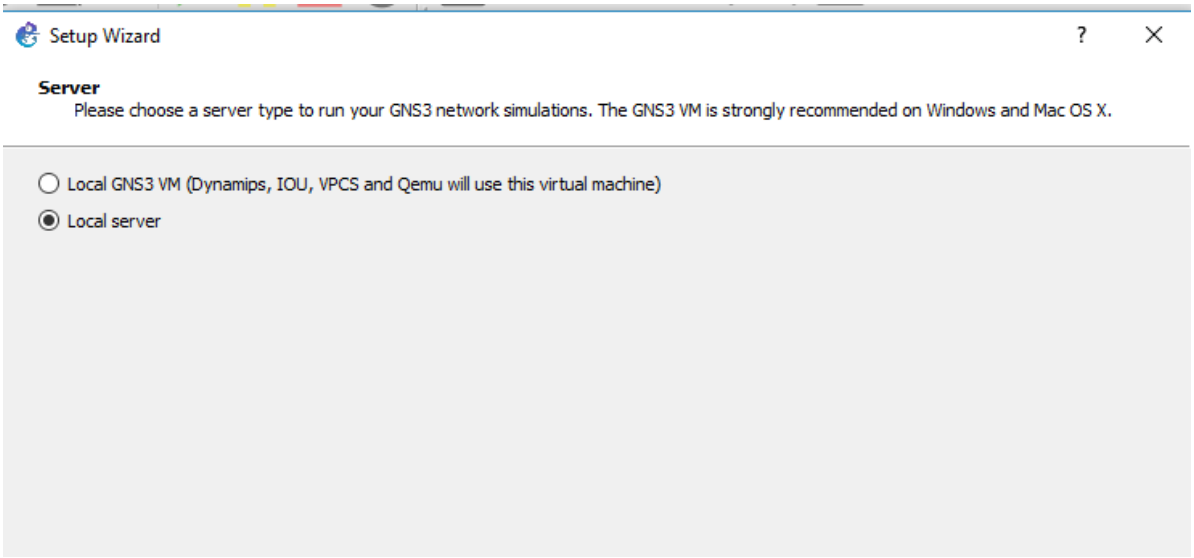
Izvor: Autor

Kod korištenja aplikacije GNS3, kad se pokrene, prva stvar koja se mora napraviti je odabrati server. Dva su odabira, prikazano je na slici 17.:

- Local GNS3 VM
- Local server.

Local GNS3 VM je virtualni server preko kojeg radi mreža koja kreira, dok je local server onaj koji se ne mora kreirati nego je ručno kreiran kroz aplikaciju. U ovom projektu je korišten local server.

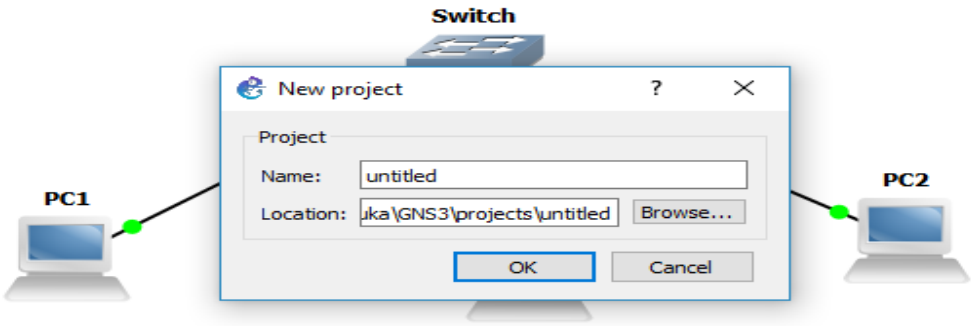
Nakon što je odabran server, moraju se odabrati usmjerivači ili virtualni strojevi koji se dodaju u aplikaciju preko kojih će aplikacija „usmjeravati“ podatke kroz virtualnu mrežu. U ovom slučaju je odabrano ubacivanje „IOS“ rutera (Cisco-vi ruteri) koje je preuzeo autor s web stranice aplikacije GNS3. Nakon što je odabrano ubacivanje „ISO“ rutera, ubacuje se datoteka s podacima rutera kako bi se mogao koristiti na projektima putem aplikacije GNS3



Slika 17. Odabir virtualnog stroja preko GNS3 aplikacije ili lokalnog servera.

Izvor: Autor

Nakon što je ubačen router, otvara se prozor preko kojeg se pokreće (otvara) projekt. Prikazano je na slici 18., upiše se željeno ime projekta i može se krenuti s radom.



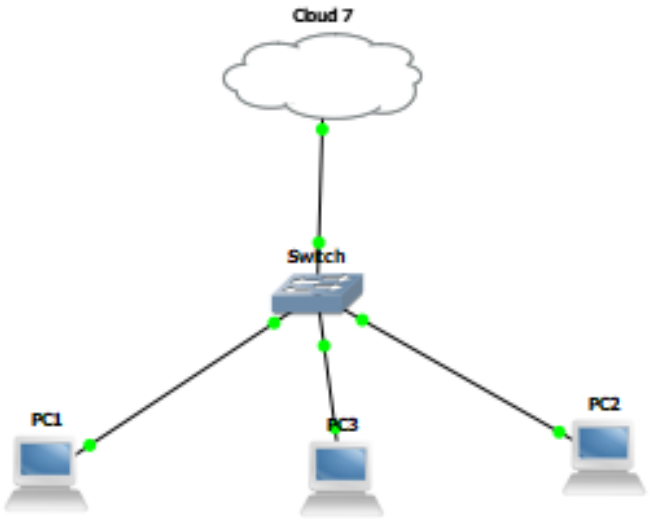
Slika 18. Otvaranje novog projekta u GNS3

Izvor: Autor

4.2. Kreiranje LAN mreže

Nakon što je pokrenut projekt (u ovom slučaju ima naziv „Projekt_X“) otvara se zaslon kao što je prikazano na slici 16. S lijeve strane su prikazani elementi od kojih se može složiti mreža prema svačijem izboru ili zadatku koji je zadan.

U ovom projektu je korišteno tri krajnja uređaja i preklopnik (switch) koji ih povezuje u cjelinu, te oblak kao što je prikazano na slici 19.

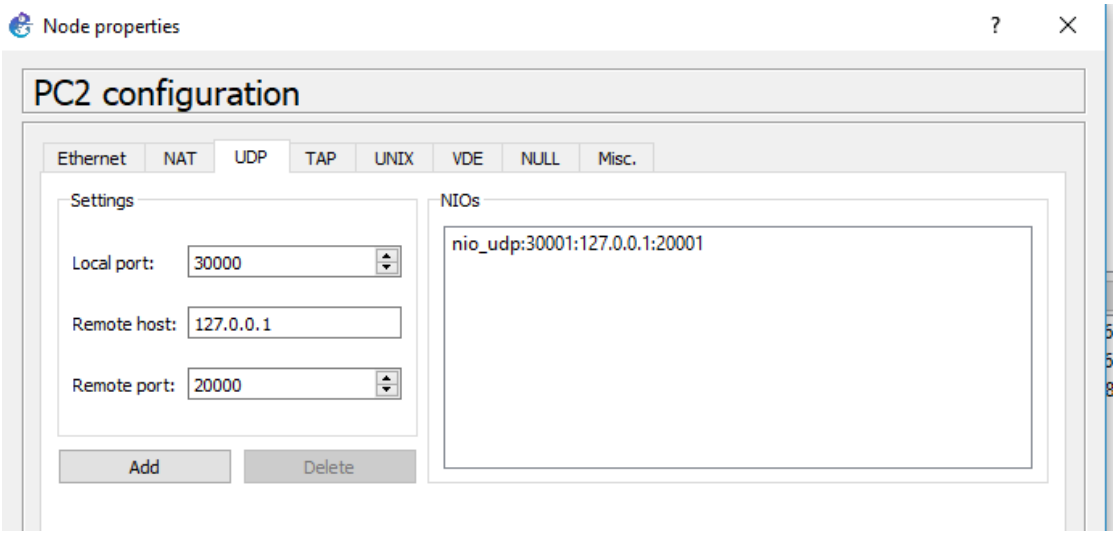


Slika 19. Prikaz kreirane mreže

Izvor: Autor

Switch koji je dodan u mrežu ima devet raspoloživih portova, što znači da na njega može biti spojeno maksimalno devet uređaja s kojima može komunicirati (ne moraju nužno biti krajnji uređaji, može biti spojen drugi switch, hub, router ili slično.). Svaki od ova 3 krajnja uređaja koji su dodani u mrežu imaju po pet portova preko (može ih biti i više, ako ih se doda, ali u ovom slučaju ih je pet) kojih se mogu spojiti na neke druge uređaje, a oni su Wi-Fi port, ethernet port, UDP port, bluetooth port i VM port za virtualnu mrežu u GNS3 aplikaciji, dok se oblaku dodaje pork prije spajanja, u ovom slučaju mu je dodijeljen Wi-Fi port.

Kad se uređaji dodaju u mrežu, prije nego što se spoje u mrežu, moraju im se dodati UDP portovi kako bi mogli komunicirati u ovom slučaju. Dodavanje UDP porta se radi tako da se klikne desnim klikom na npr. PC1 i otvori se pomoćni izbornik, klikne se na „configure“. Nakon što se klikne na configure, otvara se izbornik koji ima više opcija, i mora se odabrati na alatnoj traci kartica „UDP“ i promijeni se lokalni port na 30001 ili nešto slično (ne smije biti port zauzet), ponuđena je i IP adresa, te se još mora promijeniti ručni port na 20001, i uvijek kad se dodaje UDP port na krajnji uređaj, mora se promijeniti lokalni i ručni port. Kad je to obavljeno, klikne se na „Add“ i tako je dodan UDP port krajnjem uređaju i tako se mora učiniti sa svakim uređajem koji će se spajati u mrežu Cijeli postupak prikazan je na slici 20.



Slika 20. Dodavanje UDP porta PC-u.

Izvor:Autor

Kod dodjele porta „Cloud-u“ je malo drukčiji postupak. Klikne se na karticu ethernet, i tamo mu se dodijeli Wi-Fi port.

Dodani su svi krajnjim uređajima UDP portovi, sad se moraju spojiti na preklopnik ili switch, a to se radi tako da se klikne na lijevoj alatnoj traci na radnoj površini na posljednji gumb koji omogućuje povezivanje uređaja međusobno, tj. stvaranje mreže. Kada je to stanje povezivanja uređaja aktivno, pri kliku na željeni uređaj, otvori se izbornik u kojem se odabire na koji port će biti spojen uređaj. Ovom slučaju, kod krajnjih

uređaja, uvijek je odabran UDP port, dok je kod Switch uređaja svejedno koji port će biti odabran, samo mora biti slobodan.

4.3. Pokretanje LAN mreže

Kada je to napravljeno, klikne se na zeleni gumb na gornjoj alatnoj traci koji je znak za pokretanje, te se tako pokreće rad mreže. Da bi uređaji u mreži međusobno komunicirali, moraju im se dodijeliti IP adrese, a to se radi tako da se na gornjoj alatnoj traci klikne na padajući izbornik „Tools“, a nakon toga na „VPCS multi-host“. Kad se klikne na „VPCS multi-host“, otvori se konzola u koju se upisuju komade kako bi bila dodijeljena IP adresa svakom krajnjem uređaju.

Nakon što se otvorila konzola, mora se dodijeliti IP adresa krajnjem uređaju, a to se radi tako da se prvo upiše broj uređaja kojem se dodaje IP adresa, a nakon toga se upiše komanda „IP 10.1.1.1“ (ili neki drugi broj u ovakvom formatu) i nakon toga je dodijeljena IP adresa uređaju PC1, kao što je prikazano na slici 21.

Slika 21. Dodavanje IP adrese krajnjem uređaju.

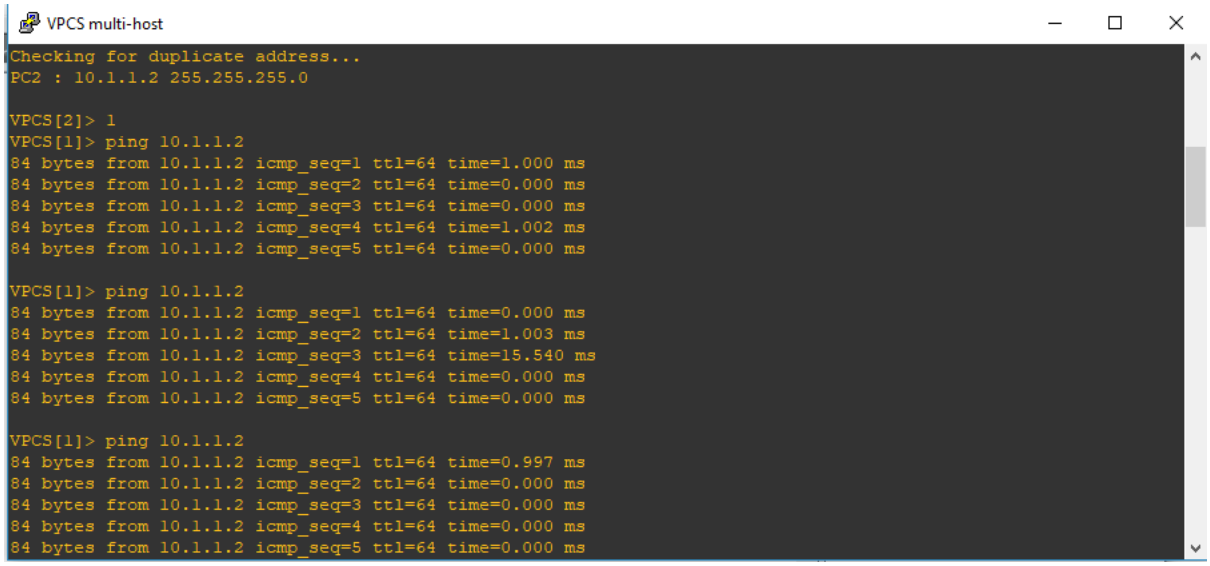
Izvor: Autor

Kao što je prikazano na slici 21., konzola vrši provjeru IP adrese, provjerava da li već postoji već ta IP adresa, te bi tad paket koji se šalje bio poslan na krivo odredište, te bi onda aplikacija zahtjevala da se uređaju dodijeli neka druga IP adresa koja bi bila jedinstvena.

4.4. Praćenje prometa putem aplikacije Wireshark

Dodane su IP adrese svim uređajima u mreži kojima je to potrebno, što znači da može početi komunikacija između uređaja u mreži. Ponovo se otvori konzola i upisuje naredba ping prema drugim uređajima u mreži. To se radi tako da se ponovo prvo upiše broj uređaja s kojeg se šalju podaci, a zatim se upiše IP adresa uređaja kojem se šalju podaci, što je prikazano na slici 22.

Kod naredbe ping, šalje se pet paketa, veličine 84 bajta i prikazano je vrijeme je koje je potrebno da stigne od točke do točke, IP adresa uređaja kojem se šalje paket, te broj paketa.



Slika 22. Korištenje naredbe ping preko konzole.

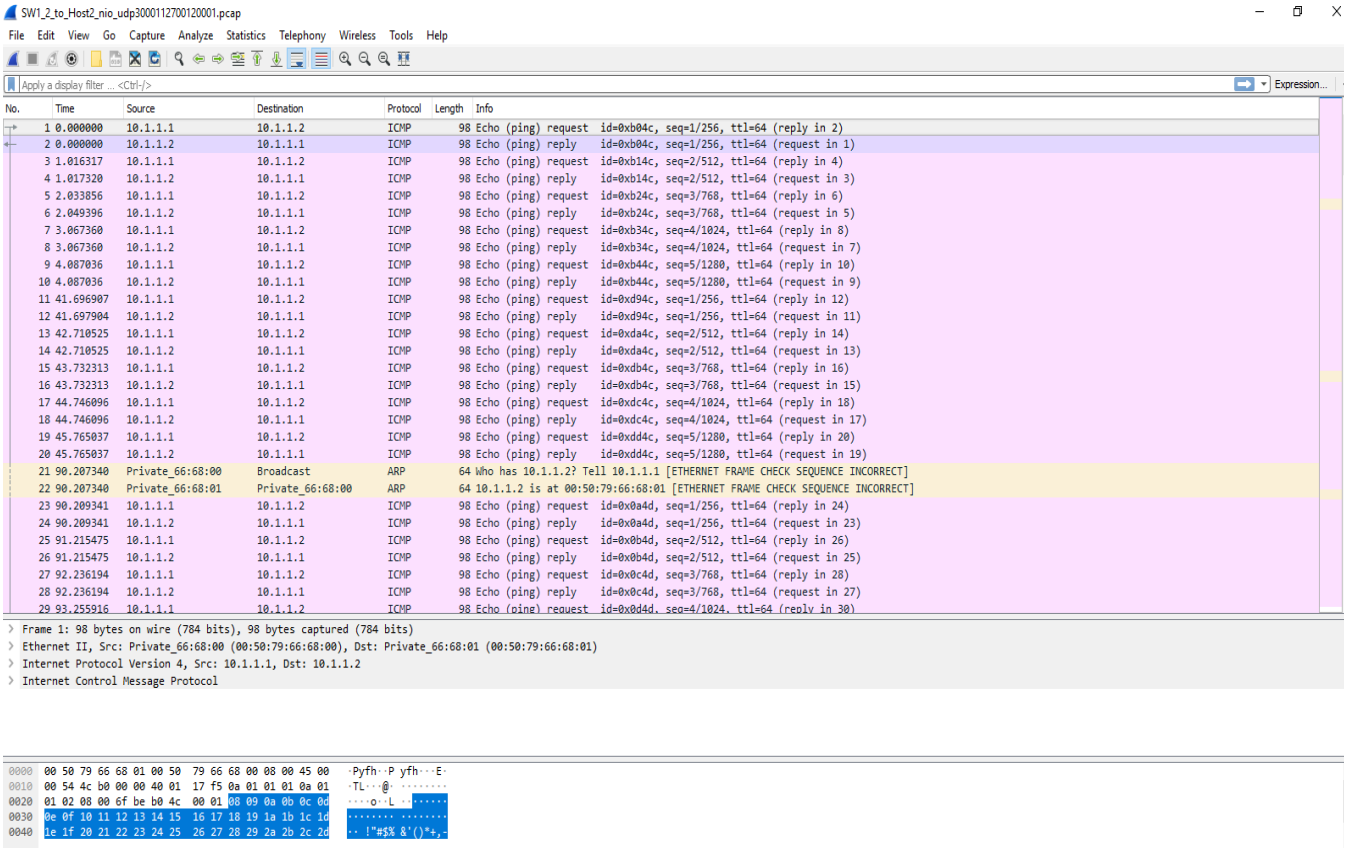
Izvor: Autor

Iz ovih podataka se može vidjeti kako je u većini slučajeva kašnjenje paketa u mreži bilo 1 milisekundi i manje, dok je kod jednog paketa kašnjenje bilo iznad 15 ms.

Iz tih podataka se može zaključiti da je došlo do degradacije kod prijenosa paketa, pa je tom jednom paketu trebalo više vremena da se prenese od PC-a 1 do PC-a 2.

Kad je odrađena naredba ping, mora se obaviti provjera da li je došlo do prijenosa paketa kako je i prikazano na konzoli. Kod aplikacije GNS3, praćenje prometa se obavlja putem aplikacije Wireshark, koja je jedna i od najpoznatijih aplikacija za praćenje telekomunikacijskog prometa.

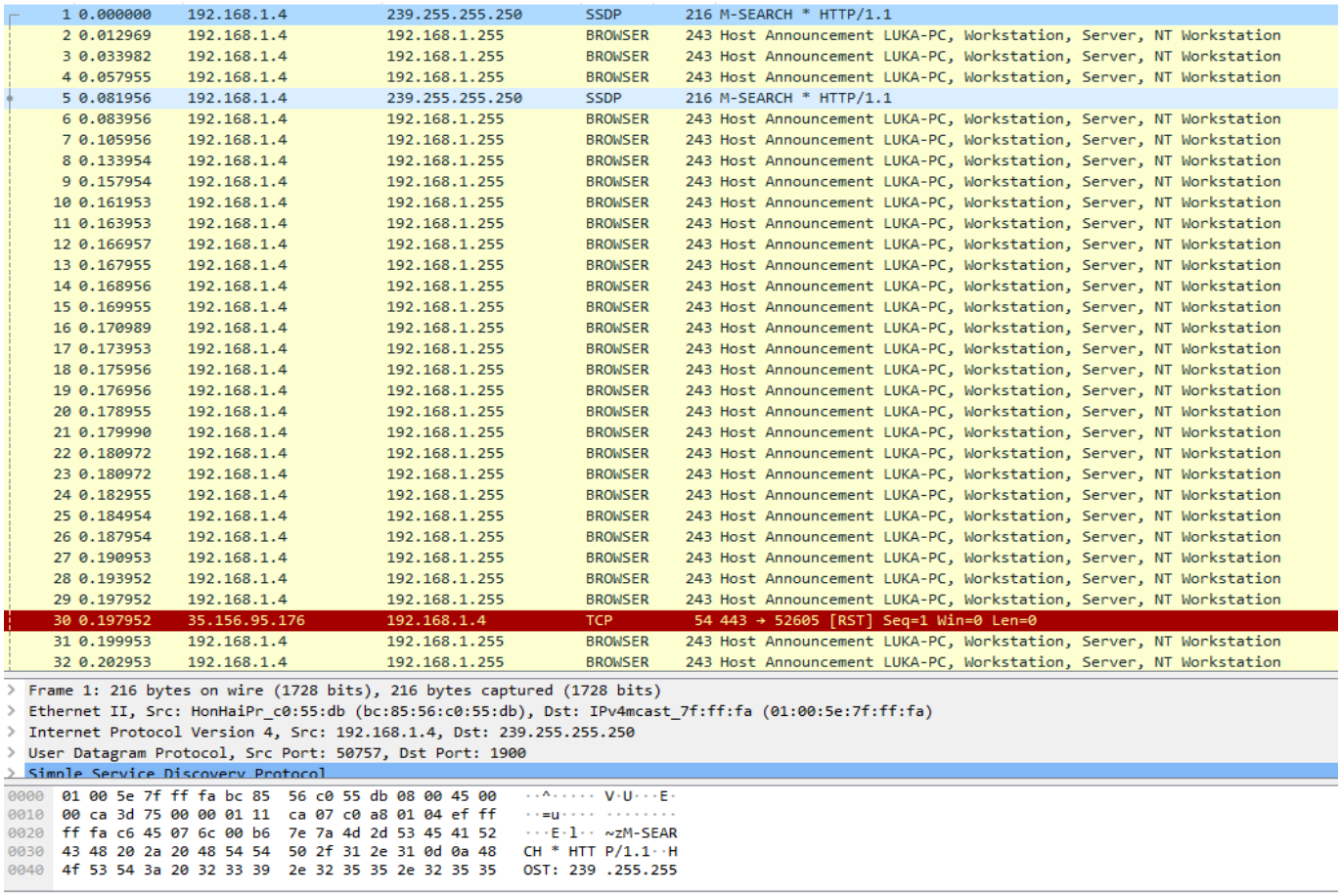
Da bi bili dobiveni podaci iz aplikacije, mora se odabrati link (veza) između uređaja s kojeg su slani podaci prema switchu te tada kliknuti desni klik. Kada se otvori izbornik, klikne se na „Start capture“ te se onda odabere veza, koja će se pratiti, a zatim se automatski pokreće aplikacija Wireshark i pokreće praćenje. Rezultat praćenja prikazan je na slici 23.



Slika 23. Rezultati praćenja prometa putem aplikacije Wireshark između PC uređaja.

Izvor:Autor

Nakon što je obavljena provjera prometa nakon naredbe ping PC uređaja, obavljena je provjera generiranja prometa u oblaku kako bi se usporedili podaci iz oba mjerenja. Prije početka praćenja generiranja prometa u oblaku, mora se označiti link između oblaka i switcha, te se klikne ponovo na start capture. Tada se otvara aplikacija Wireshark te se počinju prikazivati podaci na konzoli kao što je prikazano na slici 24.



Slika 24. Rezultati praćenja prometa između Switcha i Clouda.

Izvor:Autor

5. Zaključak

Razmatranjem svih dobivenih rezultata tokom analize i istraživanja, može se zaključiti kako su bežične mreže budućnost telekomunikacija, ionako su još uvijek nesigurne i manje pouzdane od žičnih mreža. Praktičnije je korištenje terminalnog uređaja bežično dok šećemo gradom ili u dnevnom boravku, nego korištenje uređaja koji su spojeni na žičnu mrežu.

U lokalnim bežičnim mrežama se postižu puno veće brzine prijenosa u odnosu na bežične mreže koje pokrivaju veće geografsko područje. Razlog tome je što se signal koji generira pristupna točka jači na manjim udaljenosti, nego na većim udaljenostima, zato se i postavlja više pristupnih točaka, kako bi bežične mreže bile stabilnije.

Ako uzmemo u obzir analizu prijenosa žičane i bežične mreže, jasno je vidljivo da se kod uređaja u žičanim mrežama ne izgenerira tolika količina prometa koliko kod bežičnih mreža, budući da je uglavnom više uređaja spojeno na lokalne bežične mreže nego na žične.

GNS3 aplikacija pruža široku primjenu kod simuliranja mreža i sličnih postupaka. Neke jednostavnije simulacije, kao što je ova u samom radu, lako se izkonfiguriraju i odradi se prijenos podataka kroz mrežu, prema podacima iz aplikacije Wireshark koja pokazuje da paketi koju poslani, provjeravaju se putem protokola ICMP (engl. *Internet Control Message Protocol*) koji samo detektira greške ukoliko su se dogodile, ali ih ne ispravlja.

Prednost GNS3 aplikacije je ta što koristi stvarni Cisco IOS u virtualnoj okolini putem računala. Veliki nedostatak koji sam primijetio je što GNS3 ne sadrži grafičko sučelje za analizu izlaznih rezultata, već koristi neke druge aplikacije za analizu izlaznih rezultata, odnosno praćenje prometa, kao što je Wireshark i drugi.

Kod analize prometa između prve mreže koja je bila praćena i druge mreže koja je dohvaćala podatke iz ostalih mreža u „oblak“, vidi se koliko je ta mreža kompleksnija od prve mreže. Razlog tome je što su sakupljani podaci s više uređaja u mreži koji su spojeni na Internet mrežu koja je složenija od lokalne mreže koja je bila sastavljena u svrhu ovog projekta.

Sigurnost kod bežičnih mreža je važan faktor koji se treba uzeti u obzir kod implementacije bežičnih mreža. Kod žičnih mreža onemogućen je pristup neovlaštenim osobama u mrežu, što je velika prednost žičnih mreža.

Literatura

1. Sustavi za vođenje i praćenje procesa. [Mrežno] 24. 4 2008. http://spvp.zesoi.fer.hr/predavanja%202008/WE_skripta.pdf.

2. *study.com.* [Mrežno] 2007. https://study.com/academy/lesson/types-of-networks-lan-wan-wlan-man-san-pan-epn-vpn.html.

3. *http://dbrzovic.blogspot.com.* [Mrežno] 16. 5 2012. http://dbrzovic.blogspot.com/2012/05/racunalne-mreze-lan-wan-pan-man.html.

4. **Kavran, Zvonko.** Autorizirana predavanja. *e-student.hr.* [Mrežno] 2017. http://e-student.fpz.hr/Predmeti/R/Racunalne_mreze/Materijali/5_Predavanje.pdf.

5. **Andrew S. Tanenbaum, David J. Wetherall.** *Computer Networks.* 2011.

6. [Mrežno] https://www.techwalla.com/articles/microwave-radio-communications-advantages-disadvantages.

7. [Mrežno] https://flylib.com/books/en/3.370.1.18/1/.

8. **Mrvelj, Štefica.** Autorizirana predavanja, Tehnologija telekomunikacijskog prometa I. 2017.

9. **Martina, Coban.** [Mrežno] 2017. https://zir.nsk.hr/islandora/object/fpz:1095/preview.

10. **Copar, Saša.** Lokalne bežične mreže prema IEEE 802.11 standardu. [Mrežno] 2004.

11. **Thomas Maufer.** *A Field Guide to Wireless LANs for Administrators and Power Users.* [Mrežno] 2005. https://flylib.com/books/en/2.799.1.29/1/.

12. **A. Skendžić.** *Sigurnost infrastrukturnog načina rada bežične mreže standarda IEEE 802.11.* [Mrežno] 2014.

13. WPA2 zaštita. [Mrežno] 2009. https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-06-267.pdf.

14. [Mrežno] http://www.znanje.org/abc/tutorials/internet_abc/01/060_network_lan_man_wan.htm.

15. [Mrežno] 5. 2007. http://spvp.zesoi.fer.hr/seminari/2007/seminari/NikolaPetanjak_IEEE802.pdf.

16. *www.commons.wikipedia.org.* [Mrežno] https://commons.wikimedia.org/wiki/File:CSMA_CA_Flowchart.png.

17. [Mrežno] https://slideplayer.com/slide/9758437/.

Popis slika

Slika 1. Elektromagnetski spektar

Slika 2. PAN mreža

Slika 3. Prikaz bežične(lijevo) i žične(desno) lokalne mreže

Slika 4. Prikaz MAN mreže

Slika 5. IEEE mreža u odnosu na OSI model

Slika 6. Područje interesa 802.11 standarda

Slika 7. Proširivanje spektra signala „Spread Spectrum“ tehnikom

Slika 8. Primjer korištenja ISM pojasa pomoću DSSS tehnike

Slika 9. FHSS modulacija

Slika 10. Usporedba DSSS i FHSS modulacijske tehnike

Slika 11. Princip rada mehanizma CSMA/CA

Slika 12. RTS/CTS mehanizam

Slika 13. Prikaz neovisnog (Ad-hoc) povezivanja računala

Slika 14. Prikaz infrastrukturne WLAN mreže

Slika 15. RC sustav za kriptiranje

Slika 16. Prikaz radne površine aplikacije GNS3 1.4.4.

Slika 17. Odabir virtualnog stroja preko GNS3 aplikacije ili lokalnog servera

Slika 18. Otvaranje novog projekta u GNS3

Slika 19. Prikaz kreirane mreže

Slika 20. Dodavanje UDP porta PC-u

Slika 21. Dodavanje IP adrese krajnjem uređaju.

Slika 22. Korištenje naredbe ping preko konzole.

Slika 23. Rezultati praćenja prometa putem aplikacije Wireshark između PC uređaja.

Slika 24. Rezultati praćenja prometa između Switcha i Clouda.

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni rad isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom „Simulacija WLAN mreže primjenom GNS3 aplikacije“ u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:
Luka Smiljanić

U Zagrebu, 5.9.2018.

_____
(potpis)