Analiza i usporedba performansi bežičnih mesh protokola

Dumančić, Ilija

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni studij

Analiza i usporedba performansi bežičnih mesh protokola

Diplomski rad

Ilija Dumančić

Osijek, 2018.

SADRŽAJ

1. UVOD

Bežični sustavi su u svakodnevnoj upotrebi i postaju sve veći dio sadašnjice u ulozi olakšavanja komunikacije između samih uređaja i ljudi. Tako i mesh bežične mreže imaju ulogu u sadašnjosti i bliskoj budućnosti dodatno olakšati komunikaciju. U ovom radu će biti detaljno opisan rad mesh mreže i neki od rješenja. U detaljnoj analizi rada biti će uspoređeni razni načini spajanja uređaja te njihove performanse u različitim uvjetima rada. Jedna od prednosti mesh mreža je nepostojanje središnjeg čvora preko kojega bi se odvijala cjelokupna komunikacija, svaki čvor u mreži predstavlja prijenosni sustav podataka prema drugom čvoru. Što se tiče sigurnosti u mesh mrežama može se reći da je jedan od pouzdanijih načina komunikacije zbog toga jer postoji više načina odnosno puteva za prijenos podataka između korisnika i uređaja. Čvorovi se lako i jednostavno postavljaju i automatski se konfiguriraju. Naravno, što je više čvorova to je i mreža veća i stabilnija. Mesh standard je zasnovan na ostalim bežičnim standardima kao što su 802.11 a, b i g. Mesh sustav je također koristan kada je bežični signal privremeno nedostupan ili blokiran kao npr. u NLoS (engl. Non-line-of -sight) uvjetima. Kao što je ranije već navedeno mesh mreža se sama konfigurira, sustav automatski ugrađuje nove čvorove u postojeću strukturu bez potrebe za ljudskom intervencijom odnosno mrežnog administratora. Upravo zbog lake implementacije mesh mreža se počinje koristiti u velikim kompanijama i drugim raznim ustanovama. Druga velika prednost ove tehnologije je ta što sustav ima sposobnost "samo-izlječenja". To se odvija tako što mreža automatski nalazi najbržu i najsigurniju putanju između korisnika u slanju podataka. Upravo takvim mehanizmom sprječava se zagušenje u sustavu, jer svaki poslani paket od jednog korisnika do drugog ne mora putovati do središnjeg servera. Prijenos podataka se odvija između korisnika i AP-a (engl. Access point) uz pomoć IEEE 802.11 standarda. Usmjeravanjem (engl. routing) se postiže najveća brzina slanja paketa bez većih gubitaka u prijenosu uz dodatnu zaštitu. Neki od protokola za usmjeravanje koji će se još kasnije spominjati i opisivati u radu su: B.A.T.M.A.N, AODV, DNVR, itd. Za svaki paket potreban je određeni kanal kojim će on putovati, a za određivanje tih kanala zadužen je MAC (engl. Media Access Protocol) protokol. Dodatno su se razvile bežične mesh mreže WMN (engl. Wireless mesh network) koje se ostvaruju na nekoliko načina. Bežične mesh mreže su podijeljene na ravne, hijerarhijske i hibridne mreže. U idućem poglavlju biti će detaljno opisan način rada mesh mreže. Nakon toga će se uspoređivati performanse određenih uređaja koji se koriste u mrežnoj komunikaciji. Uspoređivati će se brzina između uređaja, količina mogućeg prijenosa podataka, itd.

1.1. Zadatak diplomskog rada

Bežične mesh mreže (sa isprepletenom topologijom) sve su zastupljenije i zbog niza svojih prednosti nalaze sve širu praktičnu uporabu. Potrebno je usporediti različita rješenja i protokole koji se koriste danas za bežičnu mesh komunikaciju (analizirati sličnosti i razlike, prednosti i nedostatke svakog rješenja, te usporediti performanse mrežnog protoka podataka. Potrebno je testirati mesh performanse putem više Wi-Fi routera (multi-hop mesh) i iperf klijenta i servera. Potrebno je usporediti performanse open source mesh firmwarea (Freifunk, Libremesh, Otvorena mreža), te usporediti dostupna rješenja (Ubiquiti, MikroTik i druga). Potrebno je testirati rad fast roaming 802.11r protokola, te provesti softverske simulacije. (sumentor: Valent Turković, Otvorena mreža).

2. MESH MREŽA

Brzi razvoj Interneta zahtijevao je potrebu za brzim i sigurnim bežičnim prijenosom podataka. Upravo zbog toga se u zadnjim desetljećima razvijaju razni standardi u cilju povećanja sigurnosti i smanjenja troškova u bežičnim komunikacijama. Institucija koja je zaslužna za inovacije standarda je IEEE (engl. Institute of Electrical and Electronics Engineers) [1]. Za bežični Internet zadužen je protokol 802.11 a/b/g/n. Tablica 2.1. prikazuje samo neke od standarda i njihov kratki opis.

Tablica 2.1. IEEE standardi

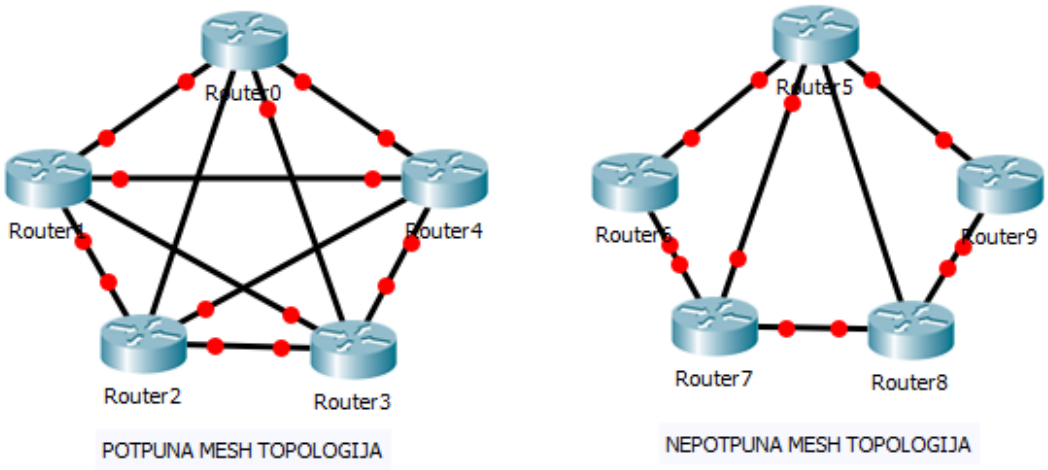
STANDARD	**OPIS**
802.1	Umrežavanje i menadžment mreže
802.2	Logička kontrola linkova
802.3	Ethernet
802.4	Token
802.5	Definira MAC sloj za token
802.9	Integrirani servisi u LAN-u
802.11 a/b/g/n	Bežični LAN i MESH (Wi-Fi)

2.1. 802.11 standard

Postoji nekoliko specifikacija koji čine bežičnu mrežu u 802.11 standardu. Svi oni komuniciraju i rade na frekvencijskom opsegu od 2.4 GHz do 5 GHz. Veće frekvencijsko područje se koristi prilikom izbjegavanja interferencije. Ubrzo nakon 802.11 standarda se pojavljuje nova verzija 802.11a koji za širenje spektra koristi OFDM (engl. Orthogonal frequency-division multiplexing) modulaciju. Pojavom standarda 802.11b povećana je propusnost od 11 Mbit/s na frekvenciji od 2.4 GHz. Taj standard je još poznatiji pod nazivom Wi-Fi [1]. Za širenje spektra koristi se DSSS sekvenca. Ovaj standard se može još usporediti za Ethernet-om. Upravo zbog frekvencije od 2.4 GHz dolazi do interferencije u komunikaciji jer ga koriste mnogi uređaji. Nakon b verzije došla je i 802.11g, radi također na 2.4 GHz i koristi OFDM modulaciju. Propusna moć je veća nego u prethodnika te iznosi 54 Mbit/s. Prilikom komunikacije neka dva uređaja, kada jedan uređaj koristi 802.11b standard, a drugi 802.11g tada se usporava protok podataka iako su hardverski kompatibilni. Pojavom verzije 802.11n propusna moć se drastično povećala na 600 Mbit/s i udvostručuje se domet u komunikaciji. Koristi se MIMO (engl. Multiple-input multiple-output) sustav. Ovaj sustav se koristi zbog toga što on upotrebljava više dolaznih i odlaznih antena radi poboljšavanja signala i ukupnih performansi. Kompatibilan je sa ostalim standardima i radi na frekvencijskom opsegu 2.4 GHz i 5 GHz.

2.2. Što je mesh mreža?

Mesh mreža predstavlja tehnologiju komuniciranja na jednoj višoj razini sve u cilju brzog i lakog ostvarivanja pristupa nekoj računalnoj mreži. Jedna od prednosti mesh mreže je ta što je lako proširiva i lako se nadograđuje na već postojeću mrežnu infrastrukturu. Jednostavna je implementacija na neku drugu mrežu te pruža prijenos podataka bez prekida i gubitaka podataka. Primjena mesh mreže je jednostavna, sve što treba za jednu mrežu su naravno klijenti i usmjeritelji (engl. Router). Drugim riječima potrebni su nam čvorovi za prosljeđivanja podataka. Ti čvorovi imaju svoje primarne ciljeve. Jedan od tih ciljeva je primanje i slanje podataka za korisnika koji koristi taj određeni čvor na koji je stigao paket. Druga svrha postojanja čvorova je prosljeđivanje paketa s drugih čvorova, jer neki čvorovi služe samo kao posrednici između korisnika. To je jedna od karakteristika koja dijeli mesh mreže od ostalih komunikacijskih mreža. Postoji potpuna i nepotpuna mesh topologija, kao što je i prikazano na slici 2.1.



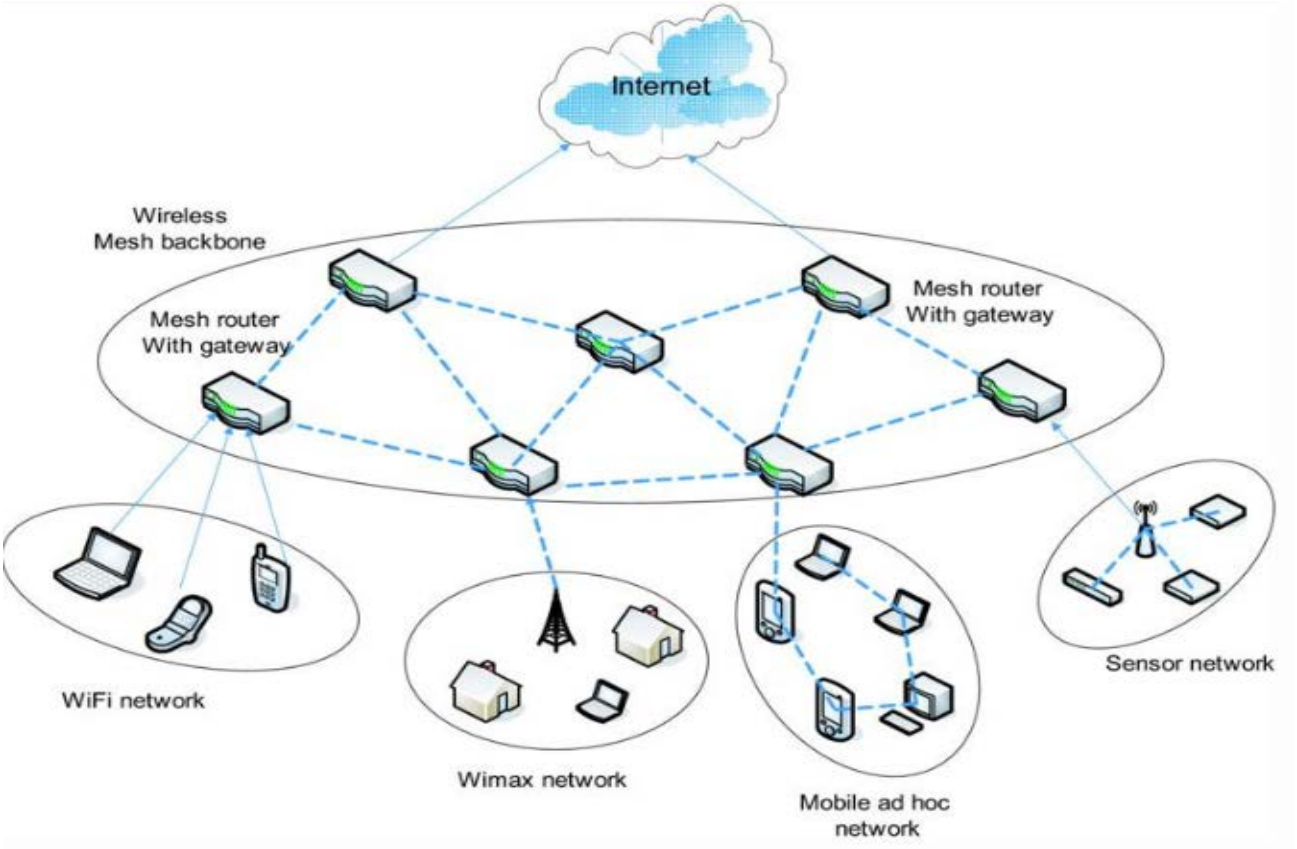
Slika 2.1. *Topologija potpune i nepotpune mesh mreže*

Prilikom dizajniranja mesh mreže postoje dvije tehnike koje se koriste. Jedna od tih tehnika je tehnika poplave (engl. flooding) u kojoj je glavni zadatak širenje podataka kroz cijelu mrežu dok ne stigne do željenog čvora. Jasno, sa ovom tehnikom zauzeće resursa je bilo preveliko pa se ona više i ne koristi. Druga i bolja tehnika je tehnika usmjeravanja (engl. routing), u ovoj tehnici se koriste optimalni putevi, tj. paketi se šalju optimalnim putem do odredišnog čvora. Sami proces prolaska podataka kroz pojedine čvorove naziva se *hopping* . Kao što je ranije napisano postoji tehnika samo-izlječenja (engl. Self-healing), tj. algoritmi koji neprestano šalju testne podatke kroz mrežu kako bi se saznalo postoje li greške u sustavu. Takvim algoritmima se omogućava neprekidan proces putovanja paketa kroz mrežu do odredišnog čvora. Svi korisnici se na određene čvorove povezuje preko mesh mreže. Mesh mreže se koriste u bežičnim mrežama (engl. Wireless mesh network, WMN).

2.3. Princip rada mesh mreže

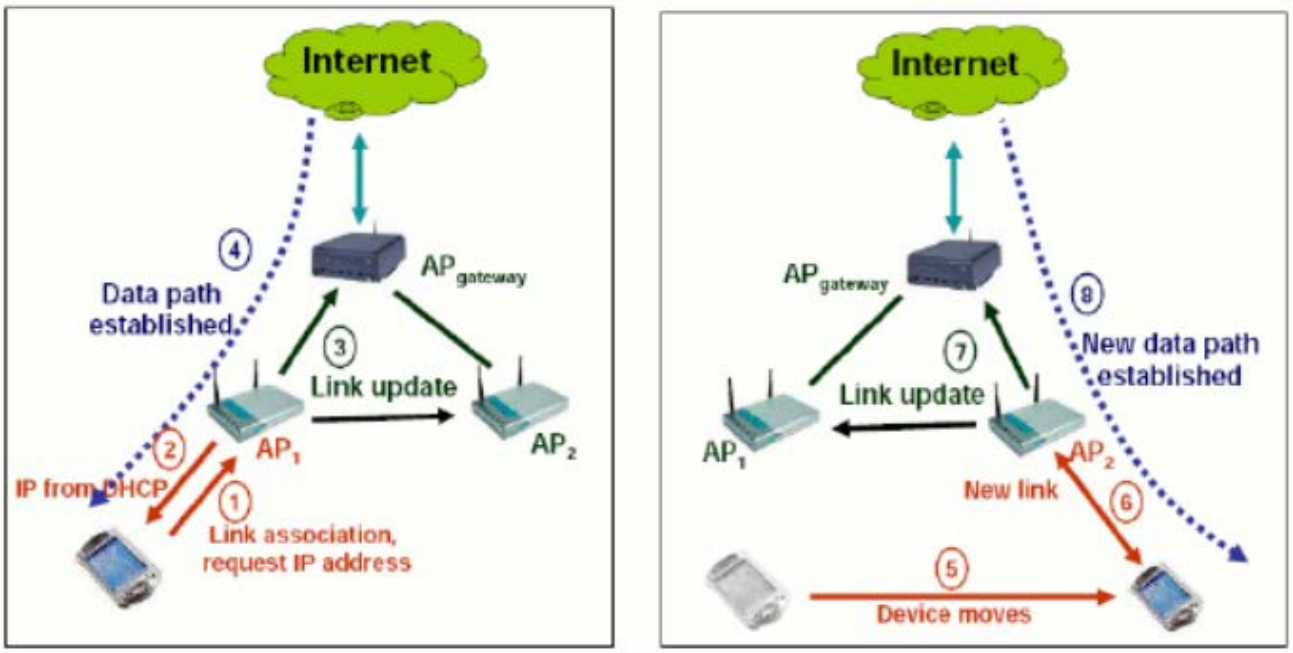
Mesh mreža može biti dizajnirana na različite načine i u različite svrhe. Npr., ako je mreža manja i namijenjena nekoj ustanovi (tvrtka ili fakultet) tada se mreža ne dizajnira prema standardu. U novije vrijeme takvih je mreža sve više. Sa druge strane imamo mesh mreže koje su namijenjene većem broju korisnika i moraju biti dizajnirane prema IEEE standardu i sa pravim načinom usmjeravanja podataka. Upravo zbog toga za velike mreže se dodjeljuju i kanali koji omogućuju istovremeni prijenos podataka

nekom mrežom. Mesh mreža je zasnovana na standardu IEEE 802.11 kojemu je osnovni cilj povezivanje korisnika. Mesh mreža se ostvaruje ukoliko se uspiju međusobno povezati sve pristupne točke (engl. Access point, AP). Upravo taj standard služi za povezivanje korisnika sa pristupnim točkama. Zbog takvog načina rada standard mora podržavati dva načina rada, a to su: Ad Hoc i distribucijski sustav. U Ad Hoc načinu rada sva se komunikacija odvija uz upravljanje pristupnim točkama, gdje podaci samo prolaze kroz čvorišta i oni nemaju pravo upravljanja tokom podataka. Dok u distribucijskom sustavu čvorišta komuniciraju međusobno i sa pristupnim točkama. U Ad hoc načinu podacima upravljaju pristupne točke. Novije mesh mreže koriste upravo taj način rada. Postoje neka pravila koje mesh mreža mora zadovoljavati prije upotrebe IEEE standarda. Ta su pravila direktno povezana sa samim performansama mesh mreže i određuju veličine i kapacitete kanala. Npr., ako je mreža velika kašnjenje paketa prema IEEE standardima će biti preveliko, propisana pravila prema standardu su: 12,5 ms na 2,5 metra udaljenosti. Da bi se smanjila kašnjenja u mreži svi čvorovi moraju podržavati standard zbog sigurnosti i optimalnog puta paketa.



Slika 2.2. *Mesh mreža zasnovana na Ad hoc načinu rada [8]*

Način rada mesh mreže preko ad hoc prikazan je na slici 2.2. gdje se bilo koji korisnik na mrežu spaja preko pristupnih točaka AP. Svaki se AP spaja sa drugim AP-om preko određenog protokola za usmjeravanje i preko usmjerivača. Na slici 2.3. možemo vidjeti način slanja podataka u mesh mreži. Prilikom slanja ili primanja paketa stvara se novi prijenosni put (engl. Data path) između korisnika i Interneta. Upravo to se odvija preko pristupnih točaka AP-ova. AP upravlja i komunikacijom neka dva korisnika. Na slici 2.3. možemo vidjeti korisnika i njegov uređaj u pokretu, na desnoj slici vidimo kako se stvara novi prijenosni put od Interneta do korisnika preko drugog AP-a. Za vrijeme prebacivanja sa jedne pristupne točke na drugu odvija se razmjena upravljačkih podataka.



Slika 2.3. *Ad hoc način rada, prikaz korisnika u pokretu [9]*

2.4. Routing protokoli u mesh mrežama

Primarni cilj i postojanje mesh mreža je uspostava komunikacije između krajnjih korisnika. Primanje i slanje podataka među njima upravo se ostvaruje pomoću protokola za usmjeravanja. Protokoli su zaduženi za protok podataka bez ikakvih problema tako što se kroz cijelu mrežu računaju optimalni putevi [10]. U tijeku procesa računanja optimalnih puteva protokoli konstantno provjeravaju

promjenjive parametre kao npr. zauzetost mreže, greške na čvorovima itd. Takvim pristupom omogućuju funkcionalnost mreže i pouzdanu komunikaciju u mreži.

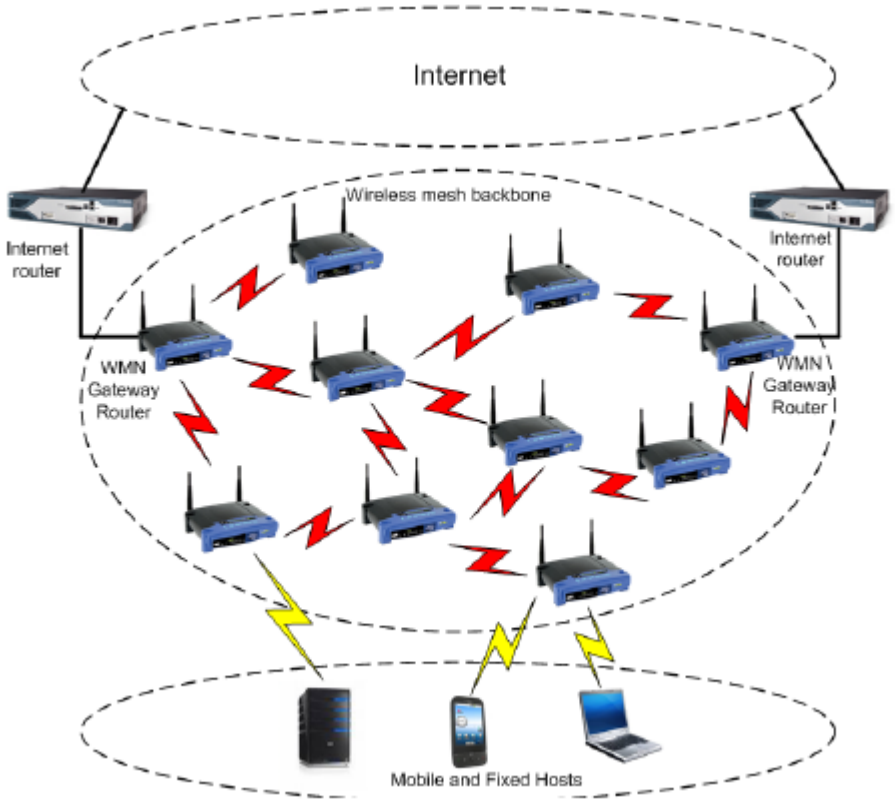
Postoji mnogo protokola za usmjeravanje, ovo su najpoznatiji:

- **AODV** (eng. Ad hoc On-Demand Distance Vector)
- **B.A.T.M.A.N** (eng. Better Approach To Mobile Ad hoc Networking)
- **DNVR** (eng. Dynamic Nix-Vector Routing)
- **DSDV** (eng. Destination-Sequenced Distance-Vector Routing)
- **DSR** (eng. Dynamic Source Routing)
- **HSLS** (eng. Hazy-Sighted Link State)
- **IWMP** (eng. Infrastructure Wireless mesh Protocol)
- **OLSR** (eng. Optimized Link State Routing protocol)
- **OSPF** (eng. Open Shortest Path First Routing)
- **PWRP** (eng. Predictive Wireless Routing Protocol)
- **TORA** (eng. Temporally-Ordered Routing Algorithm)

AODV je protokol za usmjeravanje dizajniran za korištenje u mobilnim ad hoc mrežama. Koristan za mrežu sa 1000 čvorova. Izvor, destinacija i sljedeći skok adresirani su u IP adresi. Svaki čvor sadrži tablicu za usmjeravanje koja sadrži informacije o dostupnosti drugih čvorova.

B.A.T.M.A.N. je protokol za usmjeravanje korišten u multi-hop mobilnim ad hoc mrežama, služi kao zamjena OLSR protokolu. Protokol je poznat po tome što svaki čvor ne poznaje informacije o drugom čvoru. Ta tehnika sprječava potrebu slanja svih informacije putem cijele mreže. Čvor sadrži informacije samo o čvorovima s kojima je bio u vezi tijekom slanja i primanja podataka.

Na slici 2.4. možemo vidjeti primjer jednog usmjeravanja u bežičnoj mesh mreži. Usmjeravanje je prikazano pomoću crvenih strelica kojima su povezani usmjerivači bežične mreže. Protokol za usmjeravanje se pokreće u onom trenutku kada korisnik koji je povezan na jedan od usmjerivača preda zahtjev za prijenos podataka. Tim protokolom se određuje optimalni put kojim će se poslati podaci preko interneta. Prilikom pokretanja protokola šalju se testni podaci kojima se utvrđuje postojanje optimalnog puta.



Slika 2.4. *Prikaz WMN mesh mreže [12]*

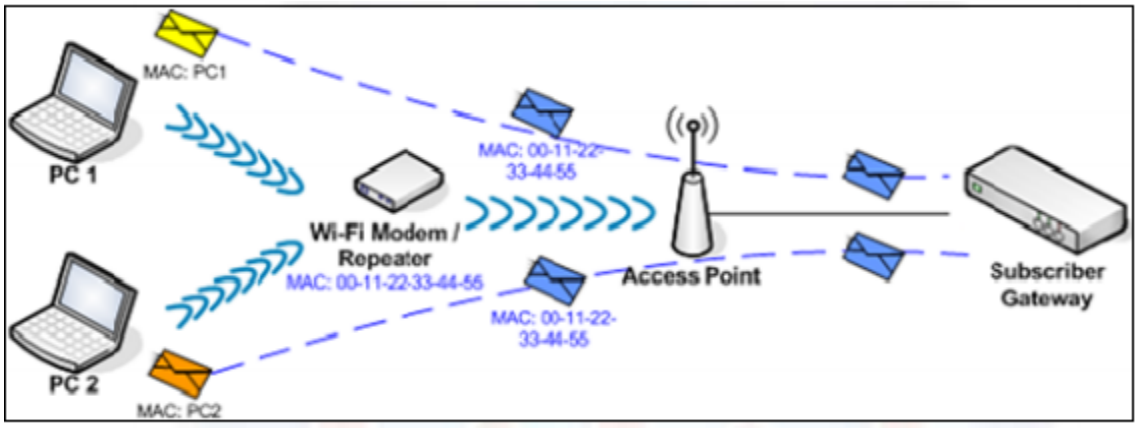
2.5. MAC u mesh mrežama

Kao što je već ranije napisano mesh mreže koriste kanale za prijenos podataka kroz čvorove. Za dodjelu tih kanala koristi se MAC (engl. Medium access control) protokol koji radi na različite principe. Dok jedni MAC protokoli dijele kanale u potkanale kako bi njima obavljali paralelnu komunikaciju čvorova, drugi protokoli koriste jednosmjernu komunikaciju. Drugi principi rada se razlikuju u enkripciji i enkapsulaciji podataka. Ono što je bitno za međusobnu komunikaciju je da svi čvorovi moraju imati jednak konfiguriran MAC protokol kako ne bi došlo do pogreške u prijenosu podataka. Neki od protokola koji se najčešće koriste su:

- Aloha
- Slotted Aloha
- CSMA (engl. Carrier sense multiple access)

- CSMA/CA (engl. Carrier sense multiple access/Collision avoidance)
- CSMA/CD (engl. Carrier sense multiple access/Collision detection)
- IEEE 802.11 protokol
- IEEE 802.11e QoS MAC protokol
- TDMA (engl. Time division multiple access)

Neke od karakteristika tih protokola su npr. kod CSMA, ako je kanal zauzet, stanica ne nastavlja dalje sa osluškivanjem da otkrije točan trenutak kada će kanal postati slobodan, nego čeka slučajno vrijeme do sljedećeg osluškivanja. Problemi nastaju u propagacijskom čekanju što znači da dva čvora ne mogu čuti jedan drugog tokom prijenosa podataka. Kod CSMA/CD protokola dvije ili više čvorova mogu istovremeno znati da je kanal slobodan i pokušati poslati paket. Čvorovi koji šalju pakete mogu saznati da je došlo do sukoba, tako što usporede signale na mediju i poslanog signala. Nakon što se otkrije sukob, čvor prekida slanje paketa, može prekinuti slanje čak i ako se poslalo pola okvira paketa. Na slici 2.5. možemo vidjeti istovremeno slanje podataka sa PC1 i PC2. Oba korisnika su spojeni na AP preko WI-Fi (engl. Wi-Fi modem/repeater). Korisnici koriste MAC protokole, koji prave potkanale kako bi korisnici poslali pakete do centralnog uređaja (Subscriber gateway) i natrag. U većini slučajeva to bude neki server za pristup Internetu.



Slika 2.5. *MAC protokol [13]*

3. BEŽIČNE MESH MREŽE

Za razliku od tradicionalnih centraliziranih bežičnih sustava bežična mesh mreža ili WMN (engl. Wireless mesh network) predstavlja stalni pomak. Bežične mesh mreže se stalno razvijaju u odnosu na bežični LAN (WLAN) i mreže za mobilnu telefoniju. Brojne su prednosti bežičnih mesh mreža kao npr. otpornost na kvarove i jednostavnost implementiranja. U Tablici 3.1. su prikazane ostale prednosti u odnosu na tradicionalne sustave.

Tablica 3.1. Usporedba svojstava tradicionalne mreže (Ad-hoc) i bežične mesh mreže

OPIS	TRADICIONALNA MREŽA	BEŽIČNA MESH MREŽA
Topologija mreže	Dinamička	Statična
Mobilnost čvorišta	Visoka	Niska
Potrošnja energije	Visoka	Niska
Infrastruktura	Bez	Fiksna
Prosljeđivanje podataka	Pokretna čvorišta	Fiksna čvorišta
Plasiranje za upotrebu	Jednostavan plasman	Zahtjeva planiranje
Svojstva prometa mrežom	Korisnički promet	Korisnički i procesni promet

Kod mreža za mobilnu telefoniju kvar jedne bazne stanice dovodi do nedostupnosti šireg geografskog područja dok bežična mesh mreža pruža visoku otpornost na greške, čak i kada veći broj čvorova prestane sa radom. To znači ako je kvar na jednom čvoru u mreži sustav će pronaći drugi optimalni put za prijenos podataka između korisnika. Kao što je i ranije rečeno jednostavno se instalira tako da se izvrši nadogradnja na postojeći čvor u mreži.

3.1. Arhitektura bežičnih mesh mreža

Arhitektura bežičnih mesh mreža se može dizajnirati na tri različita načina. Svaki način ovisi o topologiji mreže. Ova vrsta infrastrukture može biti decentralizirana (bez centralnog poslužitelja) ili centralno upravljiva (sa centralnim poslužiteljem). Obje izvedbe su relativno jeftine i mogu biti vrlo pouzdane i otporne, jer svaki čvor treba prenijeti samo do sljedećeg čvora. Čvorovi djeluju kao usmjerivači za prijenos podataka od jednog čvora do drugog čvora koji je predaleko da bi se podatak poslao u jednom skoku, što rezultira mrežom koja obuhvaća veća geografska područja. Topologija mesh mreže mora biti relativno stabilna, tj. ne smije biti previše mobilnosti.

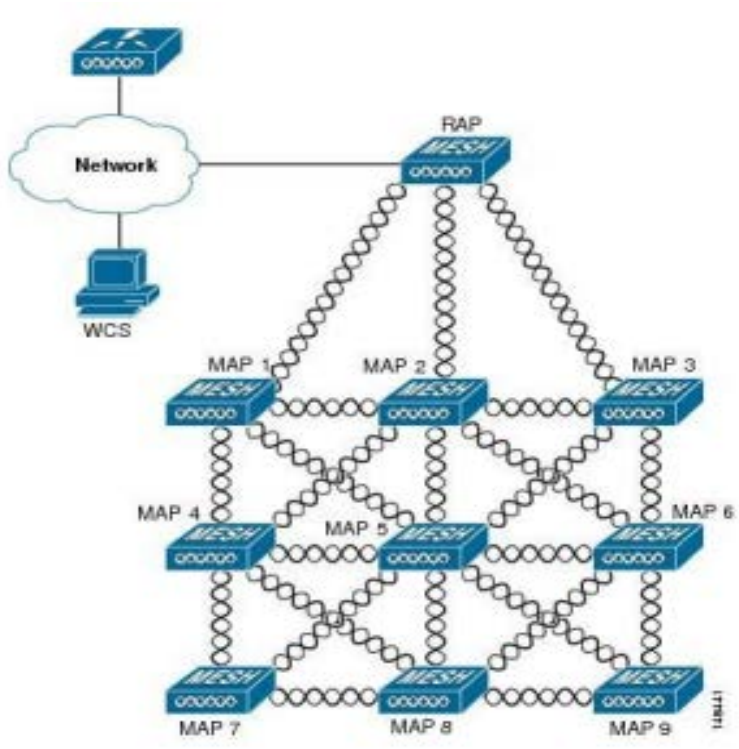
Ta tri načina su:

- Ravna bežična mesh mreža
- Hijerarhijska bežična mesh mreža
- Hibridna bežična mesh mreža

U nastavku rada svaki će način biti detaljno opisan.

3.1.1. Ravna bežična mesh mreža

U ravnoj bežičnoj mesh mreži, mreža se tvori od korisničkih mrežnih uređaja koji se mogu koristiti kao domaćini (engl. host) i kao usmjerivači (engl. router). Svaki čvor koji se tvori je na istoj razini kao i pristupna točka (engl. Access point), što se vidi na slici 3.1. Sva čvorišta se međusobno koordiniraju tako što se uvede protokol za usmjeravanje, mreža se konfigurira, rezerviraju se različiti servisi za prijenos podataka kao i potreban prostor. Najveća prednost ovom načinu mreže je jednostavnost izvedbe, dok je velika mana zauzeće mrežnih resursa i manja brzina prijenosa podataka. Problem pri dizajniranju ravne bežične mesh mreže je shema za adresiranje, usmjeravanje i shema otkrivanja usluga.

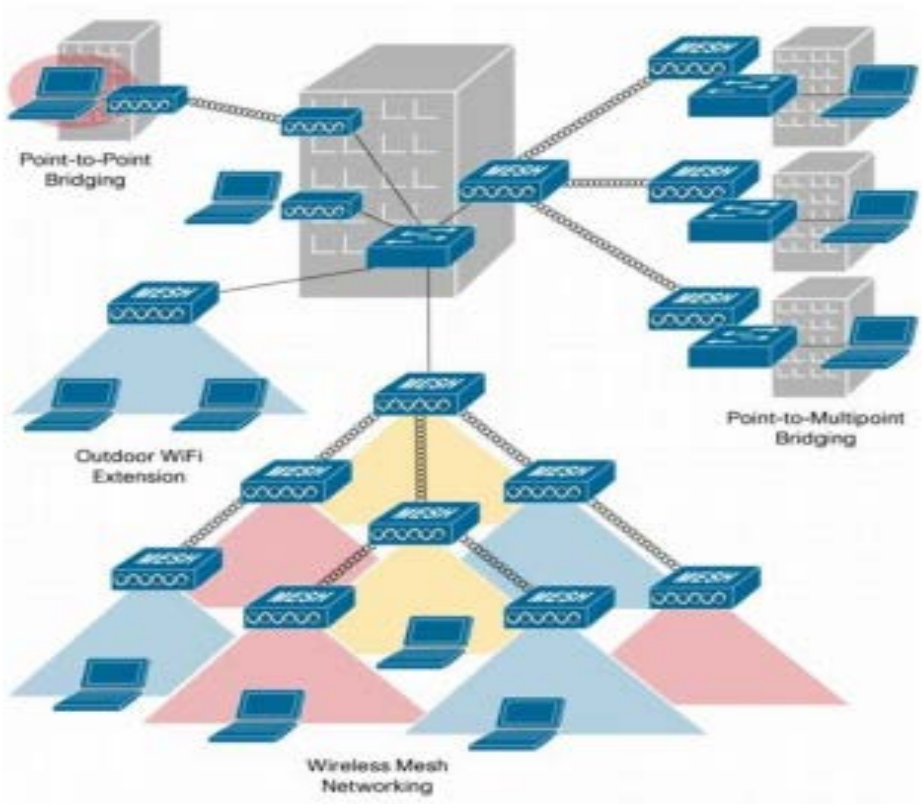


Slika 3.1. *Prikaz ravne bežične mesh mreže [14]*

Slika 3.1. prikazuje jedan način logičke primjene za fizičku konfiguraciju ravne bežične mreže, gdje je MAP5 za sve ostale MAP-ove glavni optimalni put. RAP je bežična konekcija u središtu MAP mesh-a, što je optimalna konfiguracija koja minimizira prosječan broj skokova u sustavu. RAP konekcija na rubu sustava rezultirala bi sa značajnim povećanjem skokova u sustavu.

3.1.2. Hijerarhijska bežična mesh mreža

U hijerarhijskoj arhitekturi bežičnih mesh mreža postoji više klasa ili hijerarhijskih razina, u kojima su korisnička čvorišta na dnu podjele. "Kičmu" sustava čine usmjerivači (engl.router) koji komuniciraju sa korisnicima. Korisnička čvorišta su ujedno pristupne točke (engl. Access point). U ovakvom sustavu pristupne točke odnosno korisnička čvorišta su namijenjena za uspostavljanje i prekid prijenosa podataka. Prednost ovakve strukture sustava je povećana brzina prijenosa u načinu rada u odnosu na ravne mreže i dosta su jeftinije, dok je mana povećan broj čvorova mreže.

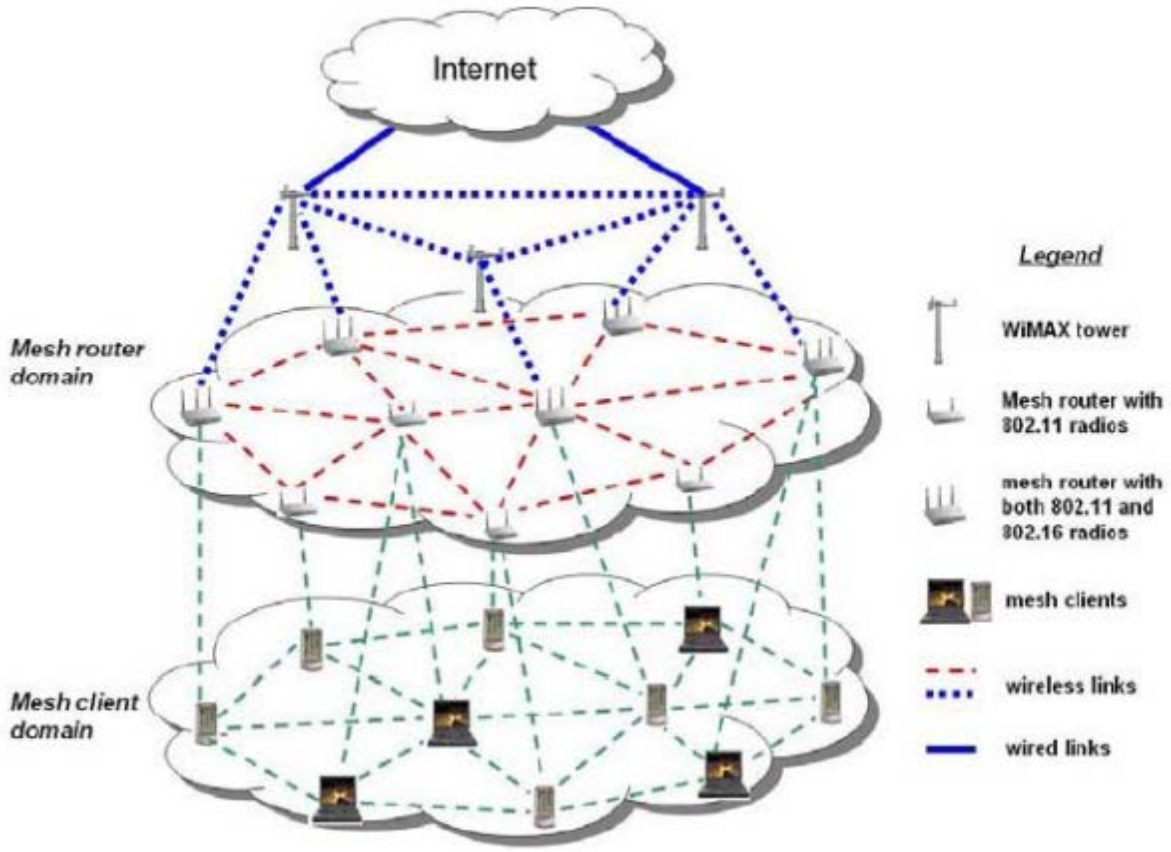


Slika 3.2. *Hijerarhijska bežična mesh mreža [14]*

Slika 3.2. prikazuje hijerarhijsku bežičnu mesh mrežu, na dnu su korisnička čvorišta koja mogu komunicirati sa usmjerivačima. Uvijek postoji jedan usmjerivač koji je gateway odnosno izlaz u vanjski svijet (Internet).

3.1.3. Hibridna bežična mesh mreža

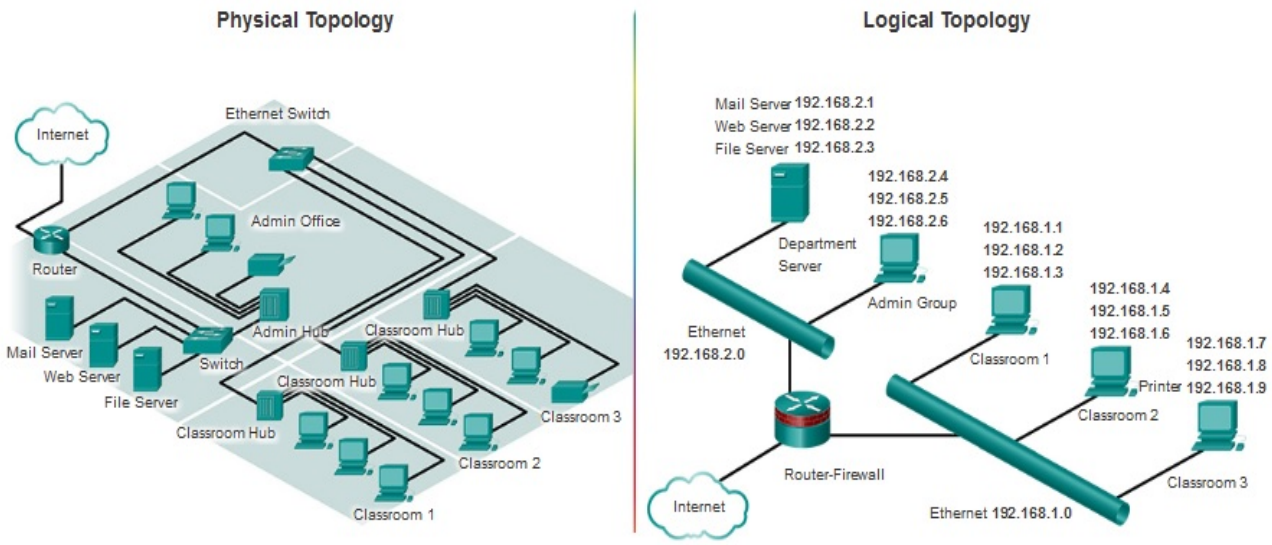
Hibridna bežična mesh mreža je posebna vrsta hijerarhijskih mesh mreža, gdje mreža koristi druge bežične mreže za prijenos podataka i komunikaciju. Primjer za bežične mreže koje mogu da se koriste posjeduju arhitekturu koja se temelji na bežičnoj mesh mreži, a to su: mobilna telefonija, WiMAX mreže ili satelitske mreže. S obzirom da bežične mesh mreže u velikoj mjeri ovise o postojećim strukturama bežične mreže ova arhitektura postaje bitna u razvoju mesh mreža.



Slika 3.3. *Prikaz hibridne bežične mesh mreže [16]*

3.2. Podjela drugih mrežnih topologija i usporedba sa mesh mrežom

Sastavni dijelovi i način rada ili povezivanja mrežnih uređaja mogu se vidjeti na osnovi mrežne topologije. Osim mesh mreže u praksi se koriste i druge mrežne topologije. Mreža se dijeli na fizičku i logičku topologiju. Mrežna topologija označava raspored i vezu između svakog čvora u mreži i putanju podataka između njih. Što znači da fizička topologija pokazuje na koji su način fizički povezani čvorovi mreže, dok logička pokazuje na koji se način širi signal između čvorova mreže. Na slici 3.4. je vidljiv prikaz i razlike između fizičke i logičke topologije. Fizička prikazuje na koji su način spojeni uređaji u mreži, dok logička prikazuje sve ostale bitne faktore mrežnih uređaja kao npr. IP adrese pojedinog uređaja.



Slika 3.4. *Prikaz fizičke i logičke topologije [17]*

- **Point-to-point mrežna topologija**: Sastoji se od dva čvora i veze između njih odnosno linka. Čvorovi neposredno komuniciraju preko linka, veza između čvorova može biti stalna ili dinamička (packet switched, circuit switched). Kada je u pitanju dinamička veza uspostavlja se komunikacijski kanal prije komunikacije odnosno slanja podataka, to je primjer telefonskog poziva. U Packet switched vezi komunikacijski kanal se dijeli i podaci se šalju u paketima. U odnosu na mesh mrežu ova vrsta mreže je jeftinija, ali je znatno manja brzina prijenosa podataka i nije sigurna kao mesh mreža.

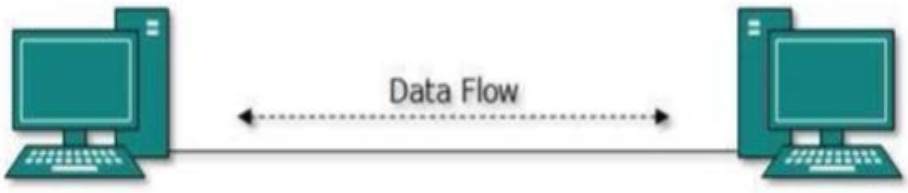
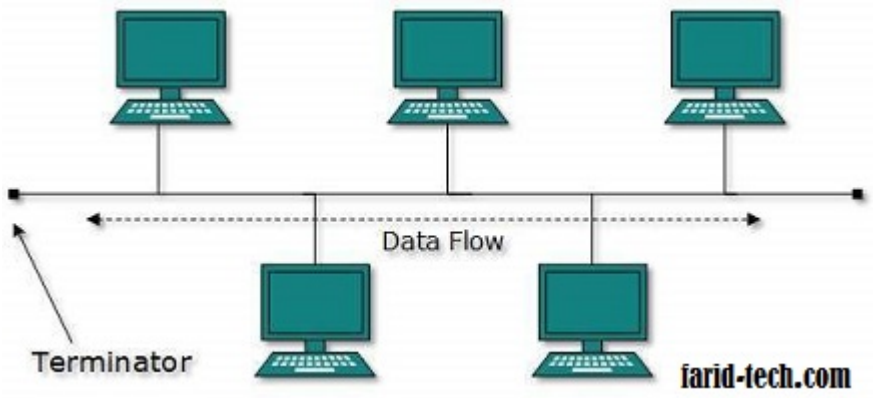


Figure: point to point topology

Slika 3.5. *Point-to-point mrežna topologija [18]*

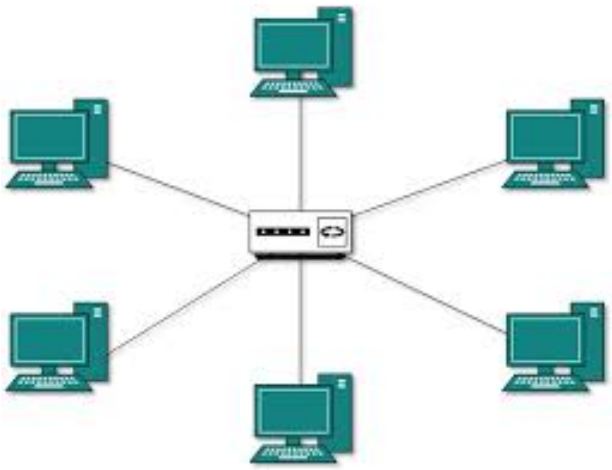
- **Bus (linijska) mrežna topologija**: Sastoji se od centralnog vodiča na koji su spojeni ostali čvorovi. Vodič je napravljen tako da ima dva kraja koji uvijek moraju biti povezani, s time

se omogućuje stalna komunikacija bez refleksije signala i smanjuje se gubitak paketa. Ovo je vrsta broadcast mreže, odnosno poslani paket se šalje centralnim vodičem te ga mogu svi "čuti". Za medij se većinom koristi koaksijalni kabel, prekid na vodiču uzrokuje prestanak komunikacije za sve čvorove. U usporedbi sa mesh mrežom mnogo je jednostavnija u izvedbi, no kao i point-to-point mrežna topologija pruža manje brzine prijenosa i nesigurnija je od mesh mreže.



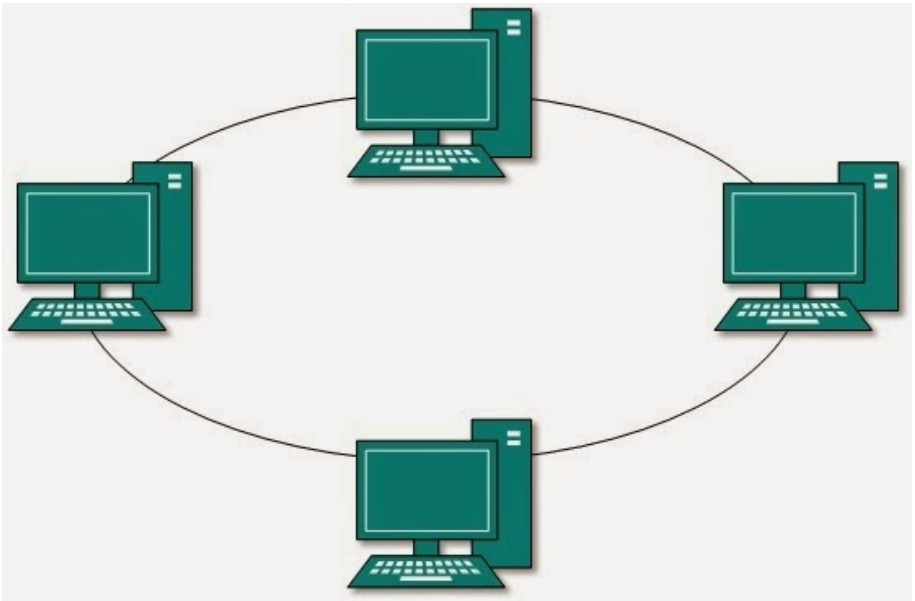
Slika 3.6. *Bus (linijska) mrežna topologija [18]*

- **Star (zvijezda) mrežna topologija**: Sastoji se od centralnog čvora na koji su preko određenog medija spojeni ostali čvorovi. Kao centralni čvor obično se postavljaju mrežni uređaji poput preklopnika (engl. Switch) ili koncentrator (engl. Hub). Postavljanjem preklopnika kao centralni čvor omogućuje se komuniciranje istovremeno više parova čvorova. Prekid rada jednog čvora ne predstavlja bitan problem u komunikaciji, dok prekid rada centralnog uređaja prekida svu daljnju komunikaciju. Koristi se u LAN (engl. Local Area Network) mrežama i za medij se obično koristi UTP (engl. Unshielded twisted pair) kabel. U usporedbi sa mesh mrežom, ova mrežna topologija je jeftinija, ali glavni problem predstavlja prekid rada centralnog čvora što dovodi do prekida komunikacije cijele mreže, što kod mesh mreže ne predstavlja problem.



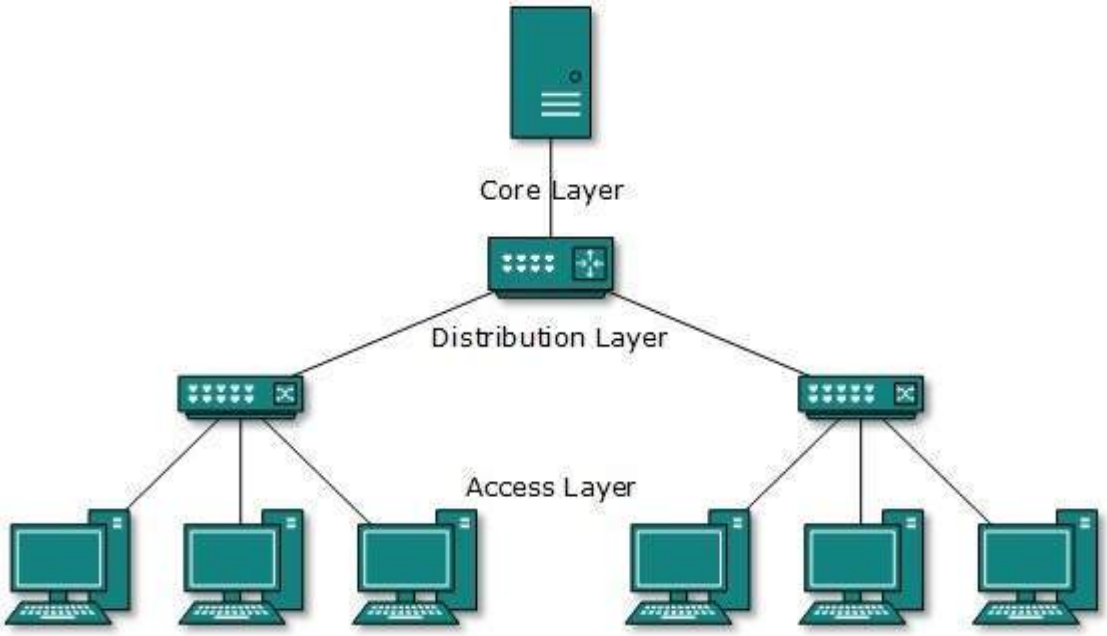
Slika 3.7. *Star (zvijezda) mrežna topologija [18]*

- **Ring (prsten) mrežna topologija**: Sastoji se od čvorova koji su povezani sa dva susjedna čvora u mreži, tako što se povezuju prvi i zadnji čvor tvori se mreža u obliku kruga odnosno prstena. Podaci se razmjenjuju u krug u jednom smjeru od jednog čvora do drugog. Prilikom implementacije ove metode koristi se i redundantni link između svaka dva čvora. U slučaju da dođe do kvara jednog čvora, redundantni preuzima njegovu ulogu. Glavna prednost ove topologije je brzina, dok je izvedba nešto kompliciranija.



Slika 3.8. *Ring (prsten) mrežna topologija [18]*

- **Tree (stablo) mrežna topologija**: Sastoji se od centralnog čvora, cijela topologija je napravljena kao hijerarhijska, tako da je centralni čvor najviši dok se na njega spajaju čvorovi na nižim slojevima. Na svaki čvor nižeg sloja spaja se čvor koji je na nižem sloju itd. Najmanja mreža koja ima tree mrežnu topologiju mora imati 3 sloja. Broj čvorova u tree mrežnoj topologiji će imati za jedan broj više čvorova u odnosu na point-to-point. Za medij se koriste bakrene žice ili optika. Ova topologija je najbliža po strukturi mesh mreži, no kvarovi na ovoj topologiji su dosta zahtjevniji u odnosu na mesh. Npr., ako se dogodi kvar na čvoru višeg sloja to uveliko otežava rad cijele mreže.



Slika 3.9. *Tree (stablo) mrežna topologija [18]*

Tablica 3.2. Prednosti i nedostatci najraširenijih mrežnih topologija

TOPOLOGIJA	PREDNOSTI	NEDOSTATCI
Point-to-point	Jednostavna za male i spore mreže. Potreban mali broj kabela za povezivanje	Greška na jednom čvoru se odražava na cijelu mrežu
Star ili zvijezda	Jednostavno proširenje mreže, lako povezivanje	Potreban veliki broj kabela, greška na centralnom čvoru se teško otklanja
Ring ili prsten	Korisna za velike mreže, jednostavno proširenje mreže i velika brzina	Cijena visoka
Mesh	Jednostavna implementacija i proširenje. Otpornost na kvarove.	Cijena visoka

3.3. Sigurnost u WMN mrežama

Mesh mreže su kao i ostale žične i bežične tehnologije izložene sigurnosnim ranjivostima. Samo neke od tih prijetnji se izražavaju u obliku presretanja podataka, te njihovo oblikovanje i prijenos do odredišta. Mrežnim resursima se može pristupiti bez dopuštenja, neka od svojstava koji takve prijetnje onemogućuju su:

- **Povjerljivost**-podaci su vidljivi samo određenim korisnicima
- **Integritet**-podaci se mijenjaju samo uz dopuštenje
- **Autentičnost**-potvrđeni identitet
- **Provjera pristupa**-samo ovlašteni pristup
- **Dostupnost**-izvode se autorizirane radnje

U cilju zaštite samoga korisnika su njegova privatnost, protok podataka i sama komunikacija. Pod privatnost korisnika ubraja se njegova anonimnost i privatnost podataka. Zaštita podataka koji putuju mrežom postiže se enkripcijom i enkapsulacijom istih.

3.3.1. Prijetnje i slabosti

Mogu se podijeliti u tri skupine:

- Prijetnje u protokolu za usmjerivanje (engl. Routing protocol threats)
- Prijetnje na razini korisničkog pristupa (engl. Client access threats)
- Fizičke prijetnje (engl. Physical security threats)

Najčešći oblici prijetnji su na protokole usmjerivanja, zahtjevaju ubavicanje paketa podataka u mrežu kroz propuste u protokolima. Neki od njih su:

- **Crna rupa** (engl. Black hole)-Šalju se pogrešni paketi podataka i stvara se novi mesh čvor
- **Siva rupa** (engl. Grey hole)-Ubacuju se lažni podaci u mrežu kako bi se saznala putanja paketa
- **Route error injection**-Napad kojim se razbija veza između čvorova mesh mreže tako što se ubacuje poruka koja sadrži grešku o usmjerivanju paketa

Poznati su protokoli za usmjeravanje koji su podložni ovim napadima, te se oni i manje koriste u nekim situacijama. Neke mesh mreže mogu izvoditi provjeru poruka za usmjeravanje i tako se smanjuje opasnost od napada.

3.3.2. Vrste napada po slojevima

Napadi na mesh mreže direktno utječu na performanse mreže. Čvorovi u mreži su međusobno ovisni jedni o drugima, i tako protokoli na MAC i mrežnoj razini koriste pretpostavku da čvorovi koji sudjeluju u mreži nemaju malicioznu namjeru. Bez mrežnog administratora takvo povjerenje zna biti kobno.

- **Napadi na fizičkom sloju**-Mesh mreže zahtjevaju da pristupne točke budu izvan dometa operatera i upravo zbog toga mogu nastati fizičke prijetnje. Vanjska implementacija predstavlja veće izazove za zaštitu sigurnosti. Mogućnost krađe mrežnih uređaja kao i mijenjanje konfiguracije. Prvi sloj odnosno fizički sloj je odgovoran za postavljanje prave frekvencije, detekciju signala, enkripciju podataka. Još jedan oblik napada je ometanje signala i oblikovanje, zauzima se frekvencijski prostor na kojemu čvorovi komuniciraju.

- **Napadi na MAC sloju-** Postoje različite vrste napada na ovom sloju, neki od njih su: pasivno prisluškivanje, ometanje, lažiranje MAC adrese, ponavljanje.

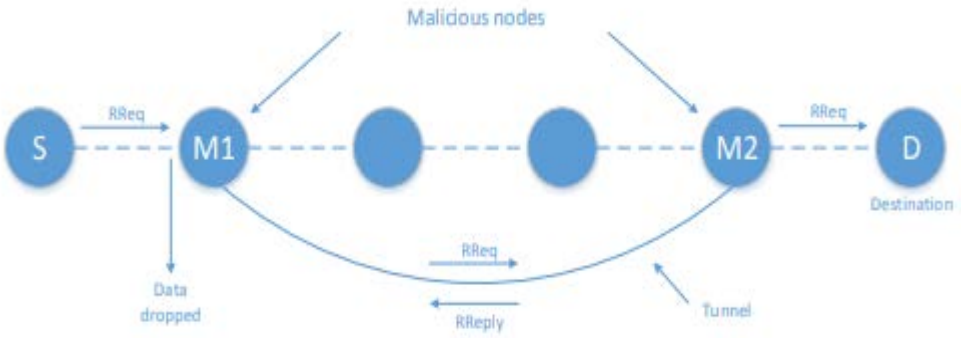
  Pasivno prisluškivanje-Multihop bežične mreže kao što je i mesh mreža su pogodne za unutarnje prisluškivanje zbog unutarnjih skokova pri čemu jedan od čvorova može da sadrži kopiju podataka koji se prenose bez znanja drugih čvorova. Jedan od načina zaštite je enkripcija podataka.

  Ometanje-Napadač šalje regularna zaglavlja MAC okvira na prijenosni kanal koji odgovara MAC protokolu koji se koristi u mreži žrtve. Ovi napadi se mogu izvršavati bez obzira na enkripciju bila ona WEP (engl. Wired equivalent privacy) ili WAP (engl.WiFi protocol access). To je moguće zato što senzori koji vrše napad prate količinu podataka i njihov redoslijed slanja.

  Lažiranje MAC adrese- MAC adresa je jedinstveni identifikator mrežnih uređaja. Izmjena MAC adrese se naziva *spoofing* i omogućuje napadaču da izbjegne sustave detekcije upada.

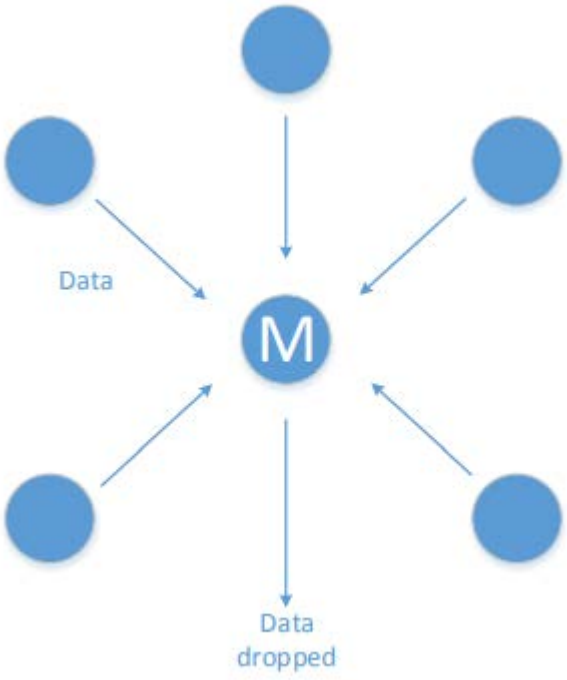
  Napad ponavljanja-Ovaj napad može da pokrene eksterni ili interni čvor u mreži. Ako eksterni čvor prenosi legitimne poruke, u kasnijoj fazi postaje legitimni čvor sa svim pravima pristupa mrežnim resursima. Tada interni čvor može da napravi kopiju prenesenih podataka, te tako izvršava ponavljanje podataka kako bi imao neovlašteni pristup mrežnim resursima.

- **Napadi na mrežnom sloju**- Ove napade možemo podijeliti na napade kontrole i na podatke. Mogu biti aktivni i pasivni. Cilj ovih napada je onemogućiti razmjenu informacija u tablicama usmjeravanja i onemogućavanje tvorbe optimalnih puteva. Napad na podatke je napad na prosljeđivanje podataka kroz mrežu. Jedan od napada je Wormhole napad, gdje dva ili više zlonamjernih čvorova uspostavljaju tunel pomoću komunikacijskog medija. Kada su takvi čvorovi uključeni u proces usjeravanja, mogu da povuku sve pakete i tako prouzrokuju napade. Na slici 3.9. se prikazuje jedan takav napad, gdje čvor zahtjeva put do odredišta preko RREQ poruka. Kako bi se spriječila ta pojava, svaki čvor prosljeđuje samo prvu poruku koju dobije, dok ostale odbacuje. Zlonamjerni čvor pokreće veliki broj tih poruka prije bilo kakve komunikacije.



Slika 3.10. *Prikaz Wormhole napada [19]*

Druga vrsta napada na mrežnom sloju su Blackhole napadi, glavni cilj je uskraćivanje DoS usluga u mreži. Koristi mehanizam otkrivanja optimalnog puta na zahtjev protokola za usmjeravanje. Zlonamjerni čvor uvijek odgovara pozitivno na RREQ (engl. Route request) zathjev. Upravo zbog toga može preusmjeriti promet prema drugom zlonamjernom čvoru.



Slika 3.11. *Blackhole napad* [19]

Na slici 3.10. se prikazuje jedan takav napad, gdje je zlonamjerni čvor prikazan preko čvora M i on odgovara pozitivno na svaki RREQ zahtjev.

Treći oblik napada na mrežnom sloju je ***Grayhole*** napad, koji je jedna od varijanti blackhole napada. Oni crpe sav promet što omogućuje laku detekciju napada. Tokom napada propušta se dio paketa selektivno i tom prilikom može ostati nezapažen duže vrijeme. Još jedan od napada je ***Sybil*** napad gdje zlonamjerni čvor stvara više identiteta u mreži, a svaki se prijavljuje kao legalan čvor.

- **Napadi na transportnom sloju-** Najveća prijetnja na ovom sloju su napadi zvani poplave (engl. Flooding attack) i desinkronizacija. Napadi poplave su mogući kada protokoli za usmjeravanje održavaju oba kraja komunikacije što dovodi do memorijske iscrpljenosti. Napad se izvodi više puta zbog iscrpljivanja resursa. Napadi desinkronizacijom se odnose na prekide postojeće veze i konstantnim napadima troše energiju izvora pokušavajući ispraviti greške.

3.3.3. Prijetnje na razini korisničkog pristupa

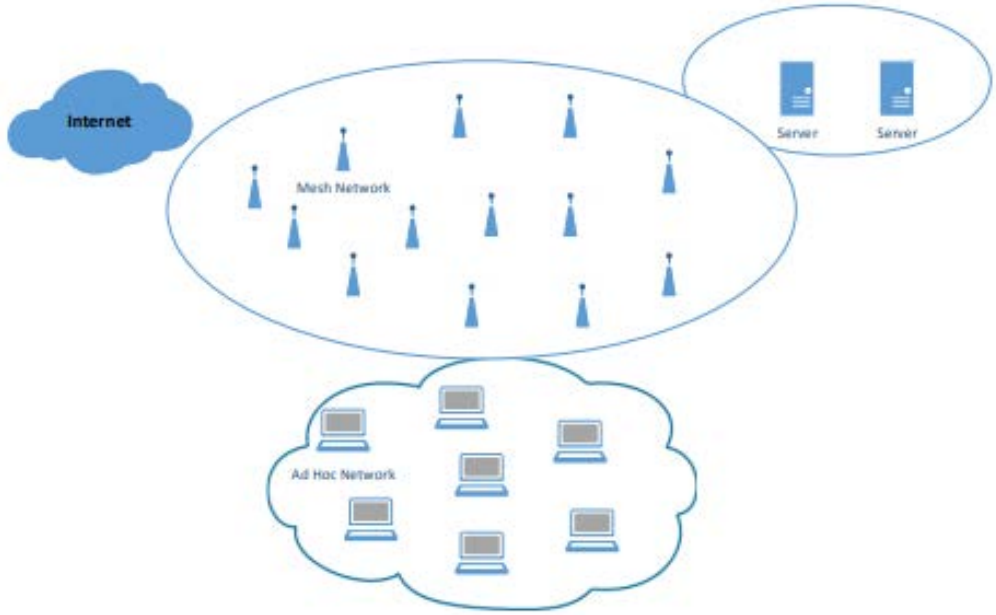
Ove vrste prijetnje ovise o vrsti mesh mreže i o strategiji pristupa mrežnim resursima. Ove prijetnje su najviše prisutne u javnom pristupu na mrežu koje su zasnovane na otvorenoj autentikaciji. Neki od njih su:

- **Lažiranje mrežne infrastrukture**-Napad koji omogućuje zajedničku autentikaciju i pristup mreži
- **Napad uskraćivanjem usluge** (engl. Denial of Service)-to su napadi na IP adrese korisnika, MAC adrese
- **Krađa usluge** (engl. Theft od Service)- Napad na korisničke podatke. Mesh mreže se od ovih napada brane tako da se nakon prve prijave odnosno autorizacije korisnika pohrane njegove IP i MAC adrese i nakon toga je pristup omogućen samo tim adresama.

3.3.4. Mehanizmi zaštite u mesh mrežama

Kako je već i ranije napisano, mesh mreža je kompatibilna sa ostalim mrežnim tehnologijama i lako se nadograđuje na postojeću infrastrukturu. Klasični WLAN sigurnosni mehanizmi (WPA2/802.11i) pružaju standardne metode zaštite i autentifikacije, enkripciju i ostalo. Zbog većeg broja postojanja mesh arhitektura postoji i različit pristup mreži samim time i zaštita istih. U

budućnosti će sve mesh mrežne arhitekture imati standardizirane mehanizme zasnovane na 802.11s standardu sigurnosti. Mehanizmi se odnose na samog korisnika, ad hoc mreže i centralnu mesh mrežu. Na slici 3.12. vidimo da je ad hoc mreža povezana na centralnu mesh mrežu.



Slika 3.12. *Ad hoc mreža povezana sa mesh mrežom [19]*

Kako mesh mrežna infrastruktura može biti žičana i bežična tako se korisnicima pruža mogućnost pristup mreži i njenim resursima. Kako većina korisnika još uvijek koristi standardne 802.11 mehanizme (LAN/WAN) tako nemaju mesh mrežne mogućnosti i zbog toga nisu sudionici ili posrednici u mesh mrežnoj komunikaciji. U novije vrijeme pružaju se korisnička mesh rješenja, i u ovisnosti vrste mreže kontrola pristupa korisnika se može mijenjati. Npr. privatne mesh mreže koriste WPA2 kontrolu pristupa dok se javne npr. Metro Wi-Fi mreže koriste Layer 3 autentifikacijom.

3.3.5. Ad-hoc sigurnost

Današnje mesh mreže se većinom koriste Ad-hoc načinom rada. Zbog toga mesh mreže podliježu raznim sigurnosnim prijetnjama i rizicima. Neki od njih su brisanje podataka, preusmjeravanje podataka, oblikovanje poruka, zauzimanje čvorova. Protokoli usmjeravanja nisu specificirali vrste zaštite podataka i zbog toga se razvija Ad-hoc sigurnosna zaštita u cilju zažtite podataka mesh mreže. Cilj očuvanja podataka i integriteta mreže svodi se na zaštitu mrežnog administratora. Cijela jedna

pristupna mreža pripada jednoj administrativnoj domeni. Neki od koncepata koje nudi 802.11s metoda zaštite sigurnosti su:

- Integritet podataka zaštićen preko javnog ili privatnog ključa. Između čvorova se šalju autentifikacijske poruke preko kojih se provjerava upad neovlaštenih korisnika.
- Autentikacija poruka za usmjeravanje poruka preko digitalnih certifikata (engl. Secure Ad-hoc On-Demand Distance Vector, SAODV)
- Zaštita podataka preko kriptografije, tj. korištenje digitalnih žigova

Postoje dva ključa enkripcije u radu, a to su:

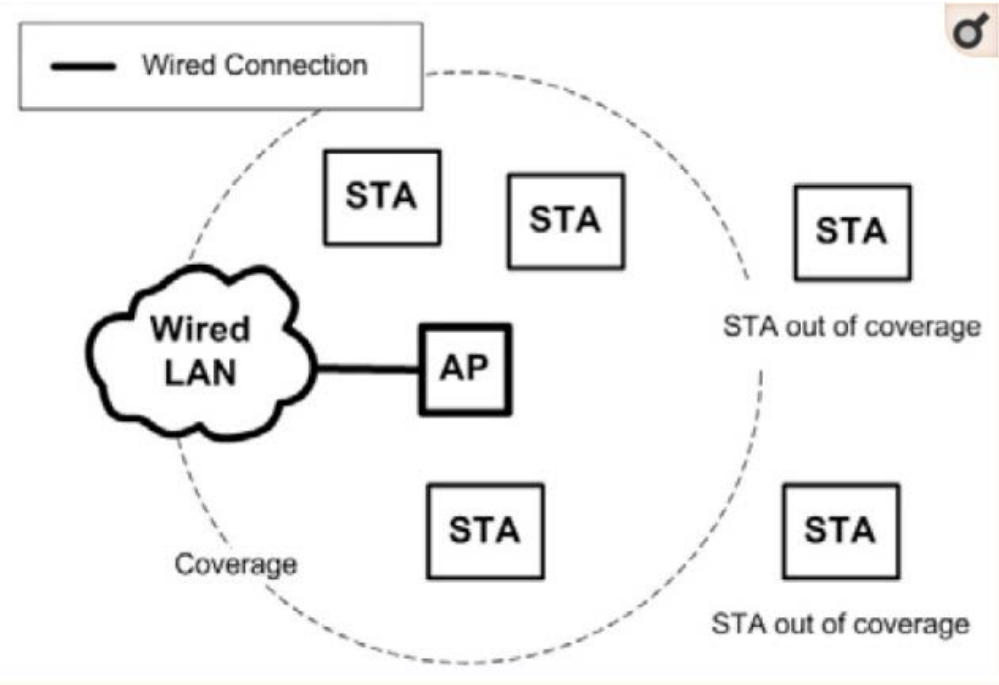
- Statički ključ enkripcije koji koristi WEP (engl. Wired equvalent privacy) ili AES (engl. Advanced encryption standard) algoritme. Model je ranjiv jer se ne mijenja enkripcija i zbog toga je uveden dinamički ključ.
- Dinamički ključ enkripcije koji koristi WPA2/802.11i protokol gdje se za svaki paket dinamički određuje enkripcija. Koristi se u komercijalnim mesh mrežama jer je sigurniji od statičkog ključa.

3.3.6. Sigurnosni standard u IEEE 802.11s

Kako je ranije napisano 802.11s standard je nadopuna na postojeću 802.11 mesh mrežu koja definira kako se mrežni uređaji međusobno bežično povezuju i kreiraju WLAN mesh mrežu zasnovanu na statičkoj topologiji i Ad-hoc mreži. Ovaj standard ovisi o standardima (802.11a,b,g,n,ac). Neki od protokola za usmjeravanje u ovom standardu su Hybrid Wireless Mesh Protocol (HWMP). Dok druge mesh mreže zahtjevaju dinamičke (OLSR ili B.A.T.M.A.N.) ili statičke (OSPF ili WDS) protokole za usmjeravanje. 802.11s mrežni uređaj ili Mesh Station (mesh STA) formira mesh linkove odnosno veze s drugim uređajima, preko putanja koji se određuju protokolima za usmjeravanje. To su pojedinačni uređaji koji koriste mesh servise za komunikaciju sa drugim uređajima u mreži. Standard uključuje mehanizme za deterministički pristup mreži, okvir za kontrolu zagušenja prometa te uštedu energije. Što se tiče sigurnosti u ovom standardu može se reći da sigurnosni protokoli moraju biti *peer-to-peer*, što podrazumijeva da svaka strana može inicirati drugu ili se obe strane pokreću istovremeno. Definira se sigurnosna provjera autentičnosti i provjera ključa koja se naziva Simultaneous Authentication of Equals (SAE). Ovaj sustav se temelji na Diifie-Hellman razmjeni ključeva korištenjem konačne ciklične grupe koje mogu biti primarne, tako da se

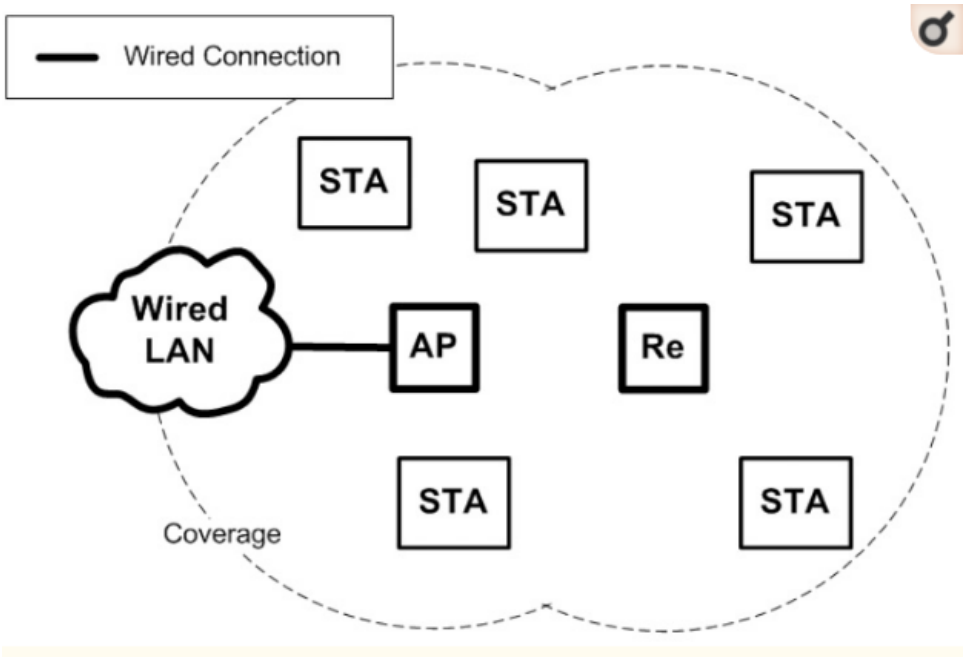
obje strane pokreću istovremeno. Zbog uparene enkripcije standard 802.11s ne može osigurati *end-to-end* enkripciju. Problem korištenja ovog sustava je nepostojanje mehanizma potvrde identiteta korisnika.

WLAN je najkorištenija tehnologija za pružanje mrežnog pristupa korisnicima bežičnih uređaja. Oni koriste pristupne točke AP (engl. Access Point) za pružanje internetske veze korisnicima. Svaka pristupna točka AP je spojena na žični LAN (engl. Local area network). Slika 3.13. prikazuje zajednički način implementacije WLAN-a. Pokrivenost je ograničena rasponom pristupnih točaka AP-a. STA izvan tog raspona se ne može povezati sa pristupnom točkom.



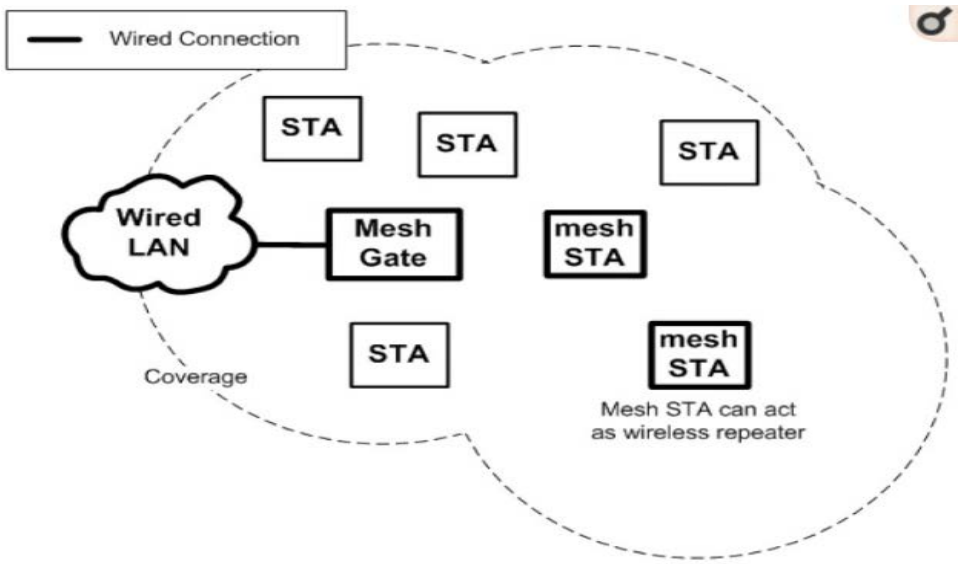
Slika 3.13. *Klasični WLAN [20]*

Postoje slučajevi kada se koriste bežični pojačivači (engl. Repeaters) za proširenje dometa bežične veze. Takvi mrežni uređaji su sposobni povezati bežične okvire (engl. frames) između AP i STA. Nije im potrebna žična povezanost, ali moraju biti bežično povezani sa nekim AP-om cijelo vrijeme. Postavljanjem ovih mrežnih uređaja značajno se smanjuju troškovi bežične mreže, a i korisni su na onim mjestima gdje nije moguće doći kabelima. Bežična veza imeđu AP-a i pojačivača postavlja se statički. Slika 3.14. prikazuje kako pojačivač može proširiti područje pokrivenosti vezom nekog AP-a kako bi se osigurala veza sa nekim STA. Na slici je prikazan kao Re.



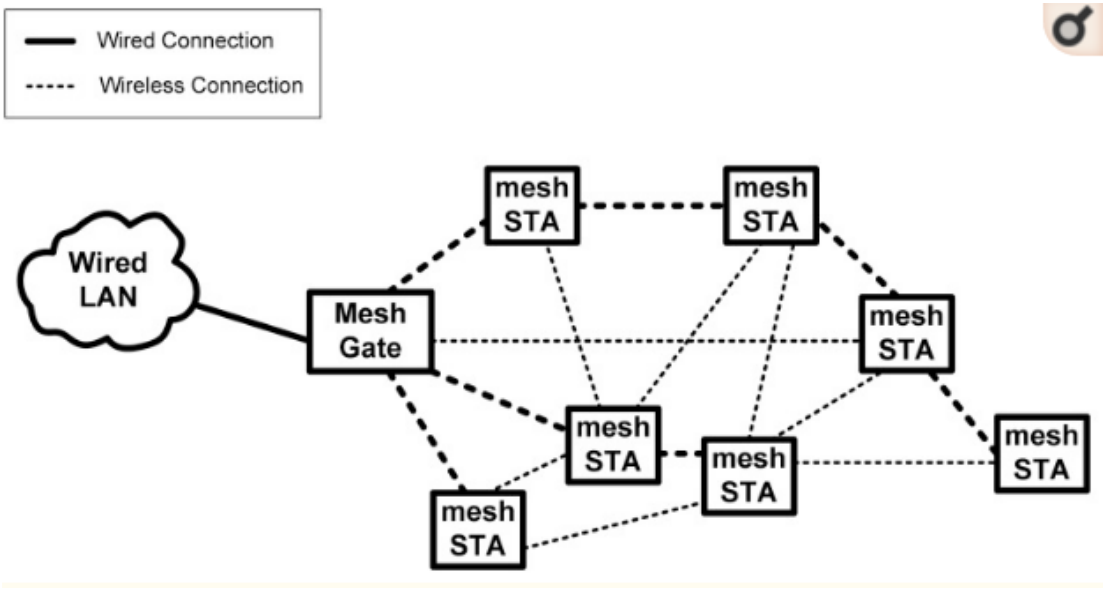
Slika 3.14. *Korištenje pojačivača (engl. Repeater) [20]*

Bežične mesh mreže omogućuje STA-u istu funkcionalnost kao AP i pojačivačima. IEEE 802.11s standard definira STA koji podržavaju funkciju kao mesh stanice (mesh STA). U mogućnosti su proslijediti bežične okvire i djelovati kao AP-ovi. Mesh STA koji povezuje bežične mesh mreže i Ethernet je definiran kao mesh gateway. Na slici 3.15. je prikazano kako bežična mreža radi kada je implementiran IEEE 802.11s. Pokrivenost se proširuje svaki put kada se mesh STA pridruži mreži.



Slika 3.15. *WLAN sa mesh STA [20]*

Idući primjer na slici 3.16. prikazuje bežičnu mesh mrežu sa dodatnim mesh STA. Najveća razlika između pojačivača i mesh STA je sposobnost mesh STA da automatski napravi bežičnu vezu i to vrlo uspješno. Optimalni put se pronalazi preko HWMP protokola koji je baziran na algoritmu za pronalaženje najkraćeg puta. S tim protokolom bežični promet može se usmjeriti na učinkovit način. ALM (engl. Airtime link metric) se koristi za izračun kvalitete veze, poznata još kao i udaljenost putanja. Ako je neki mesh STA u kvaru, nova putanja se pravi pomoću HWMP protokola.



Slika 3.16. *Bežična mesh mreža [20]*

Ova implementacija osigurava bolju pokrivenost WLAN-a. Treba imati na umu da je bežična veza i dalje puno sporija od žične veze. Ova struktura osigurava istu ili veću pokrivenost u odnosu na žičanu povezanost. Mulit-hop radnje će dodatno usporiti vezu. Kada se projektira ovaj način mreže treba uzeti u obzir da sve mesh STA mogu pristupiti odnosno da su u području mesh gateway-a sa dovoljnom širinom pojasa (engl. bandwidth). U IEEE 802.11s mesh STA i gateway se još zovu mrežna točka (engl. Mesh point MP) i mesh portal (engl.mesh portal MPP).

4. TESTIRANJE MESH PERFORMANSI

U ovom poglavlju biti će demonstrirani rezultati dobiveni u različitim mjerenjima. Mjerenja su se izvodila od najslabijih uređaja do najboljih. Prva mjerenja su se izvodila na 2 uređaja TP-LINK (TL-WR740N), jedan uređaj je bio verzije 2.3 dok je drugi verzije 4.23. Primjer uređaja prikazan je na slici 4.1.

Slika 4.1. *TP-LINK bežični usmjerivač [21]*

4.1. Mjerenja mesh performansi pomoću TP-LINK usmjerivača

Za mjerenje performansi mesh mreže koristila su se dva usmjerivača. Svaki od usmjerivača bio je direktno povezan LAN kabelom sa osobnim računalom. Međusobno su povezani tako što je jedan bio poslužitelj, a drugi klijent. Povezani su preko Iperf programa. To je alat koji mjeri kvalitetu mrežne veze i širokopojasnost (engl. bandwidth). Alat koji je još korišten uz Iperf je Jperf koji omogućuje grafički prikaz rezultata. Mrežnu vezu omogućuju dva računala koja pokreću Iperf. Kvaliteta veze se testira na sljedeći način:

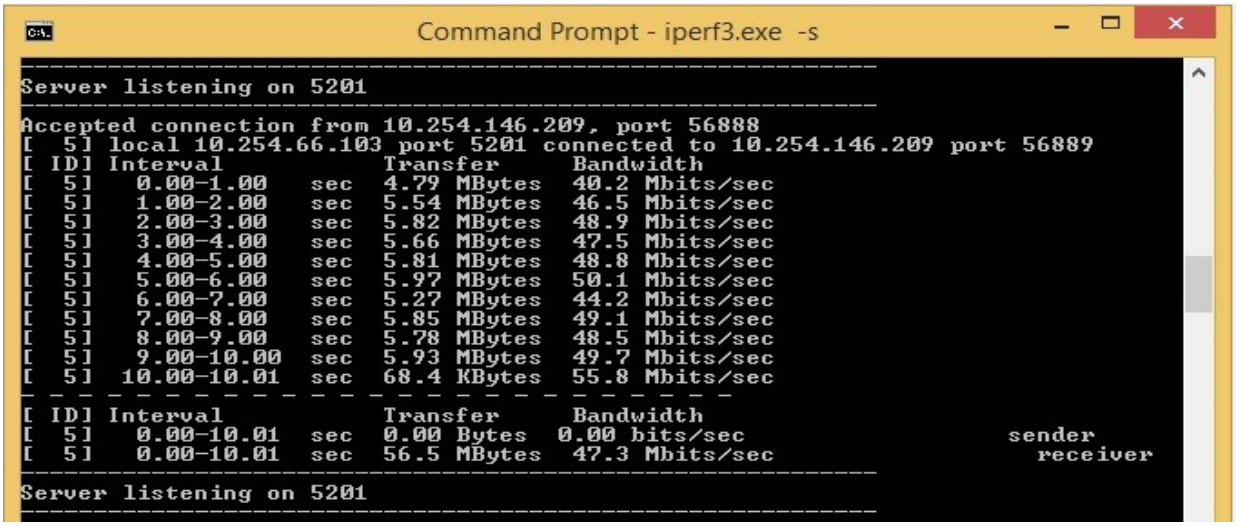
- Latencija (vrijeme odziva ili RTT)-može se mjeriti pomoću *ping* naredbe
- Jitter (varijacija latencije)-mjeri se preko Iperf UDP testa

- Gubitak datagrama-također preko UDP testa

Širina pojasa odnosno bandwidth se mjeri preko TCP testova. Razlika između TCP (Transmission control protocol) i UDP (User datagram protocol) je ta da TCP koristi procese kako bi provjerio jesu li paketi pravilno poslani prijemniku, dok UDP ne koristi nikakve provjere, prednost mu je ta što je brži. Iperf pruža različite mogućnosti i pruža statističke podatke o mrežnim vezama. Lako se instalirava na UNIX/LINUX ili Microsoft Windows sustavima. Jedan host mora predstavljati poslužitelja ili servera dok je drugi klijent. Svaki uređaj koji će se koristiti u mjerenjima prethodno su konfigurirani. Konfiguracija se sastojala od unosa novog firmware-a u sučelje svakog uređaja. Svi firmware-i su preuzeti sa OpenWrt platforme. OpenWrt projekt je Linux operacijski sustav koji se koristi na ugrađene sustave. Ovaj projekt pruža potpuni pisani sustav sa upravljanjem paketima. Ovaj postupak oslobađa korisnike od odabira aplikacije i konfiguracije i omogućuje prilagodbu uređaja kroz pakete. Za programere, OpenWrt predstavlja okvir za izgradnju aplikacije bez izgradnje kompletnog firmware-a oko njega. Dok za korisnike to znači sposobnost za potpunu prilagodbu, kako bi se uređaj koristio u sasvim drugim uvjetima.

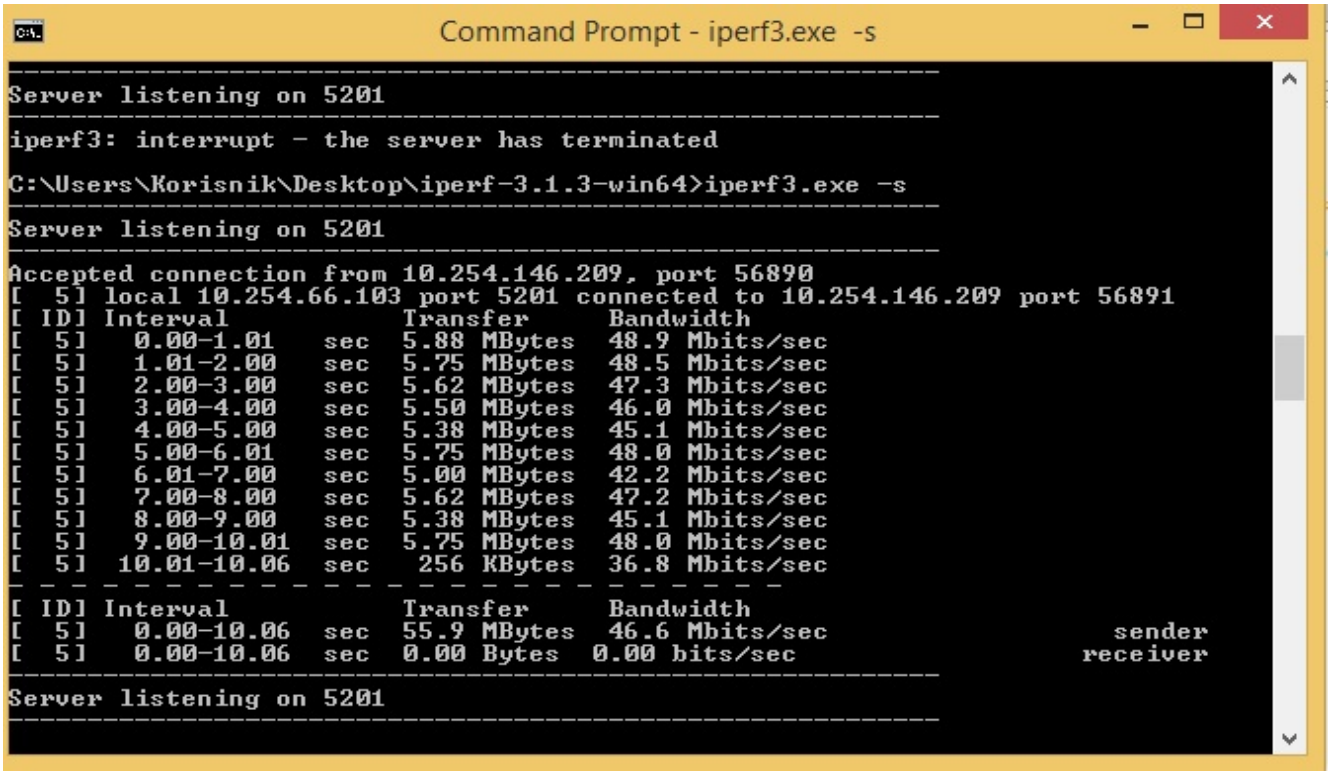
Primjer inicijalizacije poslužitelja izgleda ovako: Iperf3 –s; naredba Iperf alatu da se pokrene u server modu

Primjer inicijalizacije klijenta izgleda ovako: Iperf3 –c 192.168.1.100 –u –l 100; naredba Ipef alatu da se pokrene u klijent modu, spaja se na IP adresu servera, generiraju se UDP paketi, te duljina jednog UDP segmenta, u ovom slučaju 100 B.



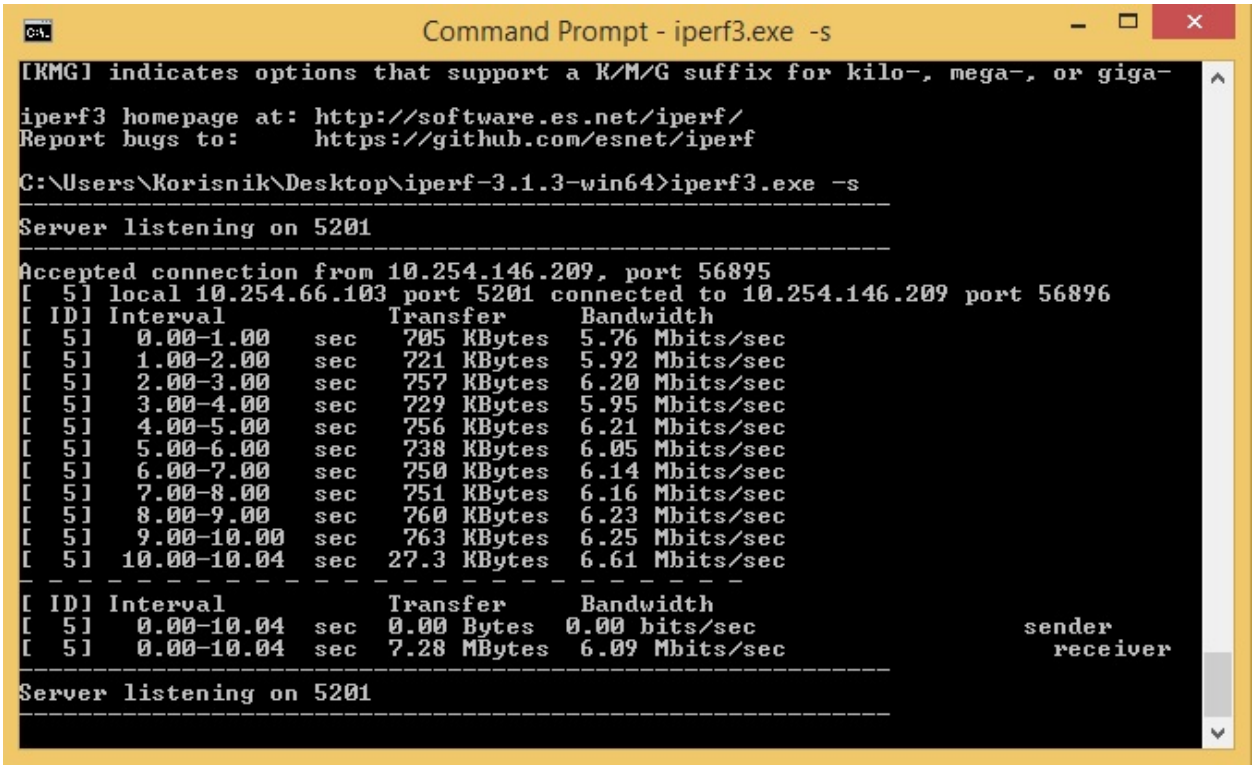
Slika 4.2. *Poslužitelj nakon spajanja na Iperf*

Na slici 4.2. prikazan je poslužitelj sa svojom IP adresom 10.254.66.103 koji je spojen na klijenta koji je na IP adresi 10.254.146.209. Prikazani su intervali od 0 do 10 sekundi i za svaki interval prenesena količina u MB i širina pojasa odnosno bandwidth za svaki interval, gdje je prosjek oko 48 Mbit/s. Bandwidth predstavlja kapacitet veze za prijenos maksimalne količine podataka s jedne točke na drugu u nekom vremenskom razdoblju, obično jednu sekundu. Opisuje brzinu prijenosa podataka, ali nije mjera brzine mreže.



Slika 4.3. *Poslužitelj nakon bi-direkcijskog bandwidth-a*

Bi-direkcijski bandwidth, naredbom –r na strani klijenta. Poslužitelj se spaja na klijenta dopuštajući bi-direkcijsko mjerenje bandwidth-a. Bandwidth se mjeri samo od strane klijenta prema poslužitelju. Za korištenje oba smjera koristi se naredba –d. Vidljivo je da od strane klijenta prema poslužitelju ide promet u intervalu od 0 do 10 sekundi i to nekih 56 MB i širinom pojasa 46 Mbit/s.

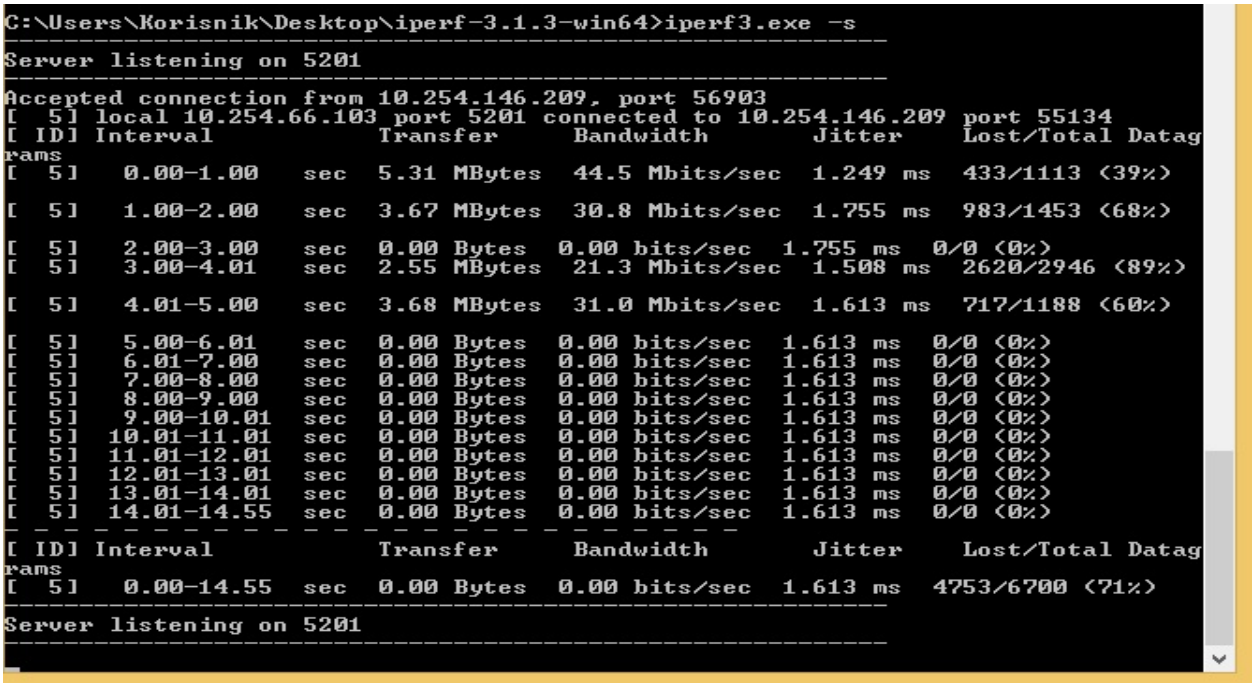


Slika 4.4. *TCP prozor promijenjen na 2000 bajtova*

Na slici 4.4. prikazana je TCP veličina prozora, naredbom –w. TCP veličina prozora predstavlja količinu podataka koji se može prenijeti tijekom konekcije bez potrebne potvrde prijemnika. Veličina može biti između 2 i 65,535. Postavili smo na 2000 jer manja vrijednost bi dala slabije performanse. Na strani poslužitelja je stiglo nekih 7 MB, dok je širina pojasa oko 6 Mbit/s.

Na slici 4.5. prikazan je poslužitelj nakon UDP testa, naredbom –u. UDP test daje nam neprocjenjive podatke u vezi kolebanja kašnjenja (engl. jitter) i gubitku paketa. Program automatski koristi TCP ako ne koristimo naredbu –u. Kako bi kvaliteta veze bila dobra, gubitak paketa ne bi trebao nikada prelaziti 1%. Visoki postotak gubitaka paketa generirati će mnogo ponovljenih TCP segmentnih podataka što se odražava na širinu pojasa (engl. bandwidth).

Kolebanje kašnjenja (engl. jitter) je u osnovi oblik latencije ali ne ovisi o latenciji. Možemo imati relativno visok postotak brzine odgovora i vrlo mali jitter. Jitter je vrlo važan u VoIP tehnologiji, visok jitter može uzrokovati prekid sesija ili poziva.

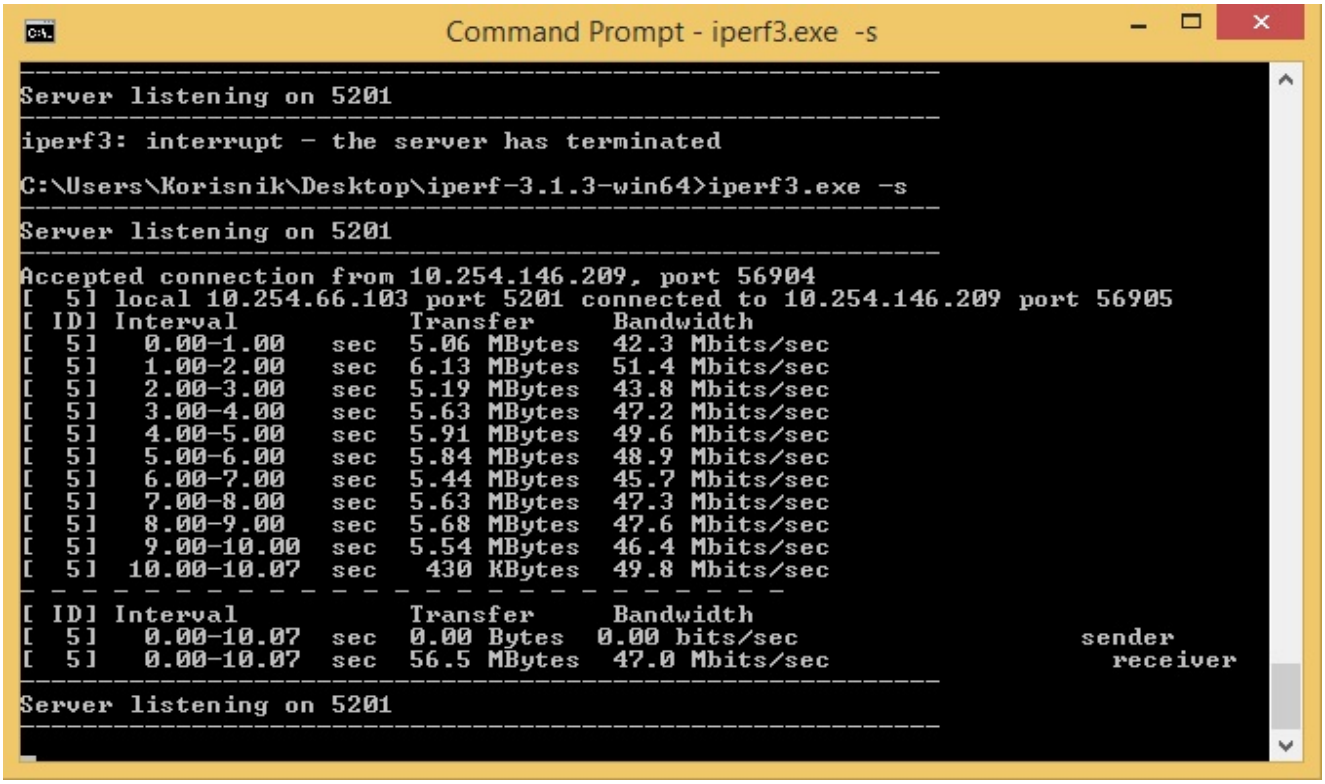


Slika 4.5. *UDP test*

Slika 4.6. prikazuje maksimalnu veličinu segmenta, koja je najveća količina podataka u bitovima, koje računalo podržava u jednom nefregmentiranom TCP segmentu. Može se izračunati na sljedeći način: MSS=MTU-IP zaglavlja, gdje su TCP i IP zaglavlja jednaka 40 bita. MTU ili *Maximum transmission unit* je najveća količina podataka koja se može prenijeti po jednom okviru. Ovo su neke od MTU veličina koji se koriste u mrežnoj topologiji:

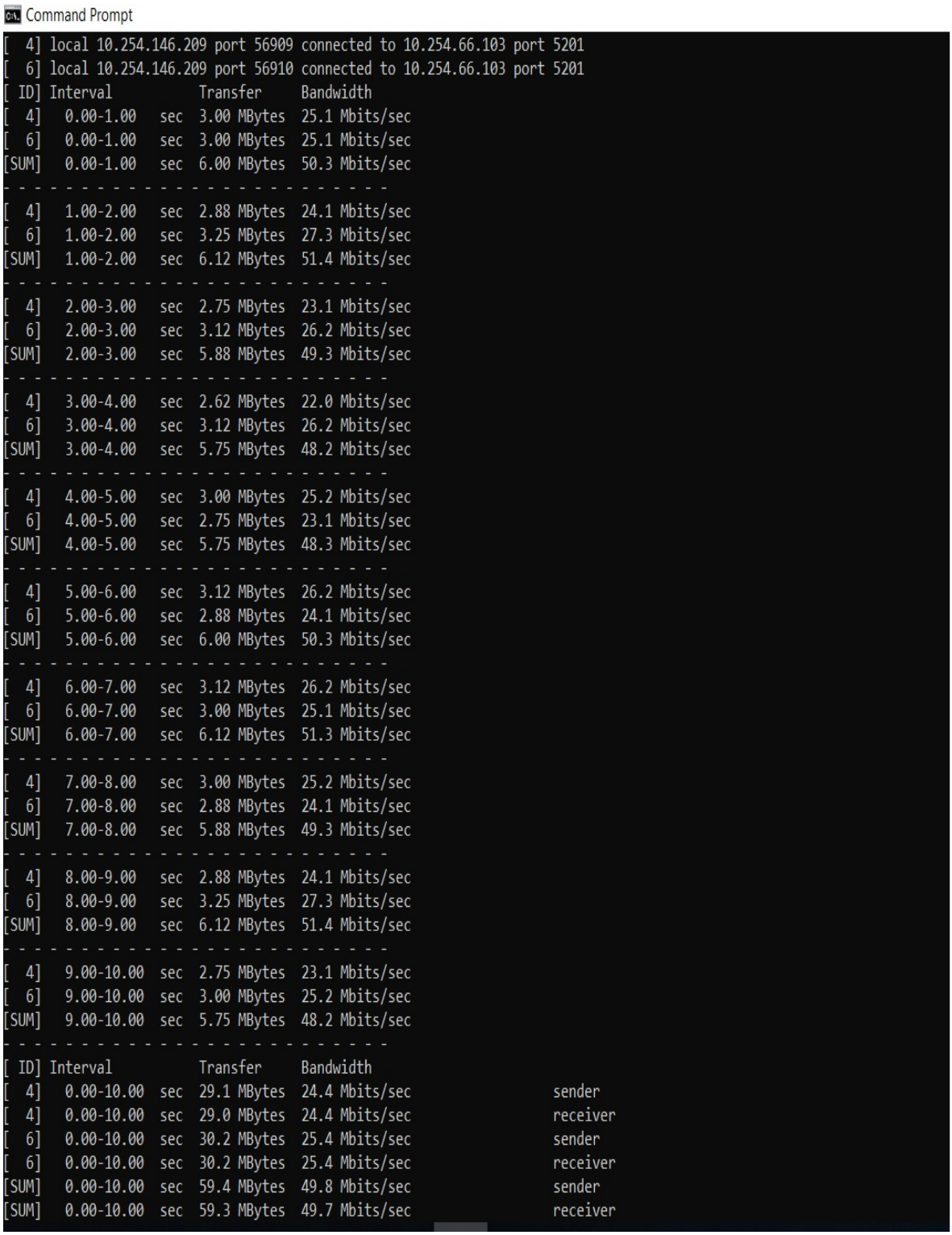
- Ethernet=1500 B, koristi se u LAN-u
- PPPoE=1492 B, koristi se u ADSL-u
- Dial-up=576 B
- Token Ring (16Mbit/s) - 17914 B

Uglavnom, što je veći MTU i MSS veća je i efikasnost širine pojasa odnosno bandwidth.



Slika 4.6. *MSS-Maksimalna veličina segmenta*

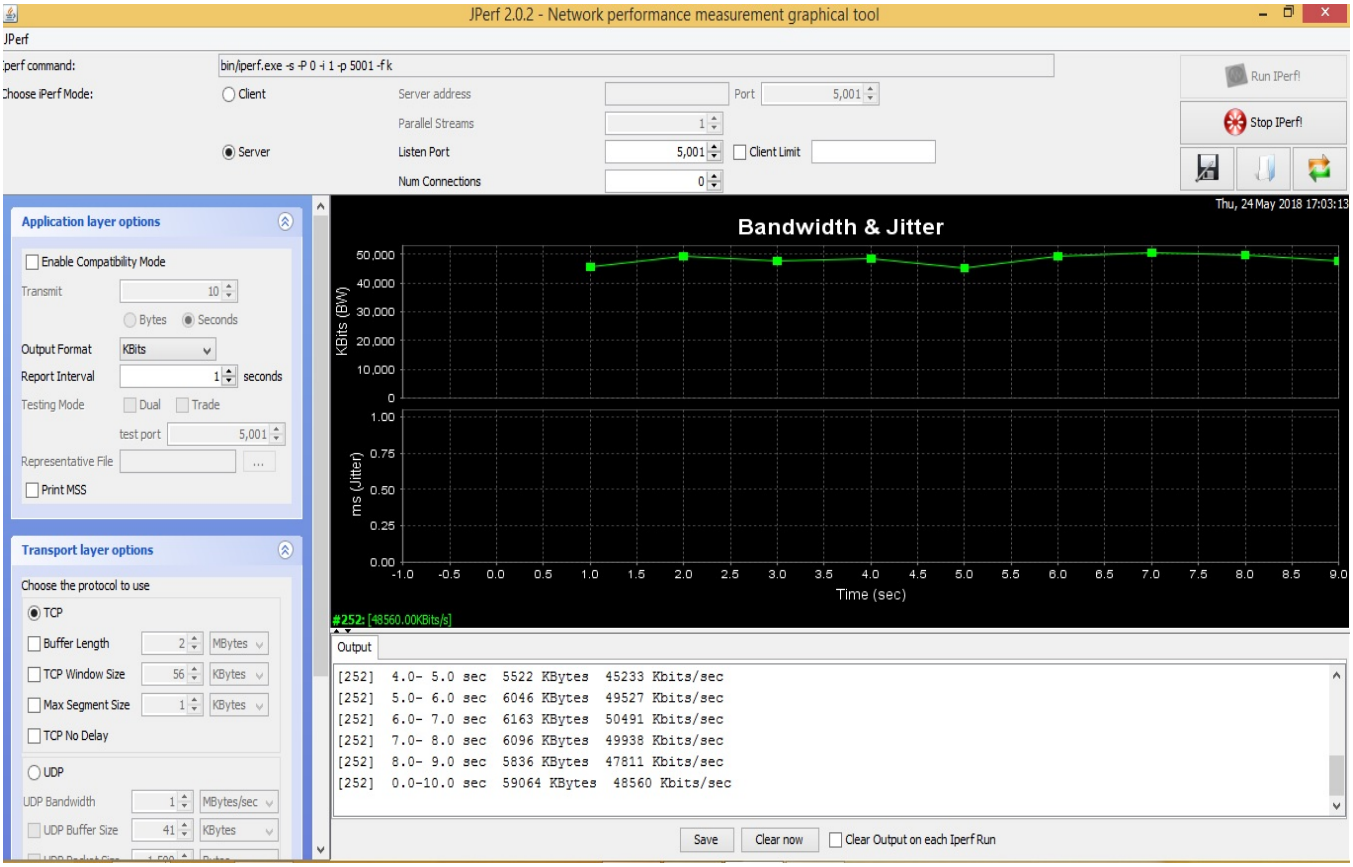
Na slici 4.7. prikazan je paralelni test. Provjerili smo protok podataka preko dvije paralelne veze koristeći Iperf. U ovom primjeru Iperf programu je naređeno da kreira dvije paralelne TCP konekcije za vrijeme prijenosa podataka. Svaka lokalna veza je spojena na različit port. Klijent je spojen na poslužitelja preko porta 56908, a dvije lokalne veze na 56909 i 56910. Svaka veza ima različite transferne vrijednosti, i na kraju možemo vidjeti da je ukupna širina pojasa 49,7 Mbit/s. Dobiveni su nešto bolji rezultati od običnog TCP-a. Značajniji rezultati bi se dobili da smo koristili 20 paralelnih TCP veza.



Slika 4.7. *Paralelni test*

4.2. Grafički prikaz mjerenja za TP-LINK usmjerivače

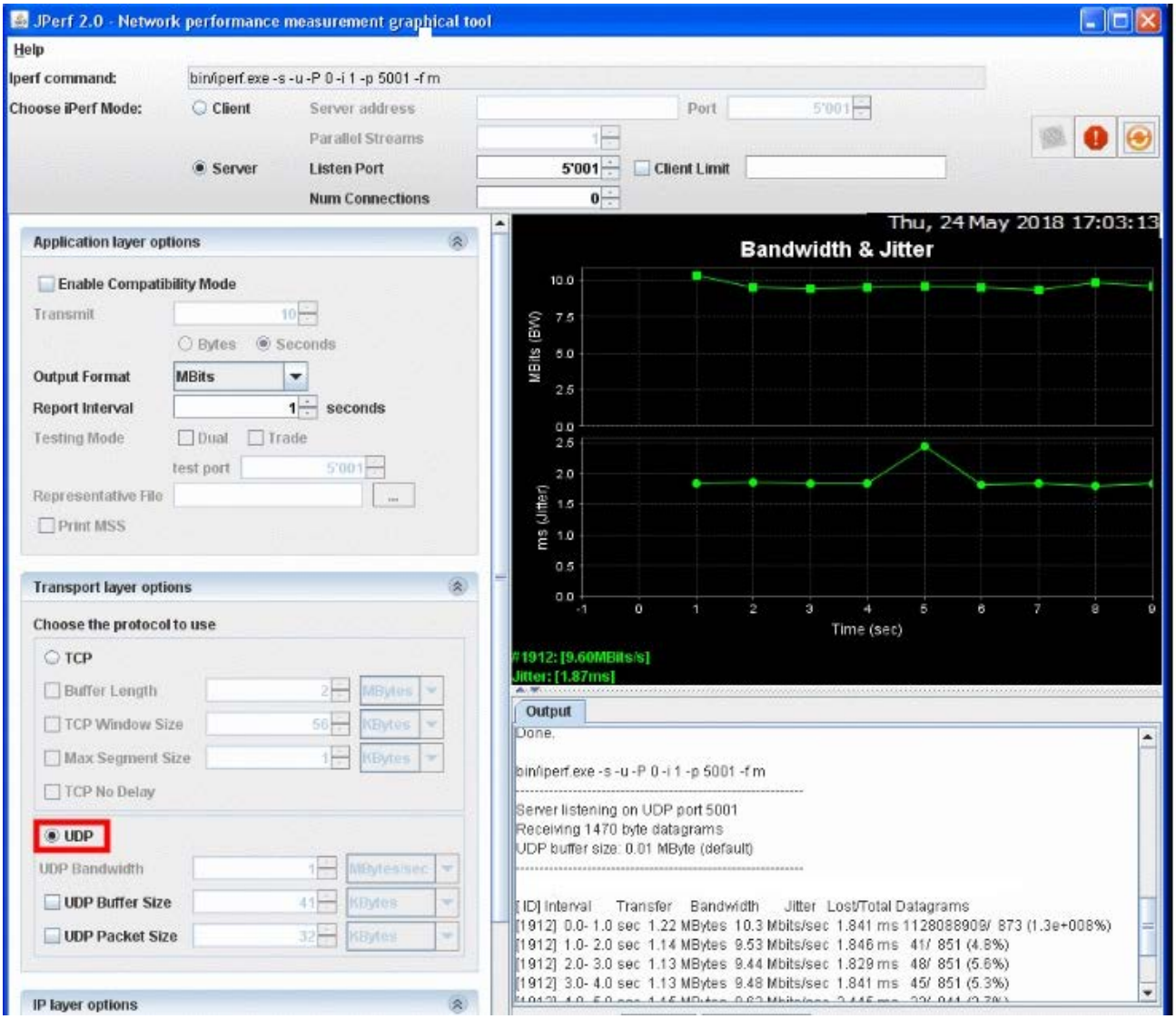
Jperf je grafički prikaz popularnog alata za testiranje mreže Iperf-a. Pomoću Jperf alata možemo brzo testirati WAN ili LAN vezu kako bi se odredio maksimalni protok podataka kroz mrežu. Rezultati testa se automatski prikazuju grafički na osi. Jperf alat se još koristi za otkrivanje gubitaka paketa, kašnjenja, jitter-a i drugih uobičajenih mrežnih problema.



Slika 4.8. *Grafički prikaz širine pojasa*

Grafički prikaz dobiven je naredbom u Iperf naredbenom retku i glasi: iperf.exe –s –P 0 –i 1 –p 5001 –f k. To je automatski prikaz TCP-a, port je 5001 na kojem poslužitelj/klijent osluškuju vezu. –i 1 označava period osluškivanja, u ovom slučaju je 1 sekunda. Iz slike 4.8. možemo očitati da je prosjek širine pojasa između 40 i 50 Mbit/s. TCP veličina prozora je postavljena na 56 kB, kako bi dobili što veći protok podataka kroz mrežu.

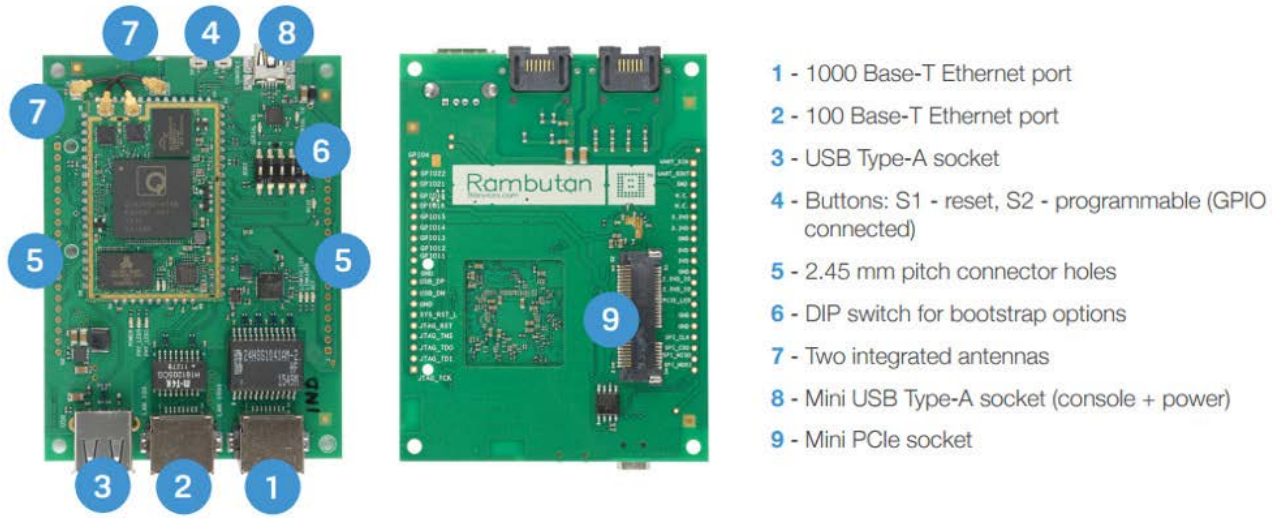
Na slici 4.9. prikazan je UDP test. Grafički prikaz dobiven je naredbom iperf.exe –s –u –P 0 –i 1 –p 5001 –f m. Jitter se kreće od 1,75 do 2,5 ms, dok je širina pojasa oko 10 Mbit/s.



Slika 4.9. *UDP test*

4.3. Mjerenje mesh performansi pomoću Rambutan uređaja

Rambutan je uređaj koji se temelji na QCA 9557 ili QCA 9550 Soc i dolazi u dvije radne temperature. Može se koristiti komercijalno (0-65°C) i industrijski (-40-85°C). Sadrži dual-band radio koji radi na dvije frekvencije 2,4 ili 5 GHz, brzina prijenosa podataka od 300 Mbit/s, 128 MB RAM-a i Flash memorije, te razvojni set sa mnogim sučeljima za priključak (npr. Gigabit Ethernet). Za konfiguraciju ovog uređaja korišten je kao i u prethodnom slučaju programski kod preuzet sa OpenWrt projekta. Ugrađeni su potrebni firmware-i. Za mjerenje mesh mreže korištena su dva ovakva uređaja, u daljnjem radu biti će prikazani rezultati dobiveni Iperf i Jperf alatima.



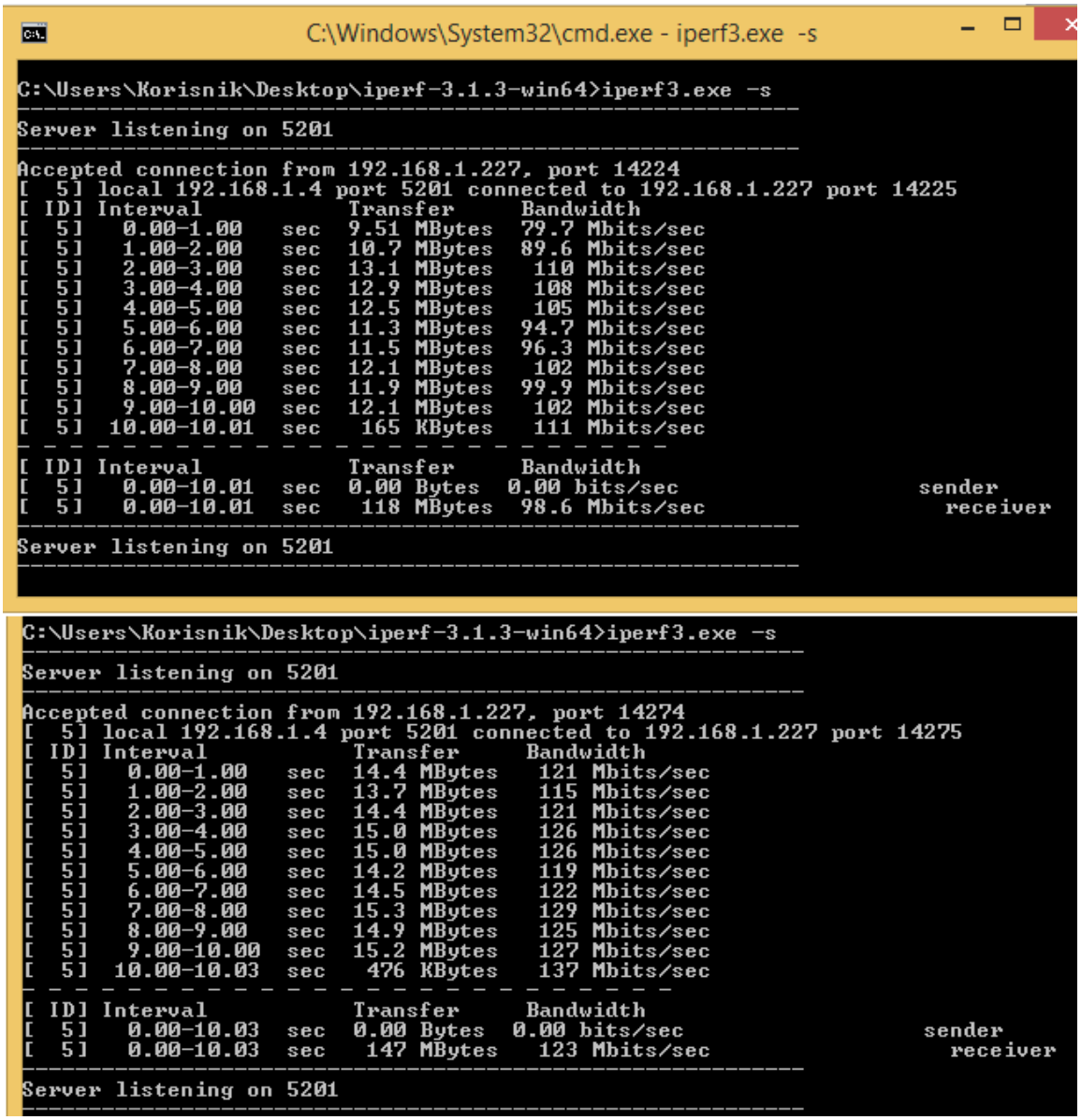
Slika 4.10. *Rambutan uređaj [22]*

Na slici 4.11. prikazana je konfiguracija rambutan uređaja. Bilo je potrebno konfigurirati default_radio0, te ubaciti mesh karakteristike uređaju. Širina pojasa kanala u modu HT20 je 20 MHz, a propusnost kanala u HT40 modu je 40 MHz. Dva susjedna 20 MHz kanala su povezana kako bi stvorila 40 MHz kanal. Jedan kanal funkcionira kao glavni kanal, a drugi kao pomoćni kanal. Kada se HT40 način rada koristi u frekvencijskom pojasu 2,4 GHz, postoji samo jedan kanal koji se ne preklapa. Stoga se ne preporuča korištenje HT40 na frekvencijskom pojasu od 2,4 GHz. Dva susjedna 20 MHz kanala su povezana kako bi stvorila 40 MHz kanal. Ako je središnja frekvencija glavnog 20 MHz kanala veća od one pomoćnog kanala, prikazuje se 40MHz-plus; inače će se prikazati 40MHz-minus. U našem slučaju korišten je VHT40, VHT (engl. Very High Throughput). Uređaju smo pristupili preko PuTTY alata, uređaj smo spojili preko USB kabela na prijenosno računalo.

Slika 4.11. *Konfiguracija uređaja*

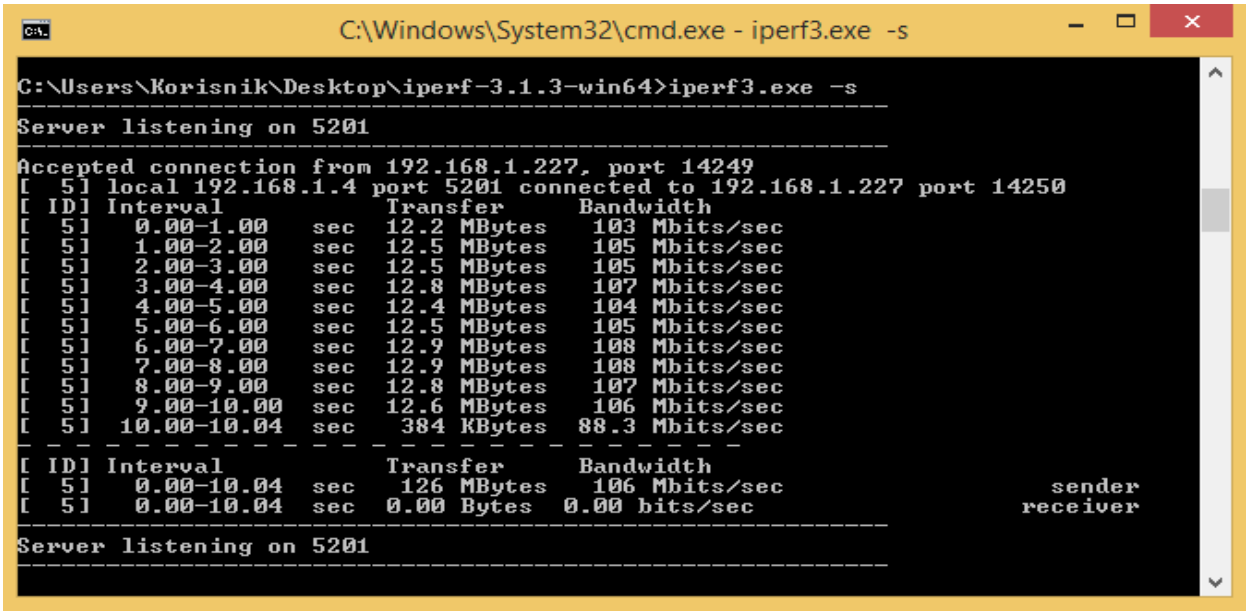
Korištenjem Iperf alata opet smo jedan uređaj postavili kao poslužitelja dok je drugi bio klijent.

Na slici 4.12. prikazan je poslužitelj nakon spajanja na Iperf alat. Gornji prikaz slike prikazuje spajanje na TCP na određeni port i širina pojasa koja je prikazana je od strane klijenta prema poslužitelju. U donjem dijelu slike prikazan je isti test samo sa uključenom radnjom u pozadini. Kao test je bio pokrenut audio/video sadržaj na youtube stranici. Vidljivo je da se promet povećao kao i širina pojasa sa 98,6 Mbit/s na 123 Mbit/s.



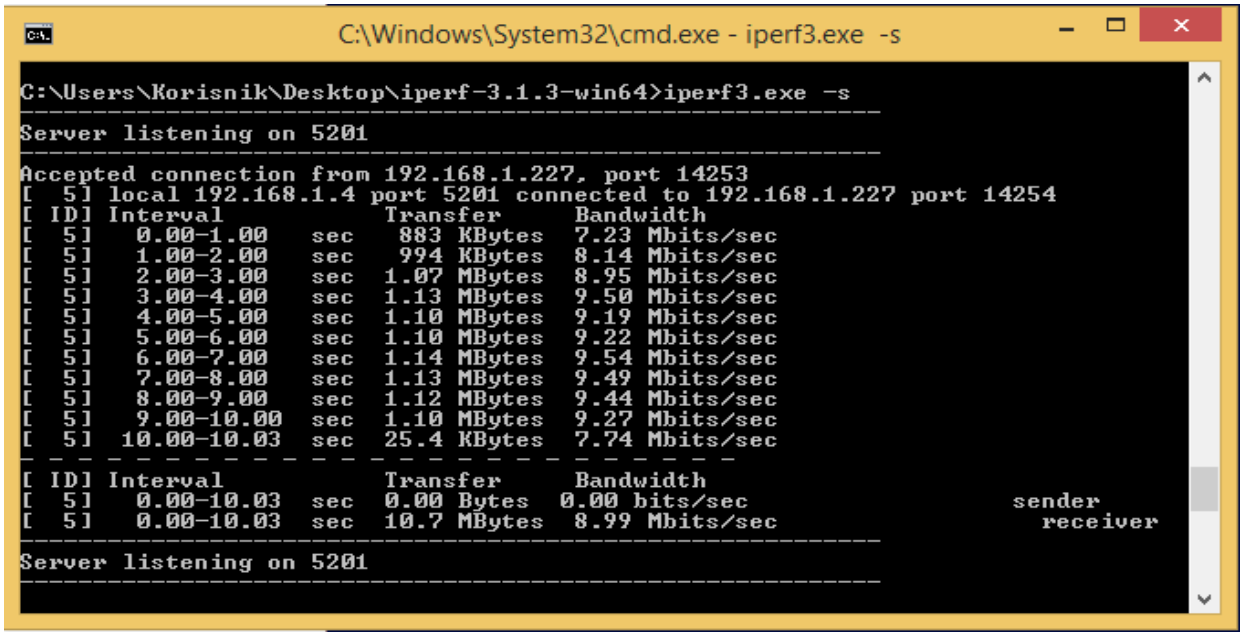
Slika 4.12. *TCP prikaz poslužitelja*

Slika 4.13. je prikaz bi-direkcijskog spajanja. Poslužitelj se spaja na klijenta dopuštajući bi-direkcijsko mjerenje bandwidth-a. Bandwidth se mjeri samo od strane klijenta prema poslužitelju. Mjerenja se provode pet puta u deset vremenskih intervala po jednu sekundu. Ukupna širina pojasa iznosi 106 Mbit/s.



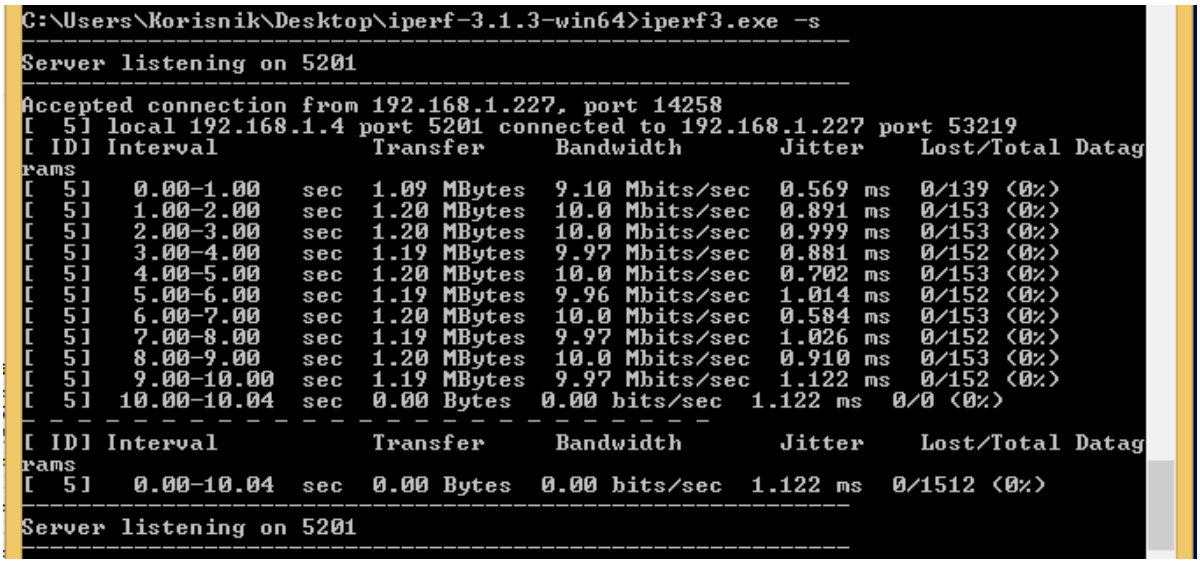
Slika 4.13. *Bi-direkcijsko mjerenje*

Na slici 4.14. prikazana je TCP veličina prozora, naredbom –w. TCP veličina prozora predstavlja količinu podataka koja se može prenijeti tijekom konekcije bez potrebne potvrde prijemnika. Veličina može biti između 2 i 65,535. Postavili smo na 2000 jer manja vrijednost bi dala slabije performanse. Na strani poslužitelja je stiglo nekih 11 MB, dok je širina pojasa oko 9 Mbit/s.



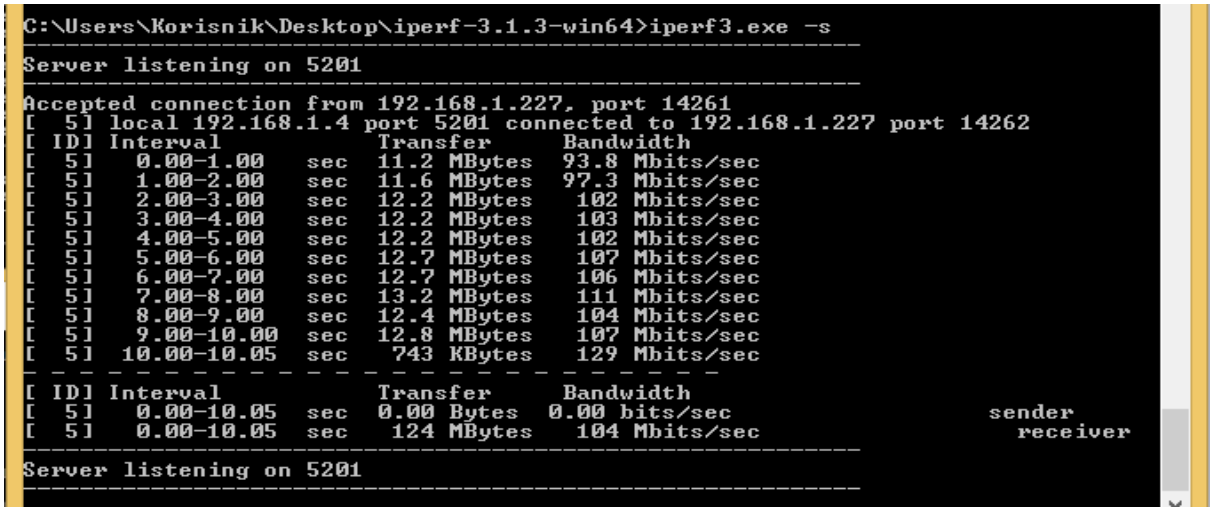
Slika 4.14. *TCP postavljen na 2000 B*

Na slici 4.15. prikazan je poslužitelj nakon UDP testa, naredbom –u. UDP test daje nam neprocjenjive podatke u vezi kolebanja kašnjenja (engl. jitter) i gubitku paketa. Kako bi kvaliteta veze bila dobra, gubitak paketa ne bi trebao nikada prelaziti 1%. Visoki postotak gubitaka paketa generirati će mnogo ponovljenih TCP segmentnih podataka što se odražava na širinu pojasa (engl. bandwidth). U ovom primjeru vidimo da nema gubitaka paketa, tj. 0%.



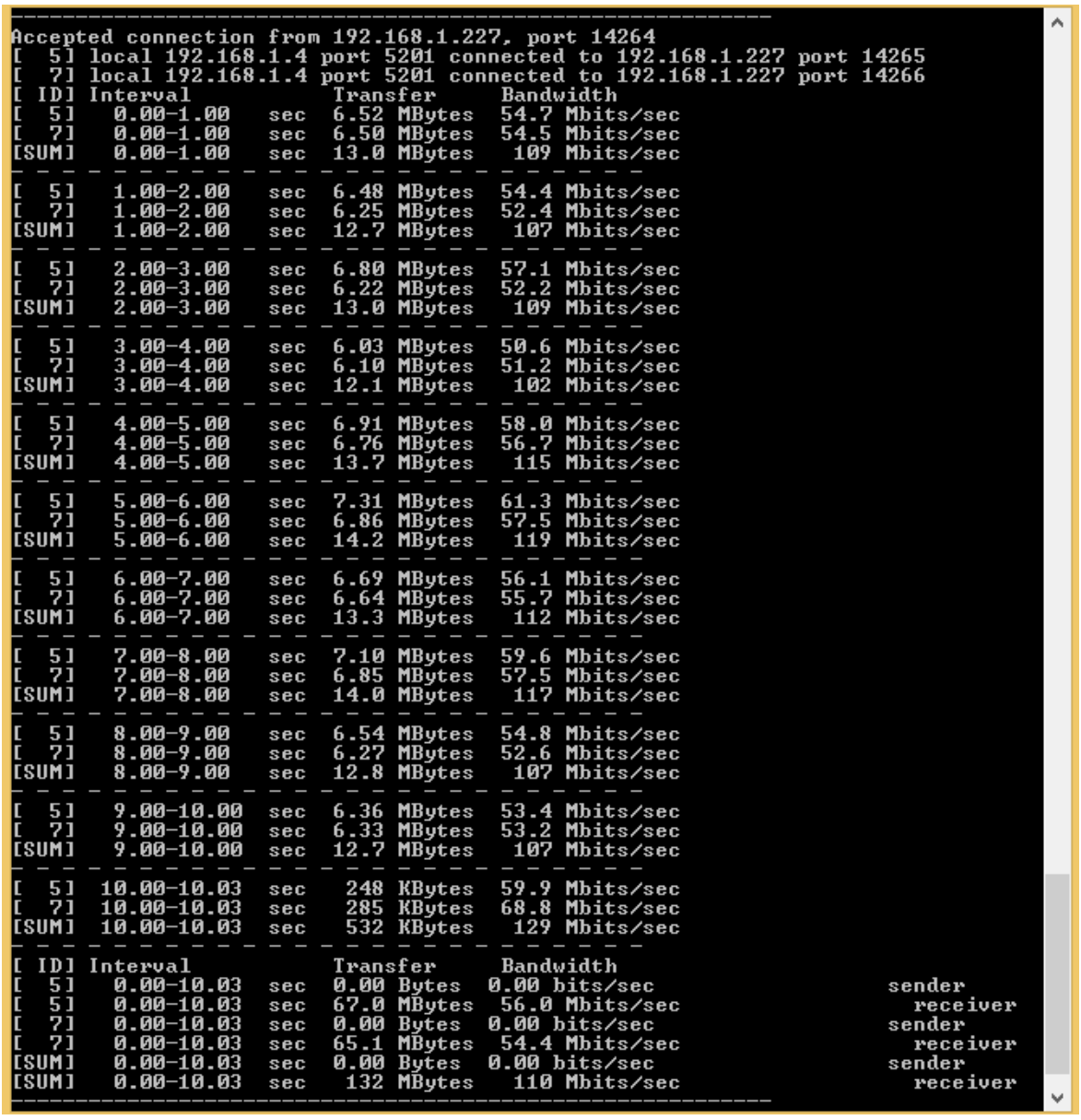
Slika 4.15. *UDP test*

Slika 4.16. prikazuje maksimalnu veličinu segmenta, koja je najveća količina podataka u bajtovima, koje računalo podržava u jednom nefregmentiranom TCP segmentu. Uglavnom, što je veći MTU i MSS veća je i efikasnost širine pojasa odnosno bandwidth.



Slika 4.16. *MSS-Maksimalna veličina segmenta*

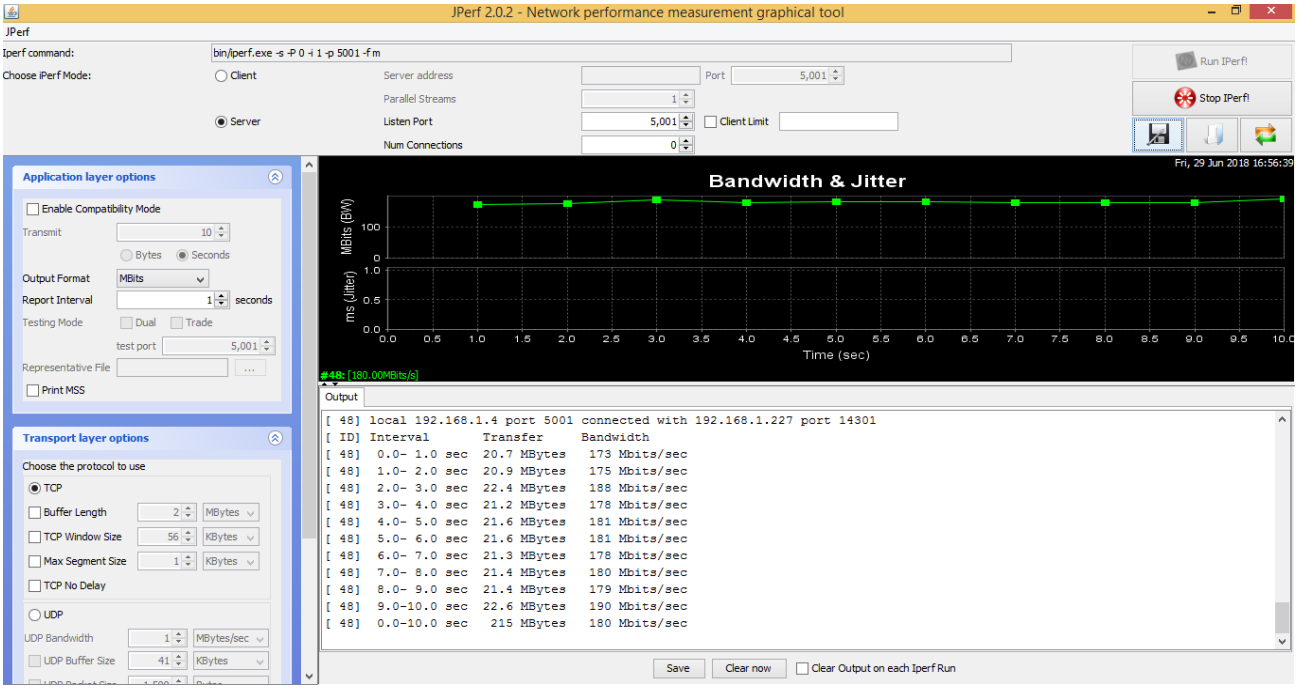
Na slici 4.17. prikazan je paralelni test. Provjerili smo protok podataka preko dvije paralelne veze koristeći Iperf. U ovom primjeru Iperf je kreirao dvije paralelne TCP konekcije za vrijeme prijenosa podataka. Svaka lokalna veza je spojena na različit port. Klijent je spojen na poslužitelja preko porta 14264, a dvije lokalne veze na 14265 i 14266. Svaka veza ima različite transferne vrijednosti, i na kraju možemo vidjeti da je ukupni protok podataka 132 MB.



Slika 4.17. *Paralelni test*

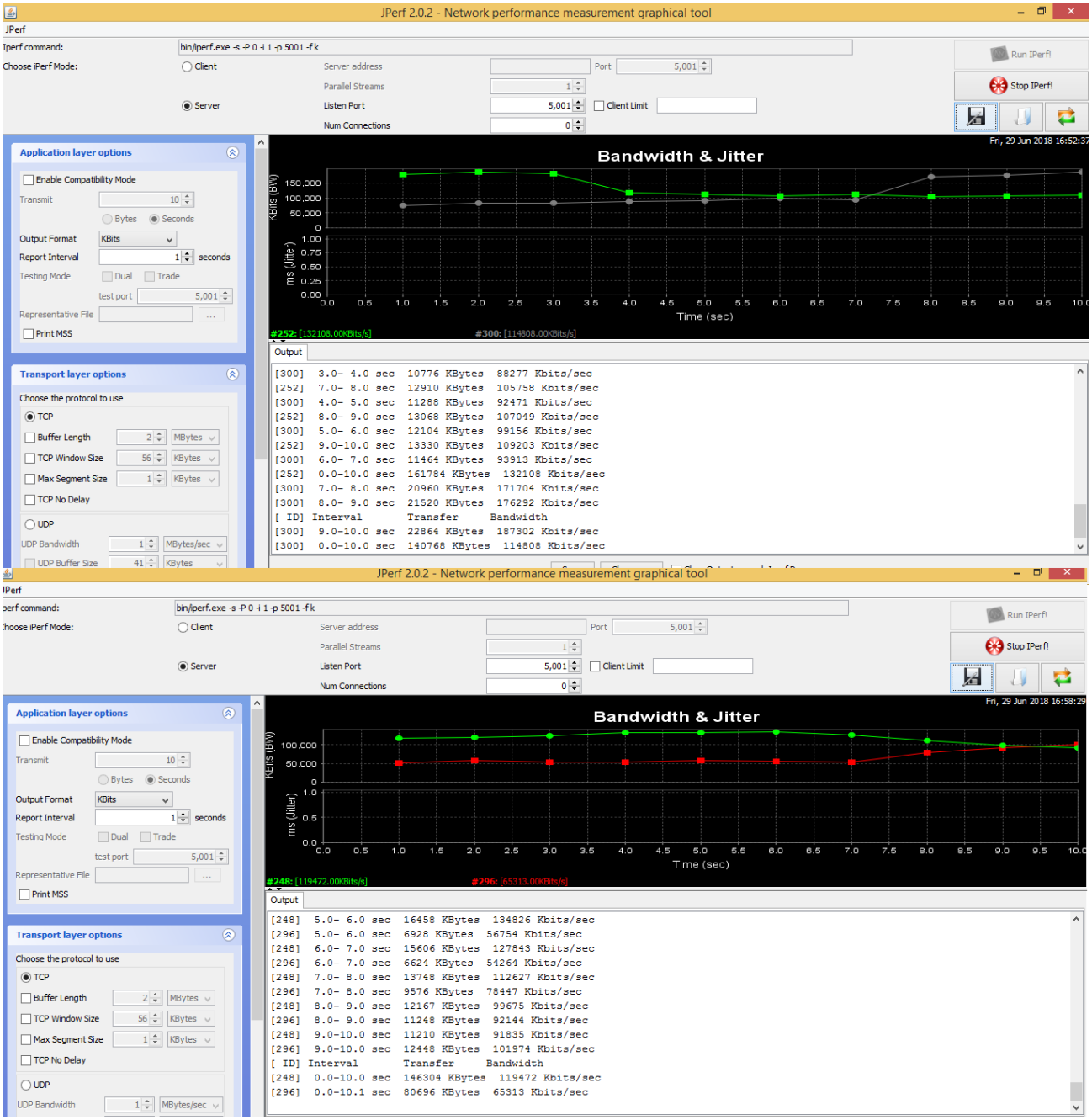
4.4. Grafički prikaz mjerenja za Rambutan uređaje

Korištenjem Jperf alata dobili smo grafički prikaz mjerenja mesh performansi. Grafički prikaz dobiven je naredbom u Iperf naredbenom retku i glasi: iperf.exe –s –P 0 –i 1 –p 5001 –f m. To je automatski prikaz TCP-a, port je 5001 na kojem poslužitelj/klijent osluškuju vezu. –i 1 označava period osluškivanja, u ovom slučaju je 1 sekunda. Iz slike 4.18. možemo očitati da je širina pojasa oko 180 Mbit/s. TCP veličina prozora je postavljena na 56 kB, kako bi dobili što veći protok podataka kroz mrežu. Mjerenja su izvršena uz pozadinsku radnju audio/video sadržaja na youtube kanalu.



Slika 4.18. *TCP prikaz uz youtube sadržaj*

U idućem slučaju korištena je naredba za obostrano bi-direkcijsko mjerenje. Izvršena su dva mjerenja, jedna bez pozadinske radnje, druga sa audio/video radnjom u pozadini. Grafički prikaz dobiven je naredbom iperf.exe –s –P 0 –i 1 –p 5001 –f k. U drugom slučaju možemo vidjeti kako se širina pojasa smanjila sa 114 Mbit/s na 65 Mbit/s.

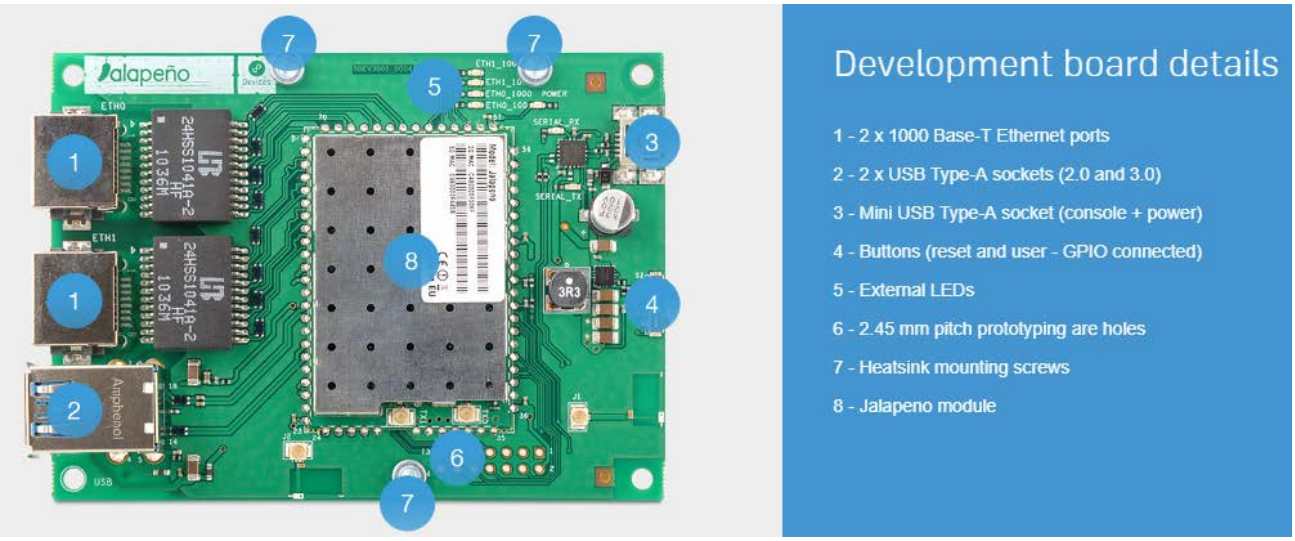


Slika 4.19. *Obostrano bi-direkcijsko mjerenje bez i sa pozadinskom radnjom*

4.5. Mjerenja mesh performansi pomoću Jalapeno uređaja

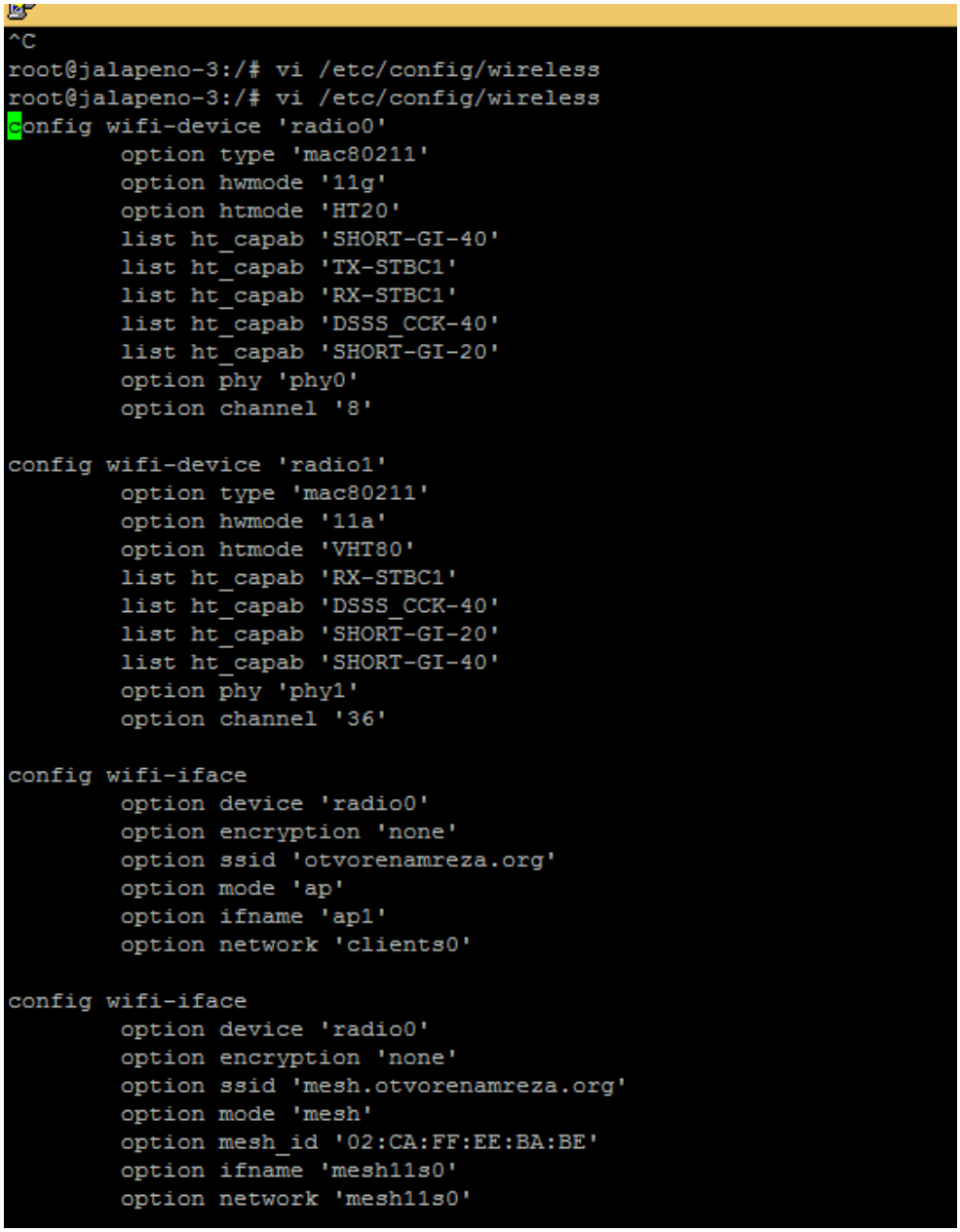
Treće mjerenje se izvodilo sa Jalapeno uređajima na malo većoj udaljenosti nego u prethodna dva mjerenja. Ovim mjerenjem se zapravo htjelo pokazat stvarno djelovanje mesh mreže u stvarnim uvjetima. Prvo mjerenje je bilo na kratkoj udaljenosti i rezultati su opravdano pokazivala visoku efikasnost mreže. Mjerenja su se provodila na 20, 40 i 80 VHT kako bi se vidjela učinkovitost. Drugo mjerenje se izvelo na udaljenosti od 30-ak metara preko 2 hopa.

Jalapeno se temelji na IPQ4018 SoC Qualcomm, što je izuzetno snažan četverojezgreni procesor, idealan za usmjerivače, gateway i pristupne točke AP (engl. Access Point). To je površinski montirani, dvostrani, Wi-Fi omogućeni Linux modul. Dolazi s dvostrukim frekvencijskim pojasom visoke snage (23 dBm po lancu) koji podržava tehnologiju 802.11ac Wave2 (2x2 MiMo) i doseže brzinu prijenosa od 1,167 Gbit/s. USB 3.0, USB 2.0, I2C, I2S, UART i GPIO su sučelja dostupna na modulu zajedno s dva Gigabit Ethernet porta. SoC ima hardverski NAT motor i vrhunske sigurnosne značajke poput kripto motora, sigurnog dizanja i drugih.



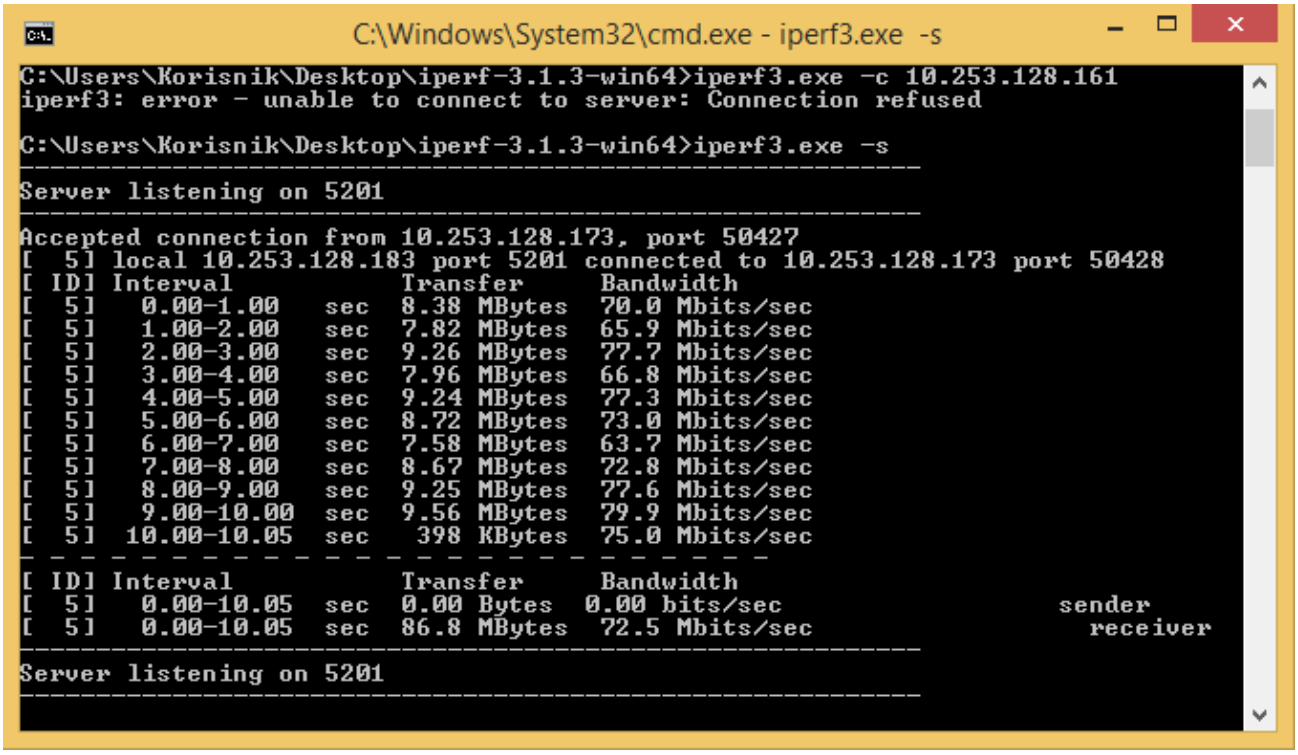
Slika 4.20. *Jalapeno uređaj [23]*

Kao i u prethodnim mjerenjima bila je potrebna konfiguracija uređaja. Koristio se firmware od OpenWrt projekta. U 3 slučaja smo mijenjali VHT vrijednost, od 20 pa do 80.

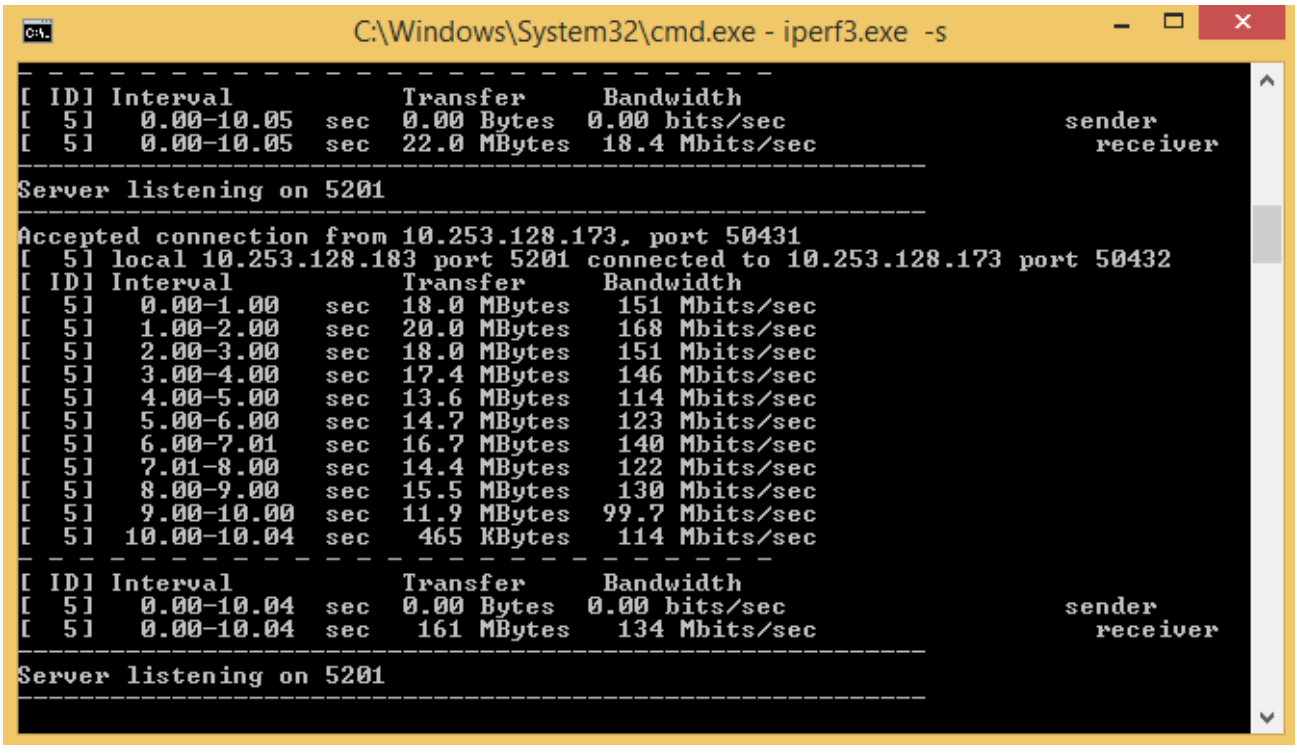


Slika 4.21. *Konfiguracija Jalapeno uređaja*

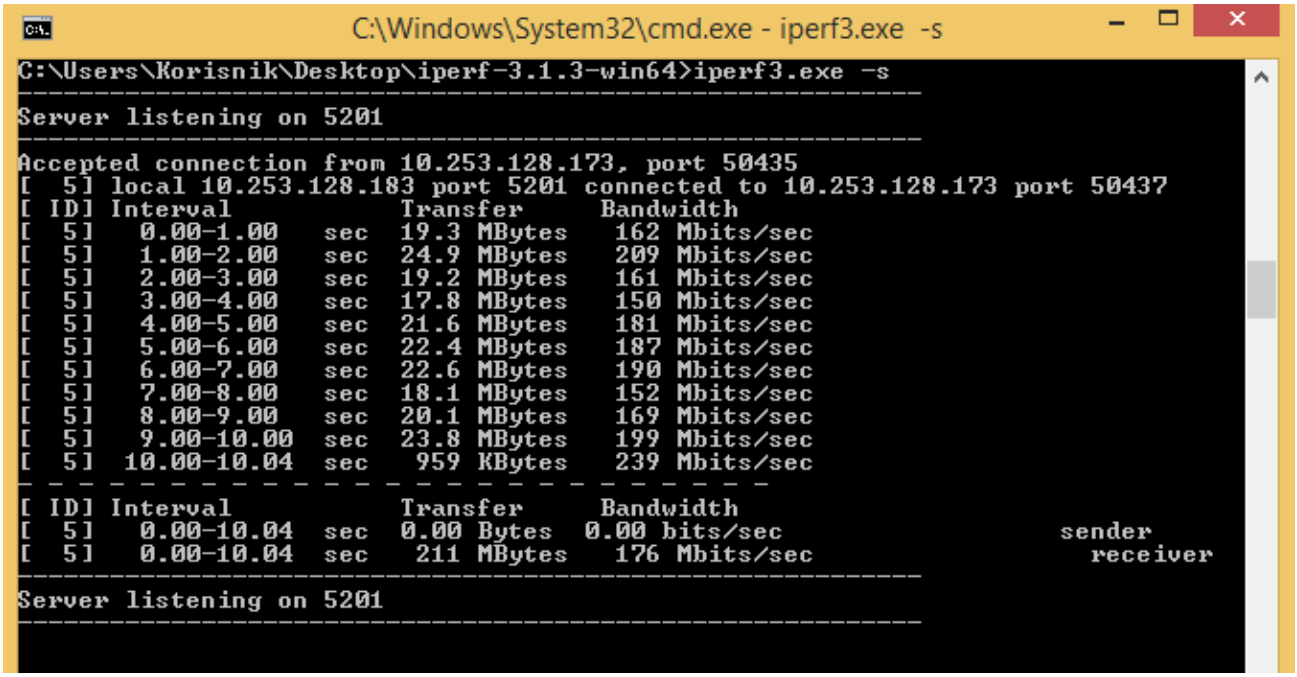
Slika 4.22. prikazuje rezultate spajanja dva takva uređaja na udaljenosti od par metara na VHT20. Prikazano je spajanje na TCP na određeni port i širina pojasa koja je prikazana od strane klijenta prema poslužitelju. Rezultati su zadovoljavajući, širina pojasa je na 72,5 Mbit/s. Na slici 4.23. VHT je postavljen na 40 i samim time su rezultati duplo bolji, 134 Mbit/s. Na slici 4.24. su rezultati kada je uređaj postavljen na VHT80, vidimo mali pomak u odnosu na VHT40, sada je širina pojasa 176 Mbit/s. Vrijednosti se nisu udvostručile kao u prethodnom slučaju.



Slika 4.22. *Jalapeno na VHT20*

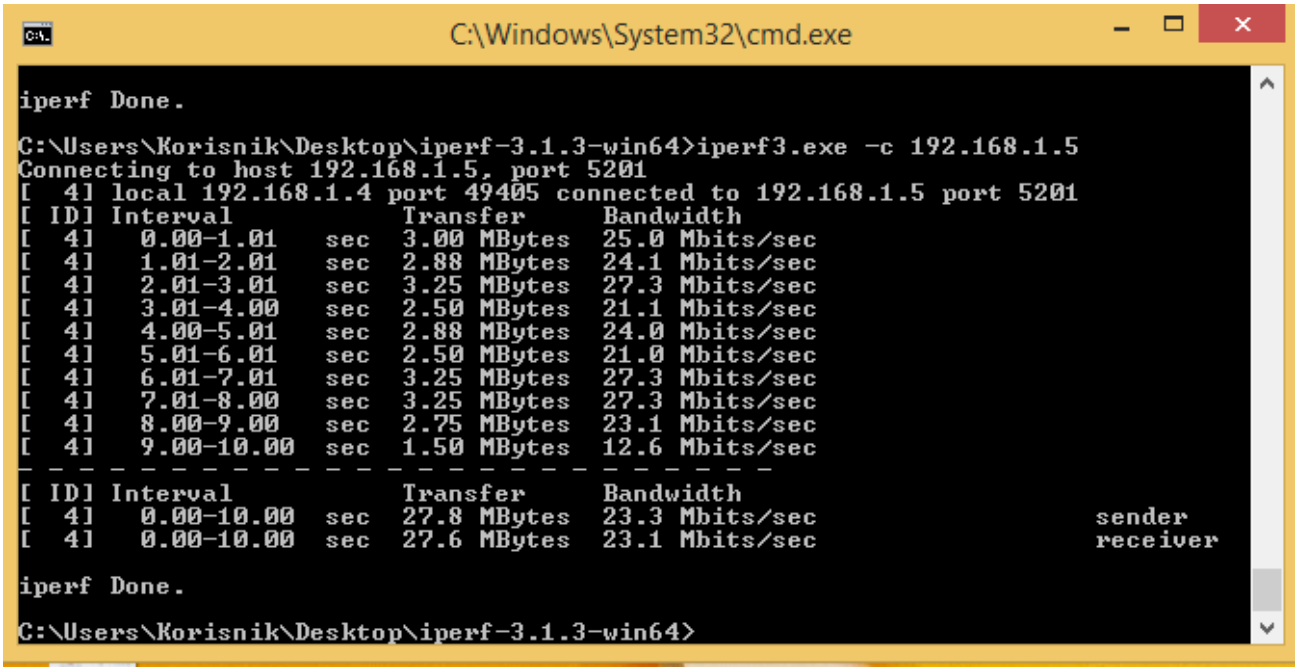


Slika 4.23. *Jalapeno na VHT40*



Slika 4.24. *Jalapeno na VHT80*

Na slici 4.25. je prikazano zadnje mjere koje je izvedeno tako što su uređaji bili udaljeni 30ak metara jedan od drugog. Veza je ostvarena preko 2 hopa, i možemo zaključiti da je veza jako loša. Prijenos podataka je samo oko 27 MB dok je širina pojasa 23.1 Mbit/s.



Slika 4.25. *Udaljenost preko 30 metara*

5. ZAKLJUČAK

U ovom radu opisan je rad i uporaba bežične mesh mreže. Mesh mreža sve je više zastupljenija i zbog svih svojih prednosti nalazi sve veću uporabu na tržištu. U radu su uspoređena različita rješenja i protokoli koji se koriste u današnoj izvedbi bežičnih mesh mreže. Analizirani su prednosti i nedostatci svakog pojedinog rješenja. U radu su uspoređene performanse mrežnih protokola. Na kraju rada bilo je potrebno testirati rada same mesh mreže, što je i prikazano. U testiranju efikasnosti mreže korištena su tri uređaja kako bi se njihov rad mogao analizirati i usporediti. Korišteni su osnovni tp-link usmjerivači kao početak mjerenja. S tim uređajima dobiveni su zadovoljavajući rezultati za jedan takav uređaj. Druga dva testiranja dovela su mesh mrežu na jednu drugu razinu. Uređaji koji su korišteni u tom dijelu testiranja su rambutan i jalapeno radio uređaji. Oba ova uređaja imaju svoje prednosti i njihova snaga prikazana je u rezultatima. Analiza je napravljena omoću programskog alata Iperf, koji je vrlo jednostavan za koristiti. Mesh mreže sve se više razvija i u budućnosti će predstavljati i već je bitan faktor u mrežnoj komunikaciji. Čvorišta mesh mreže lako se postavljaju i što je najbitnije lako se konfiguriraju. Jednostavna je u izvedbi i implementira se na već postojeću mrežu. Temelji se na već postojećim komunikacijskim standardima (802.11 a,b,g,n,s). Jedna od prednosti mesh mreže je ta da čvorišta sama pronalaze nove optimalne puteve ako dođe do pada jedne putanje. Druga prednost je već ranije spomenuta sposobnost samo-izlječenja (engl. Self-healing). Paketi ne putuju do centralnog čvora kako bi stigli do odredišta, i zbog toga se lako prilagođavaju na nove uvjete i zahtjeve korisnika. U radu je spomenuta i sigurnost ovog tipa mreže. Mesh mreža je poprilično sigurna mreža, u tekstu su spomenute neke logičke i fizičke ranjivosti, npr. Siva i crna rupa, postavljanje pristupnih točaka AP-ova, nezaštićena fizička mjesta, teren, itd. Ono zbog čega se većinom koristi ova mreža jest usmjeravanje paketa pomoću kojega se omogućava primanje i slanje paketa bilo gdje u mreži. U radu su spomenuti određeni protokoli za usmjeravanje kojima je svrha određivanja optimalnog puta u mreži. Velik broj čvorova u mreži čini ju otpornijom na kvarove u odnosu na druge. U bližoj budućnosti će sve mesh mreže imati standardizirani sigurnosni mehanizam zasnovan na 802.11s standardu. Mehanizam će se odnositi na korisnika, ad hoc mrežu, centralni mesh sustav. Mesh mreže se mogu koristiti u širokom spektru uporabe. Primjenom ovog rješenja dolazi se do najbolje opcije prilikom dizajniranja mreže u gusto naseljenim područjima. Bitan faktor u dizajniranju ove mreže je balansiranje opterećenja kako bi mreža bila što efikasnija. Taj balans mora biti ostvaren kako ne bi došlo do opterećenja gateway-a i kako se ne bi stvorilo usko grlo priklikom

formacije čvorišta. Svaki uređaj koji je bio korišten u mjerenjima prethodno je morao biti konfiguriran. Konfiguracija se sastojala od unosa novog firmware-a u sučelje svakog uređaja. Svi firmware-i su preuzeti sa OpenWrt platforme. OpenWrt projekt je Linux operacijski sustav koji se koristi na ugrađene sustave. Ovaj projekt pruža potpuni pisani sustav sa upravljanjem paketima. Ovaj postupak oslobađa korisnike od odabira aplikacije i konfiguracije i omogućuje prilagodbu uređaja kroz pakete. Za programere, OpenWrt predstavlja okvir za izgradnju aplikacije bez izgradnje kompletnog firmware-a oko njega. Dok za korisnike to znači sposobnost za potpunu prilagodbu, kako bi se uređaj koristio u sasvim drugim uvjetima. U radu su prikazani rezultati za sva tri uređaja, mjerili su se: širina pojasa, jitter, gubitak paketa. Grafički prikaz istih rezultata omogućio je Jperf alat. Najveći nedostatak meže može predstavljati njegova cijena. Mreža se ubrzano razvija, što znači da su i uređaji pristupačniji.

LITERATURA

[1] https://hr.wikipedia.org/wiki/IEEE_802.11 (10.11.2017.)

[2]802.11:Wi-Fistandards and speeds explained, https://www.networkworld.com/article/3238664/wi-fi/80211-wi-fi-standards-and-speeds-explained.html Keizh Shaw (30.01.2018.)

[3] 802.11 Standards Explained: 802.11ac, 802.11b/g/n, 802.11a, https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553, Bradley Mitchel (20.08.2018.)

[4]Mesh networks: An alternative way to connect to the internet gains steam, **https://mashable.com/2018/01/09/mesh-networks-provide-alternative-intenet-connection/#04Y0Pivhhqq7** ,Mark Kaufman (09.01.2018.)

[5]How Wireless Mesh Networks Work, **https://computer.howstuffworks.com/how-wireless-mesh-networks-work.htm**, Dave Roos

[6],,What are mesh wifi systems and how do they work" , https://www.howtogeek.com/290418/what-are-mesh-wi-fi-systems-and-how-do-they-work/, Craig Lloyd, (veljača 2017.)

[7] Ad-hoc and Mesh Networks , Manuel P. Ricardo

[8] EURASIP Journal on wireless communications and networking, Shamsad Parvin and Takeo Fujii

[9] Master rad, Bežične mesh mreže, Ivan Milovanović, 2009

[10] Wireless Mesh Networks: Routing Protocols and Challenges, https://link.springer.com/chapter/10.1007/978-3-642-14478-3_15, Pavan Kumar Ponnapalli

[11] Routing Protocols for Wireless Mesh Networks Venkat Mohan.S, Dr. Kasiviswanath.N, https://ijser.org/researchpaper/Routing-Protocols-for-Wireless-Mesh-Networks.pdf

[12] **FastM: Design and Evaluation of a Fast Mobility Mechanism for Wireless Mesh Networks** https://www.researchgate.net/figure/Diagram-of-a-Wireless-Mesh-Network_fig1_234015211

[13] A new MAC protocol for Wi-Fi mesh networks , https://ieeexplore.ieee.org/document/1620217/, Tzu jane Tsai, Hsueh-Wen Tseng, Ai-Chun Pang

[14] Chapter: Cisco Wireless Mesh Networking

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch8_MESH.html

[15] Hierarchical Wireless Mesh Networks Scalable Secure Framework

https://www.researchgate.net/publication/314834697_Hierarchical_Wireless_Mesh_Networks_Scalable_Secure_Framework, **K. Ganesh Reddy**(prosinac 2012.)

[16] V.C. Gungor, P. Pace, E. Natalizio, "AR-TP: An Adaptive and Responsive Transport Protocol for Wireless Mesh Networks," to appear in Proc. of IEEE ICC 2007, Glasgow, Scotland, (Lipanj 2007.)

[17] Exploring the Modern Computer Network: Types, Functions, and Hardware, By Cisco Networking Academy. (19.12.2013.)

[18] DCN - Computer Network Toplogies

https://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm

[19] "Unapređenje performansi obrazovnih Sistema primenom bezicnih mesh mreža", Aleksandar Zakić. (2015)

[20] A Security Analysis of the 802.11s Wireless Mesh Network Routing Protocol and Its Secure Routing Protocols, Whye Kit Tan,[1] Sang-Gon Lee,[1,*] Jun Huy Lam,[1] and Seong-Moo Yoo[2] , (02.09.2013.)

[21] TP-LINK user guide, TL-WR740N TL-WR741ND 150Mbps Wireless N Router

[22]Rambutan
https://www.8devices.com/media/products/rambutan/downloads/rambutan_datasheet.pdf

[23]Jalapeno,https://www.8devices.com/media/products/jalapeno/downloads/Jalapeno_datasheet_v1.2.pdf

SAŽETAK

U ovom radu opisan je rad i uporaba bežične mesh mreže. Mesh mreža sve je više zastupljenija i zbog svih svojih prednosti nalazi sve veću uporabu na tržištu. U radu su uspoređena različita rješenja i protokoli koji se koriste u današnoj izvedbi bežičnih mesh mreže. Čvorišta mesh mreže lako se postavljaju i što je najbitnije lako se konfiguriraju. Jednostavna je u izvedbi i implementira se na već postojeću mrežu. Temelji se na komunikacijskim standardima (802.11 a,b,g,n,s). Prednosti ove mreže su sposobnost samo-izlječenja (engl. Self-healing) i pronalazak optimalne putanje pomoću protokola. Mesh mreža je poprilično sigurna mreža. Svaki uređaj koji je bio korišten u mjerenjima prethodno je morao biti konfiguriran. Konfiguracija se sastojala od unosa novog firmware-a u sučelje svakog uređaja. Svi firmware-i su preuzeti sa OpenWrt platforme. Korišteni su osnovni tp-link usmjerivači kao početak mjerenja. S tim uređajima dobiveni su zadovoljavajući rezultati. Druga dva testiranja dovela su mesh mrežu na jednu drugu razinu. Uređaji koji su korišteni u tom dijelu testiranja su rambutan i jalapeno radio uređaji. Mesh mreže se mogu koristiti u širokom spektru uporabe. Primjenom ovog rješenja dolazi se do najbolje opcije prilikom dizajniranja mreže u gusto naseljenim područjima.

Ključne riječi: Mesh mreža, mrežni uređaji, sigurnost, Iperf, OpenWrt, performanse, mrežna topologija, IEEE standard, tp-link, rambutan, jalapeno.

SUMMARY

This thesis describes the operation and use of wireless mesh network. Mesh network is increasingly represented and because of all its advantages there is increasing use in the market. The thesis deals with different solutions and protocols used in today's wireless network performance. Network mesh nets are easy to set up and most importantly they are easy to configure. It is simple to implement and is implemented on an existing network. It is based on communication standards (802.11a, b, g, n, s). The advantages of this network are self-healing and finding the best path through the protocol. Mesh network is a pretty secure network. Each device that was used in the measurements had to be configured beforehand. The configuration consisted of entering a new firmware in the interface of each device. All firmware downloaded from the OpenWrt platform. Basic tp-link routers have been used as the beginning of the measurement. These devices received satisfactory results. The second two tests led the mesh network to another level. Devices used in this part of the test are Rambutan and Jalapeno radios. Mesh networks can be used in a wide range of applications. By applying this solution comes the best option when designing a network in densely populated areas.

Key words: Mesh Network, Network Devices, Security, Iperf, OpenWrt, Performance, Network Topology, IEEE Standard, tp-link, ramutan, jalapeno.

ŽIVOTOPIS

Ilija Dumančić rođen je 09.10.1992. godine u Ebersbergu u Republici Njemačkoj. Osnovnu školu pohađao je u Kupresu u Bosni i Hercegovini. Nakon osnovne škole upisao je Gimnaziju također u Kupresu. Tokom školovanja primio je drugu nagradu iz njemačkog jezika (C1 razina) na državnom natjecanju u Sarajevu. Školovanje završava sa odličnim uspjehom te 2013. godine upisuje Fakultet Elektrotehnike, računarstva i informacijskih tehnologija u Osijeku u Hrvatskoj. U roku završava preddiplomski studij i postaje prvostupnik elektrotehnike. Upisuje diplomski studij na istom fakultetu. Na stručnoj praksi 2017. godine u Zagrebu u Vipnetu d.o.o. stječe dodatna znanja. Nakon povratka u Osijek upisuje Cisco CCNA akademiju kao i MikroTik na fakultetskoj ustanovi. Aktivno se služi računalom i internetom. Zahvaljujući akademijama služi se programima Cisco Packet Tracer, Wireshark, GNS3, Multisim, itd. Aktivno govori njemački i engleski jezik.