Kreiranje mreˇze od tocke do toˇ cke

Juzbašić, Patrik

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

Sveučilišni studij računarstva

Kreiranje mreže od točke do točke

Završni rad

Patrik Juzbašić

Osijek, 2022.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju

Osijek, 10.09.2022.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada na preddiplomskom sveučilišnom studiju

Ime i prezime Pristupnika:	Patrik Juzbašić
Studij, smjer:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. Pristupnika, godina upisa:	R4214, 24.07.2018.
OIB Pristupnika:	21007277787
Mentor:	Doc. dr. sc. Višnja Križanović
Sumentor:	,
Sumentor iz tvrtke:	
Naslov završnog rada:	Kreiranje mreže od točke do točke
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak završnog rad:	Mreže od točke do točke (Point-To-Point, PTP) koriste se za dvije lokacije koje trebaju sigurno međusobno razmjenjivati povjerljive podatke. Visoke performanse koje se time ostvaruju rezultiraju niskim kašnjenjima u mreži. U ovom radu potrebno je konfigurirati PTP mrežu u cilju povećanja razine povjerljivosti, tako da podatkovni promet ne treba usmjeravati preko javnog interneta kada pri razmjeni mrežnog
Prijedlog ocjene završnog rada:	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 3 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 3 bod/boda Jasnoća pismenog izražavanja: 3 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene od strane mentora:	10.09.2022.
Datum potvrde ocjene od strane Odbora:	21.09.2022.

Potvrda mentora o predaji konačne verzije rada:	Mentor elektronički potpisao predaju konačne verzije.
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 21.09.2022.

Ime i prezime studenta:	Patrik Juzbašić
Studij:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	R4214, 24.07.2018.
Turnitin podudaranje [%]:	9

Ovom izjavom izjavljujem da je rad pod nazivom**: Kreiranje mreže od točke do točke**

izrađen pod vodstvom mentora Doc. dr. sc. Višnja Križanović

i sumentora ,

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

Sadržaj

1. UVOD

U svakidašnjem životu razmjena podataka putem umreženih uređaja je postala normalna, nužna i ključna aktivnost za funkcioniranje društva u cjelini. Uređaji u okruženju su sve više povezani jedni s drugima i to olakšava i ubrzava obavljanje svakodnevnih aktivnosti. Umrežavanje u sve većoj mjeri postaje prisutno u brojnim primjerima primjene. Kreiranjem mreža uređaji mogu izmjenjivati podatke kada su udaljeni od samo nekoliko metara do nekoliko stotina tisuća kilometara. Mreža od točke do točke čini malu ali važnu kariku povezivanja. Ovaj rad podijeljen je na šest poglavlja: uvod, mreža od točke do točke, protokoli koji se primjenjuju u mrežama od točke do točke, korištene tehnologije i alati, uspostavljanje mreže od točke to točke i zaključak. U drugom poglavlju opisano je što je to mreža od točke do točke, predstavljena je topologija mreže te su navedene prednosti i nedostaci mreže. Kroz treće poglavlje opisana su glavna obilježja protokola koji se koristi kod mreža od točke do točke. U četvrtom poglavlju je opisana tehnologija i alati korišteni prilikom uspostave mreže od točke do točke. U petom poglavlju je koristeći se alatima i tehnologijama spojena i uspostavljena fizička mreža od točke do točke.

1.1. Zadatak završnog rada

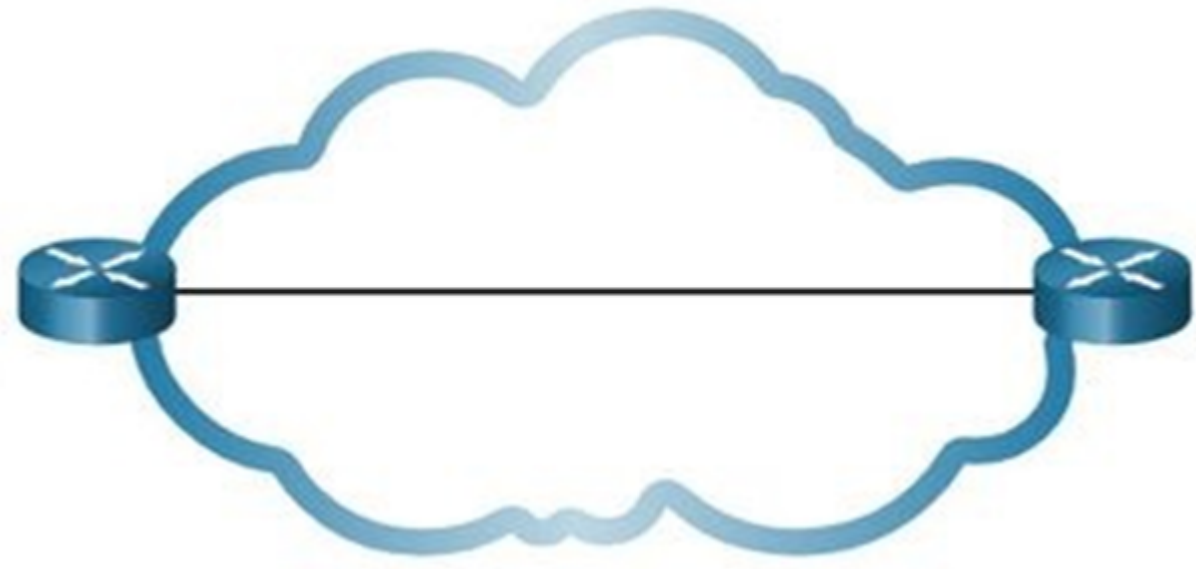
Zadatak je uspostavljanje mreže od točke to točke (engl. *Point-To-Point*, PTP), točnije uspostava sigurne mreže između dvije lokacije kojima se onda omogućuje da međusobno razmjenjuju povjerljive podatke. U ovom radu kreirat će se i konfigurirati PTP mreža u cilju povećanja razine sigurnosti razmjene podataka, to jest povećanja razine povjerljivosti.

2. MREŽA OD TOČKE DO TOČKE

Mreža od točke do točke (engl. *Point-to-Point Network*) je privatna podatkovna mreža koja sigurno povezuje dvije ili više lokacija čime se omogućuje pouzdana razmjena podataka. Mreža od točke do točke je transportna, zatvorena mreža koja ne prenosi podatke preko javnog interneta i tako je sama po sebi prilično sigurna i nije joj nužno potrebno šifriranje podataka. U mreži od točke do točke povezuju se dva čvora izravno zajedničkom vezom. Cijela propusnost zajedničke veze rezervirana je za prijenos između ta dva čvora. Veze od točke do točke koriste stvarnu duljinu žice ili kabela za povezivanje dva kraja, ali moguće su i druge opcije, poput satelitskih veza ili mikrovalova.

Veze od točke do točke dostupne su u rasponu brzina propusnosti i uključuju T1 mrežu od točke do točke, Ethernet mrežu od točke do točke ili DS3 mrežu od točke do točke. Koriste ih tvrtke za pružanje pouzdane, sigurne mrežne podatkovne usluge od točke do točke za aplikacije koje uključuju obradu kreditnih kartica, dijeljenje datoteka, sigurnosno kopiranje podataka, VOIP od točke do točke i video konferencije. Također se mogu konfigurirati za prijenos glasovnih, video, internetskih i podatkovnih usluga preko iste veze. Sustavi od točke do točke također su poznati kao veze od točke do točke, privatne linije, iznajmljene linije ili podatkovne linije.

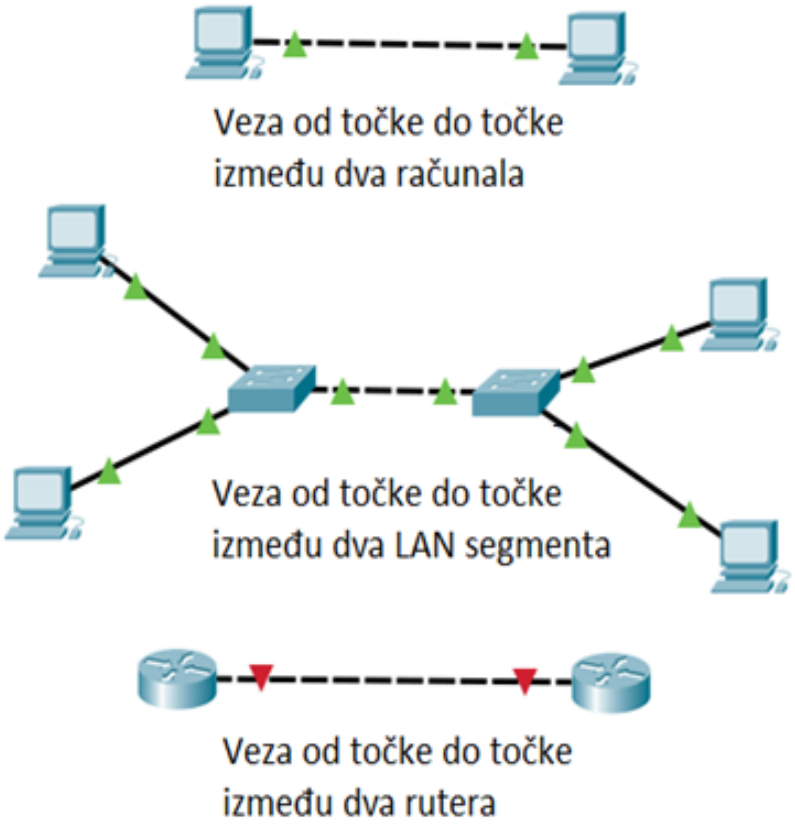
Jedna od najčešćih vrsta mreža širokog područja pokrivanja (engl. *Wide Area Network*, WAN), osobito na velikim udaljenostima komunikacije, je upravo veza od točke do točke, koja se naziva i serijska linijska veza. U WAN-u, iako se krajnje točke smještene na udaljenim mjestima ne povezuju izravno kabelom, obje kreiraju izravan tunel između njih. U tipičnom WAN-u, dva daljinska usmjerivača postavljaju tunel pomoću protokola od točke do točke (PPP-a). Veza radi na razini sloja podatkovne veze prema OSI modelu. Okviri se izravno prenose od izvora do odredišta.



SL. 2.1: *WAN mreža od točke do točke*

2.1. Mrežne topologije

Dijagrami mreže od točke do točke obično prikazuju računalnu mrežu i pristupne točke s uključenim čvorištima ili preklopnicima u uredskoj mreži. Mnogi projektanti mreže od točke do točke projektiraju dijagram topologije mreže kako bi prikazali vrstu topologije koja će se koristiti na samoj mreži od točke do točke. Ovo pomaže pri postavljanju mreže i osigurava da vrste mreža imaju ispravne mrežne uređaje, što omogućuje uspješno postavljanje. Čvorovi mreže od točke do točke međusobno prenose podatke putem zajedničkog linka. Nekoliko primjera mreže od točke do točke su dva računala koja komuniciraju putem modema (slika 2.3), računalo koje komunicira s pisačem putem kabela, itd.



SL. 2.2: *Topologija jednostavnih mreža od točke do točke*

SL. 2.3: *Topologija mreže od točke do točke s dva računala i modemima*

2.2. Prednosti i nedostaci primjene mreže od točke do točke

Kao i svaka vrsta povezivanja tako i mreža od točke do točke ima svoje prednosti i nedostatke u odnosu na druge vrste povezivanja.

Prednosti mreže od točke do točke su sljedeće:

- Brzina – mreže od točke do točke obično koriste iznajmljene linije tako da su brzine zajamčene i olakšavaju prijenos velikih količina podataka između raznih čvorova.
- Bolja sigurnost – uz širokopojasnu vezu ili SDSL poslani podaci prolaze kroz javnu mrežu, što može povećati rizik od presretanja informacija. Ali s mrežama od točke do točke to su kontrolirane privatne mreže, tako da se može prenositi podatke na siguran način.
- Kontrola i nadzor – Ako svi komunikacijski uređaji unutar određene organizacije koriste istu vezu, postaje lakše pratiti korištenje podataka na svim stranicama. To pomaže osigurati ispunjavanje i premašivanje različitih zahtjeva.
- Prioriteti – iznajmljene linije od točke do točke omogućuju da se odredi prioritet određenim vrstama podataka kako bi uspostavljena veza bila brza i pouzdana.
- Povećana produktivnost – iznajmljena mreža od točke do točke osigurava da svi djelatnici neke organizacije imaju pristup važnim centraliziranim datotekama bez obzira gdje rade.

S druge strane nedostaci mogu biti:

- Udaljenost – mreže od točke do točke obično se koriste samo za lokacije koje su blizu jedna drugoj (linija vidljivosti). Za geografski udaljene lokacije mreže od točke do točke postaju skuplje, pa bi druge opcije obično bile prikladnije.
- Ograničene veze – S mrežom od točke do točke mogu se povezati samo dvije stanice, što može biti nedostatak za veće tvrtke koje se proširuju ili koje već imaju više lokacija. Rješenje se pronalazi u mrežama od točke prema više točaka (engl. *Point-to-Multipoint Networks*) [1].
- Nedovoljna robusnost – Ako jedan čvor prestane raditi unutar mreže od točke do točke, tada će cijeli sustav prestati raditi i više se neće moći slati niti primati podatci. S drugim mrežnim konfiguracijama, kada jedan čvor prestane raditi, i dalje će se moći primati i slati podatke prema drugim čvorovima u sustavu.

3. PROTOKOLI KOJI SE PRIMJENJUJU U MREŽAMA OD TOČKE DO TOČKE

U ovom poglavlju su prikazani i objašnjeni neki od protokola koji se koriste u mrežama od točke do točke.

3.1. *Point-to-Point Protocol* (PPP)

Point-to-Point Protocol (PPP) je razvila *Internet Engineering Task Force* (IETF) u cilju slanja podataka koji primjenjuju više od jednog internetskog protokola preko iste *point-to-point* mreže u standardiziranom obliku, neovisno o tome koji je proizvođač omogućio *point-to-point* povezivanje. [2]

PPP omogućava direktnu vezu preko sinkronih i asinkronih krugova. PPP radi sa mnogo različitih protokola mrežnog sloja, kao naprimjer IP i IPv6. Ima ugrađene mehanizme sigurnosti kao naprimjer *Password Authentication Protocol* (PAP), *Challenge Authentication Handshake Protocol* (CHAP) i *Extensible Authentication Protocol* (EAP).

PPP protokol se sastoji od sljedećih glavnih komponenti i metoda:

- Metoda za enkapsulaciju datagrama preko serijskih ili drugih poveznica. *High Level Data Link Control* (HDLC), *Layer 2 Tunneling Protocol* (L2TP), i *Point-to-Point Protocol over Ethernet* (PPPoE) pružaju takve protokole.
- Protokola *Link Control Protocol* (LCP) za postavljanje, konfiguriranje i testiranje podatkovne konekcije.
- Grupa *Network Control Protocols* (NCPs) za povezivanje i konfiguriranje različitih protokola mrežnog sloja. Čest NCP je *Internet Protocol Control Protocol* (IPCP).

Metoda koju PPP koristi za prijenos mrežnog prometa je otvaranje poveznice sa kratkom izmjenom podatkovnih okvira. Kad je poveznica otvorena, mrežni promet se odvija sa jako malo dodatnih informacija. Promet se prenosi kao serija informacijskih okvira koji nisu označeni brojem, što znači da nije potreba potvrda o primanju podataka i ne šalju se retransmisije. Kada je poveznica uspostavljena, PPP se ponaša kao podatkovna cijev za protokole gornjeg sloja koje enkapsulira.

3.1.1 Arhitektura

PPP i OSI protokoli dijele isti fizički sloj, ali PPP distribuira funkcionalnosti LCP-a i NCP-a na drugačiji način. PPP radi preko bilo kojega DTE/DCE sučelja. Jedini preduvjet koji zahtjeva PPP je dvostruki sklop, namjenski ili s mogućnosti prebacivanja, koji može raditi u asinkronom ili sinkronom načinu i odgovara slojnim okvirima PPP-a. PPP ne postavlja nikakve granice kada se govori o količini podataka koji se mogu prenositi, nego to sve ovisi o posebnosti DTE/DCE sučelja nižih slojeva koji se koriste.

Većina posla koju radi PPP je kod datoteka i kod mrežnih slojeva koju obavlja LCP i NCP-ovi. LCP postavlja PPP konekciju i njezine karakteristike, zatim NCP-ovi odrađuju konfiguraciji protokola viših slojeva i na kraju LCP zatvara PPP konekciju.

3.1.2 Enkapsulacija

PPP over Ethernet (PPPoE) koristi 8 bitova *Ethernet* okvira za dodatne informacije i tako snižava maksimalnu veličinu IP paketa koja može biti prenesena bez fragmentacije sa 1500 bitova na 1492 bita. [3]

U PPP enkapsulaciji:

- Podatci dolaze u okvirima, razgraničeni sa specijalnim znakovima koji se zovu zastavice (engl. *flags*)
- Kada se ne šalje okvir, pošiljatelj neprestano prenosi zastavice. Ovo znači da postoji neprestana aktivnost na bilo kojoj sinkronoj vezi koja radi ispravno.
- Prva četiri bita PPP okvira sadržavaju jedno oktetno adresno polje koje je uvijek postavljeno na 0xFF ili binarno 11111111, jedno oktetno adresno polje koje je uvijek postavljeno na 0x03 ili binarno 00000011 i polje sučelja koje se sadrži od dva okteta i ovisi o protokolu, a lista protokola je prikazana tablicom 3.1.
- Uređaj koji prima podatke interpretira podatke tako da prati adresu i kontrolna polja u ovisnosti o enkapsulaciji okvira.

Link Control Protocol (LCP), prije nego što bilo koji drugi protokol može početi prijenos, uspostavlja PPP vezu. Svaki protokol koji se prenosi preko PPP ima svoj *Network Control Protocol* (NCP) koji postavlja opcije protokola i omogućava vezu za taj protokol

3.2. Kontrolni protokoli (engl. *Control Protocols*)

Kontrolni protokoli su oni protokoli pokrenuti od PPP-a kako bi se omogućila konekcija između dvije stanice za prenošenje specifičnih tipova protokola gornjih slojeva. *Link Control Protocol* (LCP) mora biti pokrenut prije svih drugih protokola kako bi konekcija funkcionirala.

Lokalne i udaljenje stanice dogovaraju opcije konfiguracije koje će bit korištene prilikom uspostave veze. Kako bi inicirala proces dogovora, lokalna stanica šalje okvir za konfiguraciju koji sadrži opcije konfiguracije. Onda udaljena stanica odgovara s okvirom koji može sadržavati tri odgovara: potvrda da su opcije uredu, preporuka druge opcije konfiguracije ili odbijanje opcija. Ova izmjena podataka odvija se u oba smjera i kada stanica pošalje i primi paket u kojem se nalazi potvrda za spajanje, sloj veze se smatra otvorenim.

Kontrolni protokoli sastoje se od stanja (engl. *states*), događaja (engl. *events*) i izmjena okvira (engl. *frame exchanges*). Događaju uzrokuju promjenu stanja veze. Dva važna događaja su *open* i *closed*. Njih može pokrenuti naredba upravljača ili mogu biti pokrenuti automatski iznutra, kada se naprimjer uključi uređaj ili se promjeni stanje. Kada se dogodi *open* događaj, kontrolni protokol pokuša uspostaviti vezu, a kada se dogodi *closed* događaj, gasi se veza. Drugi događaji su to da hardver postane dostupan (engl. *up*) ili nedostupan (engl. *down*), isteci vremena i dolasci okvira. Stanja kontrolnih protokola s njihovim objašnjenjima mogu se vidjeti na tablici 3.2 [5].

Protokol	**PPP tip (heksadekadski)**
LCP	0xC021
IP	0x0021
IPCP	0x8021
TCP/IP Comp	0x002D
TCP/IP Uncomp	0x002F
IPX	0x002B
IPXCP	0x802B
DECnet	0x0027
DECnetCP	0x8027
AppleTalk	0x0029
ATCP	0x8029
Multilink	0x003D
Individualna kompresija veze	0x00FB
ILCCP	0x80FB
Kompresija	0x00FD
CCP	0x80FD
Enkripcija	0x0053
ECP	0x8053
Premošćivanje	0x0031
Bridge Spanning Tree	0x0201
BCP	0x8031
Link Quality Report	0xC025
Password Authentication Protocol (PAP)	0xC023
Challenge-Handshake Authentication Protocol (CHAP)	0xC223

Tab. 3.1: *Tablica PPP mrežnih protokola*

3.2.1 *Link Control Protocol* (LCP)

LCP sloj je radni dio PPP-a. Strukturalno, LCP je na vrhu fizičkog sloja i ima ulogu u uspostavljanju, konfiguriranju i testiranju podatkovne konekcije - LCP uspostavlja *point-to-point* vezu. Usto dogovara i uspostavlja kontrolne opcije na WAN vezi, koje su onda upravljane NPC-ovima. LCP uz sve navedeno i prekida konekciju od točke do točke.

Stanje	Značenje
INITIAL	Stanje pri pokretanju, nije se dogodio *OPEN* događaj i stanje hardvera je *DOWN*.
STARTING	Dogodio se *OPEN* događaj i stanje hardvera je *DOWN*.
CLOSED	Stanje hardvera je *UP* i nije se dogodio *OPEN* događaj.
STOPPED	Stanje hardvera je *UP* i *DOWN* ili *TIMEOUT* događaj je nastupio.
CLOSING	Veza je bila uspostavljena i *CLOSE* događaj je nastupio; pokušava se prekinuti veza.
STOPPING	Veza je bila otvorena i udaljena stanica pokušava prekinuti vezu.
ACK SENT	Zahtjev za konfiguraciju sustava je poslan, čeka se odgovor.
ACK RCVD	Zahtjev za konfiguraciju je poslan, i primljena je potvrda.
ACK SENT	Zahtjev za konfiguraciju je primljen, i potvrda je poslana.
OPENED	Potvrda o konfiguraciji je poslana i primljena.

Tab. 3.2: *Tablica stanja za kontrolni protokol*

LCP također omogućava automatsku konfiguraciju protokola na svakoj točki, uključujući:

- Upravljanje različitim ograničenjima vezanim uz veličine paketa
- Pronalaženje uobičajenih problema kod pogrešne konfiguracije
- Raskidanje veze
- Određivanje da li veza radi kako treba

PPP koristi LCP da odredi enkapsulacijski format u trenutku kada je veza uspostavljena.

LCP će probati dogovoriti sljedeće opcije:

- *Maximum Receive Unit* (MRU)
- Diskriminator krajnje točke
- Diskriminator veze
- Autentifikacijski protokol
- *Link Quality Reporting* (LQR)
- Magični broj
- *Asynchronous Control Character Map* (ACCM)
- *Maximum Received Reconstructed Unit* (MRRU).

Sve druge opcije su postavljenje na predefinirane vrijednosti određene u odgovarajućem RFC-u.

3.2.2 *Network Control Protocol* (NCP)

PPP dozvoljava da više protokola mrežnih slojeva rade na istom komunikacijskom kanalu. Za svaki mrežni protokol, PPP koristi poseban NCP. Naprimjer, IP koristi *IP Control Protocol* (IPCP) i IPv6 koristi IP6CP. NCP-ovi uključuje funkcionalna polja koja sadrže standardizirane kodove kako bi uputili na mrežni protokol koji PPP enkapsulira. Svaki NCP obavlja specifičan posao koji zahtjeva njegov odgovarajući mrežni protokol. Različite NCP komponente enkapsuliraju i dogovaraju opcije za više mrežnih protokola.

3.3. Autentifikacijski protokoli

Kod PPP-a LCP je odgovoran za uspostavljanje, konfiguriranje i testiranje veze. Dio procesa konfiguracije je primjena raznih opcija koje su već navedene u odjeljku o LCP-u. Jedna od opcija je i autentifikacijski protokol koji se dogovara prije nego se dopusti prijenos podataka preko veze. Lokalni uređaj koji obavlja autentifikaciju se na engleskom jeziku naziva *authenticator*, a uređaj koji se autentificira se naziva *peer*.

Usmjerivač podržava dva autentifikacijska protokola: *Password Authentication Protocol* (PAP) i *Challenge-Handshake Authentication Protocol* (CHAP). Ovi protokoli su primarno korišteni za spajanje uređaja na usmjerivače preko ISDN poziva ili modeme koji su spojeni na sinkrone ili asinkrone ulaze usmjerivača, ali se autentifikacija može koristiti za mrežne konekcije također.

Nakon što je PPP veza uspješno uspostavljena, počinje opcionalna autentifikacijska faza prije nego se nastavi dalje, a nastavak je moguć jedino ako uspješno prođe autentifikacija na oba kraja veze.

3.3.1 *Password Authentication Protocol* (PAP)

Password Authentication Protocol (PAP) je poprilično jednostavan autentifikacijski protokol koji omogućava *peer*-u da dokaže svoj identitet tako da neprestano šalje korisničko ime i lozinku prema autentifikatoru dok gad autentifikator ne potvrdi i ne uspostavi vezu. U ovom slučaju *peer* zahtjeva autentifikaciju dok autentifikator samo vraća odgovor na zahtjev. Pojednostavljena shema je prikazana na slici 3.4.

Prenesene lozinke ovim protokolom nisu kriptirane i zato što *peer* uvijek koristi isti par korisničkog imena i lozinke, pa lozinka nema prave zaštite od pokušaja napada. PAP omogućava sličnu razinu sigurnosti kao i normalna udaljena prijava.

3.3.2 *Challenge-Handshake Authentication Protocol* (CHAP)

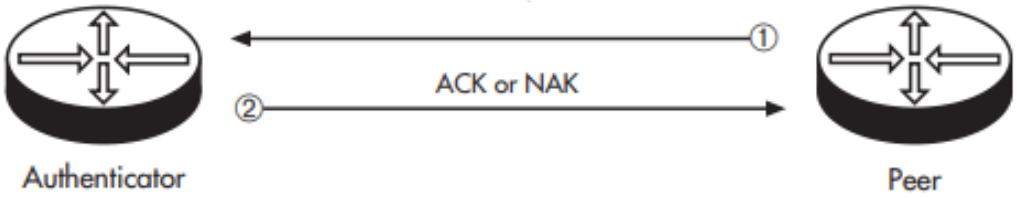
Challenge-Handshake Authentication Protocol (CHAP) je robusniji protokol koji omogućava autentifikaciju i kod *Link Establishment* faze i periodičnu verifikaciju tijekom *Network-Layer Protocol* faze.

CHAP kontrolira autentifikator koji šalje *challanger* poruku koja sadrži identifikator i posebnu vrijednost prema *peer*-u. *Peer* odgovara s korisničkim imenom, odgovarajućom lozinkom i posebnom vrijednosti, ali u posebnom obliku poznatom samo komunikatorima. Zatim autentifikator provjerava primljenu vrijednost, koristi korisničko ime da provjeri lozinku u posebnoj bazi podataka te ako su vrijednosti točne autentifikacija je odobrena u drugom slučaja prekida

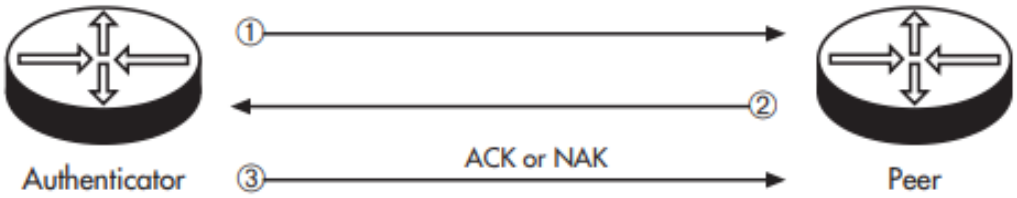
se veza. Pojednostavljena shema je prikazana na slici 3.5.

Ova provjera se osim na početku odvija i periodično tijekom *Network-Layer Protocol* faze kako bi se provjerilo da nema promjene na vezi. Svaka provjera koristi druge specijalne vrijednosti. Vrijednosti nisu periodične i gotovo nemoguće su za predvidjeti, što znači da je ova metoda autentifikacije sigurnija od napada kada je usporedimo s PAP metodom

CHAP se zasniva na činjenici da se lozinka ne šalje direktno u poruci nego je kriptirana te da je lozinka poznata objema stranama veze.



SL. 3.4: *Password Authentication Protocol shema*



SL. 3.5: *Challenge-Handshake Authentication Protocol shema*

4. KORIŠTENE TEHNOLOGIJE I ALATI

U ovom poglavlju kratko je predstavljena i opisana tehnologija i alati korišteni u radu.

4.1. MikroTik

MikroTik je Latvijska tvrtka osnovana 1966. godine koja se bavi izradom softvera i hardvera za internetsko povezivanje. Razvila je RouterOS softver za usmjerivače koje koriste u svojim proizvodima. Za praktični dio ovoga rada koriti će se upravo MicroTik usmjerivači (Slika 4.6) te njihov softver i bežični protokol nv2.

4.1.1 Nv2 protokol

Nv2 protokol je bežični protokol razvijen od tvrtke MikroTik kako bi se koristio uz njihove inovativne bežične usmjerivače. Nv2 je baziran na *Time Division Multiple Access* (TDMA) tehnologiji koja je naprednija od *Carrier Sense Multiple Access* (CSMA) tehnologije korištene u starijim uređajima. TDMA tehnologija rješava mnoge probleme koje su njezini prethodnici imali i zato nudi poboljšanu propusnost i smanjeno kašnjenje. Tako se za Nv2 protokol može reći da su mu dobre strane to što nudi korisnicima bolji propusti podataka i stabilniju vezu i sve to ga čini pogodnim korištenje u mrežama s više točaka. No naravno Nv2 ima i slabiju stranu, a ona je ta da je protokol ograničen na MikroTik usmjerivače, bilo koji drugi usmjerivač ne može se koristit s Nv2 protokolom te također Nv2 se ne može koristiti u kombinaciji s drugim starijim protokolima. [4]

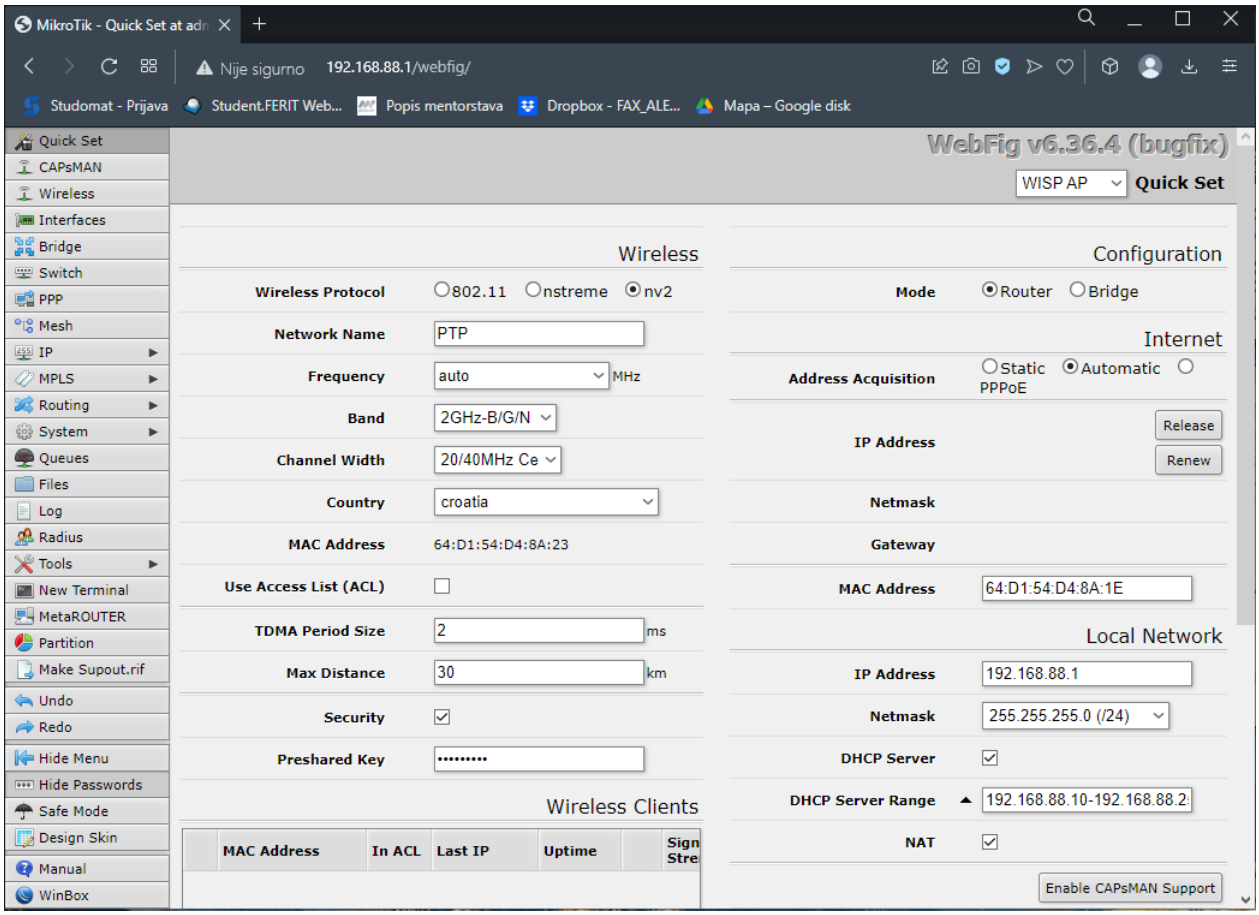
SL. 4.6: *MikroTik usmjerivač*

4.2. Winbox

Winbox je mali program koji omogućava administrativne poslove na MikroTik usmjerivačima, korištenje je brzo i jednostavno. Izvorno je napravljen za *Windows* sustave, ali može biti pokrenut na *Linux*-u ili *MacOSX*-u koristeći *Wine*. Sve *Winbox* funkcionalnosti su najbliže moguće funkcionalnostima konzole. Neke napredne i kritične konfiguracije sustava nisu moguće iz *Winbox*-a , kao naprimjer promjena MAC adrese, itd.

Winbox aplikacija može biti direktno skinuta sa usmjerivača. Tako da se u internet preglednik napiše IP adresu usmjerivača i na stranica koja se otvori (slika 4.7) može se jednim klikom na *Winbox* opciju skinuti *winbox.exe* datoteku. A također samim upisivanjem adrese u preglednik pristupamo internet verziju *Winbox*-a s koje se također može upravljati usmjerivačem.

Kao što se može vidjeti sa slike 4.8 krajnje lijevo se nalazi izbornik s prečacima za lakše i brže upravljanje usmjerivačem.



SL. 4.7: *Web Winbox aplikacija*

4.2.1 Sučelje aplikacije

Na slici 4.8 se može vidjeti početno sučelje *Winbox* aplikacije za *Windows* računala. U nastavku će se objasniti neke od prečaca s izborne trake lijevo. Prije nego se krene dalje, kada je računalo povezano s usmjerivačem njegovu MAC adresu moguće je vidjeti pod stavkom *Session* u gornjem lijevom uglu prozora. Tamo se nalaze i još opcija za sigurni način rada te opcije za vračanje promjena. Od elementa s lijeve trake može se izdvojiti *Quick Set* opciju koja služi za brzo automatsko konfiguriranje usmjerivača. *Wireless* opciju koja će biti poprilično korištena tijekom izrade mreže od točke do točke. U njoj se upravlja postavkama bežičnog povezivanja usmjerivača. *Bridge* opcija gdje se može upravljati usmjeravanje IP adresa koje se šalju i primaju na priključke usmjerivača. *Log* opcija koja može pružiti nekakve podatke o mreži. *New terminal* otvara terminal u kojem je moguće pomoću komandi odraditi nekakve akcije na usmjerivaču. Postoje još mnoge opcije koje nisu toliko važne za zadatak pa neće biti ovdje posebno objašnjene.

SL. 4.8: *Početno sučelje Winbox aplikacije*

5. USPOSTAVLJANJE MREŽE OD TOČKE DO TOČKE

U ovom poglavlju je prikazano kako uspostaviti jednostavnu mrežu od točke do točke. Korištena su dva osobna računala koja uspostavljaju *point-to-point* vezu preko dva MikroTik usmjerivača.

5.1. Fizičke komponente

Od fizičkih komponenti, koriste se dva prijenosna računala te dva MikroTik usmjerivača, svako računalo je spojeno s jednim usmjerivačem pomoću mrežnog kabela. Konačan spoj je prikazan na slici 5.9, a shema spoja na slici 5.10.

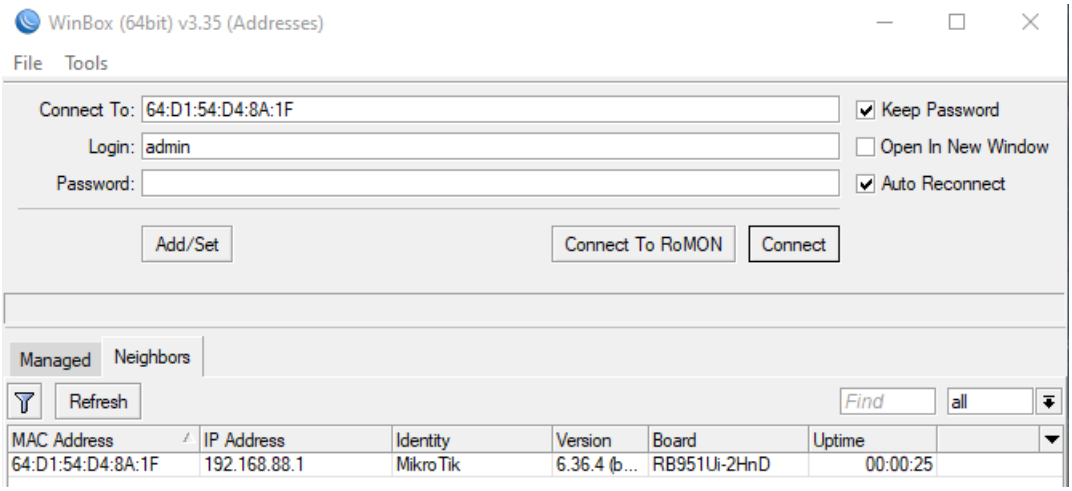
SL. 5.9: *Shema spajanja fizičkih komponenti*

SL. 5.10: *Spojene komponente prema shemi*

5.2. Uspostava veze u Winbox-u

Ako se želi koristiti računala kako bi napravili mrežu od točke do točke potrebno je prvo osigurati da se računala mogu spojiti samo preko usmjerivača. Zato im je potrebno isključiti sva mrežna povezivanja osim onoga povezivanja s usmjerivačem te isključiti vatrozid kako ne bi stvarao probleme u daljnjem radu.

Nakon što su računala pripremljena potrebno je pripremiti i usmjerivače. Pomoću alata Winbox se povezuje na usmjerivač tako što se odabire IP adresu usmjerivača među ponuđenima te se stisne gumb *Connect* kao što je prikazano na slici 5.11. Nakon što se računalo povezalo na usmjerivač potrebno je usmjerivač resetirati na tvorničke, zadane postavke. To se može odraditi u terminalu usmjerivača koristeći naredbu: *system reset-configuration*. Postupak je potrebno odraditi na oba usmjerivača. Valja spomenuti kako jedan usmjerivač ima MAC adresu 64:D1:54:D4:8A:1F a drugi D4:CA:6D:F1:73:55.



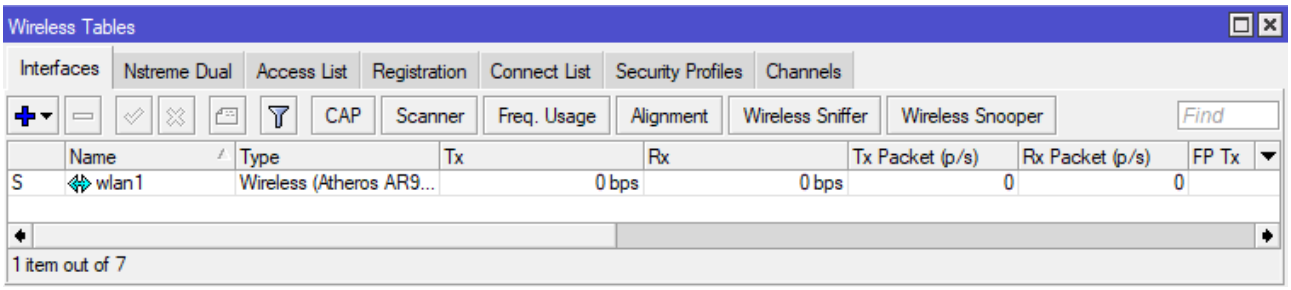
SL. 5.11: *Povezivanje s usmjerivačem*

5.3. Konfiguracija prve točke

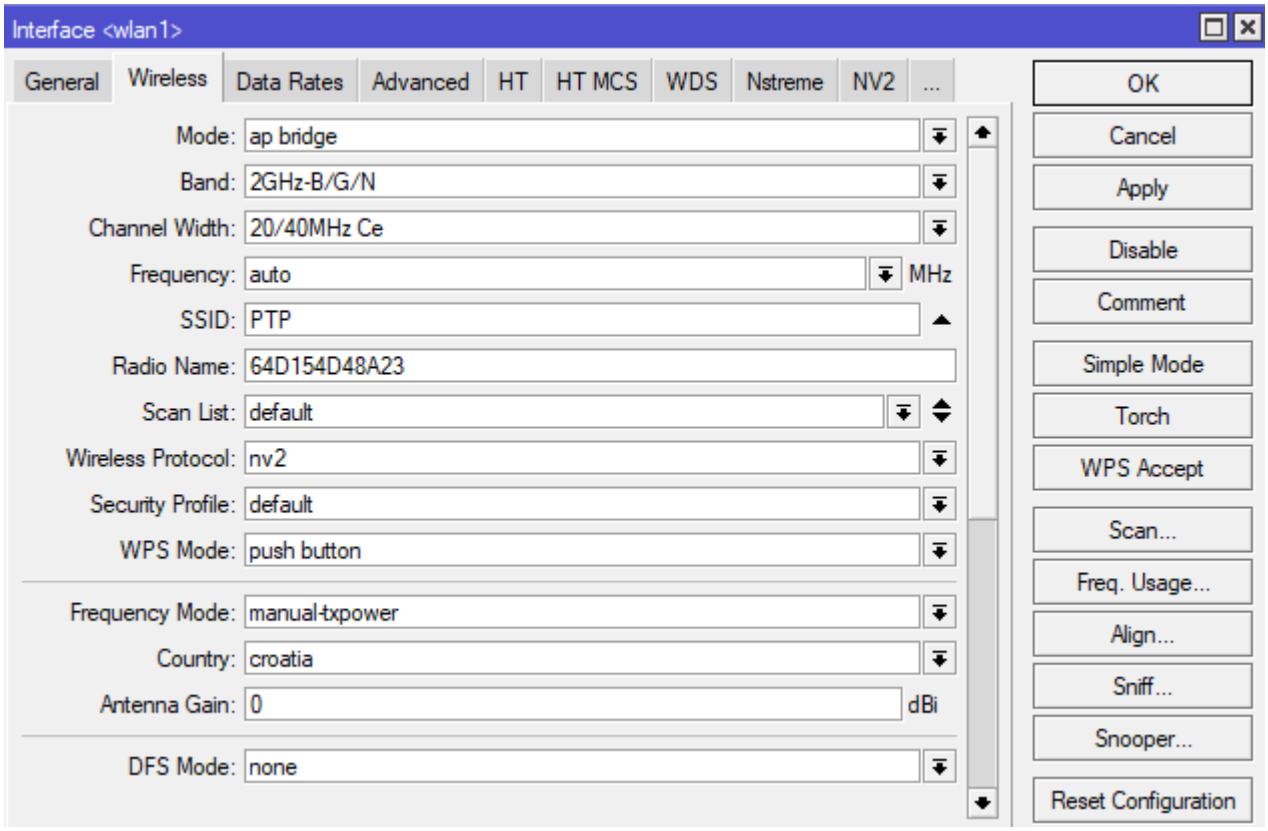
Nakon što je sve spremno započinje se s uspostavom veze i prilagođavanjem konfiguracije. Kreće se s konfiguracijom prve točke.

Za početak potrebno je odabrati *Wireless* prozor u kojem se nalazi "*wlan1*" stavka (slika 5.12). Potrebno je otvoriti *wlan1* stavku te u podstavci *Wireless* promijeniti konfiguraciju tako da *Mode* postavimo u *ap bridge*, poželjno je promijeniti SSID, u ovom slučaju je postavljen u "PTP", *Wireless protocol* postaviti u *nv2* te na kraju promijeniti opciju *Country* u zemlju gdje se nalazimo trenutno. Ovo će omogućiti prijenos podataka iz točke jedan prema van koristeći protokola nv2 koji je poseban protokol dizajniran od strane MikroTik-a i omogućuje veću brzinu i smanjenje kašnjenja u odnosu na druge protokole. Nakon što je sve gore navedeno odrađeno potrebno je pritiskom na *Apply* sačuvati promijene kao što je prikazano na slici 5.13.

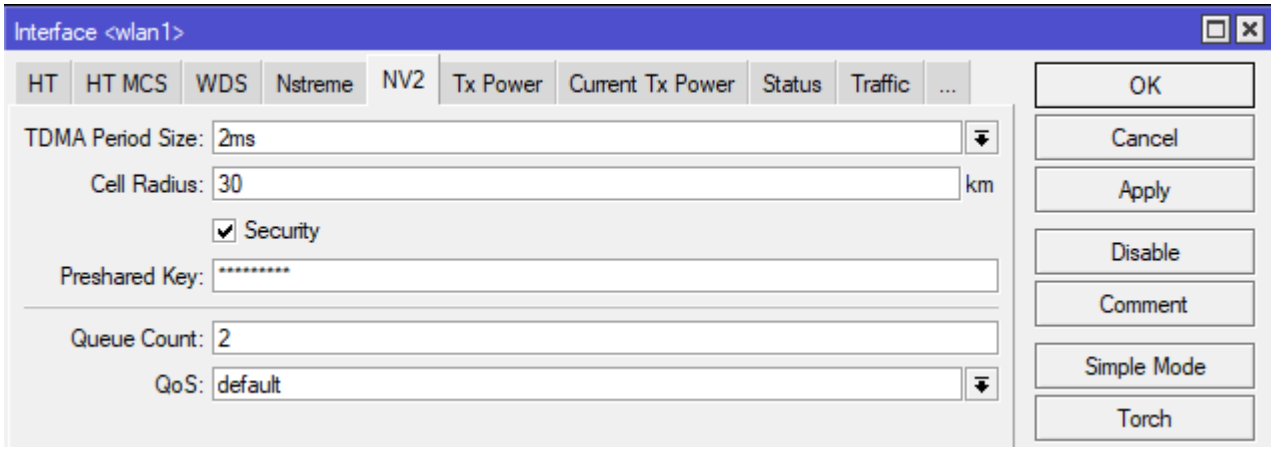
Nakon odrađenih izmjena potrebno je još i dodati sigurnosnu mjeru, tako što će se otići u *nv2* podstavku te označiti kvadratić *Security* i u *Preshared Key* upisati željenu lozinku te sve to ponovno sačuvati pritiskom na tipku *Apply* (slika 5.14.



SL. 5.12: *Wireless stavka na točki jedan*



SL. 5.13: *wlan1 konfiguracija*



SL. 5.14: *Dodavanje zaporke na točki jedan*

5.4. Konfiguracija druge točke

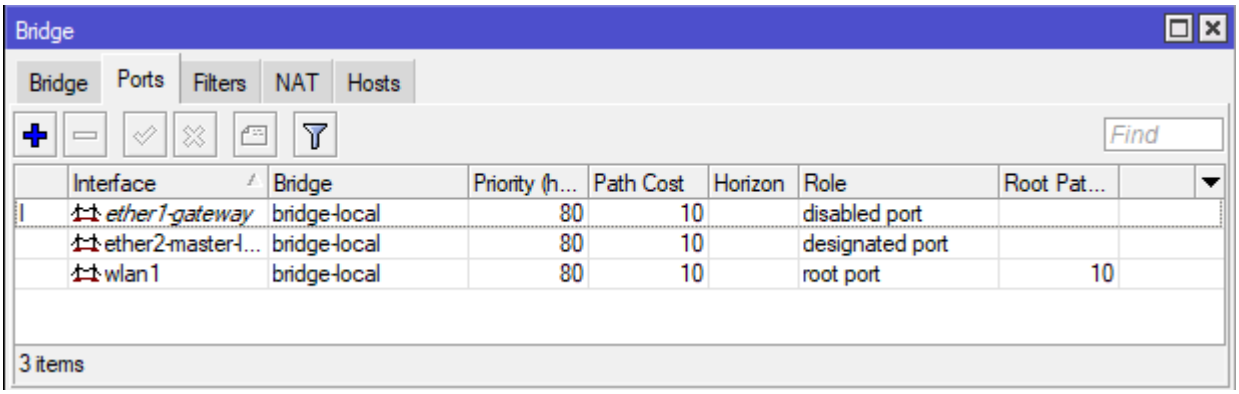
Nakon što je odrađena konfiguracija prve točke potrebno je i konfigurirati drugu točku mreže. Nakon što se konfigurira drugu točku trebala bi biti uspješno uspostavljena vezu između točaka.

Prva stvar koju je potrebno napraviti na drugoj točki je u meniju Winbox-a odabrati stavku *Bridge* te unutar nje dodati *Interface ether1-gateway* s *Bridge* opcijom postavljenu u *bridge-local*. Ovo će omogućiti da svi priključci na usmjerivaču dva (*ether2* i *wlan1*), uspješno preko mosta (engl. *bridge*) prime IP adrese s drugih točaka, u ovom slučaju s točke jedan (slika 5.15).

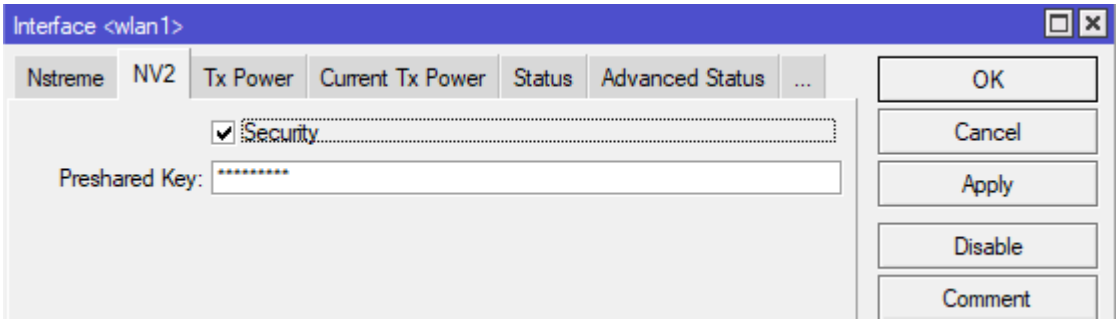
Potom je potrebno otići u *Wireless* prozor i konfigurirati *wlan1* druge točke tako da pod *Wireless*, postaviti *Mode* u *station bridge*, postaviti SSID u isti kao na prvoj točki, dakle u "PTP" te odabrati *nv2* kao *Wireless protocol* i postaviti odgovarajuću državu pod *Country* (slika 5.17).

Nakon toga potrebno je dodati točnu zaporku kako bi se uređaji mogli povezati, potrebno je u podstavci *nv2* označiti kvadratić *security* i upisati istu zaporku koja je postavljena u točki jedan.

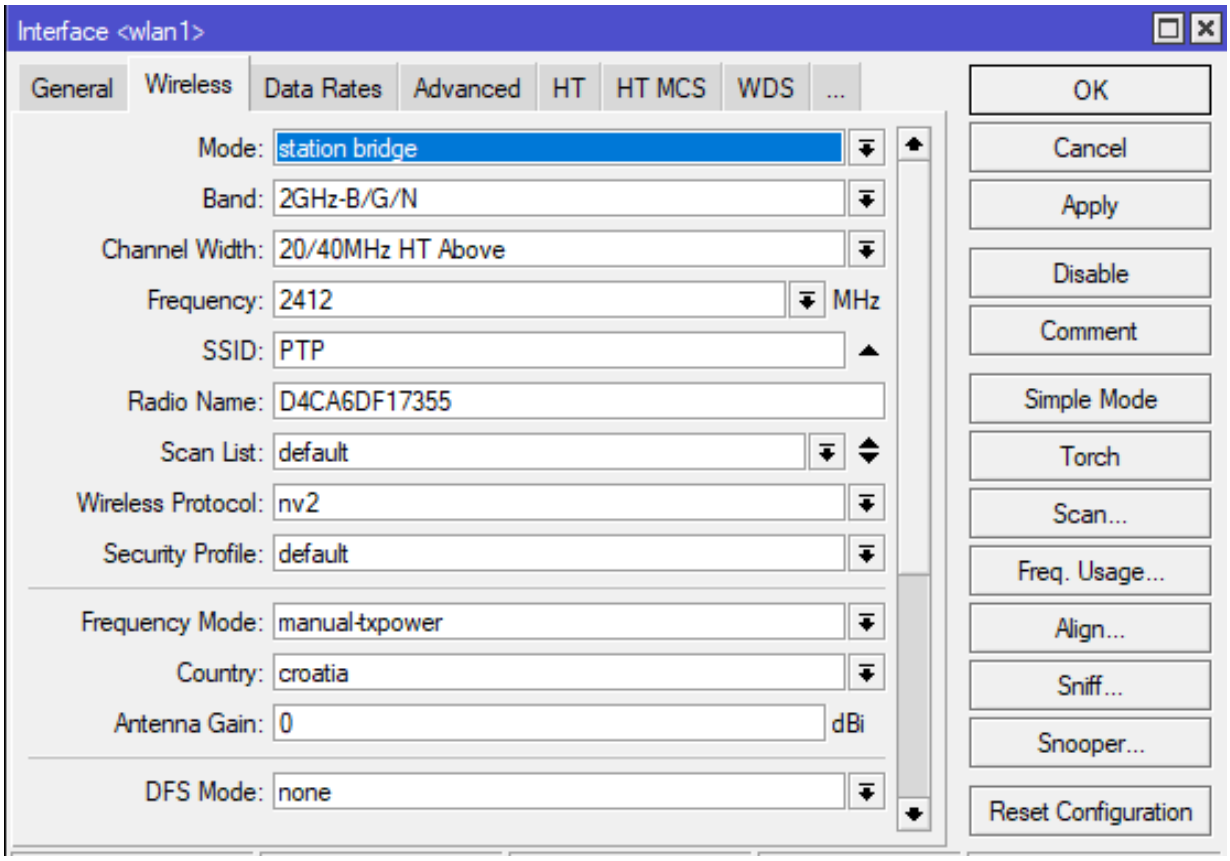
Za kraj je potrebno još modificrati *DHCP Client* postavke. Potrebno je promijeniti DHCP klijenta u *bridge-local*, to će nam omogućiti da sve adrese koje se primaju u točki dva od točke jedan budu proslijeđene na *bridge-local*, a zbog promjene koje su već bile napravljene kada se dodao *Interface ether1-gateway* svi priključci usmjerivača će dobiti IP adrese. I od ovoga trenutno status klijenta je povezan (engl. *bound*).



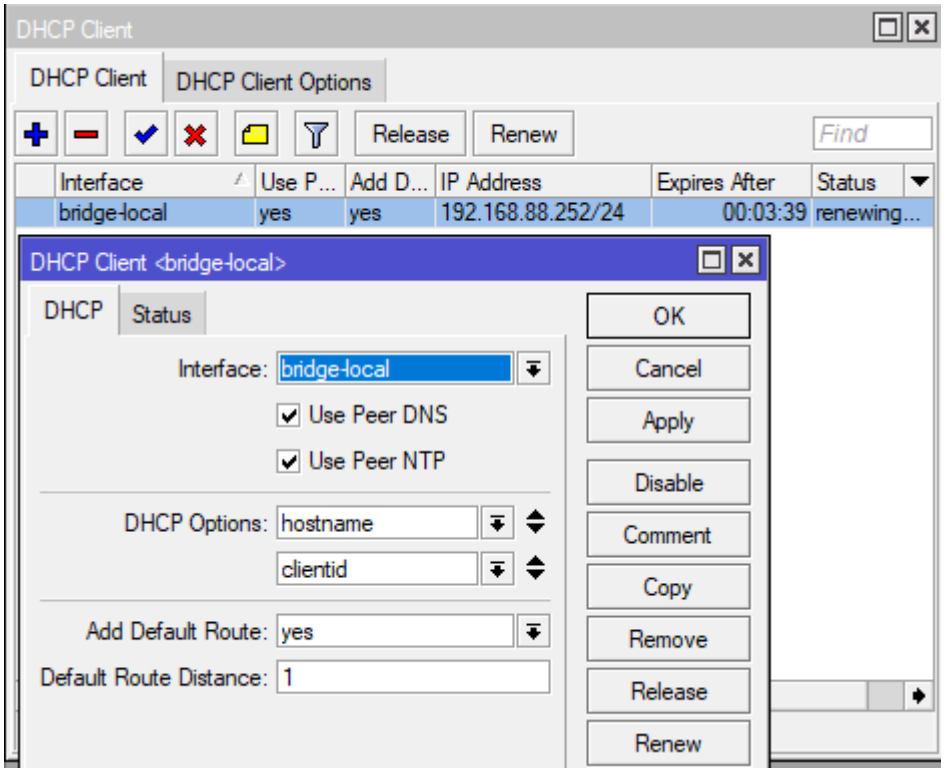
SL. 5.15: *Dodavanje ether1-gateway u stavci Bridge*



SL. 5.16: *Dodavanje zaporke na točki dva*



SL. 5.17: *wlan1 konfiguracija*

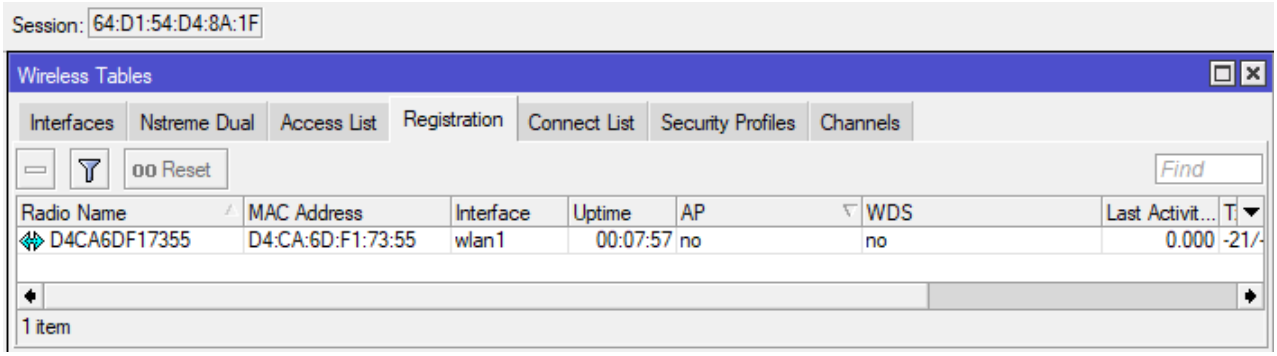


SL. 5.18: *Modifikacija DHCP Client-a*

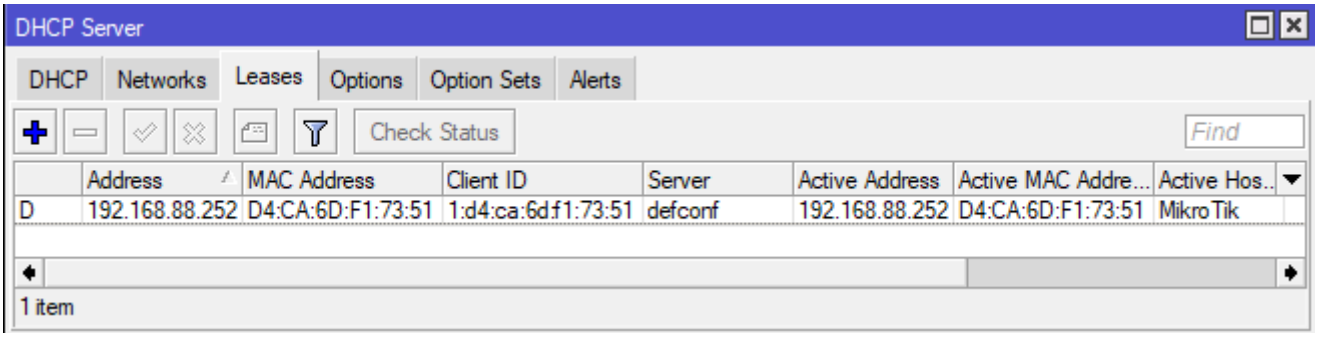
5.5. Dokaz uspostavljene veze

Nakon konfiguracije mreža je uspostavljena i omogućena je komunikacija. A to se može potvrditi tako da se u *Wireless* prozoru odabere podstavku *Registration*, tamo se mogu pronaći podatci kao MAC adrese i ostale podatci uređaja s kojim je usmjerivač spojen i kao što je prikazano na slici 5.19 usmjerivač jedan je spojen s usmjerivačem dva preko sučelja *wlan1*, također vidi se koliko dugo veza traje te ostale pojedinosti veze.

Također može se vidjeti uređaj s kojim je usmjerivač povezan ako odemo u prozor *DHCP Server* (slika 5.20).



SL. 5.19: *Registrations na točki jedan*



SL. 5.20: *DHCP Server na točki jedan*

6. ZAKLJUČAK

U ovom završnom radu prikazano je kreiranje jednostavne mreže od točke do točke. Kako bi se moglo razumjeti za što služi i što je mreža od točke do točke, bilo ju je nužno objasniti, predstaviti topologiju mreže te navesti njezine prednosti i mane. Također bilo je nužno objasniti protokol *Point-to-Point* koji se koristi prilikom prijenosa podataka od jedne točke ka drugoj u mreži od točke do točke, arhitektura, enkapsulaciju i način zaštite podataka u njemu. Prilikom uspostave jednostavne mreže od točke do točke koristila se tehnologija tvrtke MikroTik, njihovi usmjerivači i softver. Kao alat za konfiguraciju samih točaka u mreži bio je korišten Winbox koji je također napravljen od iste tvrtke. Valja primijetiti da ova vrsta mreža nije rijetka u svijetu i da postoji još mnogo drugih tehnologija i uređaja s kojim bi se mogao odraditi zadatak, no dostupnost i jednostavno korištenja čine MikroTik pravim izborom.

LITERATURA

[1] A. Ortega, V. A. Bettachini, J. I. Alvarez-Hamelin, PDF datoteka, Point-to-point and Point-to-multipoint CDMA Access Network with Enhanced Security , 2009.

[2] Alliedtelesis, Point-to-Point Protocol (PPP) Feature Overview and Configuration Guide, 2016.

[3] International Journal of Computer Applications Technology and Research, Izdanje 11, Advantages and Disadvantages of Mikrotik Nv2 Protocol on Wireless Networks, 2015.

[4] MikroTik inc, MirkoTik Manual:Nv2

[5] W. Simpson, Daydreamer, The Point-to-Point Protocol (PPP), 1993.

[6] Ivan Testa, Računalne mreže i umrežavanje , završni rad, 2019.

[7] Izv. prof. dr. sc. Krešimir Grgić, „KM PR1 - Uvod u komunikacijske mreze“ [Powerpoint prezentacija], FERIT, 2021.

[8] Gl Comunications Inc, PPP-MLPPP-Overview-Presentation, 2021.

SAŽETAK I KLJUČNE RIJEČI

U ovom završnom radu prikazano je kreiranje jednostavne mreže od točke do točke. Kako bi se moglo razumjeti za što služi i što je mreža od točke do točke, bilo ju je nužno objasniti, predstaviti topologiju mreže te navesti njezine prednosti i nedostatke. Također bilo je nužno objasniti protokol *Point-to-Point* koji se koristi prilikom prijenosa podataka od jedne točke ka drugoj u mreži od točke do točke, arhitektura, enkapsulaciju i način zaštite podataka u njemu. Prilikom uspostave jednostavne mreže od toče do točke korištena je tehnologija tvrtke MikroTik, njihovi usmjerivači i softver.

KLJUČNE RIJEČI

Mreže, MirkoTik, protokol, *Point-to-Point*, Winbox

CREATING A POINT-TO-POINT NETWORK

SUMMARY

In this paper, a simple Point-to-Point Network was established. To understand for what is this Point-to-Point Network used and what it is,it was important to explain it, to show topology and to list some advantages and disadvantages of using the point-to-point network. Also it was necessary to explain Point-to-Point protocol which is used in point-to-point networks, architecture, encapsulation, and ways of protection of data. Tools and technology which were used in creating a point-to-point network are made by company MikroTik.

KEYWORDS

Networks, MikroTik, protocol, *Point-to-Point*, Winbox

ŽIVOTOPIS

Patrik Juzbašić rođen je 30.07.1999. godine u Vinkovcima. 2014. godine završava Osnovnu školu Ivana Kozarca Županja u Županji te upisuje Gimnaziju u Županji, smjer Prirodoslovno-matematička gimnazija. Gimnaziju završava 2018. godine kada upisuje preddiplomski studij računarstva na Fakultetu elektrotehnike računarstva i informacijskih tehnologija koji je dio sveučilišta Josipa Jurja Strossmayera u Osijeku.