Kreiranje višestrukih identifikatora postavljenog servisa

Kuna, Renato

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni preddiplomski studij Elektrotehnike, smjer Komunikacije i Informatika

KREIRANJE VIŠESTRUKIH IDENTIFIKATORA POSTAVLJENOG SERVISA

Završni rad

Renato Kuna

Osijek, 2021.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

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

Osijek, 09.09.2021.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada na preddiplomskom sveučilišnom studiju

Ime i prezime studenta:	Renato Kuna
Studij, smjer:	Preddiplomski sveučilišni studij Elektrotehnika i informacijska tehnologija
Mat. br. studenta, godina upisa:	4062, 21.07.2015.
OIB studenta:	92204798316
Mentor:	Izv. prof. dr. sc. Krešimir Grgić
Sumentor:	
Sumentor iz tvrtke:	
Naslov završnog rada:	Kreiranje višestrukih identifikatora postavljenog servisa
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Predložena ocjena završnog rada:	Vrlo dobar (4)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 2 razina
Datum prijedloga ocjene mentora:	09.09.2021.
Datum potvrde ocjene Odbora:	22.09.2021.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

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

IZJAVA O ORIGINALNOSTI RADA

Osijek, 27.09.2021.

Ime i prezime studenta:	Renato Kuna
Studij:	Preddiplomski sveučilišni studij Elektrotehnika i informacijska tehnologija
Mat. br. studenta, godina upisa:	4062, 21.07.2015.
Turnitin podudaranje [%]:	12%

Ovom izjavom izjavljujem da je rad pod nazivom**: Kreiranje višestrukih identifikatora postavljenog servisa**

izrađen pod vodstvom mentora Izv. prof. dr. sc. Krešimir Grgić

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

Kreiranje višestrukih identifikatora postavljenog servisa omogućuje postavljanje različitih sigurnosnih zaštita u lokalnoj mreži nekog kućanstva ili poduzeća. Primjerice, možemo kreirati SSID (eng. *Service Set Identifier*) naziva "Ured" koji će spajati više računala na printer i omogućiti međusobnu razmjenu dokumenata i drugi SSID naziva "Klijent" koji pridošlim klijentima u ured omogućuje samo spajanje na internet [1]. U javnim i poslovnim prostorima vrlo je bitno postaviti značajna imena SSID-eva kako bi korisnici lakše pronašli traženu Wi-Fi mrežu.[2]

Vrlo je bitno znati da korištenje SSID-a kao jedine sigurnosne mjere nije dobro za cjelokupnu sigurnost mreže. SSID je poprilično lako pronaći korištenjem programa koji se nazivaju "snifferi". Snifferima se otkrivaju skriveni SSID-evi preko kojih se može pristupiti nezaštićenoj mreži. Iz tog razloga, SSID bi se prvenstveno trebao koristiti za segmentiranje mreže, a ne kao jedinu sigurnosnu mjeru.

U drugom poglavlju ovog završnog rada govorit će se o WLAN (eng. *Wireless Local Area Network*) mrežama, njihovim načinima implementacije i načinima lociranja WLAN mreža.

U trećem poglavlju govorit će se općenito o pojmu identifikatora postavljenog servisa (SSID) i njegovom utjecaju na sigurnost WLAN mreža.

U četvrtom poglavlju opisati će se korištena oprema i simulator koji su potrebni za obavljanje simulacije kreiranja višetrukih identifikatora postavljenih servisa.

U petom poglavlju biti će prikazan detaljan postupak i opis odrađene simulacije za kreiranje višestrukih identifikatora postavljenih servisa.

1.1. Zadatak završnog rada

Identifikator postavljenog servisa (SSID) jedinstveni je ID koji se koristi za imenovanje bežičnih mreža. Kad se više bežičnih mreža preklapa na određenoj lokaciji, SSID-ovi osiguravaju da se podaci šalju na točno odredište. SSID je niz znakova koji osigurava da se naziv mreže razlikuje od ostalih obližnjih mreža. U ovom radu je potrebno konfigurirati SSID u usmjerivaču tako da svaki paket poslan bežičnom mrežom koja uključuje. SSID osigurava da podaci koji se šalju bežičnim putem stignu na točno odredište.

2. BEŽIČNA LOKALNA MREŽA (WLAN)

WLAN (engl. *Wireless Local Area Network*) je komunikacijski sustav koji pomoću elektromagnetskih valova prenosi podatke od jedne do druge točke. Ukoliko se elektromagnetski valovi prenose na više različitih frekvencija, tada je moguće postaviti više nositelja valova kako nebi došlo do međusobne interferencije valova i stvaranja potencijalnih smetnji u prijenosu. WLAN se implementira kao alternativa ili kao proširenje žičanih sustava. [3, str. 14]

2.1. Prednosti WLAN-a

Prednosti wireless mreža naspram žičnih su:

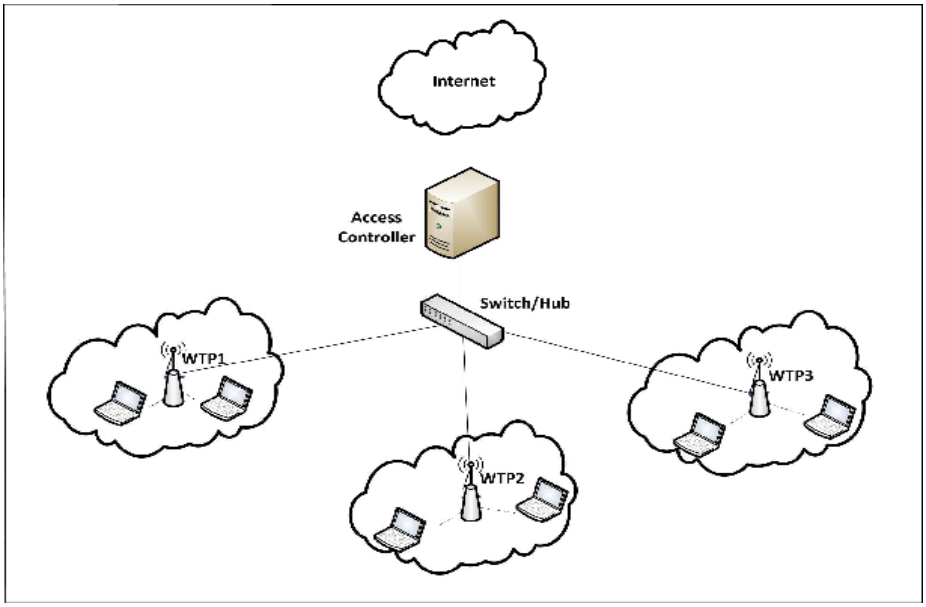
- Mogući pristup mreži sa bilo koje lokacije unutar dometa pristupnih točki
- Korisnik nije potreban biti vezan za jedno mjesto (npr. stol na kojem se nalazi računalo), nego se može slobodno kretati u prostoru dometa i ostati spojen na internet.
- Proširivost mreže je znatno lakša jer nije potrebno nadodavati kablove za spajanje na internet
- Manja cijena postavljanja i proširenja [4]

2.2. Implementacije WLAN-a

Postoje tri načina implementacije bežične lokalne mreže:

1. Centralizirana implementacija:

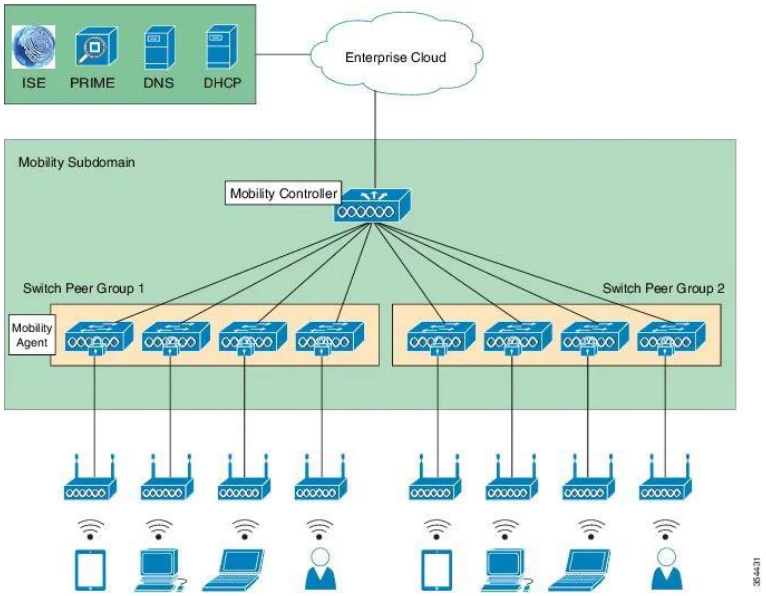
Centralizirana implementacija je najrašireniji tip implementacije bežičnih mreža. Najviše se koristi u kompleksima gdje su zgrade blisko zbijene. Ovakav raspored učvršćuje bežičnu mrežu, te olakšava moguće proširenje postojeće mreže. Upravljači (engl. *Controller*) su postavljeni u središnjem području mreže.[4]



Slika 2.1. Centralizirana implementacija [5]

2. Konvergirana implementacija:

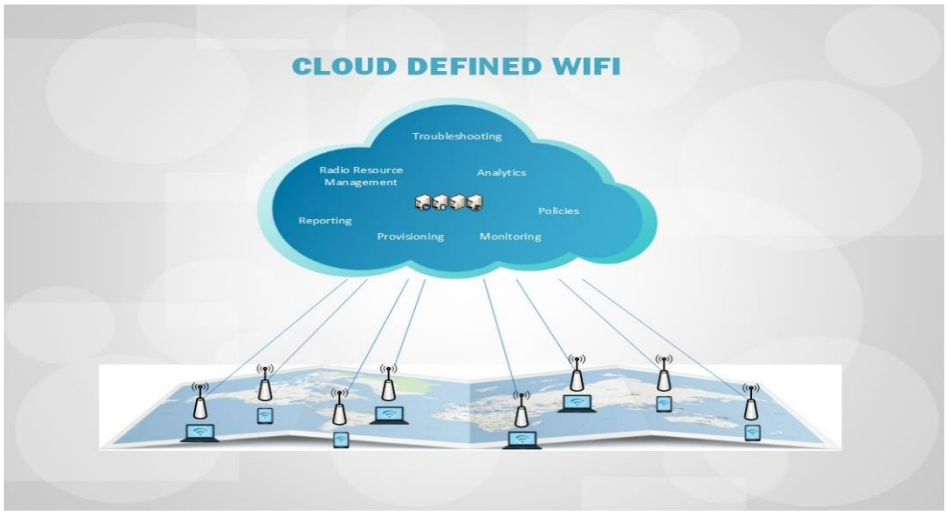
Većinom se koristi za manje lokacije kao što su na primjer kućanstva i manji uredi. Koristi se mješavina bežične i žične mreže spojene putem pristupnih preklopnika (engl. *Acces switch*) koji ima dualnu ulogu preklopnika i upravljača.[4]



Slika 2.2 Konvergirana implementacija WLAN-a [6]

3. Cloud implementacija

Sustav koristi cloud za upravljanje mrežnim uređajima koje nalaze na više različitih lokacija.[4]



Slika 2.3. Cloud implementacija WLAN-a [7]

2.3. Lociranje WLAN-a

Nakon početnog postavljanja i konfiguriranja WLAN uređaja, uređaj pokreće skeniranje okoline kako bi locirao WLAN mreže koje se nalaze u njegovoj blizini. Također, klijentski uređaj pokušava otkriti može li pristupiti nekoj od lociranih mreža. [3, stranica 14, 15]

Prilikom pretraživanja okoline za pronalazak bežične pristupne točke (engl. *Access point, AP*), klijentski uređaj osluškuje tragove koje ostavlja ta pristupna točka. Ti tragovi su identifikatori postavljenog servisa (engl. *Service Set Identifiers, SSID*) i *beacon* okviri (engl. *Beacon Management Frames*) koji omogućavaju klijentskom uređaju spajanje na WLAN mrežu. [3, stranica 15]

Ovisno o korištenom standardu, u WLAN mrežama postoji više različitih podržanih brzina prijenosa. Beacon okvir koji šalje pristupna točka sadrži sve informacije o podržanim brzinama. [3, stranica 17]

Postoje dva tipa skeniranja bežičnih mreža: pasivno skeniranje i aktivno skeniranje. [3, stranica 15]

2.3.1. Pasivno skeniranje

Pasivno skeniranje je postupak skeniranja kojim se određeno vrijeme, nakon inicijalizacije, osluškuje svaki kanal koji sadrži *beacon* okvire. Na temelju informacija koje sadrži *beacon* okvir, uređaj koji provodi skeniranje izrađuje tablicu koja sadrži sve karakteristike dohvaćenih pristupnih točaka. Nakon što uređaj koji provodi skeniranje "čuje" okvir koji sadrži SSID mreže kojoj se želi pridružiti, uređaj se pokušava spojiti na mrežu putem pristupne točke koja je poslala taj *beacon* okvir. [3, stranica 17]

U konfiguracijama WLAN mreža u kojima postoji više pristupnih točaka, te pristupne točke odašilju SSID one mreže kojoj se klijentski uređaj želi pridružiti. Nakon što se uređaj uspješno spojio na mrežu koju želi, uređaj i dalje vrši pasivno skeniranje. To skeniranje se i dalje provodi iz razloga ukoliko se uređaj iz nekog razloga odspoji od pristupne točke, smanjuje se vrijeme potrebno za ponovno spajanje na mrežu.[3, stranica 17, 18]

2.3.1. Aktivno skeniranje

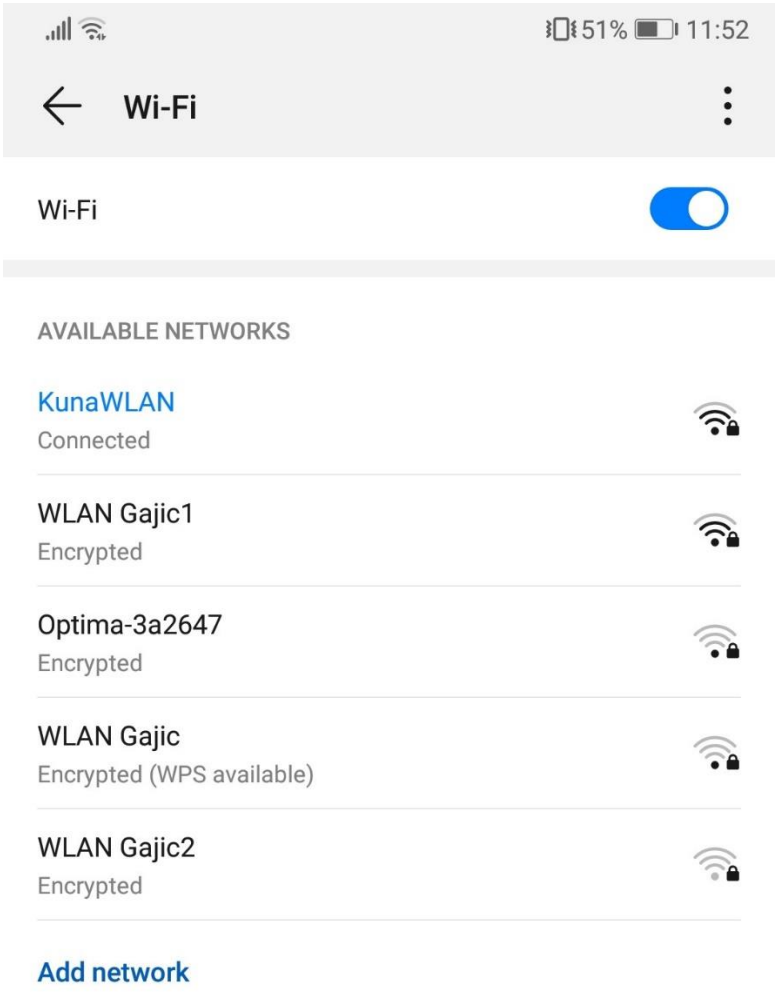
Aktivnim skeniranjem se sa klijentskog uređaja šalje *beacon* okvir koji u sebi sadrži zahtjev za sondiranjem. U povratnom odgovoru mreže, šalje se sondirajući okvir koji ili sadržava SSID mreže kojoj se uređaj želi pridružiti ili sadržava broadcast SSID-a. Aktivnim sondiranjem se traže sve pristupne točke kojim se klijentski uređaj može priključiti na mrežu. Ukoliko je klijentski uređaj pronašao odgovarajući SSID kojim se može spojiti na mrežu, uređaj podnosi autentikacijske i asocijacijske korake kojima će se pridružiti mreži preko te pristupne točke. [3, stranica 18]

3. IDENTIFIKATOR POSTAVLJENOG SERVISA (SSID)

Identifikator postavljenog servisa je jedinstvena, znakovno osjetljiva alfanumerička vrijednost, duljine od 2 do 23 znaka, koja se koristi kao mrežno ime bežičnih lokalnih mreža. [3, stranica 15]

U javnim i poslovnim prostorima vrlo je bitno postaviti značajna imena SSID-eva kako bi korisnici lakše pronašli traženu Wi-Fi mrežu. [2]

SSID se odašilje u *beacon* okvirima, zahtjevima i odgovorima za sondiranje i drugim tipovima okvira. Klijentski uređaj mora koristiti odgovarajući SSID ukoliko se želi pridružiti mreži. Određeni uređaji imaju mogućnost konfiguracije tako da koriste bilo koji SSID. Ukoliko se klijent želi neometano kretati između pristupnih točaka u grupi, klijent i sve pristupne točke moraju biti konfigurirane istim SSID-em. [3, stranica 15]



Slika 3.1. Lista SSID-eva u dometu mobilnog uređaja

3.1. Sigurnost SSID-a

Odabiranje imena za identifikatore postavljanog servisa se koristi u svrhu segmentiranja mreže, kao najjednostavnija sigurnosna mjera, te u procesu pridruživanja mreži. U pravilu, SSID filtriranje bi se trebalo koristiti samo za najosnovniju kontrolu pristupa. Prilikom autentikacije i asocijacije klijenta sa postavljenim servisom koristi se jedan od dva načina autentikacije ili asocijacije:

- Infrastrukturni mod - SSID klijentskog uređaja mora se poklapati sa SSID-om pristupne točke
- Ad-Hoc mod - SSID klijentskog uređaja mora se poklapati sa SSID-om drugih uređaja [3, stranica 123]

Korištenjem *sniffer* programa vrlo je lako pronaći SSID mreže zato što se SSID mreže odašilje u čistom obliku u svakom *beacon* okviru pristupne točke. [3, stranica 123]

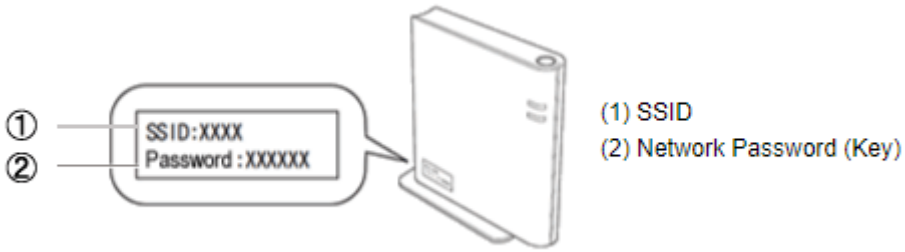
Stoga, pristupne točke nekih proizvođača imaju sposobnost sakriti SSID iz *beacon* okvira ili odgovora na sondiranje. U takvom slučaju, na klijentskom uređaju je potrebno ručno unijeti SSID pristupne točke kako bi se uređaj uspješno pridružio mreži. Sustav koji je konfiguriran na ovaj način naziba se zatvoreni sustav. [3, stranica 123]

Neke od najčešćih pogrešaka vezanih uz korištenje SSID-a u bežičnim mrežama su:

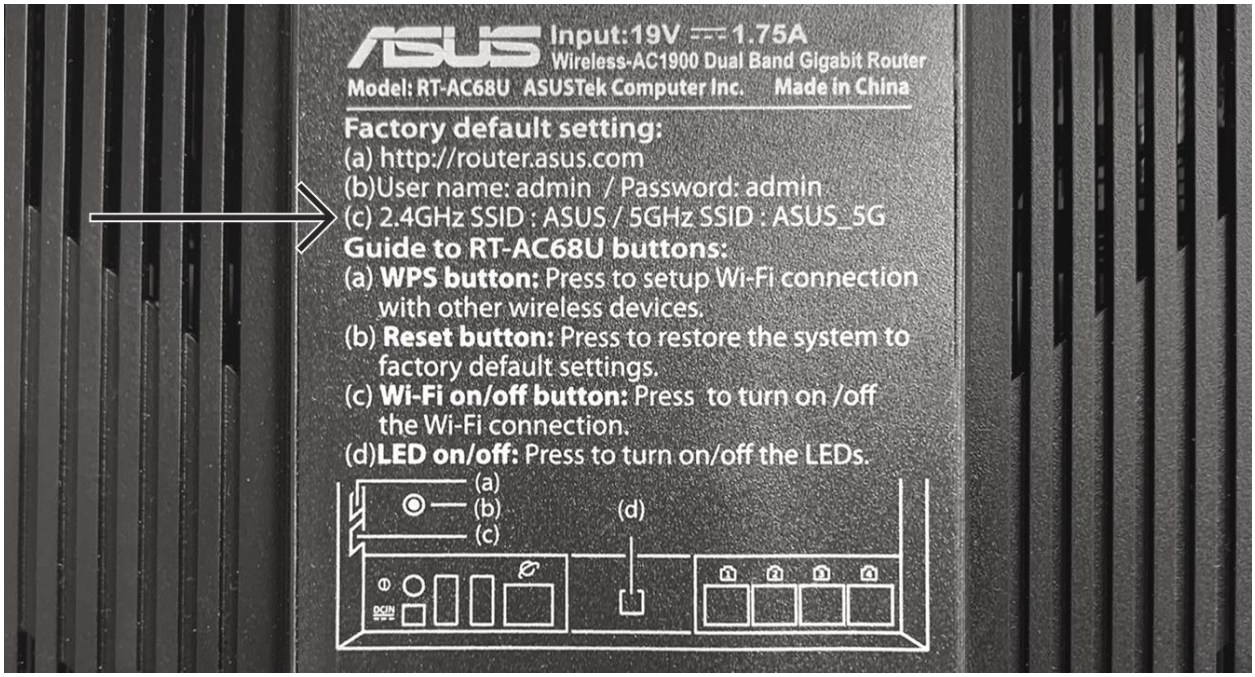
- Korištenje pretpostavljenog SSID-a
- Korištenje SSID imena povezanog s podacima o tvrtci
- Korištenje SSID-a kao jedine sigurnosne mjere u bežičnoj mreži
- Nepotrebno odašiljanje SSID-a [3, stranica 124]

3.1.1 Korištenje pretpostavljenog SSID-a

Korištenjem *sniffera* moguće je pronaći MAC adrese (eng. *Media Access Control Address*) pristupnih točaka. Ti jedinstveni identifikatori MAC adresa koje su dodjeljene svakom proizvođaču se nalaze unutar OUI (engl. *Organizationally Unique Identifier*) tablice koja je javno dostupna. Te se tablice obično mogu pronaći na web stranicama proizvođača. Pretraživanjem OUI tablice napadač može pronaći informaciju o proizvođaču pristupne točke i tako doći do pretpostavljenog SSID-a. [3, stranica 124]



Slika 3.2. Prikaz lokacije pretpostavljenog SSID-a na usmjerivaču [8]



Slika 3.2. Prikaz pretpostavljenog SSID-a na usmjerivaču [9]

3.1.2. Korištenje SSID imena povezanog s podacima o tvrtci

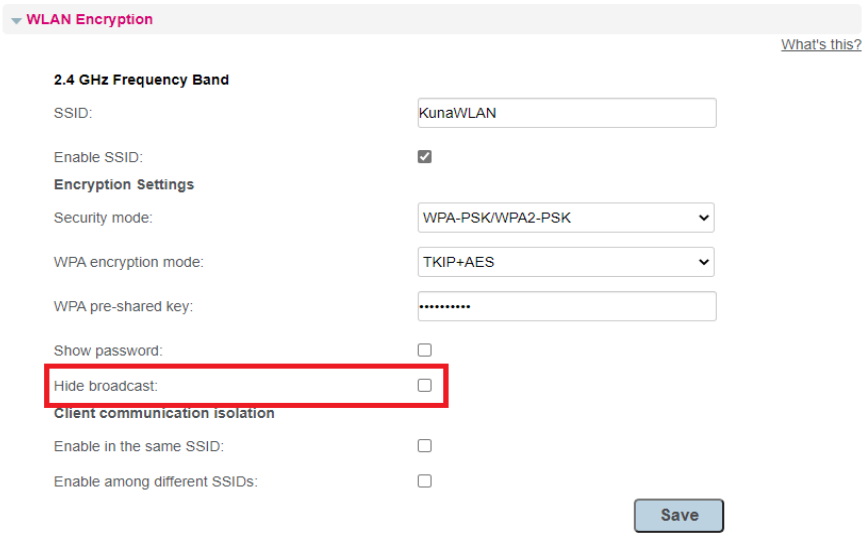
Ukoliko se koristi SSID koji u sebi sadrži podatke o tvrtci, takva konfiguracija predstavlja veliki sigurnosni rizik jer napadaču omogućava laki pronalazak fizičke lokacije tvrtke i njezinih podataka. No, čak i nakon detektiranja bežičnog WLAN-a, nalaženje izvora signala u mnogo slučajeva može zahtijevati mnogo vremena i napora. Kako bi se ovakav rizik u potpunosti uklonio, potrebno je vrijednost SSID-a postaviti na onu vrijednost koja je nevezana uz same podatke tvrtke. [3,stranica124]

3.1.3. Korištenje SSID-a kao jedine sigurnosne mjere u bežičnoj mreži

Ovakav način korištenja SSID-a je posebno rizična sigurnosna mjera jer korisnik samo treba svoj uređaj konfigurirati na SSID mreže i tako se vrlo lako spojiti na mrežu. U pravilu, SSID bi trebao biti korišten samo u potrebe segmentiranja mreže, a ne kao jedinu sigurnosnu mjeru. [3, stranica 124]

3.1.4 Nepotrebno odašiljanje SSID-a

Ukoliko pristupna točka posjeduje mogućnost skrivanja SSID-a iz *beacon* okvira i odgovora sondiranja, potrebno je koristiti tu mogućnost. Ova mogućnost pomaže u odvraćanju slučajnih prisluškivaća od upada u bežične mreže. [3, stranica 124]



Slika 3.3. Prikaz opcije za prestanak odašiljanja SSID-a

4. KORIŠTENA OPREMA I SOFTWARE

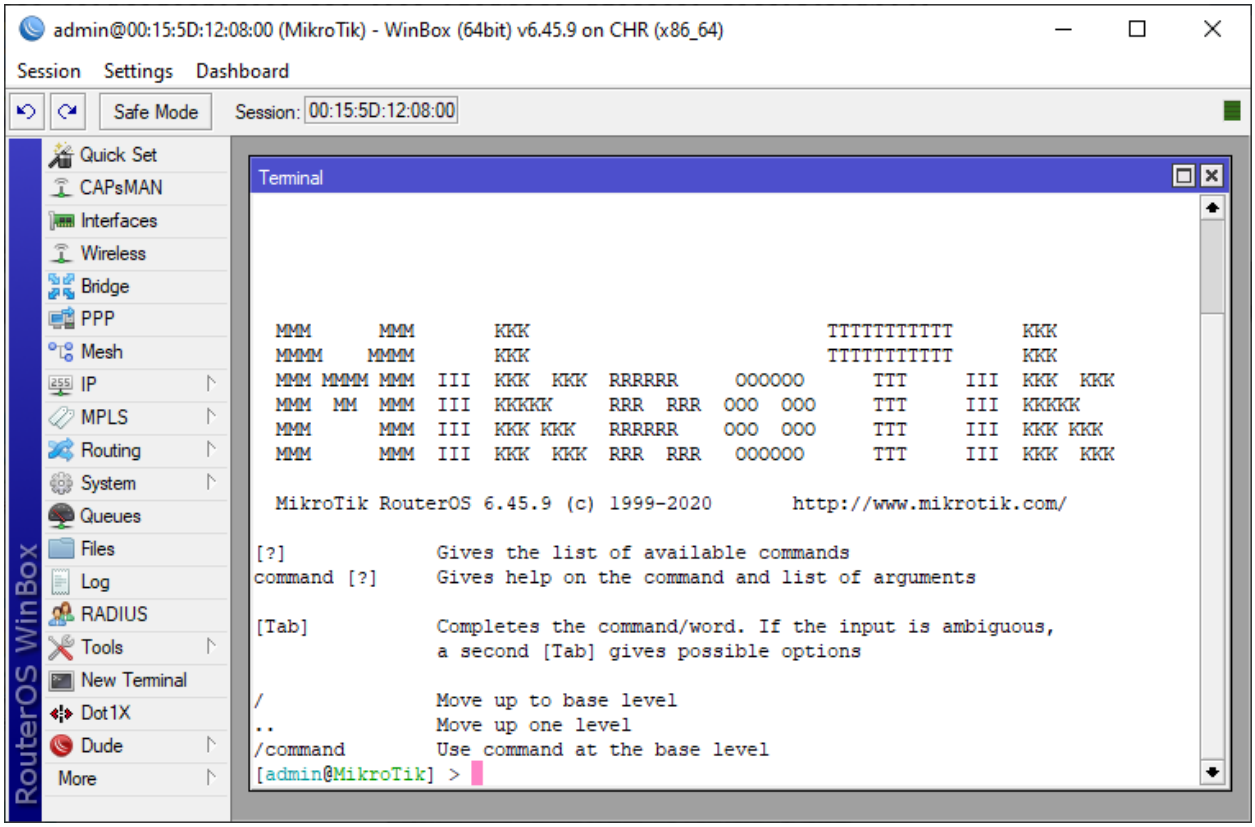
Kako bi se izvršio zadani zadatak završnog rada, za potrebe testiranja koristit će se MikroTik-ov RouterBOARD 951Ui 2HnD usmjerivač i WinBox software.

4.1. MikroTik

MikroTik je Latvijska tvrtka koja je osnovana 1996. godine s ciljem proizvodnje usmjerivača i bežičnih sustava za pružanje internet usluge. 1997. godine izradili su RouterOS operacijski sustav koji pruža opsežnu stabilnost, kontrole i fleksibilnost za razna podatkovna sučelja i usmjeravanje. 2002. godine tvrtka je pokrenula svoj RouterBOARD brand isporučivši svoj prvi hardver. U današnje vrijeme, MikroTik pruža hardware i software za povezivanje putem interneta u većini zemalja diljem svijeta. [10]

4.1.1. RouterOS

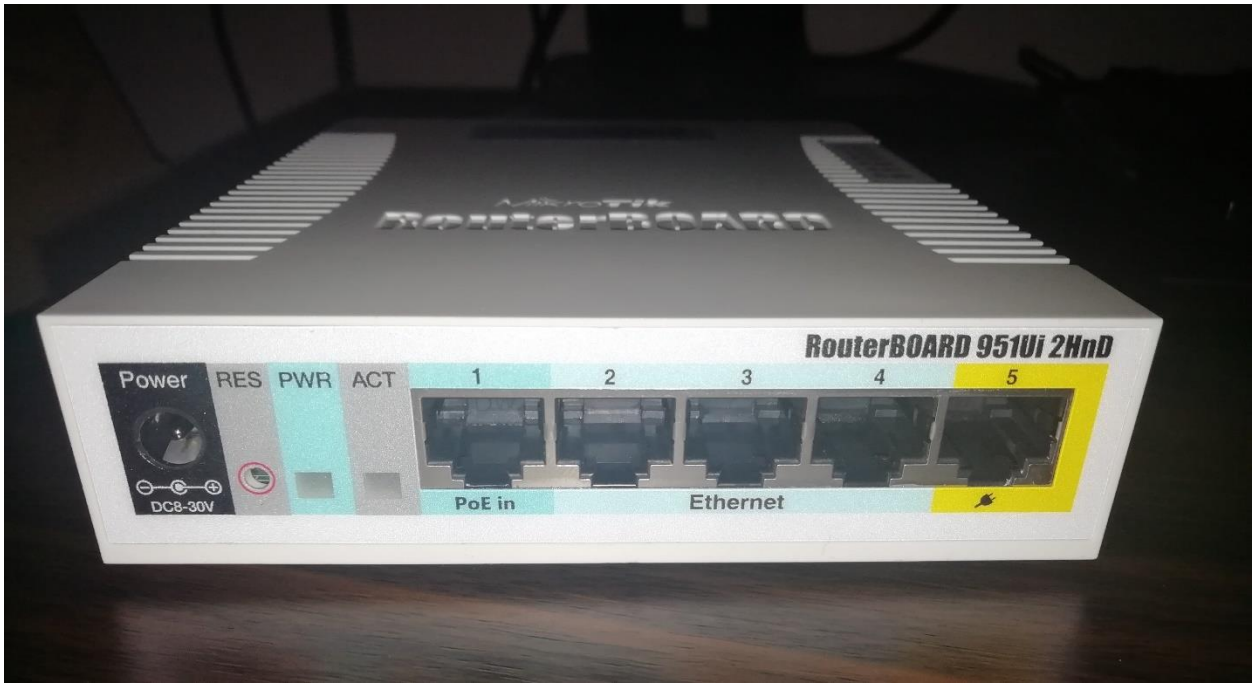
MikroTik RouterOS je zaseban operacijski sustav baziran na Linux operacijskom sustavu koji pokreće MikroTik RouterBOARD opremu. RouterOS je moguće korisititi i na osobnim računalima kao operacijski sustav, što efektivno omogućava da se osobno računalo koristi kao namjenski usmjerivač (eng. Dedicated Router). Unutar RouterOs-a postoje razni alati za upravljanje usmjerivača, kao na primjer: Konfiguracijski alat, Firewall, routing alati, MPLS, VPN, alati za upravljanje bežičnih mreža, DHCP, alati za žarišnu točku (eng. Hotspot), alati za održavanje kvalitete usluge i slični alati. Iako se licenca za RouterOS može nabaviti zasebno za osobna računala ili druge uređaje, kupnjom bilo kojeg MikroTik-ov RouterBOARD uređaja licenca za RouterOS je već instalirana na tom uređaju. [11][12]



Slika 4.1. Prikaz RouterOS-a unutar WinBox programa [13]

4.1.2. RouterBOARD 951Ui 2HnD

RouterBOARD je brand pod kojim MikroTik prodaje svoje uređaje. Ti uređaji mogu biti Komutatori, Ethernet usmjerivači, Bežični uređaji za dom i ured i slično. U ovom radu koristit će se RouterBOARD 951Ui 2HnD. RouterBOARD 951Ui 2HnD je bežični SOHO AP (SOHO pristupna točka) sa novom generacijom Atheros centralne procesorske jedinice (CPU) i većom procesorskom snagom od 600MHz u usporedbi sa prijašnjim inačicama. Ima 5 Ethernet portova od kojih 5. port podržava PoE output, jedan USB 2.0 port i snažnu 2.4GHz 802.11b/g/n bežičnu pristupnu točku sa ugrađenim antenama.[14]



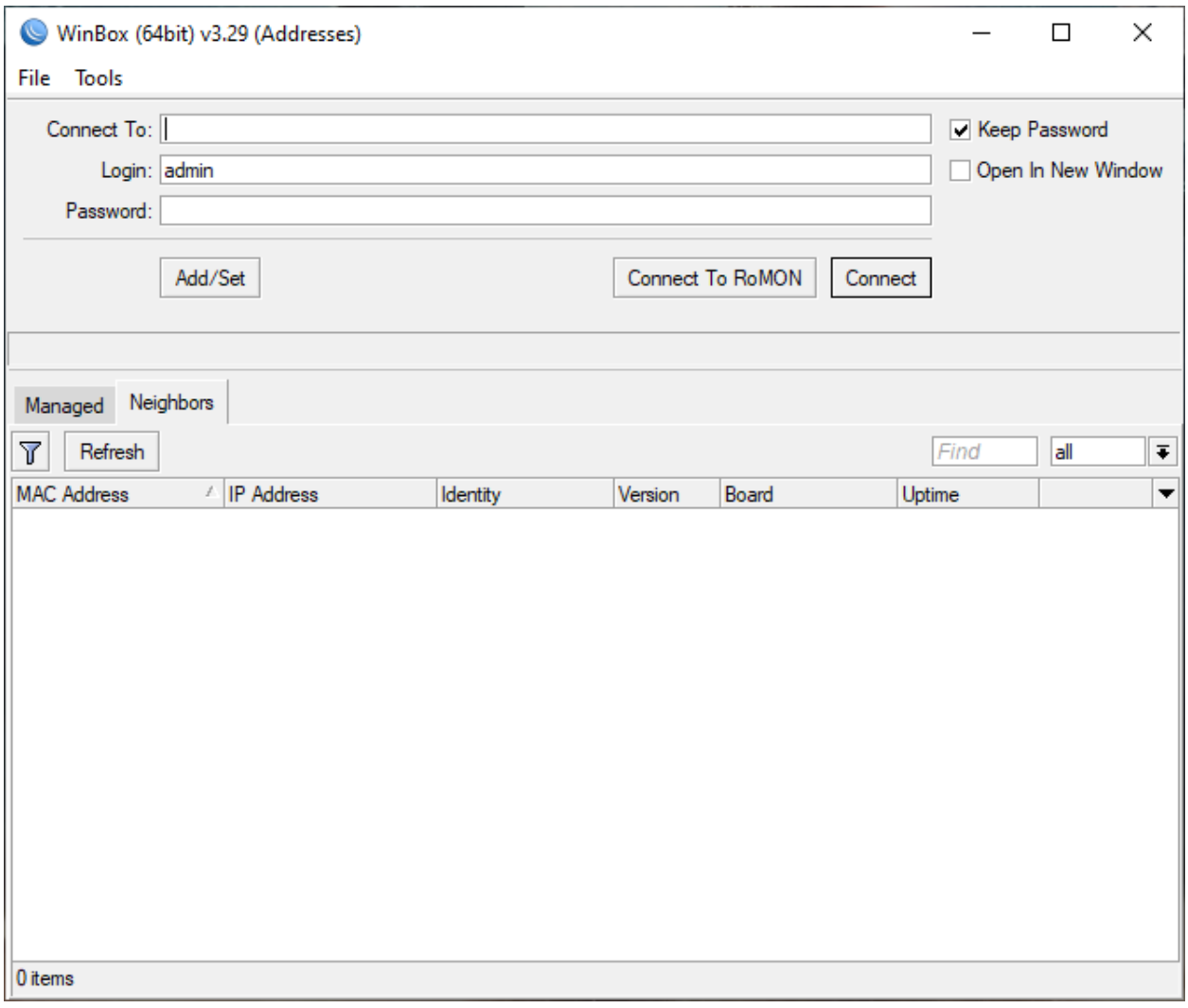
Slika 4.2. Prikaz Ethernet konektora uređaja

Slika 4.3. Prikaz bočne strane na kojoj se nalazi USB 2.0. port

Slika 4.4. Prikaz gornje strane uređaja sa LED oznakama

4.1.3. WinBox

WinBox je mali uslužni program koji omogućuje administraciju MikroTik-ovog RouterOS-a preko svog brzog i jednostavnog sučelja. Izvorno je stvoren za Win32, no moguće ga je pokrenuti i na Linux i MacOS operacijskim sustavima pomoću Wine emulatora.[15]



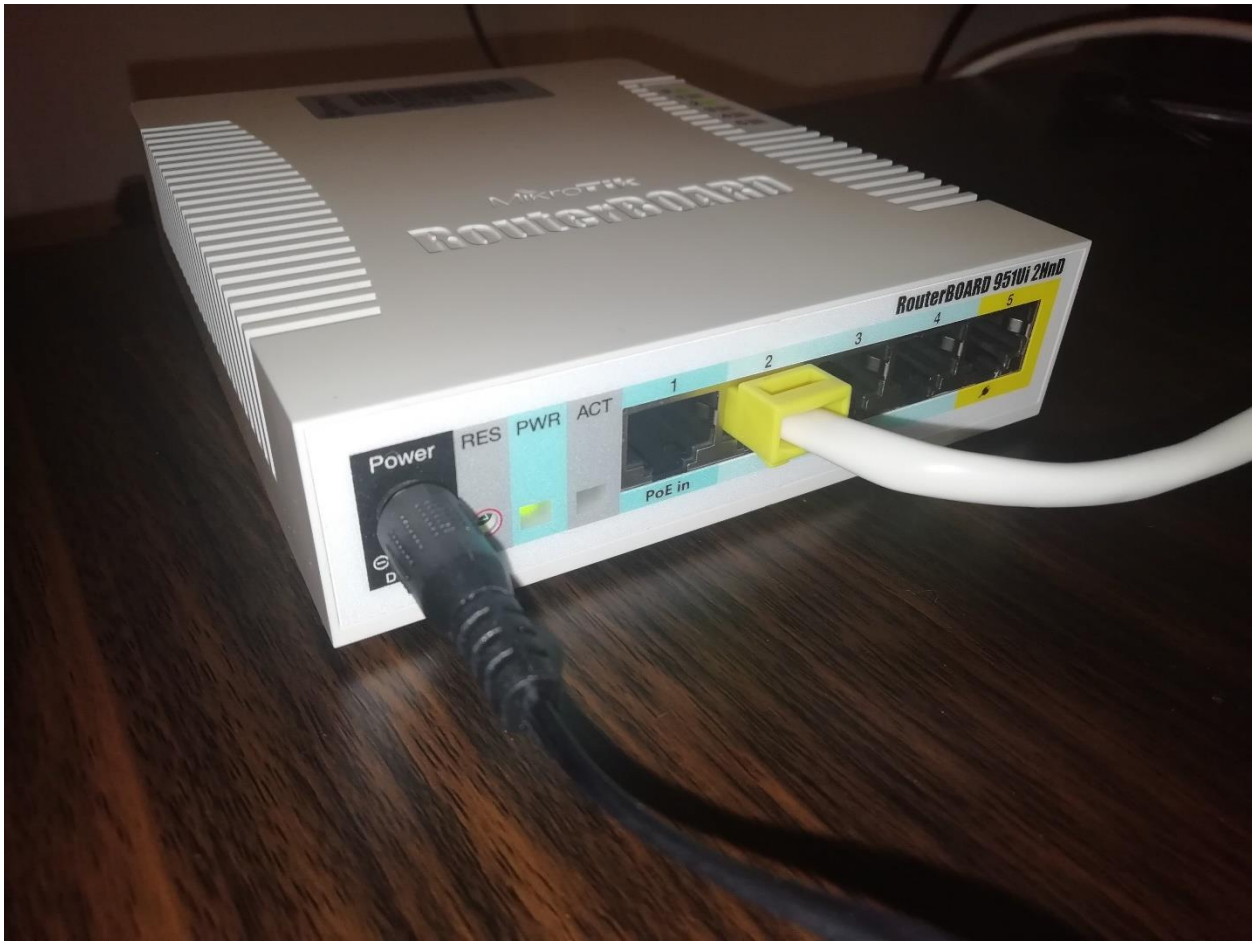
Slika 4.5. Početni prozor WinBox programa

5. POSTUPAK KREIRANJA VIŠESTRUKIH IDENTIFIKATORA POSTAVLJENOG SERVISA

Prije samog postupka kreiranja višestrukih identifikatora postavljenog servisa, potrebno je konfigurirati usmjerivač.

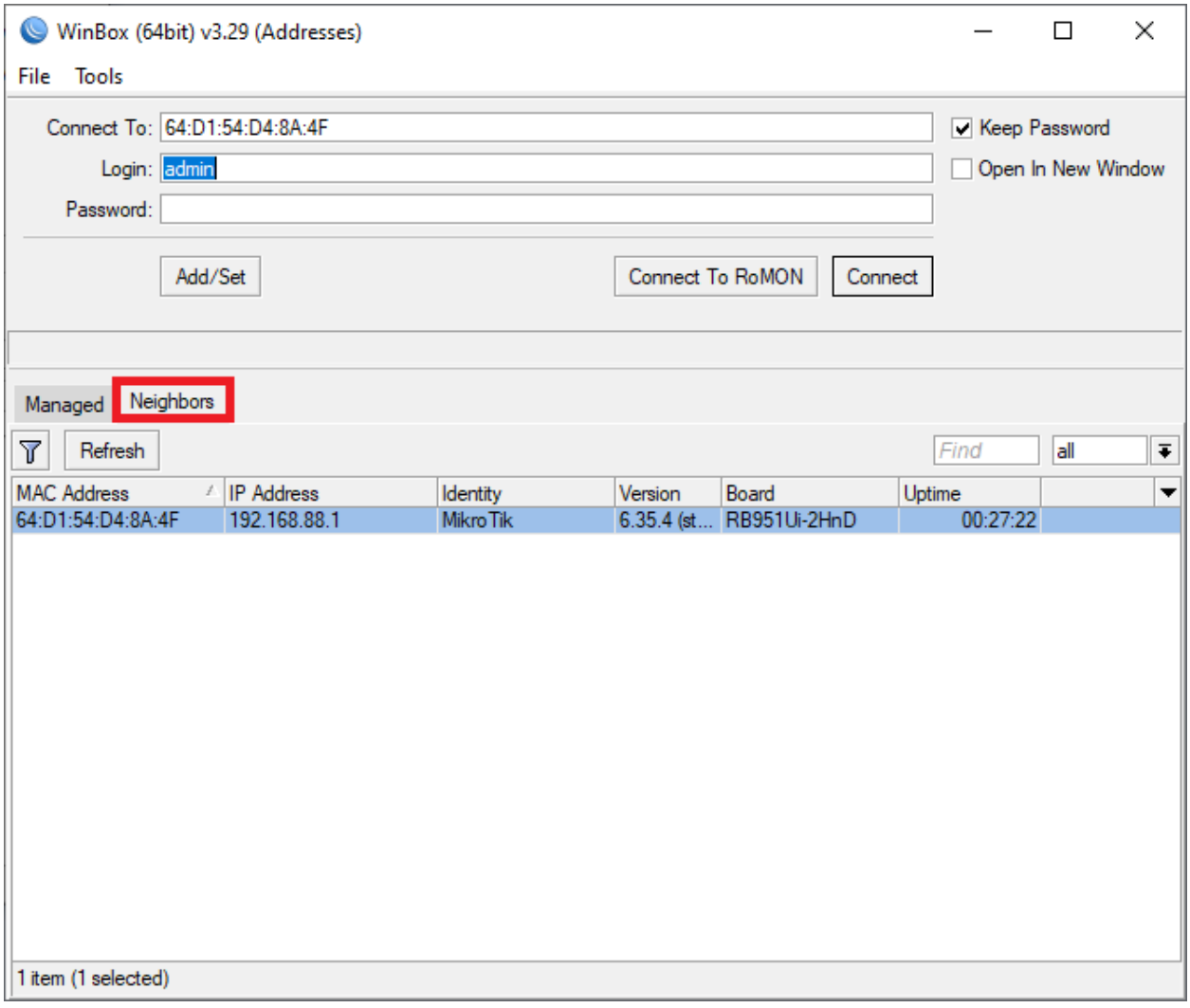
5.1. Početno konfiguriranje RouterBOARD 951Ui 2HnD usmjerivača

Prilikom spajanja usmjerivača na računalo, potrebno je ethernet kabl uključiti u jedan od ethernet portova od 2 do 5. Uključivanjem ethernet kabela u port 1 nije moguće konfigurirati usmjerivač iz razloga što je taj port zaštičen Vatrozidom (eng. Firewall).



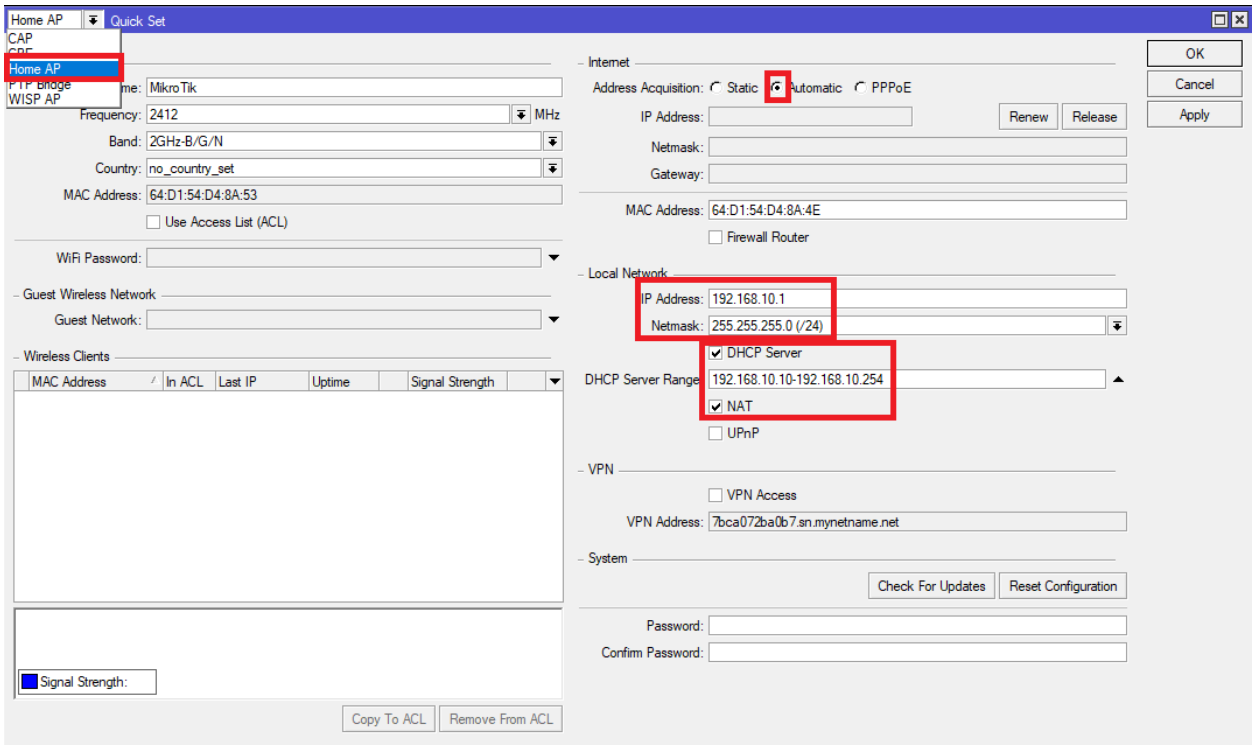
Slika 5.1. Ethernet kabl uključen u port 2 usmjerivača

Nadalje, potrebno je otvoriti WinBox program koji će se konfigurirati usmjerivač. Kada se program otvori, potrebno je kliknuti na tab "*Neighbors*", kliknuti "*Refresh*" kako bi se prikazao spojeni usmjerivač. Zatim, potrebno je kliknuti na MAC adresu usmjerivača i na gornjoj strani prozora unutar "*Connect To*" polja će se pojaviti kliknuta MAC adresa. U "*Login*" polje se unosi "admin", a polje "*Password*" je potrebno ostaviti prazno. Login i password podaci su postavljeni tvornički. Pritisnuti "*Connect*" tipku kako bi pristupili alatima WinBox programa.



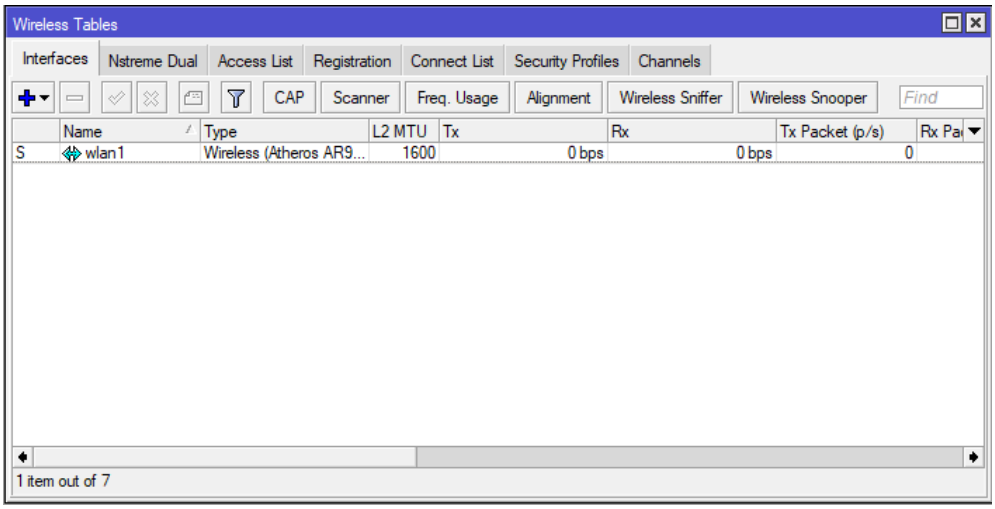
Slika 5.2. Početni ekran sa odabranom "*Neighbors*" karticom i unešenim podacima

Na idućem koraku potrebno je odabrati "*Quick Set*" opciju ponuđenu na traci s lijeve strane prozora. U padajućem izborniku u gornjem lijevom kutu novootvorenog prozora odabrati "*Home AP*" opciju. Pod "*Internet*" dijelom za "*Address Aquisition*" odabrati "Automatic". U "*Local Network*"postaviti "*IP Address*" na npr. "192.168.10.1". Na polju gdje se nalazi 10 u ovom primjeru moguće je odabrati bilo koji broj osim 0 ili 1 iz razloga što većina usmjerivača koriste "192.168.0.1" ili "192.168.1.1" te odabirom bilo kojeg broja osim 0 ili 1 uklanjamo mogućnost stvaranja konflikta između adresa. Za masku odabrati "255.255.255.0 (/24)". Staviti kvačicu na "*DHCP Server*", u polje "*DHCP Server Range*" upisati "192.168.10.10-192.168.10.254". U tom polju rezerviramo IP adrese za razne uređaje koji će se spajati na mrežu. U danom primjeru rezervirane su adrese od 10 pa sve do 254. Staviti kvačicu na opciju "*NAT*".



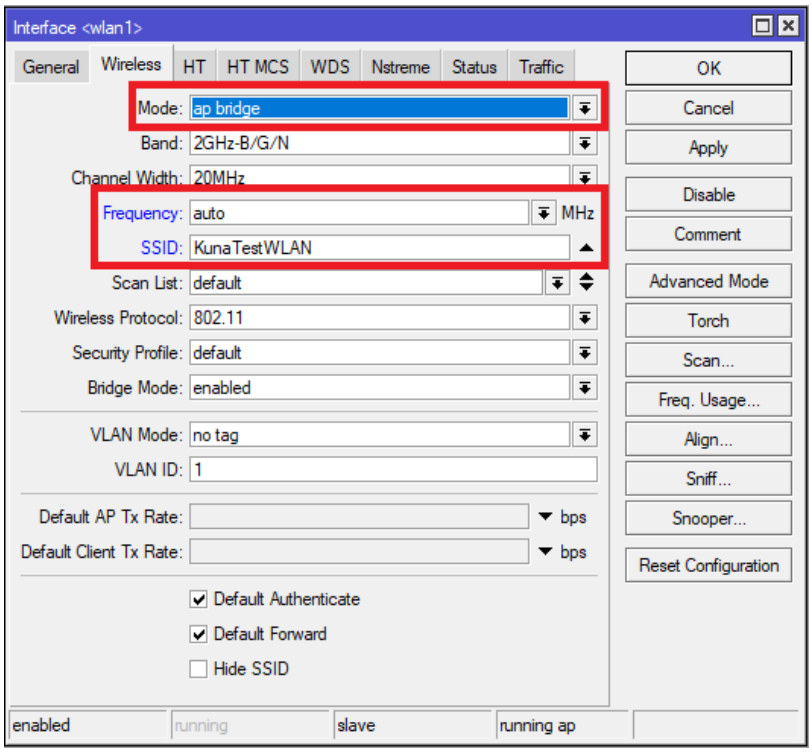
Slika 5.3. Konfiguracija pomoću "*Quick Set*" opcije

U idućem koraku odabrati "*Wireless*" opciju na traci s lijeve strane. Pojavit će se prozor sa tablicom u kojoj se samo nalazi "*wlan1*".



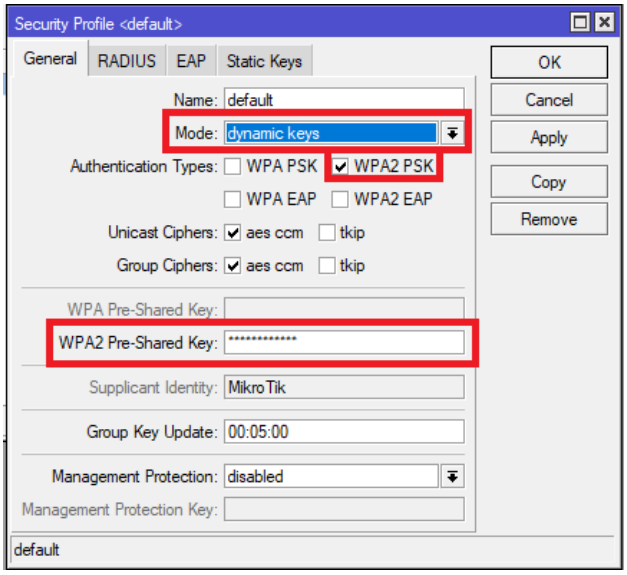
Slika 5.4. Prikaz izlistanih sučelja u "*Wireless*" tablici

Dvoklikom na "*wlan1*" otvorit će se prozor za konfiguraciju sučelja "*wlan1*". Odabrati "*Wireless*" karticu. U "*Mode*" padajućem izborniku odabrati "*ap bridge*" i pod "*Frequency*" odabrati opciju "*auto*". SSID postaviti na proizvoljno ime, u ovom radu će to biti "KunaTestWLAN". Kliknuti tipku "*Apply*".



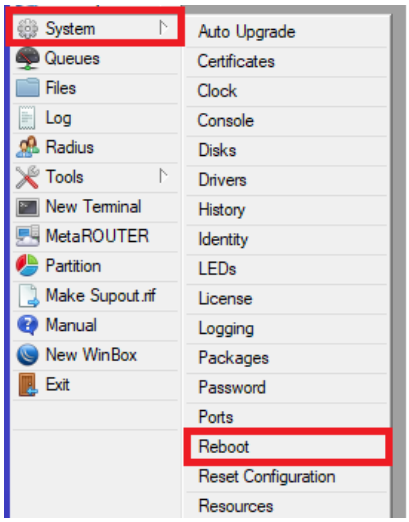
Slika 5.5. Konfiguriranje sučelja "*wlan1*"

Na prozoru sa "*Wireless*" tablicom odabrati karticu "*Security Profiles*". Dvokliknuti na ime "*default*". Na novootvorenom prozoru pod karticom "*General*" na padajućem izborniku "*Mode*" odabrati "*dynamic keys*" i pod "*Authentication Types*" staviti kvačicu na "*WPA2-PSK*". Koristi se "*WPA2-PSK*" zbog pojačane sigurnosti. Pod poljem "*WPA2 Pre-Shared Key*" postaviti proizvoljnu lozinku koju je potrebno upisati kako bi se omogućio pristup mreži. U ovom radu lozinka je "kunawlantest". Pritisnuti "*Apply*" tipku i vratiti se na glavni zaslon.



Slika 5.6. Konfiguriranje sigurnosnog profila

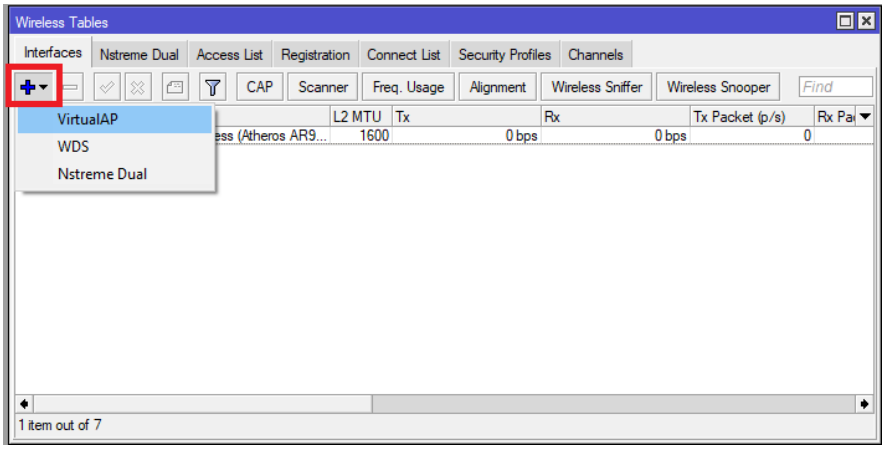
Zadnji korak početnog postavljanja je resetiranje rutera. To se postiže odabiranjem opcije "*System*" na traci s lijeve strane i zatim klikom na opciju "*Reboot*".



Slika 5.7. Resetiranje usmjerivača

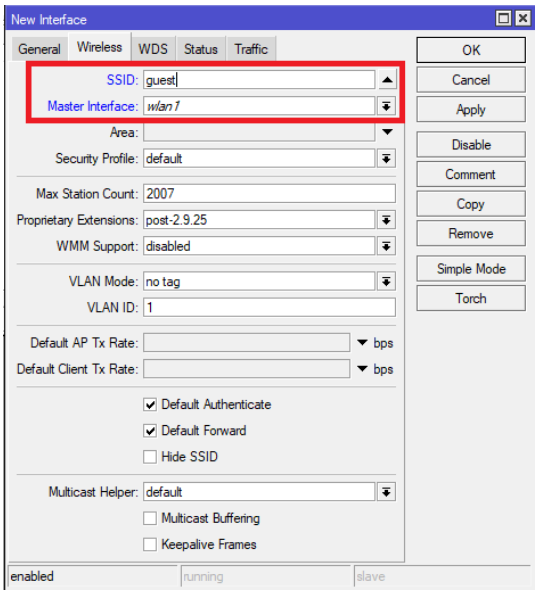
5.2. Kreiranje višestrukih identifikatora postavljenog servisa

Nakon obavljene početne konfiguracije i uspješnog reseta usmjerivača, moguće je sada kreirati višestruke identifikatore postavljenog servisa (SSID). U glavnom prozoru WinBox programa odabrati kategoriju "*Wireless*" i na novootvorenom prozoru pod karticom "*Interfaces*" gdje se nalazi "*wlan1*" sučelje kliknuti na plavu plus ikonicu. Na padajućem izborniku odabrati "*VirtualAP*" opciju.



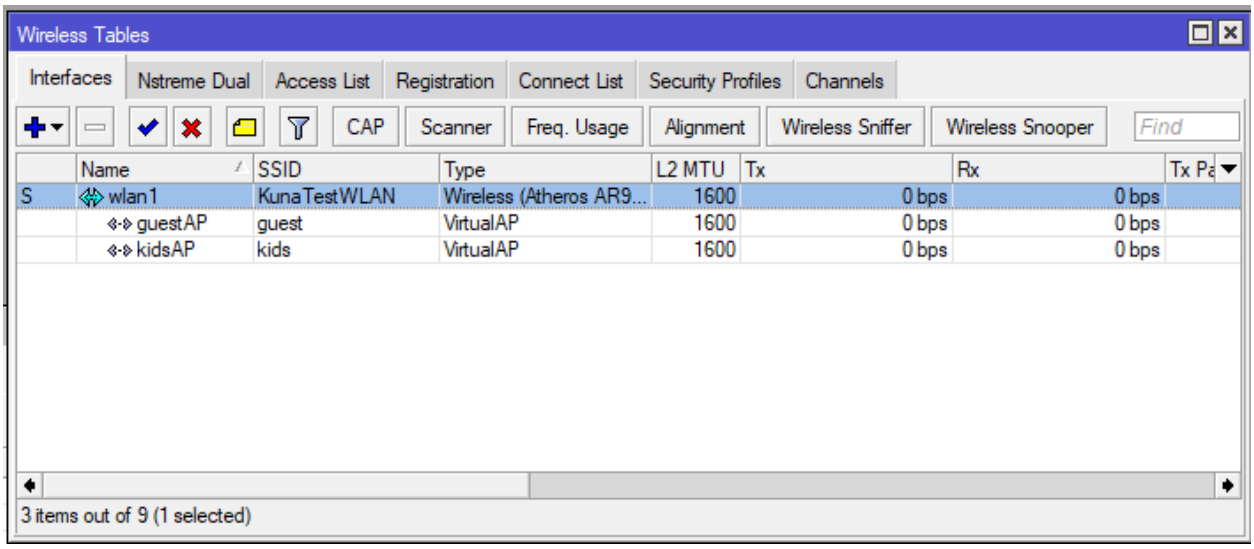
Slika 5.8. Kreiranje virtualne pristupne točke (eng. Virtual Acess Point)

U novootvorenom prozoru odabrati "*Wireless*" karticu, pod "*Master Interface*" poljem mora stajati "*wlan1*" sučelje. Postaviti proizvoljno ime pod "*SSID*", u ovom radu će SSID biti "guest"



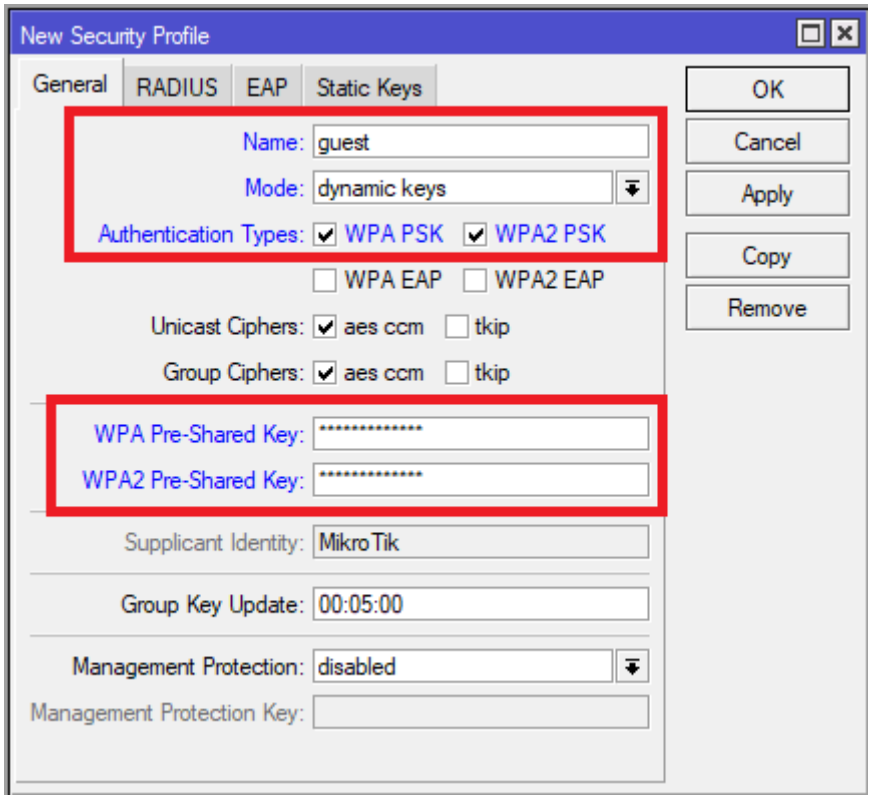
Slika 5.9. Postavljanje "guest" SSID-a virtualne pristupne točke

Ovisno o broju potrebnih pristupnih točaka ponoviti postupak. Za potrebe ovog rada bit će ukupno dvije virtualne pristupne točke. SSID druge virtualne pristupne točke bit će "kids". Za svaku virtualnu pristupnu točku promjeniti ime dvoklikom na nju i pod "*General*" karticom promeniti ime. U ovom radu postavljena su imena na "guestAP" i "kidsAP". Ovaj korak nije nužan ali ga je dobro napraviti radi lakšeg dodavanja virtualne pristupne točke u standardni most.

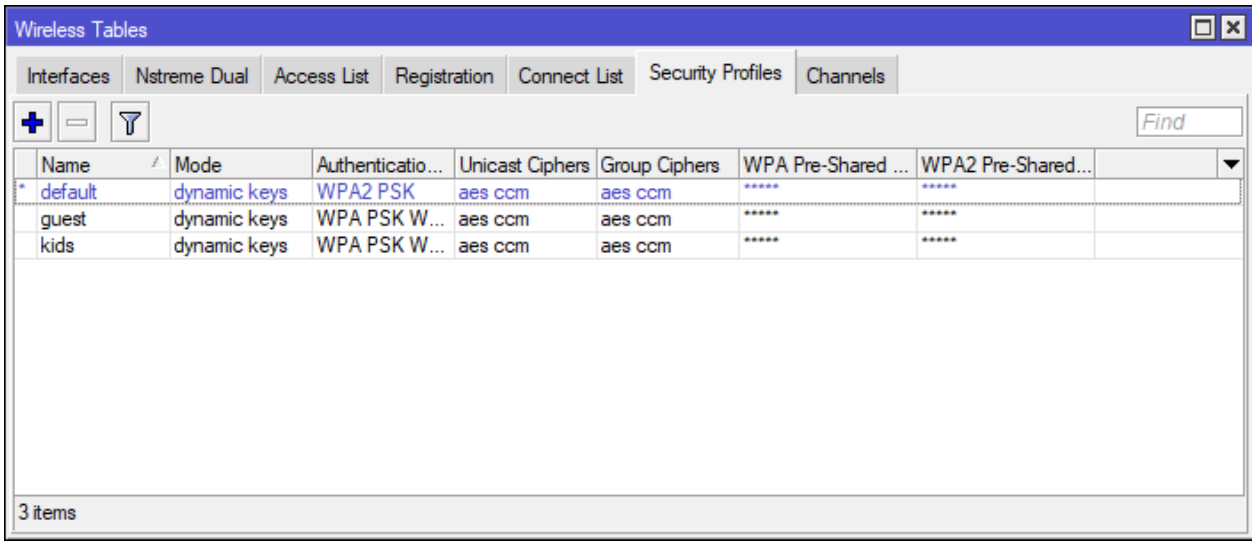


Slika 5.10. Prikaz liste sučelja nakon dodavanja virtualnih pristupnih točaka

Nakon kreiranja proizvoljnog broja virtualnih pristupnih točaka potrebno je svakoj toj točki pridodati zaseban sigurnosni profil. Sigurnosni profili se kreiraju u "*Wireless*" prozoru pod karticom "*Security Profiles*" klikom na plavu plus ikonicu. Na novootvorenom prozoru pod karticom "*General*" pod "*Name*" napisati ime sigurnosnog profila. Preporučljivo je napisati isto ime kao i SSID virtualne pristupne točke za lakšu dodjelu profila. Pod "*Mode*" odabrati "*dynamic keys*", na "*Authentication Types*" staviti kvačicu na "*WPA PSK*" i "*WPA2 PSK*". Ovdje je dodan i "*WPA PSK*" u slučaju spajanja starijeg uređaja na mrežu. Postaviti lozinke na "*WPA Pre-Shared Key*" i "*WPA2 Pre-Shared Key*". Preporučljivo je staviti identične lozinke za oba načina. Postupak ponoviti za svaku virtualnu pristupnu točku koja je kreirana.

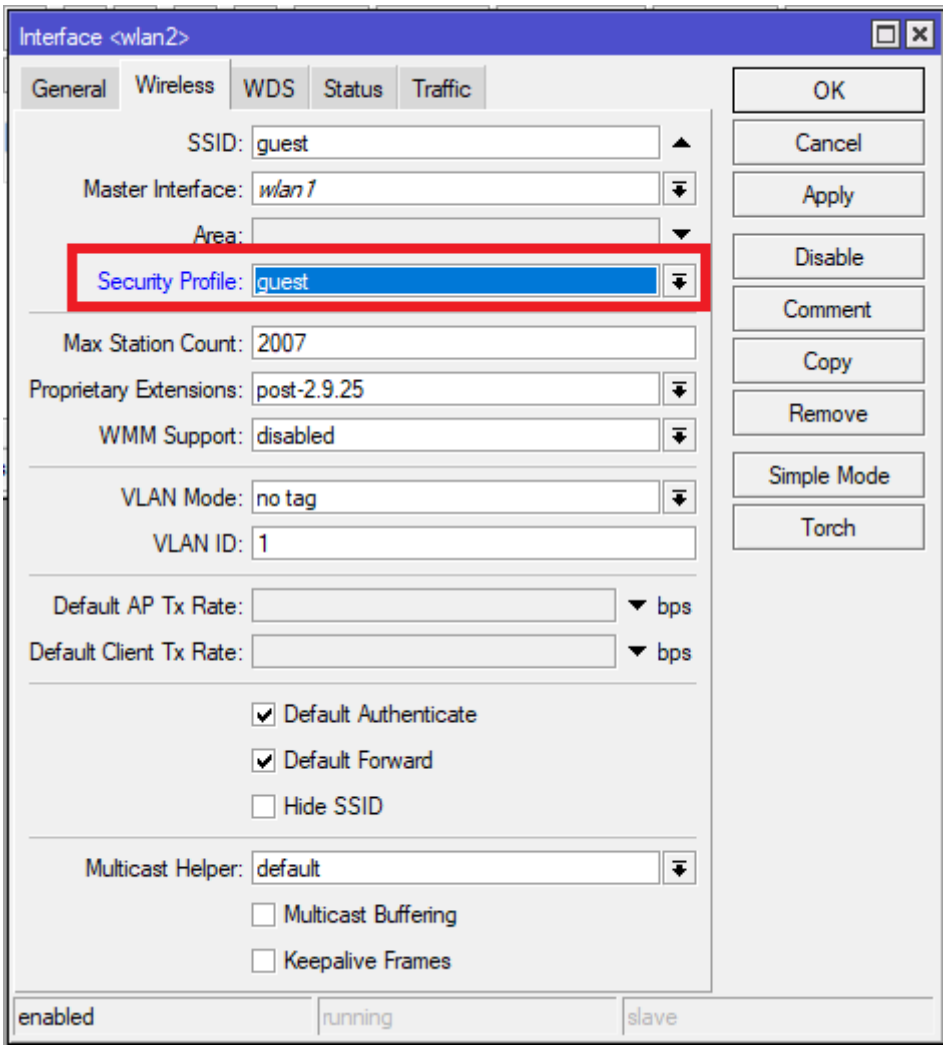


Slika 5.11. Konfiguriranje sigurnosnog profila



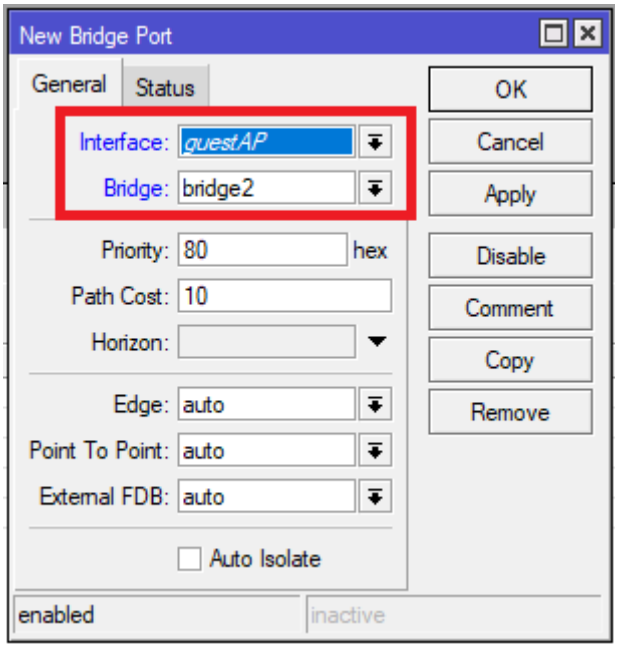
Slika 5.12. Izgled liste sigurnosnih profila nakon dodavanja novih profila

Sada je potrebno dodijeliti sigurnosne profile odgovarajućoj virtualnoj pristupnoj točki. Na prozoru "*Wireless*" odabrati karticu "*Interfaces*", dvokliknuti na virtualnu pristupnu točku i na "*Security Profile*" padajućem izborniku odabrati odgovarajući sigurnosni profil za tu pristupnu točku. Ponoviti postupak za svaku virtualnu pristupnu točku.



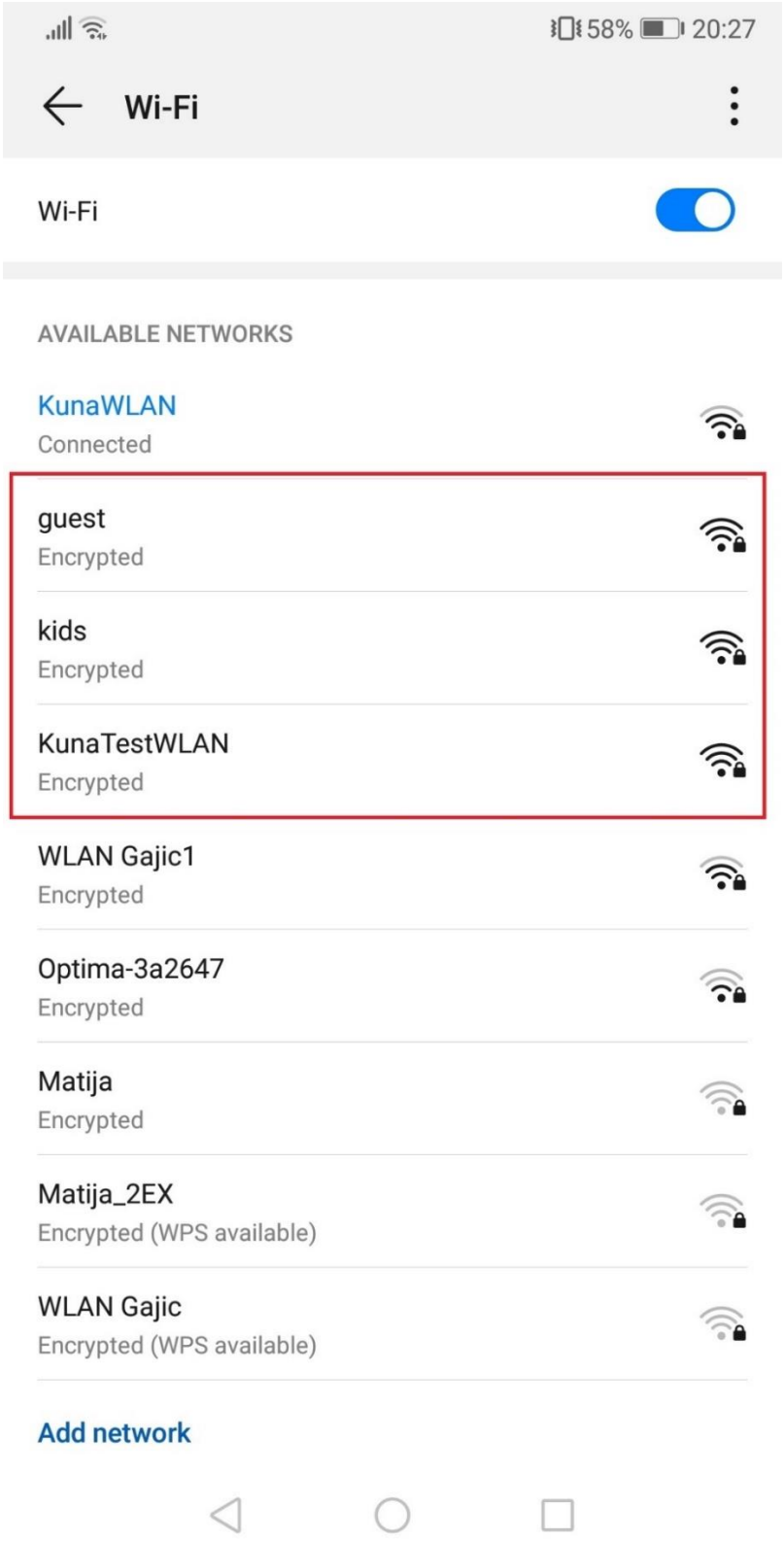
Slika 5.13. Postavljanje kreiranih sigurnosnih profila za virtualnu pristupnu točku

Nakon dodijele sigurnosnih profila, potrebno je virtualne pristupne točke dodati u zadani most (eng. Default Bridge). U glavnom prozoru WinBox programa odabrati "*Bridge*". Na novonastalom prozoru odabrati karticu "*Ports*" i kliknuti na plavu plus ikonicu. U novootvorenom prozoru pod "*General*" karticom na "*Interface*" polju odabrati "guestAP", u polju "*Bridge*" postaviti na "*bridge2*" koji je u ovom radu zadani most. Postupak ponoviti za svaku kreiranu virtualnu pristupnu točku.



Slika 5.14. Dodavanje virtualne pristupne točke u zadani most

Pogledom na uređaj, vidi se da su uređaju vidljive sve pristupne točke koje su kreirane. Ovisno o korisnikovim pravima i potrebama, spaja se na mrežu preko odgovarajućeg SSID-a.



Slika 5.15. Lista SSID-eva koje dohvaća vanjski uređaj

6. ZAKLJUČAK

Cilj ovog rada bio je pojasniti pojam identifikatora postavljenog servisa i njegov utjecaj na sigurnost bežičnih mreža, te prikazati postupak i prednosti kreiranja višestrukih identifikatora postavljenog servisa.

Pomoću WLAN-a omogućeno je lakše spajanje uređaja na internet neovisno o tome gdje se taj uređaj nalazi u području djelovanja WLAN mreže. Kako bi se područje djelovanja proširilo, koriste se pristupne točke pomoću kojih se uređaji spajaju na mrežu. Ukoliko se te pristupne točke ne konfiguriraju sa vlasitim identifikatorom postavljenog servisa (SSID), moguće je da će na uređaju doći do interferencije na mjestima gdje se područja djelovanja pristupnih točaka preklapaju.

Također, postavljanjem različitih identifikatora postavljenog servisa moguće je na određenim pristupnim točkama imati različitu razinu sigurnosti. Primjerice, jedna tvrtka može koristiti SSID "*Zaposlenici*" na pristupnoj točki kojoj se pristupa radi obavljanja internih poslova tvrtke sa minimalnim ograničenjima na mreži. Dok u isto vrijeme na drugoj pristupnoj točki sa SSID-em "*Klijenti*" klijenti te tvrtke mogu pristupiti osnovnim mogućnostima spajanja na mrežu sa većim ograničenjima.

LITERATURA

[1] wireless networking - How do multiple SSIDs provide security - Super User, dostupno na: https://superuser.com/questions/354958/how-do-multiple-ssids-provide-security#:~:text=The%20purpose%20of%20multiple%20SSIDs,that%20only%20provides%20Internet%20access [22.06.2021]

[2] S. Seneviratne, F. Jiang, M. Cunche and A. Seneviratne, "SSIDs in the wild: Extracting semantic information from WiFi SSIDs," 2015 IEEE 40th Conference on Local Computer Networks (LCN), 2015, pp. 494-497, doi: 10.1109/LCN.2015.7366361. dostupno na: https://ieeexplore.ieee.org/abstract/document/7366361 [02.06.2021]

[3] Hamidović, H. (2009). WLAN bežične lokalne računalne mreže: Priručnik za brzi početak, Zagreb: Impresum, Info press

[4] What Is a Wireless Network?, Cisco, dostupno na: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/wireless-network.html#~introduction [13.06.2021]

[5] An evaluation of IEEE 802.11 MAC layer handoff process in CAPWAP centralized WLAN - Scientific Figure on ResearchGate., dostupno na: https://www.researchgate.net/figure/Centralized-WLAN-Architecture-In-Local-MAC-Architecture-the-whole-MAC-functionalities_fig1_282687337 [22.06.2021]

[6] Converged Access: Solution Overview, Cisco, 5. Kolovoz, 2019 , dostupno na: https://content.cisco.com/chapter.sjs?uri=%2Fsearchable%2Fchapter%2Fcontent%2Fen%2Fus%2Ftd%2Fdocs%2Fswitches%2Flan%2Fcatalyst3850%2Fsoftware%2Frelease%2F16-1%2Fconverged_access_deployement_guide%2Fm_conAccess_deploy_guide%2Fconverged_access_solution_overview.html.xml&platform=Cisco%20Catalyst%203850%20Series%20Switches [22.06.2021]

[7] A. Gupta, Is Cloud-defined WiFi the future of WiFi?, TaraSpan, 28. Prosinac, dostupno na: https://www.taraspan.com/blog/is-cloud-defined-wifi-the-future-of-wifi/ [22.06.2021]

[8] What is an SSID and how to find it, Brother, dostupno na: https://help.brother-usa.com/app/answers/detail/a_id/157105/~/what-is-an-ssid-and-how-to-find-it [23.06.2021]

[9] How to find the default sign-in details for your router, 12. Travanj, 2021, dostupno na: https://www.expressvpn.com/es/support/troubleshooting/default-passwords-expressvpn-router-app/ [23.06.2021]

[10] MikroTik Routers and Wireless - About, dostupno na:

MikroTik Routers and Wireless - About [01.09.2021]

[11] MikroTik RouterOS - Feature Catalog, MikroTik, Q1-Q2 2010, dostupno na: what_is_routeros.pdf (mt.lv) [02.09.2021]

[12] What is MikroTik RouterOS?, Samantha Albano, 27. Prosinac, 2019. ,dostupno na: What is MikroTik RouterOS? (minim.com) [02.09.2021]

[13] Wikimedia Commons, dostupno na: File:Winbox displaying RouterOS shell.png - Wikimedia Commons [02.09.2021]

[14] MikroTik Routers and Wireless - Products: RouterBOARD 951Ui 2HnD, MikroTik, dostupno na: MikroTik Routers and Wireless - Products: RB951Ui-2HnD [03.09.2021]

[15] Manual:Winbox - MikroTik Wiki, MikroTik, dostupno na: Manual:Winbox - MikroTik Wiki [03.09.2021]

SAŽETAK

U okviru ovog završnog rada obavljena je simulacija i konfiguracija identifikatora postavljenog servisa na opremi MikroTik RouterBOARD 951Ui 2HnD koja je dodijeljena od strane fakulteta. Prije obavljanja same simulacije provedeno je istraživanje WLAN mreža u kojima se koriste identifikatori postavljanog servisa. Opisane su prednosti WLAN mreža naspram žičnih mreža, način njihove implementacije te načini kojima se mogu detektirati. Definiran je pojam identifikatora postavljenog servisa i njegov utjecaj na sigurnost bežičnih mreža. Naposlijetku, kratko je opisana korištena oprema i svi popratni programi koji su bili potrebni za ostvarivanje simulacije. Simulacija je pokrivala i početnu konfiguraciju opreme koja je bila potrebna za daljnji postupak.

Ključne riječi: Beacon okvir, Bežična mreža, Identifikator postavljenog servisa, Pristupna točka, Skeniranje

ABSTRACT

Creating multiple Service Set Identifiers

As part of this final paper, a simulation and configuration of service set identifiers was performed on MikroTik RouterBOARD 951Ui 2HnD equpment which was provided by the college. Before performing the simulation, a research of WLAN networks was conducted in which the service set identifiers are used. The advantages of WLAN networks over wired networks, their implementation and the ways in which they are detected are described. The notion of service set identifier and its impact on wireless network security is defined. Finally, the used equipment and all the accompanying programs that were needed to perform the simulation are briefly described. The simulation also covered the initial configuration of the equipment needed for the further procedure.

Keywords: Beacon Management Frame, Wireless network, Service set identifier, Access point, Scanning