UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Adrijan Bradaschia

DINAMIČNO DODELJEVANJE NAVIDEZNIH KRAJEVNIH OMREŽIJ V BREZŽIČNIH OMREŽJIH

DIPLOMSKO DELO
UNIVERZITETNI ŠTUDIJSKI PROGRAM PRVE STOPNJE
RAČUNALNIŠTVO IN INFORMATIKA

MENTORICA:
Doc. dr. Mojca Ciglarič

Ljubljana, 2013

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tržaška 25
1001 Ljubljana, Slovenija
telefon: 01 476 84 11
01 476 83 87
faks: 01 426 46 47
01 476 87 11
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00146/2013
Datum: 02.09.2013

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **ADRIJAN BRADASCHIA**

Naslov: **DINAMIČNO DODELJEVANJE NAVIDEZNIH KRAJEVNIH OMREŽIJ V BREZŽIČNIH OMREŽJIH**

DYNAMIC VLAN ASSIGNMENT IN WIRELESS NETWORKS

Vrsta naloge: Diplomsko delo univerzitetnega študija prve stopnje

Tematika naloge:

Preučite možnosti za odpravljanje varnostne ranljivosti zastrupljanja tabele ARP v omrežju Eduroam s pomočjo navideznih krajevnih omrežij. Pojasnite pomanjkljivosti omrežja Eduroam, ki onemogočajo preprosto odpravo te ranljivosti. Predlagajte arhitekturo in tehnično rešitev, ki bi odpravo vendarle omogočala, ter realizirajte prototipno rešitev. Rešitev preizkusite ter kritično ovrednotite.

Mentor:
M. Ciglarič
doc. dr. Mojca Ciglarič

Dekan:
prof. dr. Nikolaj Zimic

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Spodaj podpisani **Adrijan Bradaschia**, z vpisno številko **63090042**, sem avtor diplomskega dela z naslovom:

Dinamično dodeljevanje navideznih krajevnih omrežij v brezžičnih omrežjih

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom doc. dr. Mojce Ciglarič
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identične s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki »Dela FRI«

V Ljubljani, dne 12. septembra 2013 Podpis avtorja:

Hvala doc. dr. Mojci Ciglarič za mentorstvo.
Hvala Andreju Krevlu, ki mi je s strokovnimi nasveti pomagal pri izdelavi diplomske naloge.
Hvala družini in vsem ostalim, ki so med podpirali med študijem in v času pisanja diplomske naloge.

Kazalo vsebine

Povzetek

Uporaba brezžičnih omrežij se vsakodnevno povečuje in s tem tudi število uporabnikov, ki so zaradi napadov na omrežja lahko v nevarnosti pred zlorabo njihovih podatkov. V diplomskem delu smo pod drobnogled vzeli brezžično omrežje Eduroam, ki je sicer zelo varno, vendar pa ima kljub temu tudi nekatere varnostne slabosti. Cilj diplomske naloge je bil odpraviti te slabosti s pomočjo uporabe cenovno ugodnih dostopnih točk.

V prvem delu opisujemo omrežje Eduroam, njegovo strukturo, prednosti in ranljivosti, ki bi jih lahko odpravili, da bi uporabnikom zagotovili večjo varnost pri uporabi omrežja. Opisana je ideja, ki uporabnike ločuje v navidezna krajevna omrežja in s tem napadalcu preprečuje izvajanje napada zastrupljanje tabele ARP, saj se zaradi izolacije uporabnikov nahaja v omrežju, ki ga uporablja le on.

Drugi del diplome opisuje postopek, kako postaviti brezžično omrežje z uporabo dinamičnega dodeljevanja navideznih krajevnih omrežij na cenovno ugodnih dostopnih točkah. Uspešna izolacija uporabnikov v navidezna krajevna omrežja tako preprečuje napad in uporabniku zagotovi večjo varnost pri uporabi omrežja.

Ključne besede: brezžično omrežje, strežnik, FreeRadius, stikalo, dostopne točke, DHCP, Eduroam, varnost.

Abstract

The wireless network usage is increasing everyday and with it the number of users that risk data abuse due to the network attacks. This diploma thesis inspects the Eduroam wireless network that is known to be very safe; however, it still shows some security vulnerabilities. The aim of the thesis was to eliminate these vulnerabilities by making use of low-cost access points.

The first part of the thesis describes the Eduroam network, its structure, advantages, and disadvantages that we could overcome in order to provide the users with greater security when using the network. We describe the idea of separating users into virtual local area networks, thereby preventing the attackers to carry out the ARP table poisoning attack. The user isolation makes the attackers use their own network.

The second part describes the procedure of setting up a wireless network using a dynamic allocation of virtual local area networks on low-cost access points. The successful isolation of users in virtual local area networks prevents the network attacks and in this way provides greater user safety.

Keywords: wireless network, server, FreeRadius, switch, access point, DHCP, Eduroam, security.

1 Uvod

Živimo v času, kjer si skoraj nihče več ne predstavlja dneva brez uporabe interneta. Skoraj vsak od nas dnevno uporablja brezžična omrežja za dostop do interneta tako s prenosnih računalnikov kot z mobilnih telefonov. Število brezžičnih dostopnih točk se povečuje iz dneva v dan, saj večina ustanov (npr. šole) nudijo svojim obiskovalcem možnost dostopa do interneta.

Pri tem se pojavijo tudi težave. Velikokrat se namreč najde kdo, ki bi rad javna brezžična omrežja izkoristil v svoj prid in se s tem dokopal do zasebnih podatkov uporabnikov omrežij. Ker tudi sami uporabljamo omrežje Eduroam in smo seznanjeni z možnostmi napadov in zlorab omrežja, smo se v diplomi posvetili iskanju rešitve, ki bi uporabnikom omrežja zagotovila večjo varnost.

Zaradi znanih varnostnih lukenj omrežja Eduroam smo izvedli raziskavo, v kateri smo želeli ugotoviti, ali lahko njegovo varnost izboljšamo tudi na cenovno ugodnih dostopnih točkah. Pri uporabi istega brezžičnega omrežja uporabniki vedno uporabljajo isto lokalno omrežje. Tako ima napadalec možnost izkoristiti napad zastrupljanja tabele ARP, kjer izvede napad s posrednikom *(Man-in-the-middle)*. Pri tem promet med dvema uporabnika poteka preko napadalca, ki prometu prisluškuje. Pri uporabi fizičnih omrežij je ločevanje uporabnikov mogoče tudi brez uporabe navideznih krajevnih omrežij z uporabo večjega števila usmerjevalnikov. Uporaba navideznih krajevnih omrežij sicer ločevanje poenostavi. Tako lahko ločimo uporabnike različnih interesnih skupin (primer podjetja: računovodstvo, uprava, delavci, gostje) in s tem preprečimo, da bi prišlo do napada s strani zunanjih napadalcev.

Pri uporabi brezžičnih omrežij je sistem ločevanja bolj zapleten. Potrebujemo drage dostopne točke in sistem, ki bo uporabnike ločeval v omrežja, ali pa preprosto na dostopni točki oddajamo več različnih brezžičnih omrežij in tako uporabnike ločujemo v različne interesne skupine. Problem se pojavi, če imamo interesnih skupin veliko in bi radi ločevali v ločena omrežja tudi goste, da bi s tem vsakemu uporabniku zagotovili enako visoko stopnjo varnosti. Od tukaj izhaja ideja o dinamičnem dodeljevanju navideznih krajevnih omrežij vsakemu uporabniku v omrežju in preprečitev napada zastrupljanja tabele ARP. V nadaljevanju diplomskega dela je predstavljeno omrežje Eduraom, njegove slabosti in ideja za nadgradnjo, s katero bi te slabosti odpravili. Drugi del opisuje tehnično izvedbo rešitve.

2 Omrežje Eduroam

Poglavje opisuje značilnosti omrežja Eduroam povzeto po [5, 21, 22].

2.1 Kaj je Eduroam?

Eduroam je sistem gostovanja odjemalcev brezžičnih omrežij in skupina brezžičnih omrežij Eduroam v Sloveniji. Cilj sistema je zagotoviti enostaven dostop do interneta, visoko varnost pri dostopu, gostovanje uporabnikov brez zamudnega prenastavljanja naprav in prožno arhitekturo z možnostjo poljubne centralizacije ali decentralizacije sistemov. Avtentikacijski strežnik in/ali imenik uporabnikov je lahko na ravni univerze, šolskega centra, okraja ali pa na ravni posamezne fakultete, šole, oddelka, …

2.2 Arnes

Akademska in raziskovalna mreža Slovenije – Arnes (ponudnik omrežja Eduroam) je javni zavod, ki zagotavlja omrežne storitve organizacijam s področja raziskovanja, izobraževanja in kulture. Hkrati omogoča njihovo povezovanje in medsebojno sodelovanje ter sodelovanje s sorodnimi organizacijami v tujini [4].

2.3 Tehnične lastnosti

Omrežje je zgrajeno na standardu 802.11b/g ter WPA2. Prijava uporablja protokol 802.1X z močno avtentikacjo EAP-TTLS. Uporabniki se v omrežje prijavijo s svojim uporabniškim imenom in geslom. Vsako omrežje, pridruženo Eduroam, se oglašuje pod SSID imenom Eduroam, s čimer oznanja pripadnost le temu.

V Sloveniji testira brezžično opremo Arnes, nudi pomoč in vzdržuje vzorčne nastavitve, ki so potrebne za postavitev takega omrežja na brezplačnem operacijskem sistemu Linux z OpenLDAP in s strežnikom FreeRadius. Rešitev podpira naslednje avtentikacijske mehanizme EAP:

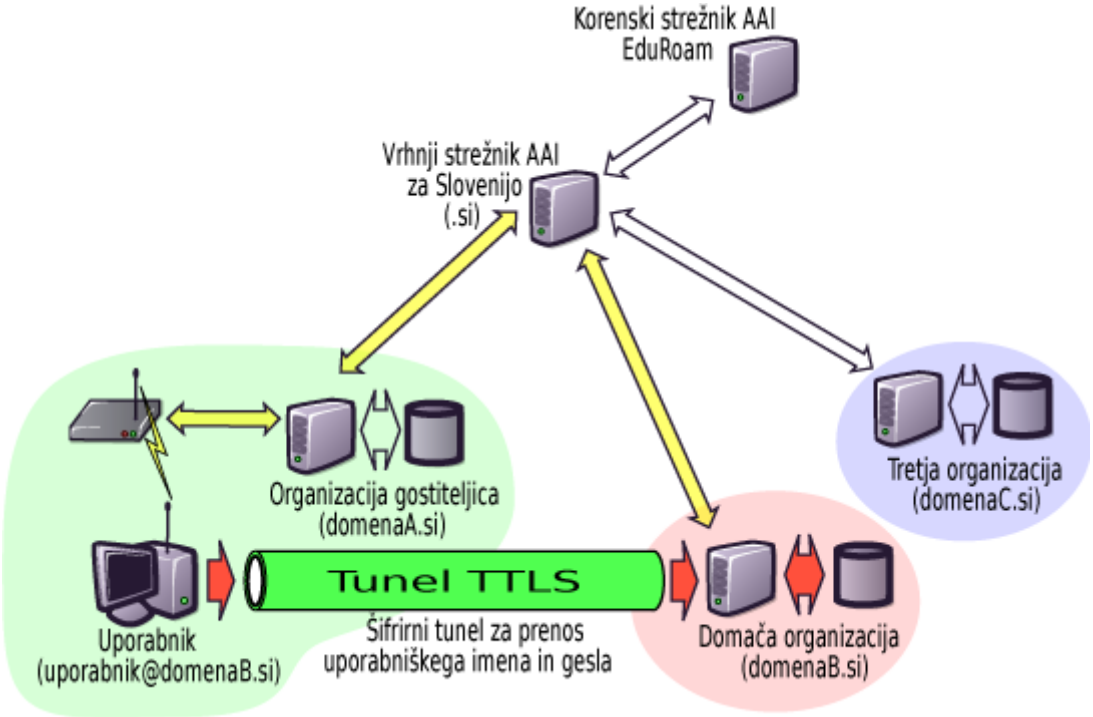
- EAP-TTLS + PAP;
- EAP-TTLS + MSCHAPv2;
- PEAP;
- EAP-TLS.

Arnes priporoča uporabo EAP-TTLS + PAP zaradi najboljšega razmerja med varnostjo in uporabnostjo ter zaradi podpore odjemalca Eduroam klient SecureW2, ki skrbi za nastavitve brezžične povezave Eduroam v sistemih Windows in namesti varnostno pomembne certifikate.

2.4 EAP-TTLS

EAP-TTLS je namenjen je vzpostavitvi šifriranega tunela med odjemalcem in avtentikacijskim strežnikom Radius. Pri vzpostavljanju tunela se preveri veljavnost in pravilnost strežnikovega certifikata, s čimer strežnik potrdi svojo istovetnost. Ko je

tunel vzpostavljen, uporabnik pošlje uporabniško ime in geslo za dostop, strežnik pa ga odobri oziroma v primeru napačnih podatkov zavrne.



Slika 1: Delovanje avtentikacije v omrežju Eduroam [5]

Slika 1 prikazuje prijavo uporabnika v omrežje. Računalnik vzpostavi povezavo z dostopno točko, ki posreduje zahtevo strežniku Radius. Strežnik posreduje zahtevo naprej po hierarhiji Radius vse do domačega strežnika. Nato uporabnik in strežnik vzpostavita tunel TLS in preveri se istovetnost strežnika. Uporabnik nato posreduje uporabniško ime in geslo, strežnik pa v nadaljevanju odbori ali zavrne avtentikacijo. Zaradi šifriranega tunela nihče drug kot uporabnik in strežnik ne more videti gesla.

2.5 Naslovni prostor

Priporočila omrežja Eduroam prepovedujejo uporabo zasebnega naslovnega prostora. Za upravljanje dostopnih točk je uporaba zasebnega naslovnega prostora sicer dovoljena, a odsvetovana.

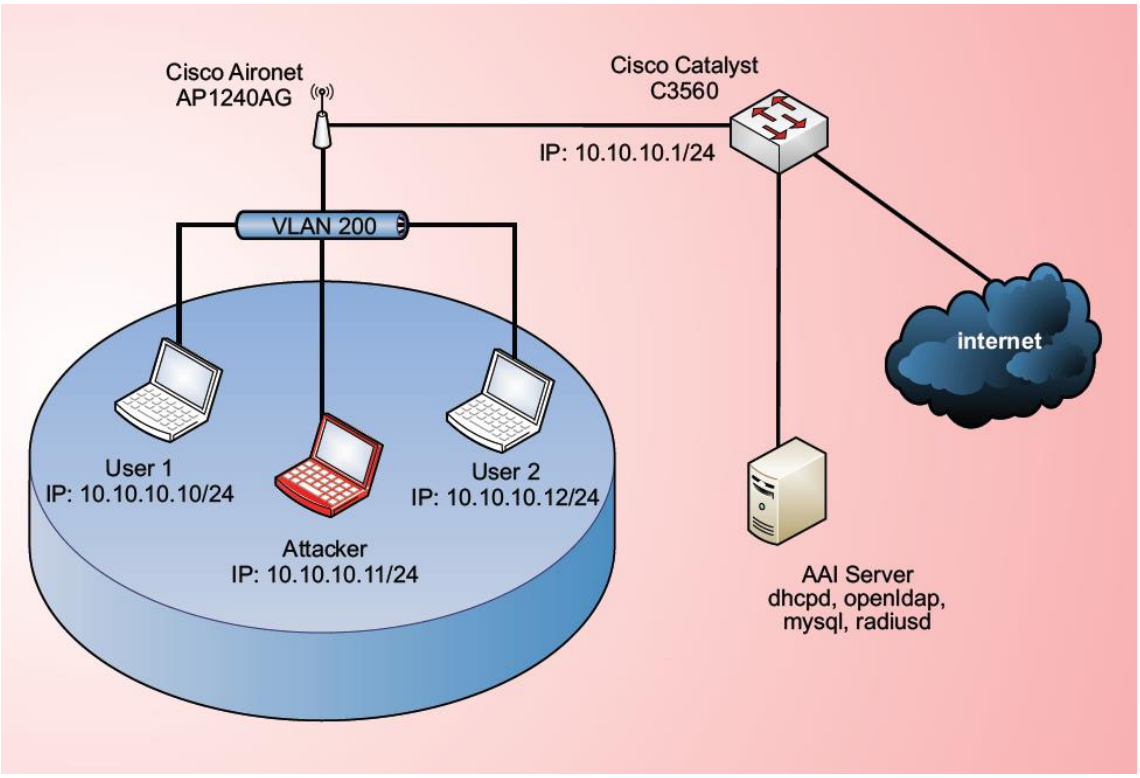
2.6 Ločevanje omrežja v ločena omrežja VLAN

Kot je razvidno iz vzorčnih konfiguracij omrežja Eduroam, omrežje zahteva ločevanje uporabnikov in dostopnih točk v ločeni omrežiji VLAN.

2.7 Pomanjkljivosti omrežja Eduroam

Brezžično omrežje Eduroam ima svoje varnostne pomanjkljivosti. Mogoča je zloraba z napadom *Man-in-the-middle attack* (napad, s katerim se napadalec postavi med žrtve in prisluškuje prometu), z zastrupljanjem tabele ARP [20] (tabela ARP služi za pretvorbo naslova IP v strojni naslov) in pridobitev naslova IP ob uspešni avtentikaciji z uporabo virtualnega računalnika in uporabo mostu (*bridge* je način za povezovanje dveh lokalnih

omrežij) med avtenticiranim odjemalcem in virtualnim računalnikom brez možnosti izsleditve napadalca [1, 2, 3].



Slika 2: Napad *man-in-the-middle* [1]

2.8 FreeRadius

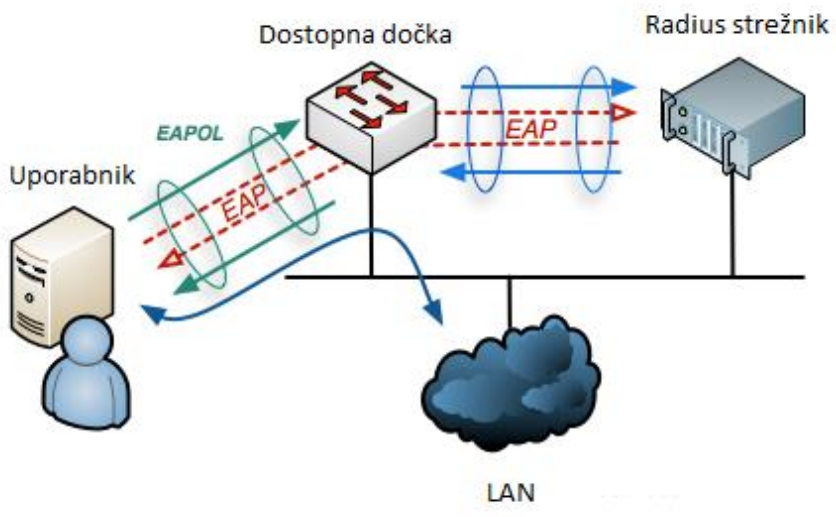
FreeRadius *(Free Remote Authentication DialIn User Service)* je strežnik, namenjen Unixu in podobnim operacijskim sistemom, ki ga lahko uporabljamo za avtentikacijo pri dostopu do nekega omrežja. Uporabniške račune lahko shranjujemo v podatkovnih bazah (Mysql, PostgreSQL, Oracle) ali v LDAP *(Lightweight Directory Access Protocol).* Podpira vse najpogosteje uporabljene možnosti avtentikacije vključno z EAP-TTLS. [6, 9]

2.9 802.1X

802.1x je standard, ki specificira način za avtentikacijo. Čeprav se večinoma uporablja za brezžična omrežja, je bil razvit za uporabo na žičnih omrežjih. Poznan je tudi kot EAPol – EAP preko LAN-a *(EAP over LAN).* 802.1X definira le proces za avtentikacijo, ne specificira pa vrste avtentikacije ali enkripcije med odjemalcem in strežnikom. Uporablja se ga v kombinaciji s strežnikom Radius za avtentikacijo. V avtentikaciji sodelujejo tri strani: odjemalec, avtentikator in avtentikacijski strežnik. Odjemalec je lahko računalnik/prenosnik, ki se želi povezati v omrežje LAN/WLAN, avtentikator, ki je lahko dostopna točka ali stikalo, ter avtentikacijski strežnik, na katerem teče strežnik Radius. [7, 8]

Potek avtentikacije je sledeč:

- avtentiktor pošlje odjemalcu paket z zahtevo EAP takoj, ko zazna, da je odjemalec aktiven;
- odjemalec pošlje avtentikatorju odziv EAP, ki ga posreduje strežniku Radius;
- strežnik za preverjanje pristnosti pošlje izziv nazaj avtentikatorju, ta pa ga posreduje odjemalcu;
- odjemalec odgovori na izziv avtentikatorju in pri tem posreduje podatke za dostop;
- če odjemalec posreduje pravo identiteto, strežnik odgovori s sporočilom, da je odjemalec sprejet. Avtentikator tako dovoli odjemalcu dostop do omrežja LAN/WLAN.



Slika 3: Delovanje standarda 802.1x [7]

2.10 SecureW2

SecureW2 je programska oprema, ki omogoča uporabo avtentikacije EAP-TTLS na operacijskih sistemih Windows XP, Vista in 7. Uporaba odjemalca na operacijskem sistemu Windows 8 ni potrebna, saj je podpora že vgrajena v sam operacijski sistem. Enako velja tudi za operacijske sisteme Linux in Mac OS.

2.11 WPA in WPA2

WPA in WPA2 sta tehnologiji za varen dostop do brezžičnega omrežja. WPA2 (AES-CCMP) je na voljo v vseh brezžičnih napravah od leta 2006. Narejen je bil z namenom povečanja varnosti uporabe brezžičnega omrežja v primerjavi z WPA (RC4-TKIP), saj uporablja močnejšo enkripcijo. Algoritem TKIP *(Temporal Key Integrity Protocol)* ima varnostne luknje, zato ni priporočljiv za uporabo z WPA2. WPA2 je sposoben uporabe TKIP ali pa priporočen algoritem za kriptiranje AES. [16]

2.12 AES in TKIP

AES in TKIP sta algoritma za šifriranje brezžične povezave. TKIP je bil razvit z namenom povečanja varnosti brezžične povezave brez menjave vezja v napravah zaradi odkritih varnostnih lukenj pri uporabi načina zaščite WEP (algoritem za zaščito brezžičnega omrežja, ki zaradi varnostnih lukenj ni primeren za uporabo). Za zagotavljanje še večje varnosti je bil razvit algoritem AES *(Advanced Encryption Standard)*. Z uporabo algoritma AES zagotovimo večjo varnost, vendar je mogoče, da ga vse naprave, ki bi omrežje uporabljale, ne podpirajo. [16]

2.13 DHCP – omrežni protokol za dinamično nastavljanje naprave

DHCP je protokol, uporabljen za dinamično nastavljanje internetnega naslova gostitelja. Skrbi za dodeljevanje naslovov IP uporabnikom omrežja, da lahko med sabo komunicirajo. Implementiran je v modelu klient-strežnik, kjer klient zahteva podatke za konfiguracijo, kot so naslov IP, omrežni prehod in imenski strežnik. Strežnik mu te podatke vrne in tako lahko uporabnik začne uporabljati omrežje. DHCP hkrati skrbi za vzdrževanje baze prostih naslovov IP. Ko strežnik dobi odjemalčevo zahtevo, najprej ugotovi, na katero omrežje je uporabnik priključen, nato pa klientu dodeli pravilno konfiguracijo. Strežnik DHCP dodeli naslov IP svojim klientom le za določen čas. Ti morajo poskrbeti za obnovo njihovih naslovov IP, preden se dodeljeni čas naslova izteče.

Dodeljevanje naslova IP poteka v štirih fazah [24]:

- Prva faza: računalnik ob priklopu na omrežje pošlje sporočilo »DHCPDISCOVER«. Ker še nima omrežnih nastavitev, je sporočilo poslano z naslova IP 0.0.0.0 cilju z naslovom IP 255.255.255.255. Strežnik DHCP prejme sporočilo.
- Druga faza: ko strežnik DHCP sprejme sporočilo »DHCPDISCOVER«, nanj odgovori s sporočilom »DHCPOFFER«. V sporočilu pošlje strežnik odjemalcu nastavitve za konfiguracijo omrežne kartice. Sporočilo je poslano kot promet *broadcast* na naslov IP 255.255.255.25.
- Tretja faza: odjemalec strežniku odgovori s sporočilom »DHCPOFFER«. S tem mu sporoči, da želi uporabiti nastavitve omrežja, ki mu jih je strežnik posredoval v sporočilu »DHCPOFFER«. »DHCPREQUEST« ima kot izvorni naslov IP še vedno nastavljen 0.0.0.0, saj še nima dovoljenja za uporabo nastavitev, poslanih s strežnika DHCP.
- Četrta faza: ko strežnik prejme odjemalčev »DHCPREQUEST, pošlje odjemalcu sporočilo »DHCPACK« in mu s tem sporoči, da ima dovoljenje za uporabo dodeljenega naslova IP.

2.14 IP helper

IP helper služi za pomoč pri dodeljevanju naslova IP klientu. Če strežnik DHCP ni lociran v lokalen omrežju, usmerjevalnik blokira promet *broadcast*, ki je potreben za pridobivanje naslova IP s strani strežnika DHCP. Ukaz »ip helper-address« omogoča usmerjevalniku, da pakete, namenjene strežniku DHCP, odda na določen strežnik, katerega IP naslov določimo s tem ukazom. [23]

2.15 VLAN – navidezna krajevna omrežja *(Virtual Local Area Network)*

Navidezna krajevna omrežja omogočajo upravljalcu omrežja logično segmentacijo LAN-a v ločene domene *broadcast*. Ker gre za logično in ne fizično segmentacijo, lociranje delovnih postaj na isti lokaciji ni več potrebno. Uporabniki v različnih zgradbah lahko tako pripadajo istim omrežjem LAN. VLAN omogoča definiranje domene *broadcast* tudi brez uporabe usmerjevalnikov. Programska oprema nato določi, kateri uporabnik bo pripadal kateri domeni *broadcast*. Usmerjevalnike potrebujemo za komunikacijo med različnimi omrežji VLAN. [18]

2.15.1 Zakaj uporabljati VLAN?

- Zmogljivost. V omrežjih, kjer se pretaka veliko prometa preko *broadcasta* in *multicasta*, VLAN-e uporabljamo za zmanjševanje pošiljanja prometa na nepotrebne lokacije. Primer: če imamo v omrežju 10 uporabnikov in jih le 5 uporablja promet *broadcast*, lahko tako omrežje razdelimo v dve ločeni omrežji VLAN. S povečanjem prometa preko usmerjevalnika se povečujejo odzivni časi, kar posledično vpliva na zmogljivost omrežja. Uporaba VLAN-ov zmanjšuje uporabo usmerjevalnikov, saj lahko ustvari domene *broadcast* kar s stikali.
- Kreiranje virtualnih delovnih skupin. Večja podjetja, v katerih so oddelki ločeni na različnih lokacijah in je med uporabniki veliko prometa *broadcast* in *multicast*, uporabljajo VLAN-e za združevanje uporabnikov v enaka omrežja LAN. Brez VLAN-ov bi sodelovanje oddelkov bilo mogoče le, če bi vse zaposlene premaknili na isto lokacijo.
- Lažja administracija. V primeru premikanja uporabnika med omrežji LAN ima upravljalec omrežja z njim dodatno delo (konfiguracija stikal in usmerjevalnikov). V primeru uporabe omrežja VLAN ne potrebujemo ne fizičnih posegov in ne nove dodatne opreme.
- Varnost. Uporabnikom, ki uporabljajo iste podatke, lahko dodelimo isto omrežje VLAN. S tem zmanjšamo možnost, da bi ostali uporabniki omrežja prišli do podatkov.

2.15.2 Delovanje omrežja VLAN

Ko stikalo dobi podatke od naprave, te podatke označi z identifikatorjem VLAN. Ta pove, iz katerega omrežja VLAN je podatek prišel. Taka metoda označevanja se

imenuje eksplicitno označevanje. Kakšnemu VLAN-u pripadajo podatki, je mogoče določiti tudi z implicitnim označevanjem. Določevanje, iz katerega VLAN-a so prišli podatki, je določeno z informacijo o vratih, iz katerih je podatek prišel. Označevanje prometa je mogoče na več načinov:

- z informacijo o vratih, na katere je uporabnik priklopljen;
- z porabno strojnega naslova omrežne kartice (MAC);
- z uporabo internetnega naslova;
- z uporabo kombinacije naštetih načinov.

Če želimo uporabljati katero koli od zgoraj naštetih metod, morajo imeti vsa stikala enotno bazo podatkov za označevanje prometa. Primer: če uporabljamo označevanje na podlagi vrat, mora baza vsebovati podatke, katera vrata pripadajo kateremu VLAN-u. Stikala določajo, ali bo podatek potoval naprej po omrežju LAN ali VLAN. Ko stikalo to določi, mora hkrati tudi določiti, ali bo podatek potreboval identifikator VLAN ali ne. Če je podatek namenjen napravi, ki omrežja VLAN prepozna, je podatku dodan identifikator VLAN (takšne naprave so priklopljene na vrata v načinu *trunk*). V nasprotnem primeru se napravi pošlje podatek brez identifikatorja (naprava priklopljena na vrata v načinu *access*).

2.15.3 Podatkovni okvir

Podatkovni okvir služi za enkapsulacijo podatkov in ustvari paket za pošiljanje preko omrežja. Sestavljen je iz preambule (začetek okvirja), izvornega strojnega naslova, ciljnega strojnega naslova, tipa, podatkov in podatkov za zaznavanje napak. [25]

Preambula	Začetek ločila okvirja	ponorni naslov MAC	izvorni naslov MAC	Tip	Podatki	CRC

Slika 4: Zgradba podatkovnega okvirja

2.15.4 standard VLAN: IEEE 802.1Q

IEEE 802.1Q je mrežni standard, ki podpira uporabo VLAN-ov v omrežjih. Standard definira sistem označevanja mrežnih okvirjev in sprejema postopke, ki jih stikala in mostovi uporabljajo pri obravnavi teh okvirjev. [26]

2.15.5 Protokol 802.1Q za označevanje v okvirju

802.1Q doda podatkovnemu okvirju 32-bitno informacijo o označevanju prometa. [26]

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID

Slika 5: 32 bitov, ki jih standard doda okvirju

- TPID: 16 bitov podatkov, ki definirajo okvir kot IEEE 802.1Q označen okvir
- TCI: informacije o označevanju;
- PCP: 3-bitna vrednost, ki pove kakšno prioriteto ima okvir;

- DEI: 1-bitno polje služi za označitev okvirjev, primernih za pasti v primeru zastojev;
- VID: definira, kateremu VLAN-u pripada okvir.

2.15.5.1 Vrste VLAN-ov

- Fizična plast – VLAN pripadnost glede na vrata: Pripadnost, kateremu VLAN-u pripada katera naprava, lahko določimo glede na to, kateremu VLAN-u pripadajo vrata, na katere je naprava priključena. Slabost takega načina uporabe je, da ne omogoča mobilnosti. Če se uporabnik premakne na drugo lokacijo, mora upravljalec omrežja znova nastaviti VLAN na novi lokaciji.
- Povezovalna plast – pripadnost VLAN glede na naslov MAC: Uporabnik je postavljen v omrežje VLAN, glede na njegov strojni naslov omrežne kartice. Takšen način uporabe dodeljevanja VLAN-ov uporabnikom odstrani problem mobilnosti, vendar se pojavi nova težava. Uporabnikom je potrebno predhodno določiti, kateri VLAN jim bo dodeljen. Pri omrežjih z velikim številom uporabnikov to opravilo ni lahko.
- Podatkovna plast – pripadnost VLAN glede na vrsto protokola (IP, IPX, AppleTalk, Decnet, …): Pripadnost VLAN-u lahko določimo glede na vrsto protokola, ki jo dobimo v glavi povezovalne plasti.
- Omrežna plast – pripadnost VLAN glede na podomrežni naslov: Pripadnost je vezana na informacijo iz omrežne plasti. Podomrežni naslov omrežja je lahko uporabljen za določevanje pripadnosti VLAN-u.
- Višje plasti – Postavitev uporabnika v VLAN-e je mogoča tudi glede na aplikacijsko plast.

2.15.6 Vrste povezav VLAN

Glede na sposobnost uporabe VLAN-ov priključenih naprav so naprave v omrežjih lahko povezane na tri načine:

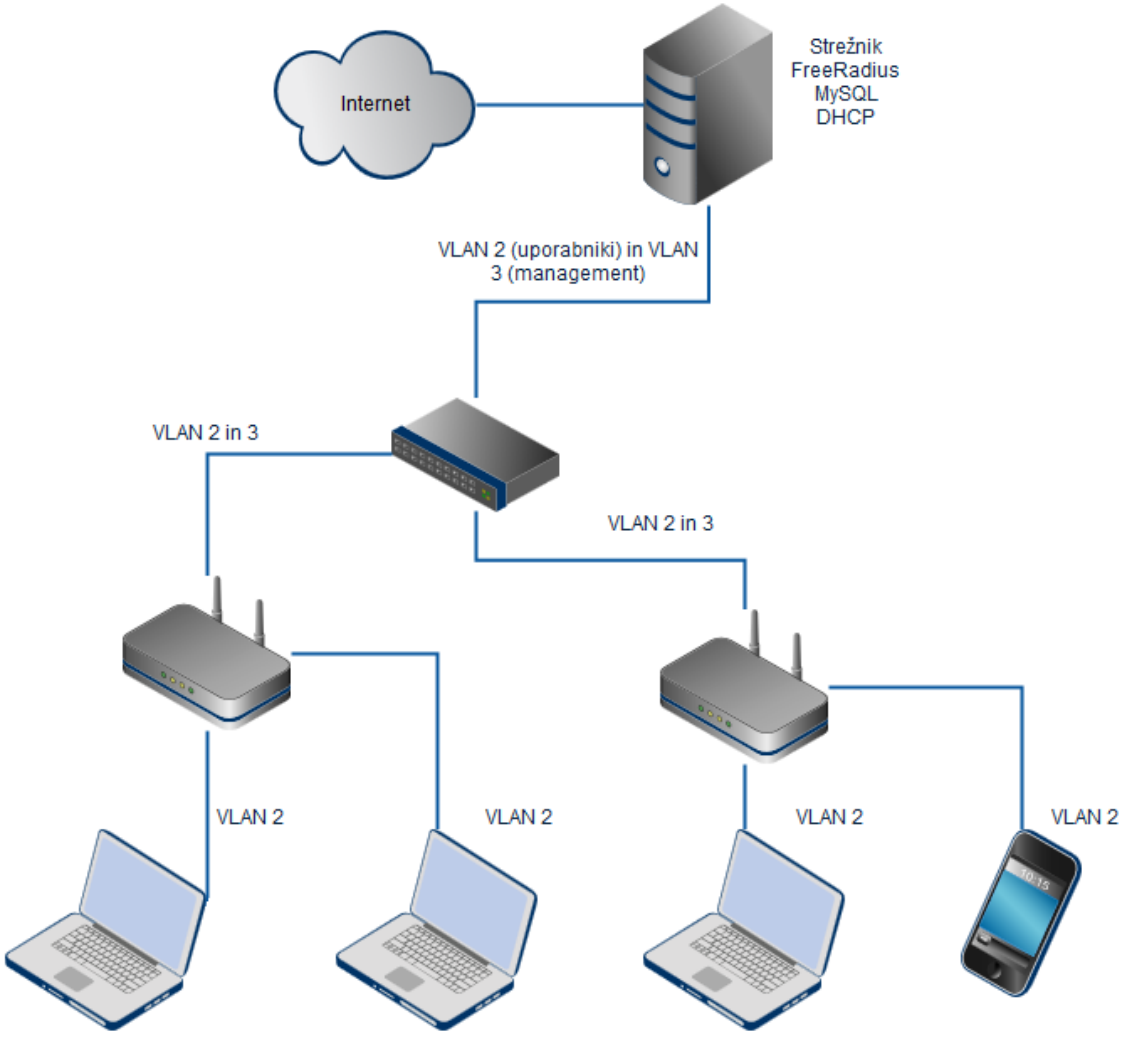
- *Trunk link*: vse naprave, povezane na tak način, morajo znati prepoznati označevalni okvir. Vsak poslan okvir mora imeti dodano posebno vrsto glave.
- *Access link*: uporabljamo ga za priklop naprav, ki ne znajo uporabljati omrežij VLAN. Vsi okvirji na *access linku* morajo biti implicitno označeni.
- *Hybrid link*: To je kombinacija prvih dveh načinov povezovanja naprav v omrežja VLAN. Razlika med hibridnim in načinom *trunk* je, da vrata *trunk* vse neoznačene pakete pošljejo v privzet VLAN, hibridni način pa dovoli pošiljanje takih paketov tudi v ostale VLAN-e.

3 Opis problema

Cilj diplomske naloge je dinamično razvrščanje uporabnikov v omrežja VLAN na dostopnih točkah. Za realizacijo take vrste dodeljevanja omrežij VLAN uporabnikom je potrebna draga omrežna oprema. Zato bomo v nadaljevanju poizkušali ugotoviti, ali je mogoče takšno dodeljevanje implementirati tudi na cenejših dostopnih točkah. V našem primeru bomo uporabili Linksys WRT54GL in računalnik Raspberry Pi.

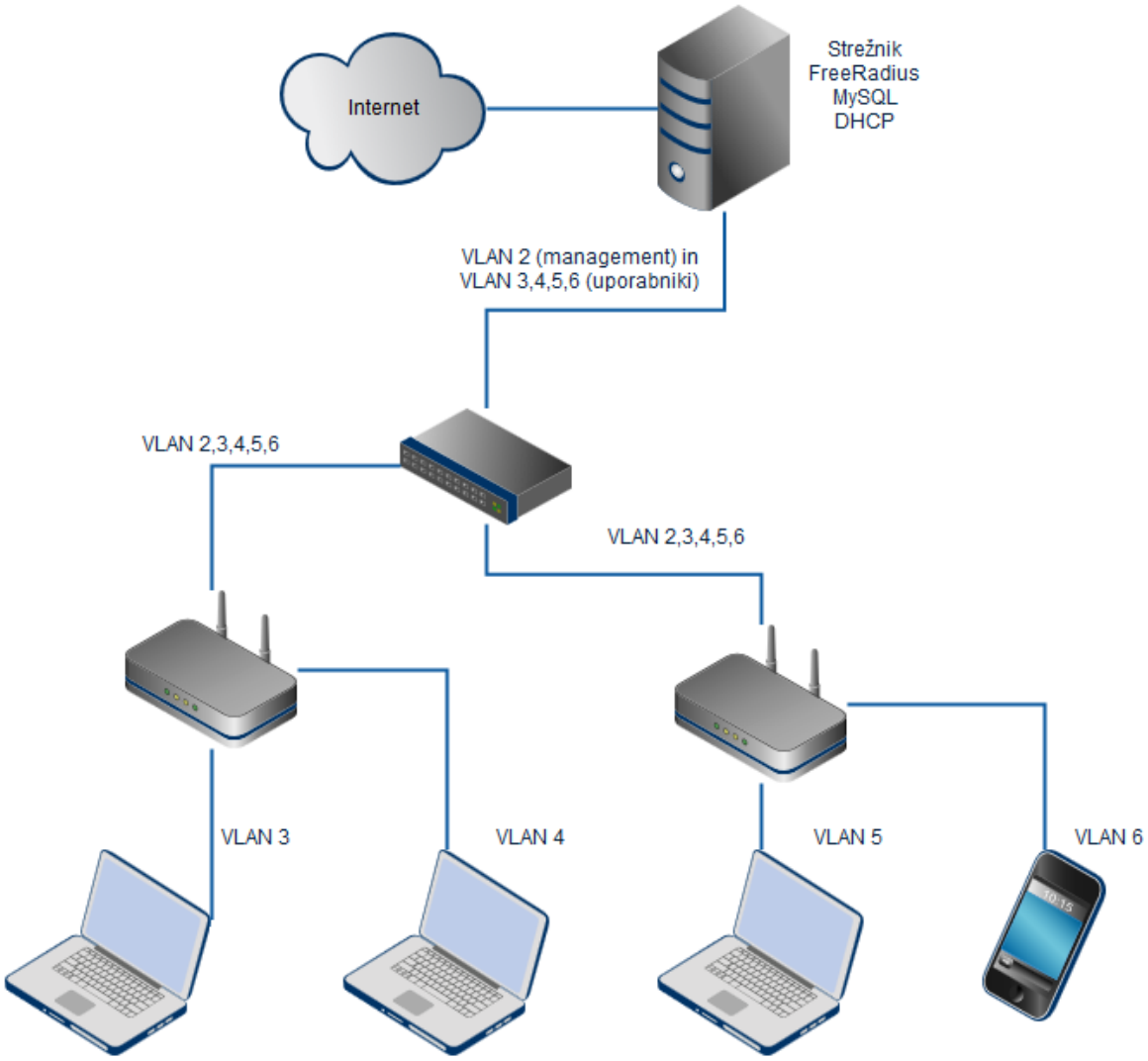
Ker je želja doseči čim boljšo varnost in omogočiti uporabo dostopnih točk v omrežju Eduroam, smo se odločili, da bomo poizkusili nadgraditi varnost omrežja. Omrežje Eduroam po specifikacijah zahteva ločevanje uporabnikov v uporabniško omrežje VLAN, dostopne točke pa ločuje v t. i. omrežje za upravljanje. Tako bo na strežniku nameščen strežnik FreeRadius, ki bo skrbel za avtentikacijo uporabnikov. Uporabljali bomo avtentikacijo EAP-TTLS in šifriranje povezave AES, podobno kot to uporablja omrežje Eduroam.

Na Sliki 6 je prikazan primer omrežja Eduroam, ki uporabnike in dostopne točke ločuje v dve različni omrežji VLAN. Uporabniki tako dobijo dostop do omrežja VLAN 2, za upravljanje dostopnih točk pa bomo uporabili omrežje VLAN 3.



Slika 6: Struktura omrežja Eduroam

Za zagotavljanje višje varnosti omrežja bomo uporabnike ločevali v ločena omrežja VLAN in s tem preprečili določene napade, ki so mogoči na omrežje Eduroam. Kot je prikazano na Sliki 7, bomo dostopne točke upravljali z omrežjem VLAN 2, vsakemu uporabniku pa bo dodeljen natanko en VLAN.



Slika 7: Nadgradnja omrežja Eduroam

4 Rešitev

4.1 Konfiguracija strežnika

Na strežniku bomo uporabili ustrezne nastavitve za postavitev želenega omrežja. V ta namen potrebujemo na našem strežniku nameščen strežnik MySql, FreeRadius in DHCP. V nadaljevanju bomo opisali, kako omenjene strežnike nastavimo, da so primerni za uporabo v takšnem omrežju.

4.1.1 MySQL

Ker bomo za hranjenje uporabniških računov uporabili podatkovno bazo, je potrebno na strežniku, na katerem teče operacijski sistem Linux Ubuntu, najprej namestiti programski paket MySQL. To naredimo z ukazom: »Apt-get install mysql-server-5.5«.
Med namestitvijo strežnika MySQL vpišemo podatke, ki so potrebni za zaključek namestitve (npr. geslo za uporabnika »root«).
Na strežniku, na katerem imamo nameščen MySQL, ustvarimo novo podatkovno bazo, ki jo bo uporabljal strežnik FreeRadius.

```
root@diploma:~# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 82
Server version: 5.5.31-0ubuntu0.13.04.1 (Ubuntu)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reser
ved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input stat
ement.

mysql> CREATE DATABASE radius;
```

Slika 7: Dodajanje nove baze z imenom »radius«

Dodamo novega uporabnika in mu nastavimo geslo, s katerim bo dostopal do podatkov v naši bazi MySql:

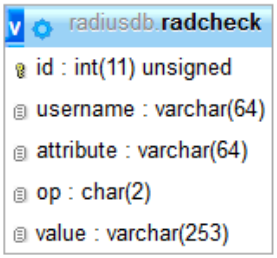
```
mysql> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "geslo";
Query OK, 0 rows affected (0.00 sec)

mysql>
```

Slika 8: Dodajanje uporabnika z imenom »radius« in geslom »geslo«

Ko imamo ustvarjenega uporabnika in tabelo, ki jo bo uporabljal FreeRadius, v bazo uvozimo tabele, potrebne za delovanje strežnika FreeRadius:

```
root@diploma:~# mysql -u root -p radius < /etc/freeradius/sql/mysql/sche
ma.sql
```

Slika 9: Uvoz sheme v podatkovno bazo



Slika 10: Tabela »radcheck«, v katero bomo shranjevali uporabnike

Uvožena shema v podatkovni bazi vsebuje več tabel, za postavitev testnega omrežja pa potrebujemo le tabelo »radcheck«. Vanjo bomo v nadaljevanju shranili uporabniške račune.

S tem imamo pripravljeno podatkovno bazo, ki jo bo uporabljal strežnik FreeRadius.
Da se bomo lahko avtenticirali z uporabniškim imenom in geslom, dodamo v našo podatkovno bazo še enega uporabnika:

```
root@diploma:~# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 79
Server version: 5.5.31-0ubuntu0.13.04.1 (Ubuntu)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reser
ved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input stat
ement.

mysql> use radius;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> INSERT INTO radcheck (UserName, Attribute, Value) VALUES ('uporab
nik2','Password','geslo');
Query OK, 1 row affected (0.04 sec)

mysql>
```

Slika 11: Dodajanje novega uporabnika v podatkovno bazo, ki bo uporabljal avtentikacijo Radius

Geslo bi lahko shranili v bazo tudi šifrirano, vendar to za demonstracijo trenutno ni potrebno. Če bi želeli v bazi shranjevati šifrirana gesla, bi to storili z uporabo stavka SQL na sledeči način:
INSERT INTO `radcheck` (`id` ,`username` ,`attribute` ,`op` ,`value`) VALUES (NULL , 'test', 'MD5-Password', ':=', MD5 ('geslo')).

Tako bi v bazo shranili geslo, šifrirano z algoritmom MD5, strežnik FreeRadius pa bi ob prejeti zahtevi za avtentikacijo uporabnika njegovo geslo šifriral z istim algoritmom in ga primerjal z geslom v bazi. Zato moramo biti pozorni in v polju »attribute« nastaviti lastnost gesla »MD5-Password«, saj bo v tem primeru strežnik FreeRadius vedel, da je geslo, shranjeno v bazi, šifrirano z algoritmom MD5.

4.1.2 Strežnik DHCP

Strežnik DHCP bo dodeljeval naslove IP uporabnikom našega omrežja. Na njem najprej poženemo ukaz za namestitev strežnika DHCP. Obstaja več strežnikov DHCP (isc-dhcp-server, udhcpd …), ki jih lahko namestimo na strežnik. Izbrali smo strežnik isc-dhcp-server, zato ga tudi namestimo z ukazom »Apt-get install isc-dhcp-server«.
Za omrežno kartico, ki bo priklopljena na naše stikalo, nastavimo v datoteki /etc/default/isc-dhcp-server naslednje nastavitve:
INTERFACES="eth0"
Za vsako omrežje VLAN je potrebno nastaviti še nastavitve DHCP. To storimo v datoteki /etc/dhcp/dhcpd.conf.
Primer konfiguracije strežnika DHCP za VLAN 2 in VLAN 3:

```
#VLAN 2
subnet 10.10.12.0 netmask 255.255.255.0 {
  range 10.10.12.5 10.10.12.30;
  option domain-name-servers 8.8.8.8;
  option routers 10.10.12.1;
  option broadcast-address 10.10.12.255;
  option subnet-mask 255.255.255.0;
}

#VLAN3
subnet 10.10.13.0 netmask 255.255.255.0 {
  range 10.10.13.5 10.10.13.30;
  option domain-name-servers 8.8.8.8;
  option routers 10.10.13.1;
  option broadcast-address 10.10.13.255;
  option subnet-mask 255.255.255.0;
}
```

Slika 12: Nastavitve strežnika DHCP

4.1.3 Omrežni vmesnik

V datoteki /etc/network/interfaces nastavimo potrebne VLAN-e. Primer nastavitev za VLAN2 in VLAN3:

```
#VLAN2
auto eth0.2
iface eth0.2 inet static
address 10.10.12.1
netmask 255.255.255.0
network 10.10.12.0
broadcast 10.10.12.255
vlan_raw_device eth0

#VLAN3
auto eth0.3
iface eth0.3 inet static
address 10.10.13.1
netmask 255.255.255.0
network 10.10.13.0
broadcast 10.10.13.255
vlan_raw_device eth0
```

Slika 13: Nastavitve omrežnega vmesnika

Trenutne nastavitve omrežnih vmesnikov lahko vidimo z ukazom »ifconfig«. Spodaj je prikazan primer uporabe ukaza. Dodamo mu ime omrežne kartice in tako dobimo informacije o njej.

```
root@diploma:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:00:21:03:19:de
          inet addr:10.10.10.1  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::200:21ff:fe03:19de/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:15568 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8732 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3310403 (3.3 MB)  TX bytes:3651197 (3.6 MB)
```

Slika 14: Pregled nastavitev omrežne kartice eth0

Na strežniku moramo omogočiti pretok prometa med omrežno kartico, na katero je priklopljena povezava v internet, in tisto, na katero bo priklopljeno stikalo. To naredimo na naslednji način: v datoteki /etc/sysctl.conf nastavimo »net.ipv4.id_forward=1«. Tako z ukazom omogočimo, da strežnik deluje kot usmerjevalnik prometa.

```
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
```

Slika 15: Nastavitev usmerjanja podatkov

Nato dodamo v datoteko /etc/rc.local nastavitve »iptables« (tabela, ki določa pravila in ukaze za paketno filtriranje [17]), ki se bodo zagnale ob zagonu našega računalnika:

```
 GNU nano 2.2.6       Datoteka: /etc/rc.local          Spremenjeno

#!/bin/sh -e

sudo /sbin/iptables -P FORWARD ACCEPT
sudo /sbin/iptables --table nat -A POSTROUTING -o UPLINK -j MASQUERADE

exit 0
```

Slika 16: Nastavitev pravil »iptables«

Funkcija »MASQUERADE« omogoča, da računalniki na zasebnih naslovih IP uporabljajo internet preko prehoda (strežnik Linux) in se v internetu predstavljajo z njegovim javnim naslovom. V primeru uporabe javnih naslovov IP ta funkcija ni potrebna.

4.1.4 FreeRadius

Najprej je potrebno na strežnik namestiti programski paket FreeRadius. Ker ga uporabljamo v kombinaciji s strežnikom MySQL, ki bo poskrbel za hranjenje uporabniških podatkov, je potrebno ob nameščanju namestiti tudi paket, ki bo poskrbel da bo strežnik FreeRadius znal uporabljati podatkovno bazo MySQL. Zato namestimo sledeče programske pakete: »Apt-get install freeradius freeradius-mysql«.
Ker smo za hranjenje podatkov uporabili bazo MySQL, bomo najprej nastavili konfiguracijo FreeRadius-a za dostop do podatkov v njej. V datoteki /etc/freeradius/sql.conf popravimo naslednje podatke:

```
        # Connection info:
        server = "localhost"
        port = 3306
        login = "radius"
        password = "geslo"
```

Slika 17: Podatki za dostop do podatkovne baze v konfiguraciji FreeRadius

S temi nastavitvami omogočimo, da se bo FreeRadius povezal na že prej ustvarjeno podatkovno bazo, ki smo ji že dodali potrebne tabele.

V datoteki /ect/freeradius/eap.conf nastavimo nastavitve za želeno vrsto avtentikacije:

```
eap {
    default_eap_type = ttls
}

ttls {
    default-eap-type = mschapv2
}
```

Da bo strežnik preverjal uporabniška imena in gesla iz podatkovne baze MySQL, v datoteki spremenimo naslednje nastavitve:

```
authorize{
        sql
}
accounting {
        sql
}
session{
         sql
}
```

Da bodo dostopne točke lahko uporabljale strežnik FreeRadius, moramo v nastavitve v datoteki /etc/freeradius/clients.conf dodati še naslove IP dostopnih točk:

```
client 10.10.10.2 {
        secret = testing123
        shortname = accesspoint1
}
client 10.10.10.3 {
        secret = testnogeslo
        shortname = accesspoint2
}
```

Slika 18: Dodajanje klientov v datoteko clients.conf

4.2 Nastavitve usmerjevalnika Cisco 3560

Za prikaz delovanja omrežja smo uporabili stikalo Cisco 3560. Za samo delovanje omrežja bi lahko uporabili katero koli stikalo, ki podpira uporabo omrežij VLAN. Na stikalu je potrebno nastaviti pripadnost vrat VLAN-om. Nanj se preko terminala povežemo s serijskimi vrati. Slika 19 prikazuje, kako nastavimo vrata 1, da lahko uporabljajo VLAN-e od 2 do 10.

```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#description "opis vrat"
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan 2-10
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

Slika 19: Konfiguracija stikala Cisco

Na stikalo bomo povezali strežnik in vse naše dostopne točke. Na Sliki 20 je prikazan primer konfiguracije stikala za tri vrata. Na prva in druga vrata bomo priključili strežnik in dostopno točko. Takšen način imenujemo *trunk access.* Nanje priklopimo naprave, ki se VLAN-ov zavedajo. Na vratih številka 3 je prikazan *access link.* Na taka vrata lahko priklopimo naprave, ki se VLAN-ov ne zavedajo.
Na stikalu Cisco pogledamo nastavitve z ukazom »show running-config«. Po končani konfiguraciji bi morale nastavitve na stikalu zgledati tako, kot prikazuje Slika 20.

```
interface FastEthernet0/1
 description "Server"
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-110
 switchport mode trunk
!
interface FastEthernet0/2
 description "dostopna tocka"
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-110
 switchport mode trunk
!
interface FastEthernet0/3
 description "uporabniska vrata"
 switchport access vlan 2
!
```

Slika 20: Pregled nastavitev na stikalu Cisco

Za zagotavljanje pravilnega delovanja VLAN-ov in strežnika DHCP za vrata, na katera bomo priklopili naprave, ki se VLAN-ov ne zavedajo, moramo na stikalu dodatno nastaviti naslednje nastavitve:

```
interface Vlan2
 ip address 10.10.12.2 255.255.255.0
 ip helper-address 10.10.12.1
!
interface Vlan3
 ip address 10.10.13.2 255.255.255.0
 ip helper-address 10.10.13.1
!
```

Slika 21: Nastavitve VLAN-ov

4.3 Konfiguracija dostopnih točk

4.3.1 Linksys WRT54GL

Linksys WRT54GL je usmerjevalnik, ki smo ga uporabili kot dostopno točko. Na njem teče programska oprema, zgrajena okoli operacijskega sistema Linux. Operacijski sistem DD-WRT usmerjevalniku omogoča brezplačno uporabo večjega števila funkcij. V usmerjevalniku se nahaja Broadcomov procesor BCM5352, s frekvenco 200MHZ, 16MB RAM-a in 4MB pomnilnika. [19]

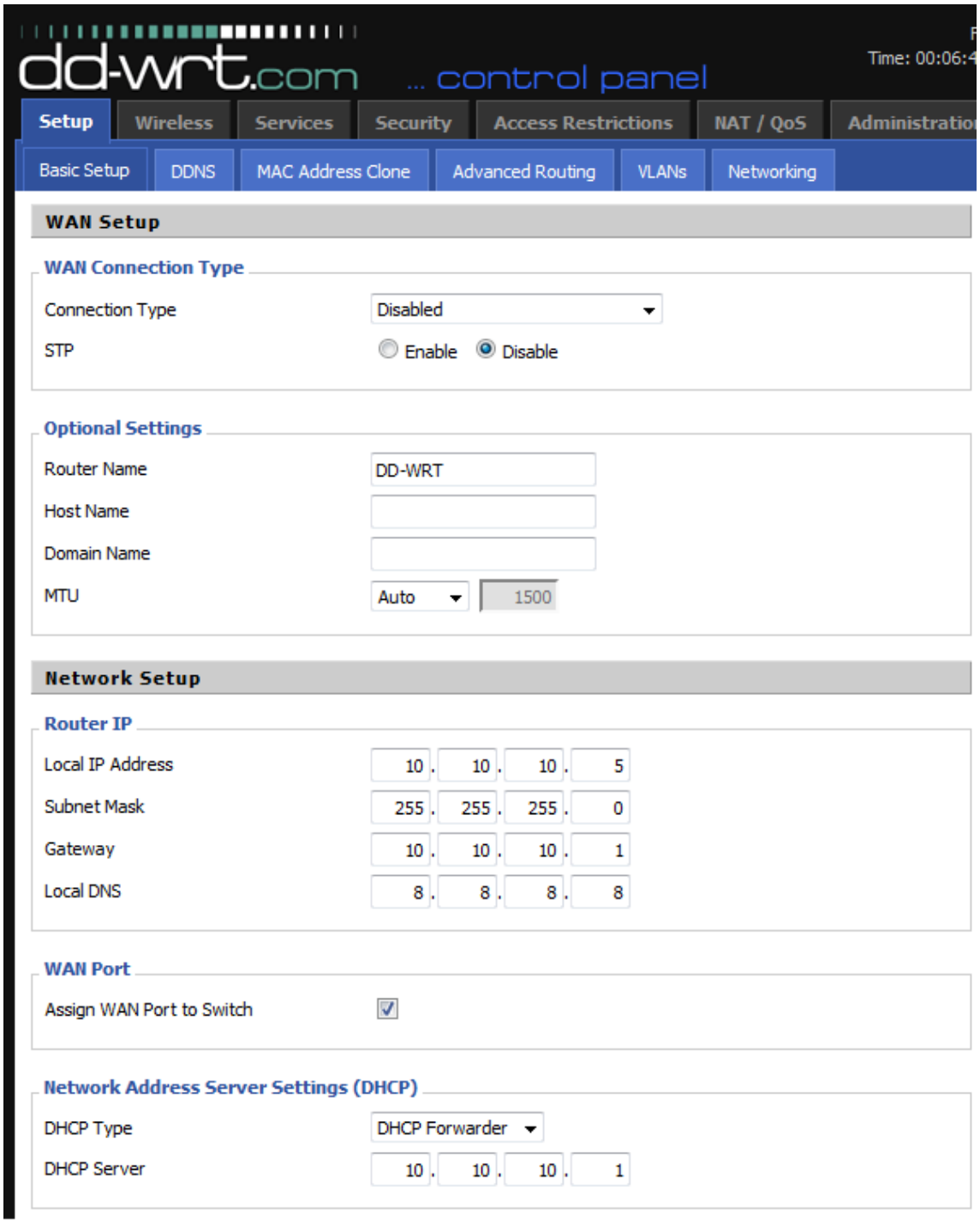
4.3.1.1 DD-WRT

DD-WRT je programska oprema, zasnovana na Linuxu za brezžične usmerjevalnike in dostopne točke. Namenjen je velikemu številu usmerjevalnikov in dostopnim točkam z namenom zamenjave prvotne originalne programske opreme, ki nudi večje število funkcionalnosti. Obstaja več izvedenk DD-WRT (Micro, Mini, Nokaid, Standard, VOIP, VPN, Mega), ki jih lahko uporabimo, odvisno od tega kakšen usmerjevalnik imamo. [11]

4.3.1.2 Konfiguracija dostopne točke WRT54GL z naloženim DD-WRT

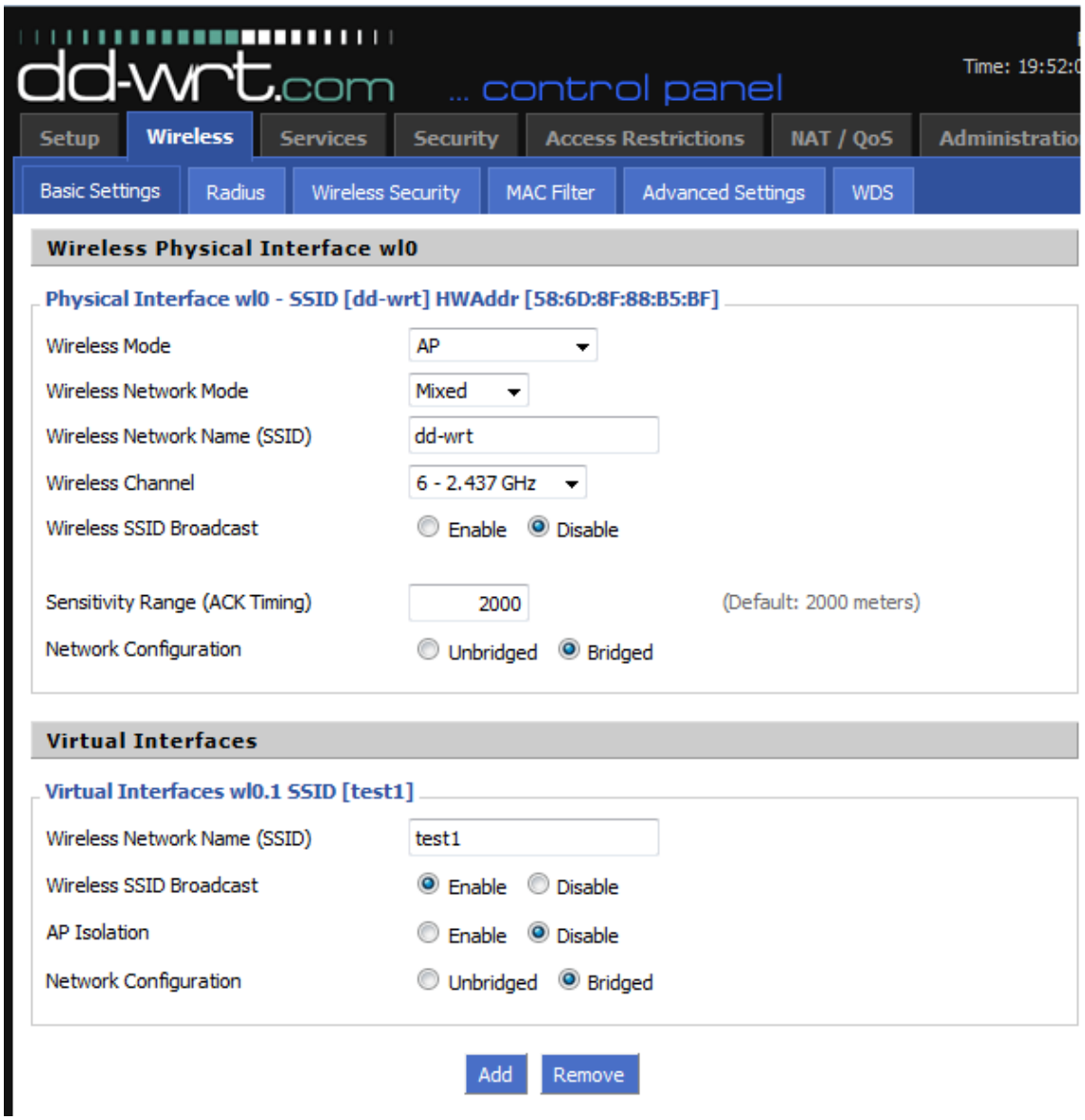
Na dostopni točki moramo pravilno nastaviti konfiguracijo, da bomo uporabnike imeli v ločenem omrežju VLAN, in avtentikacijo, za katero bomo uporabili že nastavljeni strežnik FreeRadius.

Na Sliki 22 so prikazane nastavitve, potrebne za pravilno delovanje dostopne točke. Na dostopni točki vpišemo podatke za pravilen dostop do omrežja ter naslov IP strežnika DHCP.



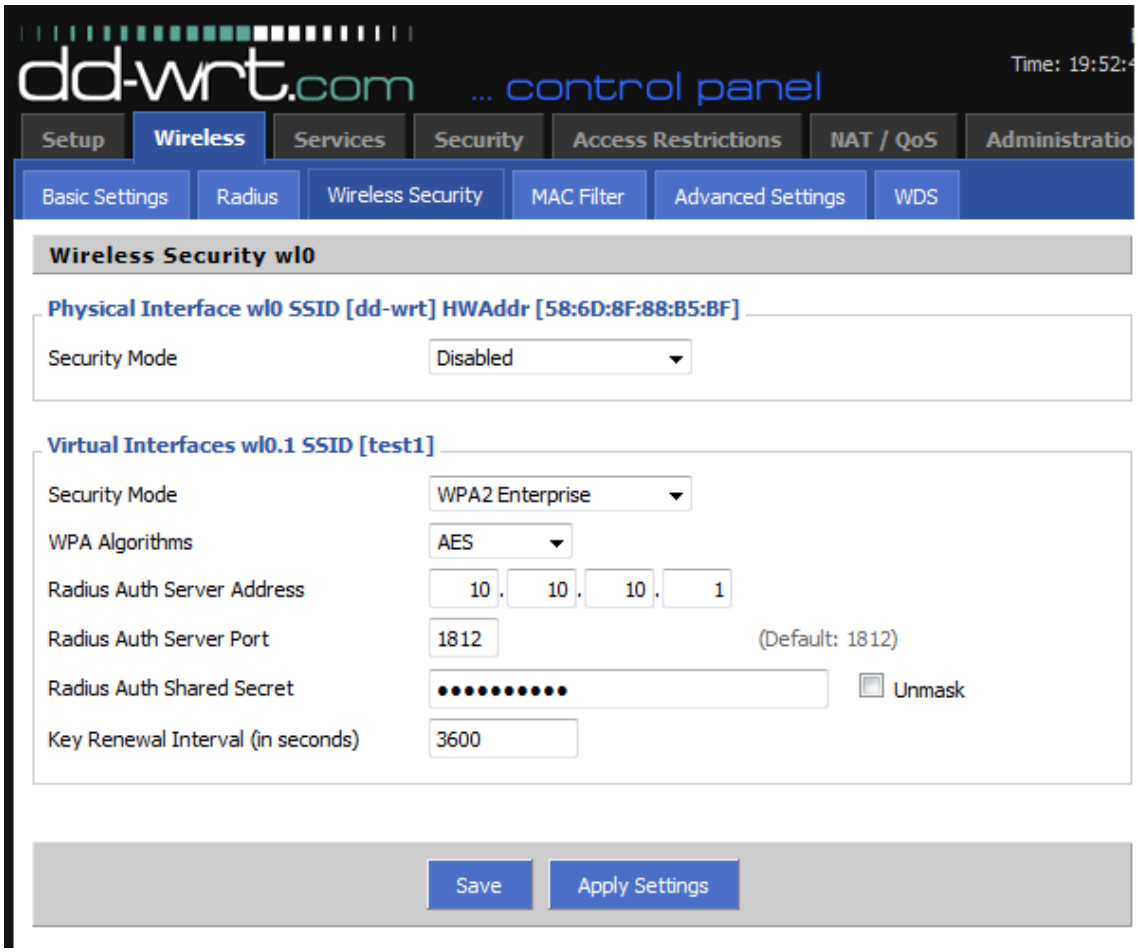
Slika 22: Nastavljanje omrežnih podatkov na dostopni točki Linksys

Nato ustvarimo novo virtualno dostopno točko, ki jo bomo kasneje prestavili v ločen VLAN, kot prikazuje Slika 23.



Slika 23: Dodajanje novega brezžičnega vmesnika

Na dostopni točki moramo nastaviti vrsto zaščite. Ker smo se odločili za uporabo avtentkacije EAP-TTLS s strežnikom FreeRadius, to storimo na način, ki je prikazan na Sliki 24. Za vrsto zaščite izberemo WPA2 Enterprise in v naslov strežnika FreeRadius vnesemo naslov IP strežnika. V datoteki client.conf na strežniku smo že prej dodali naslove IP dostopnih točk ter gesla, ki jih bo dostopna točka uporabljala pri preverjanju avtentikacije. Geslo, ki smo ga nastavili za to dostopno točko, uporabimo tudi v teh nastavitvah.



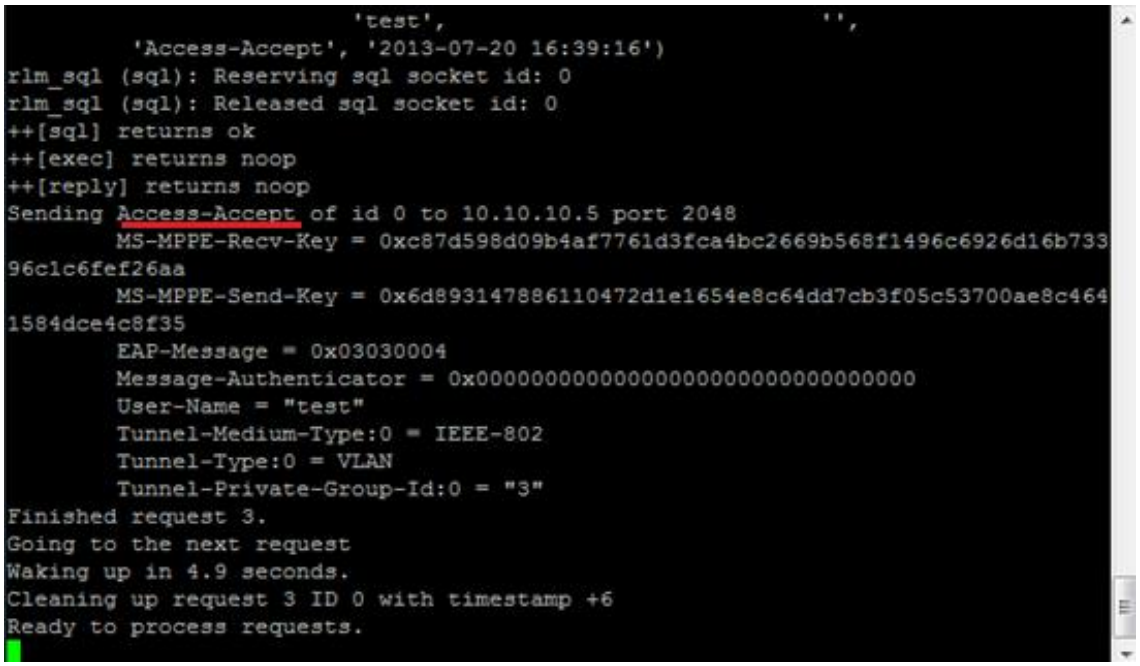
Slika 24: Nastavljanje načina avtentikacije za dostopno točko

Nastavili smo vse potrebne nastavitve za uporabo dostopne točke. Sedaj lahko omrežje testiramo in ugotovimo, če deluje. V ukazno vrstico na strežniku vpišemo ukaz »freeradius -X« in ga zaženemo v razhroščevalnem načinu.

```
 Module: Checking post-auth {...} for more modules to load
 } # modules
} # server
radiusd: #### Opening IP addresses and Ports ####
listen {
        type = "auth"
        ipaddr = *
        port = 0
}
listen {
        type = "acct"
        ipaddr = *
        port = 0
}
listen {
        type = "auth"
        ipaddr = 127.0.0.1
        port = 18120
}
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on authentication address 127.0.0.1 port 18120 as server inner-tunnel
Ready to process requests.
```

Slika 25: Zagon strežnika FreeRadius

Strežnik tako čaka na zahteve s strani dostopnih točk. Nato se z računalnikom povežemo na dostopno točko z uporabniškim imenom in geslom. Zaradi uporabe načina avtentikacije EAP-TTLS, moramo na računalnike, kateri imajo nameščen operacijski sistem, ki te avtentikacije ne podpira namestiti dodatno programsko opremo (SecureW2). V primeru, da imamo pravilno nastavljeno omrežje in dostopne točke, nam bo FreeRadius ob avtentikaciji vrnil obvestilo, ali je bila avtentikacija uspešno izvršena ali ne (Slika 26).



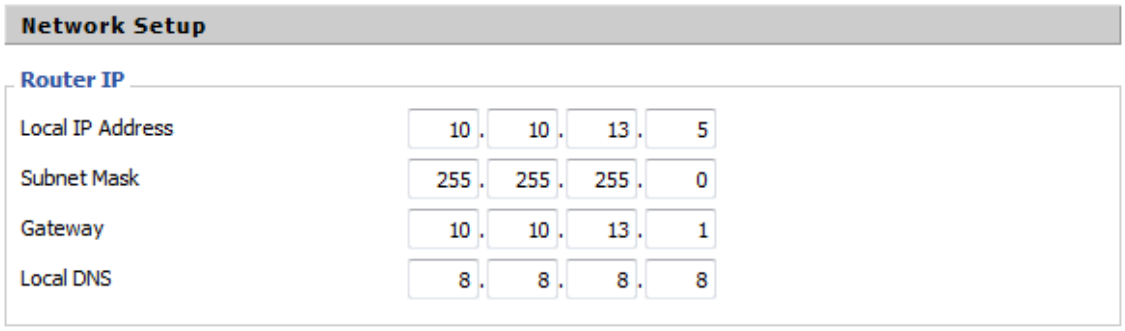
Slika 26: Uspešna avtentikacija

V primeru ustrezne avtentikacije vrne strežnik FreeRadius sporočilo *Access-Accept* (dostop sprejet). Uporabnik je uspešno avtenticiran in lahko uporablja omrežje.

4.3.1.3 WRTGL54 in VLAN-i

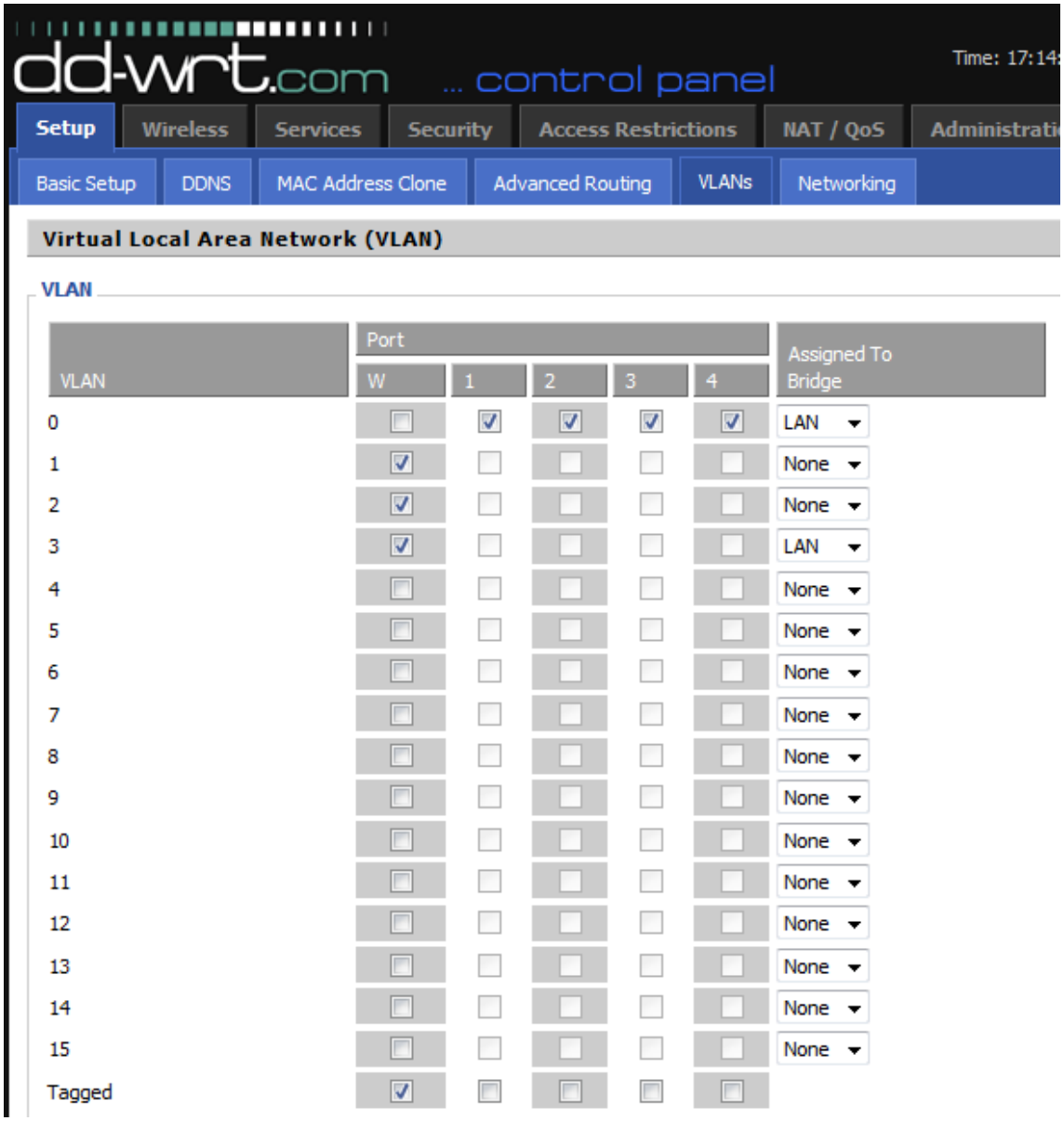
Cilj diplome je ločiti uporabnike v ločena omrežja VLAN, zato bomo v tem poglavju poiskali možnosti, ki nam jih poceni dostopna točka ponuja. Kakor zahtevajo specifikacije omrežja Eduroam, bomo ločili uporabnike in omrežje za upravljanje z dostopnimi točkami. Za demonstracijo bodo uporabniki uporabljali omrežje VLAN 2, dostopne točke pa VLAN 3.

Na dostopni točki bomo popravili nastavitve omrežja. Kot prikazuje Slika 27, je potrebno spremeniti naslov IP in prevzeti prehod.



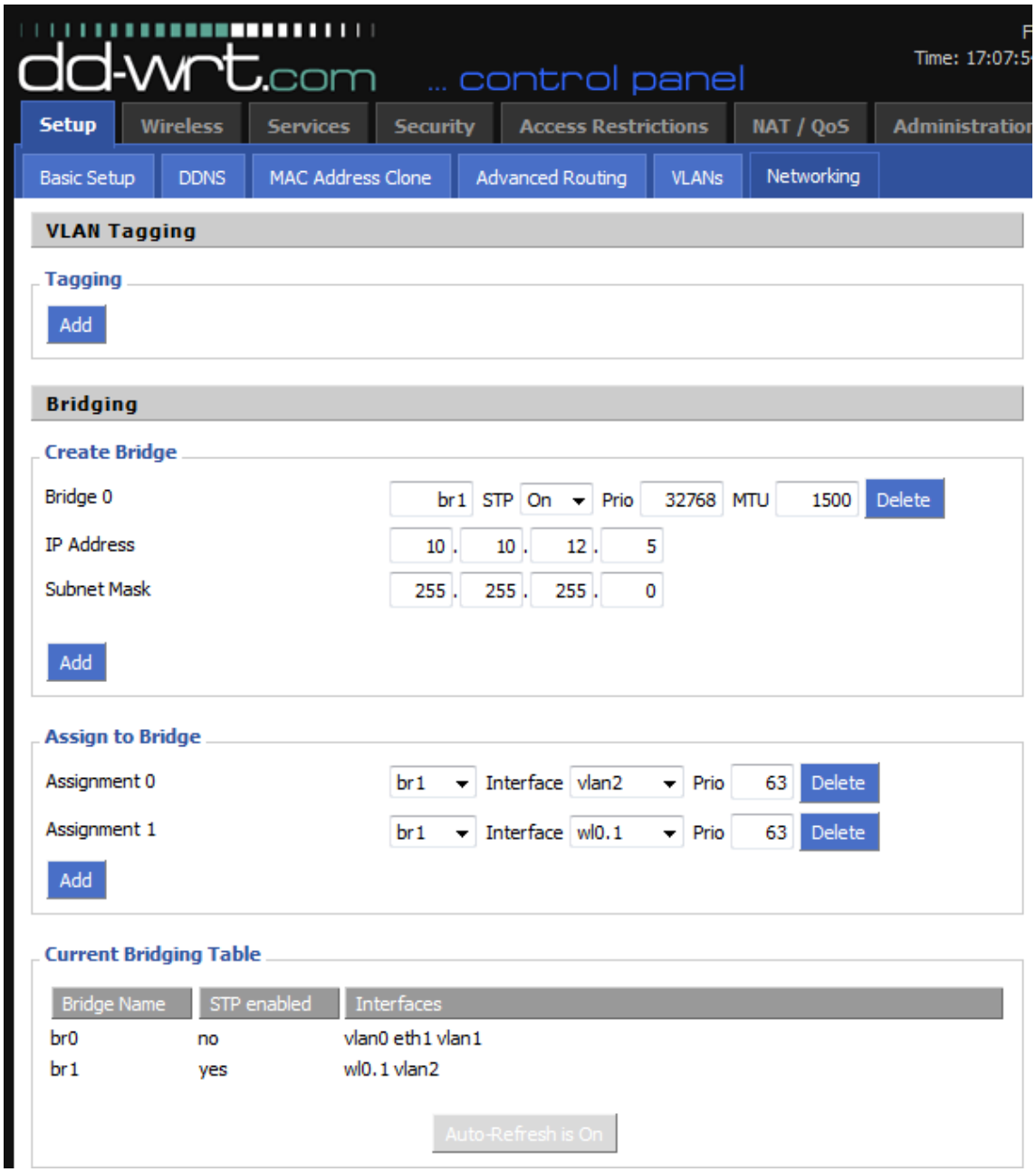
Slika 27: Spremembe omrežnih nastavitev

Ker bo na vrata WAN dostopne točke prišel označen promet, je potrebno nastaviti, do katerih VLAN-ov bo imela dostopna točka dostop. Ker bomo imeli za uporabnike omrežje VLAN 2, za dostopne točke pa VLAN 3, nastavimo naslednje nastavitve:



Slika 28: Nastavitve VLAN-ov

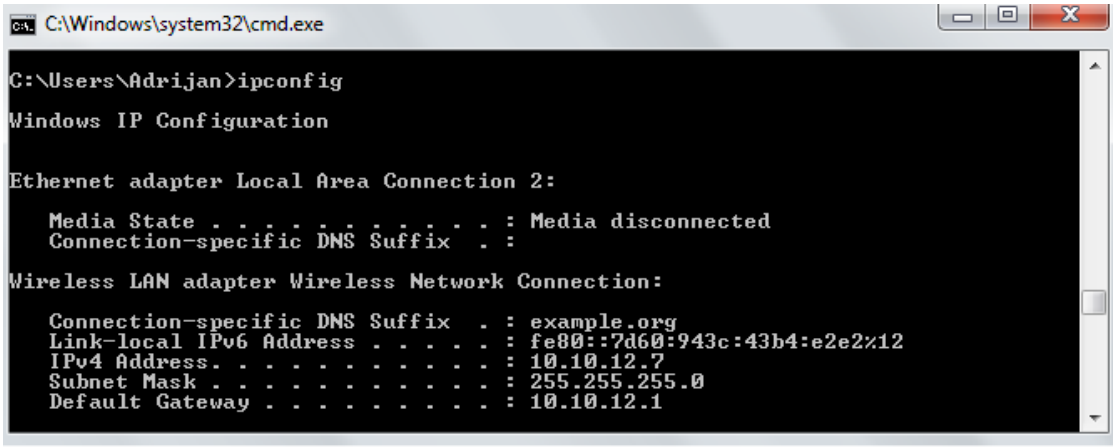
Ko imamo pravilno nastavljena omrežja VLAN in nastavitve dostopne točke za dostop do omrežja, lahko premaknemo naše brezžično omrežje v VLAN 2. Zato ustvarimo nov most, ki mu dodelimo prost naslov IP iz omrežja VLAN 2. Mostu nato dodamo omrežje VLAN 2 in naše virtualno brezžično omrežje wl0.1.



Slika 29: Nastavitev mosta med VLAN2 in wl0.1

Tako smo uspešno ločili omrežje za upravljanje dostopnih točk in uporabnikov. Za preverbo pravilnega delovanja nastavitev je potrebno pregledati, ali se promet pravilno pretaka po našem omrežju in da so na napravi, ki uporablja brezžično omrežje, dodeljeni pravilni naslovi IP.

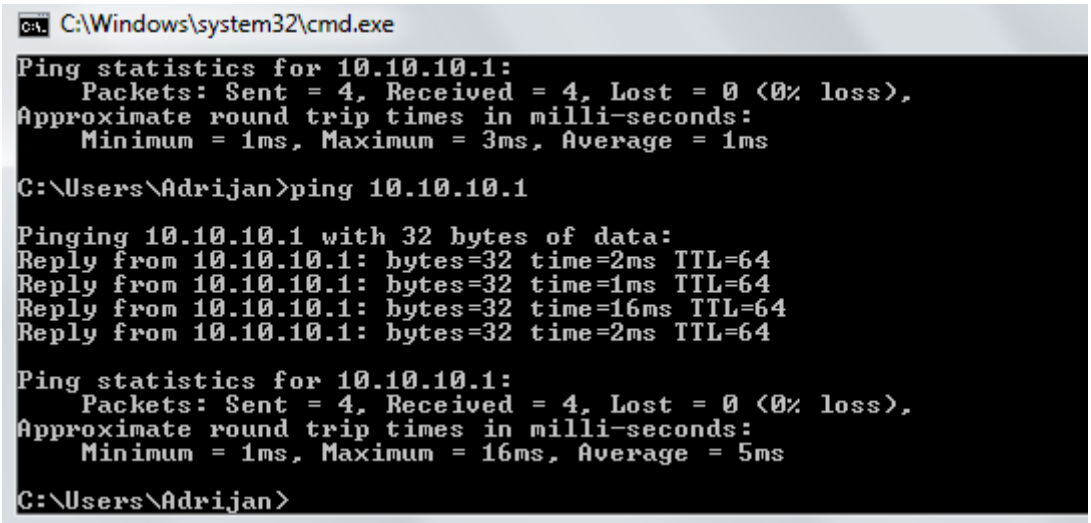
Na brezžični napravi (v našem primeru na prenosniku) poženemo ukazno vrstico in izvršimo ukaz »ipconfig«. S tem preverimo, če smo dobili pravi naslov IP iz omrežja VLAN 2 (Slika 30).



Slika 30: Pregled nastavitev IP, dodeljenih uporabniku

Kot je razvidno iz Slike 30, je naslov brezžične omrežne kartice 10.10.12.7 in prevzeti prihod 10.10.12.1, kar ustreza nastavitvam omrežja VLAN 2. Za resnično pravilnost nastavitev je potrebno še opazovanje pretakanja prometa po omrežju.

Na prenosniku, povezanem na brezžično omrežje, poženemo ukazno vrstico in izvedemo ukaz »ping 10.10.10.1« (naslov strežnika).



Slika 31: Pošiljanje podatkov strežniku

Na strežniku z ukazom »tcpdump vlan 2 and icmp« preverimo promet v omrežju VLAN 2. Iz Slike 32 je razvidno, da so bili vsi štirje poslani paketi prejeti in da so potovali po omrežju VLAN 2.

```
root@diploma:~# tcpdump vlan 2 and icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol deco
de
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
23:24:39.798595 IP 10.10.10.1 > 10.10.12.7: ICMP echo reply, id 1, seq 2
7, length 40
23:24:40.804687 IP 10.10.10.1 > 10.10.12.7: ICMP echo reply, id 1, seq 2
8, length 40
23:24:41.818714 IP 10.10.10.1 > 10.10.12.7: ICMP echo reply, id 1, seq 2
9, length 40
23:24:42.832721 IP 10.10.10.1 > 10.10.12.7: ICMP echo reply, id 1, seq 3
0, length 40
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
root@diploma:~#
```

Slika 32: Pregled prometa v omrežju VLAN 2

V primeru poslušanja z ukazom »tcpdum vlan 3 and icmp« prejetih paketov ne vidimo.

```
root@diploma:~# tcpdump vlan 3 and icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol deco
de
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```

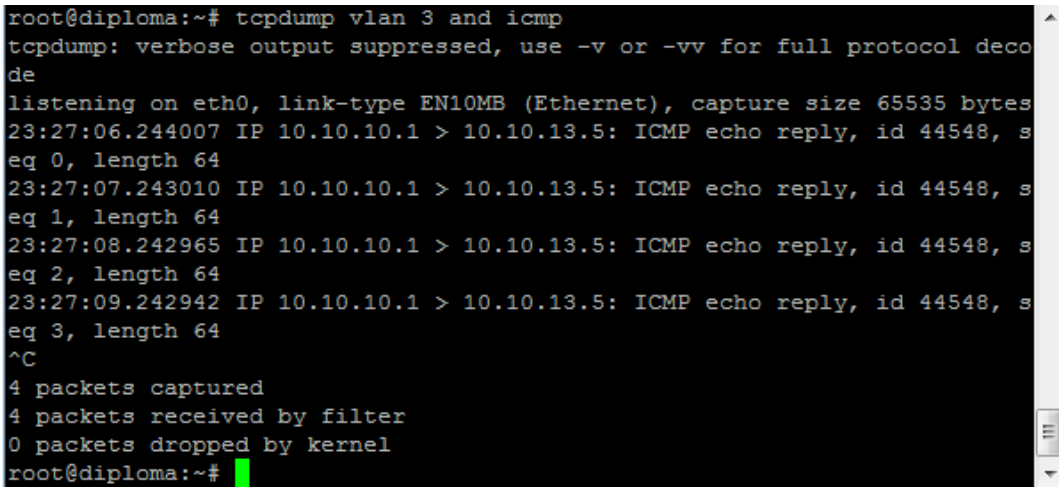
Slika 33: Pregled prometa v omrežju VLAN 3

Enak postopek ponovimo z dostopno točko. Nanjo se povežemo preko protokola SSH. Pred tem moramo v nastavitvah na dostopni točki omogočiti dostop SSH. Nanjo se povežemo preko terminala in protokola SSH in poženemo ukaz »ping 10.10.10.1«.

```
root@DD-WRT:~# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1): 56 data bytes
64 bytes from 10.10.10.1: seq=0 ttl=64 time=0.748 ms
64 bytes from 10.10.10.1: seq=1 ttl=64 time=0.726 ms
64 bytes from 10.10.10.1: seq=2 ttl=64 time=0.750 ms
64 bytes from 10.10.10.1: seq=3 ttl=64 time=0.776 ms
64 bytes from 10.10.10.1: seq=4 ttl=64 time=0.797 ms
64 bytes from 10.10.10.1: seq=5 ttl=64 time=0.742 ms
64 bytes from 10.10.10.1: seq=6 ttl=64 time=0.753 ms
64 bytes from 10.10.10.1: seq=7 ttl=64 time=0.771 ms
64 bytes from 10.10.10.1: seq=8 ttl=64 time=0.732 ms
^X
--- 10.10.10.1 ping statistics ---
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 0.726/0.755/0.797 ms
root@DD-WRT:~#
```

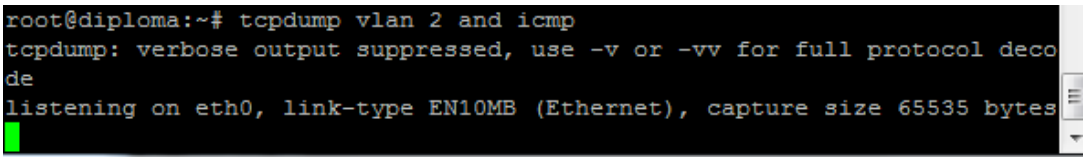
Slika 34: Pošiljanje podatkov iz dostopne točke na strežnik

Nato na strežniku ponovno poženemo ukaz »tcpdum vlan3 and icmp« in ter opazujemo poslane pakete. Kot je razvidno iz Slike 35, se promet tokrat nahaja v VLAN 3.



Slika 35: Pregled prometa v omrežju VLAN 3

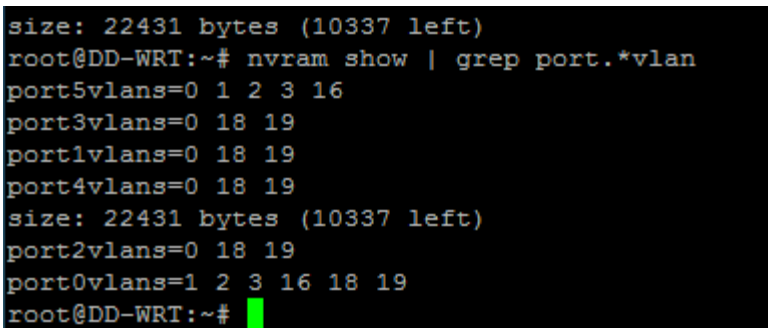
Podobno kot prej v omrežju VLAN 3 tudi v omrežju VLAN 2 ni prometa.



Slika 36: Pregled prometa v omrežju VLAN 2

4.3.1.4 Dinamično razvrščanje uporabnikov v VLAN-e na Linksysu WRT54GL

Enake nastavitve, kot smo jih nastavili preko grafičnega vmesnika, bi lahko nastavili na dostopni točki tudi preko terminala. Da bi uspeli dinamično dodeljevati VLAN-e uporabnikom, smo morali bolje raziskati samo delovanje programske opreme DDWRT in dostopne točke Linksys WRT54GL. Pri tem smo ugotovili, da ima čip dostopne točke omejene zmožnosti pri delovanju z VLAN-i. Pri taki strojni opremi smo omejeni na največ 16 VLAN-ov zaradi 16-bitnega registra, ki uporablja le 4 bite za označevanje VLAN-ov.



Slika 37: Nastavitve vrat na dostopni točki

Čeprav smo na dostopni točki uspeli nastaviti VLAN 100, ga zaradi omenjene omejitve ni bilo mogoče uporabiti. Na Sliki 38 je prikazan ustvarjen VLAN 100.

```
root@DD-WRT:~# vconfig add eth0 100
root@DD-WRT:~# ifconfig vlan100
vlan100   Link encap:Ethernet  HWaddr 58:6D:8F:88:B5:BD
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@DD-WRT:~#
```

Slika 38: Dodajanje VLAN 100

Za preizkus smo nastavili delovanje vrat 4 z VLAN-om 100, vendar zaradi omejitve dostopna točka Linksys WRT54GL ni primerna za ločevanje uporabnikov v ločena omrežja VLAN.

```
root@DD-WRT:~# nvram set port5vlans="1 2 3 100"
root@DD-WRT:~# nvram set port0vlans="1 2 3 16 18 19 100"
root@DD-WRT:~# nvram set port5vlans="1 2 3 100"
root@DD-WRT:~# nvram set port4vlans="100"
root@DD-WRT:~# nvram show | grep port.*vlans
port5vlans=1 2 3 100
port3vlans=0 18 19
port1vlans=0 18 19
port4vlans=100
size: 22376 bytes (10392 left)
port2vlans=0 18 19
port0vlans=1 2 3 16 18 19 100
root@DD-WRT:~#
```

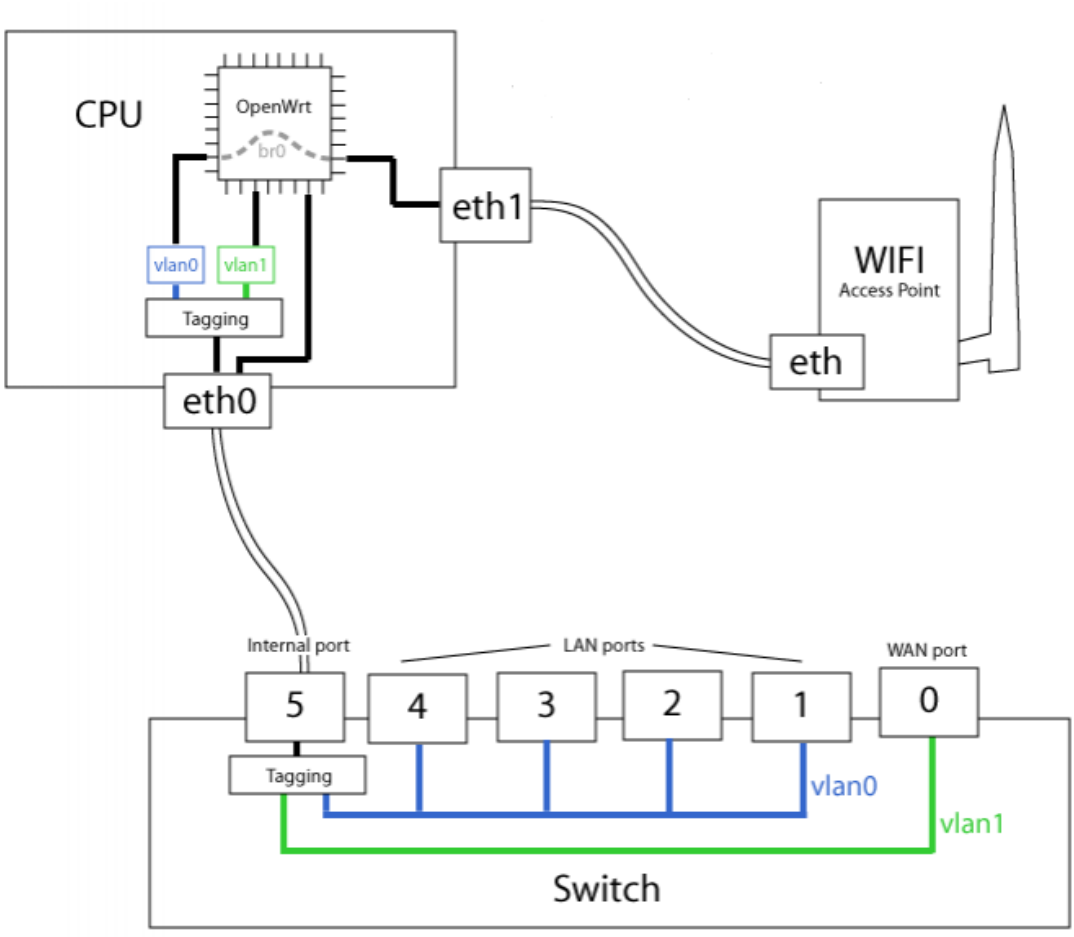
Slika 39: Nastavitev vrat za uporabo omrežja VLAN 100

Kot prikazuje Slika 40, lahko damo v most eno omrežje VLAN in eno mrežno kartico, ne moremo pa ustvariti več VLAN-ov na brezžični oz. omrežni kartici.

```
root@DD-WRT:~# brctl show
bridge name     bridge id               STP enabled     interfaces
br0             8000.586d8f88b5bd       no              vlan0
                                                        vlan3
                                                        eth1
br1             8000.586d8f88b5bd       yes             wl0.1
                                                        vlan2
root@DD-WRT:~#
```

Slika 40: Mostovi na dostopni točki

Na Sliki 41 je prikazana zgradba usmerjevalnika WRT54GL. Usmerjevalnik ne omogoča uporabe več omrežij VLAN na eni virtualni omrežni kartici, zato dinamično razvrščanje uporabnikov v VLAN-e na usmerjevalniku ni mogoče.



Slika 41: Zgradba dostopne točke Linksys WRT54GL [10]

4.3.2 Raspberry Pi kot dostopna točka

Zaradi omejitve z dostopno točko Linksys WRT54GL smo se v nadaljevanju osredotočili na iskanje rešitve s splošno namenskim računalnikom Raspberry PI. Računalnik smo v nadaljevanju uporabili kot brezžično dostopno točko.

4.3.2.1 Izbira prave omrežne kartice USB

Za pravilno delovanje omrežne kartice mora ta podpirati način *master mode* oziroma *ap/vlan*. V nadaljevanju bomo predstavili, kako ugotoviti, ali naša omrežna kartica to zmore. Najprej bomo pogledali, če naš računalnik omrežno kartico sploh prepozna (Slika 42). [15]

```
root@raspberrypi:~# lsusb
Bus 001 Device 002: ID 0424:9512 Standard Microsystems Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 003: ID 0424:ec00 Standard Microsystems Corp.
Bus 001 Device 004: ID 0ace:1215 ZyDAS ZD1211B 802.11g
Bus 001 Device 005: ID 1a40:0101 Terminus Technology Inc. 4-Port HUB
Bus 001 Device 006: ID 04d9:1702 Holtek Semiconductor, Inc.
Bus 001 Device 022: ID 0458:0007 KYE Systems Corp. (Mouse Systems)
root@raspberrypi:~#
```

Slika 42: Pregled naprav, priklopljenih na USB

Z ukazom »lsusb« izpišemo seznam naprav, ki so priklopljene na USB. Kot vidimo, imamo na seznamu tudi brezžično omrežno kartico »ZyDAS ZD1211B 802.11g«. V našem primeru je bilo za pravilno delovanje kartice s čipom zd1211 potrebno namestiti dodatno programsko opremo, in sicer z ukazom »apt-get install zd1211-firmware«. Po namestitvi tega programskega paketa je omrežna kartica delovala pravilno. Ko imamo omrežno kartico na seznamu, preverimo, če kartica podpira potreben način delovanja za postavitev dostopne točke.

Na računalnik z ukazom »apt-get install iw« namestimo programski paket »iw«. Nato poženemo ukaz »iw list« in preverimo, če omrežna kartica podpira način AP/VLAN (Slika 43).

```
Supported interface modes:
         * IBSS
         * managed
         * AP
         * AP/VLAN
         * monitor
         * mesh point
```

Slika 43: Pregled načinov podpore omrežne kartice

Ko se odločamo za nakup omrežne kartice, moramo biti pozorni, da gonilniki za njeno čipovje podpirajo omenjena načina uporabe omrežne kartice.

4.3.2.2 Raspberry Pi

Računalnik, ki so ga razvili v Angliji v fundaciji Raspberry Pi, ki je bila ustanovljena leta 2009. Namen fundacije je bil spodbujanje učenja osnov računalništva v šolah. Na računalnik lahko namestimo različne operacijske sisteme (Raspbian, Fedora, Arch…), ki podpirajo izvajanje ukazov na procesorju ARM. Sestavljen je iz procesorja ARM1176JZF-S in deluje pri frekvenci 700 Mhz. Na plošči je nameščen tudi pomnilnik v velikosti 256 ali 512MB. Podatke hranimo na SD kartici. [12]

Slika 44: Računalnik Raspberry Pi

Raspbian je operacijski sistem, ki bazira na brezplačnem operacijskem sistemu Debian in je prilagojen za delovanje na računalniku Raspberry Pi. Raspbian ni samo operacijski sistem, ampak prihaja s kar 35000 paketi vnaprej pripravljene programske opreme, ki jo je mogoče enostavno namestiti na računalnik. [13]

Za postavitev dostopne točke bomo na računalniku Raspberry Pi namestili programski paket »hostapd«. To storimo z ukazom »apt-get install hostapd«. Ko imamo nameščen programski paket, lahko pričnemo z nastavljanjem nastavitev.

4.3.2.3 Nastavitve omrežne kartice

Na dostopni točki Raspberry Pi je potrebno nastaviti pravilne nastavitve za delovanje omrežja. V datoteki »/etc/network/interfaces« bomo za demonstracijo nastavili VLAN 2, 3 in 4.

```
  GNU nano 2.2.6                File: /etc/network/interfaces

auto lo

auto eth0.2
iface eth0.2 inet static
address 10.10.12.4
netmask 255.255.255.0
network 10.10.12.0
gateway 10.10.12.1

auto eth0.3
iface eth0.3 inet static
address 10.10.13.4
netmask 255.255.255.0
network 10.10.13.0
gateway 10.10.13.1

auto eth0.4
iface eth0.4 inet static
address 10.10.14.4
netmask 255.255.255.0
network 10.10.14.0
gateway 10.10.14.1
```

Slika 45: Nastavitve omrežnega vmesnika

Za upravljanje dostopne točke bomo uporabil VLAN 2. VLAN-i z oznakami, ki so višje od 2, so namenjeni uporabnikom.

4.3.2.4 Nastavitve programa »hostapd«

V datoteki /etc/default/hostapd najprej nastavimo pot do datoteke, v kateri bo shranjena naša konfiguracija za program »hostapd«. [14]

```
#
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

Slika 46: Pot do nastavitvene datoteke

Z ukazom »pico /etc/hostapd/hstapd.conf« kreiramo novo datoteko, kjer bodo shranjene nastavitve. V datoteko dodamo pravilne nastavitve za delovanje naše dostopne točke. Dostopna točka bo za avtentikacijo uporabnikov uporabljala strežnik FreeRadius, ki teče na glavnem strežniku z naslovom IP 10.10.10.1. Da bomo lahko uporabljali dinamično dodeljevanje omrežij VLAN, je potrebno v konfiguraciji nastaviti sledeče nastavitve:

- dynamic_vlan=2 – strežnik FreeRadius mora obvezno posredovati informacijo, v kateri VLAN bo uporabnik umeščen;
- vlan_tagged_interface=eth0 – podatek pove, na katero omrežno kartico pridejo VLAN-i, ki jih bomo uporabljali z brezžično omrežno kartico;
- Vlan_file=/etc/hostapd.vlan – pot do informacij o omrežjih VLAN, ki jih bo uporabljala dostopna točka .

```
 GNU nano 2.2.6                File: /etc/hostapd/hostapd.conf

interface=wlan0
driver=nl80211
ssid=test1
hw_mode=g
channel=6
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0

##### IEEE 802.1X

ieee8021x=1

##### RADIUS dostop

auth_server_addr=10.10.10.1
auth_server_port=1812
auth_server_shared_secret=testing123

wpa=2
wpa_key_mgmt=WPA-EAP
wpa_pairwise=CCMP TKIP

#konfiguracija za dinamicno dodeljevanje VLANov
dynamic_vlan=2
vlan_tagged_interface=eth0
vlan_file=/etc/hostapd.vlan
```

Slika 47: Nastavitve dostopne točke »hostapd«

Po uspešni konfiguraciji datoteke »hostapd.conf« moramo ustvariti datoteko /etc/hostapd.vlan. V njej bomo hranili VLAN-e, ki jih bo strežnik »hostapd« uporabljal in jih dinamično dodeljeval uporabnikom.

```
  GNU nano 2.2.6                          File: /etc/hostapd.vlan

#VLAN ID | mrezna kartica
3 wlan0.3
4 wlan0.4
```

Slika 48: Datoteka z VLAN-i, ki jih bo uporabljala dostopna točka

4.3.2.5 Nastavitve mostov

Po nastavljeni konfiguraciji ponovno zaženemo strežnik »hostapd« z ukazom »service hostapd restart«. Po ponovnem zagonu in ob zagonu ukaza »brctl show« vidimo naslednje stanje:

```
root@raspberrypi:~# brctl show
bridge name     bridge id               STP enabled     interfaces
brvlan3         8000.0023cdbef9c7       no              wlan0.3
brvlan4         8000.0023cdbef9c7       no              wlan0.4
root@raspberrypi:~#
```

Slika 49: Pregled mostov

Sledi postavitev mostu med brezžičnimi omrežji VLAN in omrežji VLAN omrežne kartice (Slika 50).

```
root@raspberrypi:~# brctl addif brvlan3 eth0.3
root@raspberrypi:~# brctl addif brvlan4 eth0.4
root@raspberrypi:~# brctl show
bridge name     bridge id               STP enabled     interfaces
brvlan3         8000.0023cdbef9c7       no              eth0.3
                                                        wlan0.3
brvlan4         8000.0023cdbef9c7       no              eth0.4
                                                        wlan0.4
root@raspberrypi:~#
```

Slika 50: Dodajanje naprav mostovom

Za nadaljevanje postopka so potrebne pravilne nastavitve na strani strežnika FreeRadius, ki bo dostopni točki posredoval informacije, v kateri VLAN mora biti uporabnik uvrščen.

4.4 Dinamično razvrščanje uporabnikov v omrežja VLAN

Namen naloge je, da bo vsak uporabnik pri uporabi brezžičnega omrežja uporabljal drugo omrežje VLAN. Zato je bilo potrebno implementirati dva programa, kjer eden od njiju preverja prosta omrežja VLAN, drugi pa jih posreduje strežniku FreeRadius.

Za ugotavljanje prostih omrežij VLAN je potrebno na strežnik namestiti program »dhcpstatus«. Ta nam poda informacijo o stanju strežnika DHCP, na podlagi katere ugotovimo prosta omrežja VLAN.

```
root@diploma:/home/radius# dhcpstatus
DHCP Subnet Information

Subnet: 10.10.10.0    Netmask: 255.255.255.0
IP range: 10.10.10.1 - 10.10.10.254    Router: 10.10.10.1
IPs defined: 26    IPs used: 0    IPs free: 26

Subnet: 10.10.12.0    Netmask: 255.255.255.0
IP range: 10.10.12.1 - 10.10.12.254    Router: 10.10.12.1
IPs defined: 26    IPs used: 0    IPs free: 26

Subnet: 10.10.13.0    Netmask: 255.255.255.0
IP range: 10.10.13.1 - 10.10.13.254    Router: 10.10.13.1
IPs defined: 26    IPs used: 1    IPs free: 25

Subnet: 10.10.14.0    Netmask: 255.255.255.0
IP range: 10.10.14.1 - 10.10.14.254    Router: 10.10.14.1
IPs defined: 26    IPs used: 0    IPs free: 26

Subnet: 10.10.15.0    Netmask: 255.255.255.0
IP range: 10.10.15.1 - 10.10.15.254    Router: 10.10.15.1
IPs defined: 26    IPs used: 0    IPs free: 26

Subnet: 10.10.100.0    Netmask: 255.255.255.0
IP range: 10.10.100.1 - 10.10.100.254    Router: 10.10.100.1
IPs defined: 26    IPs used: 1    IPs free: 25
```

Slika 51: Pregled stanja strežnika DHCP

Da bomo informacije lahko uporabili, je potrebno uporabiti ustrezen program, ki iz podatkov dobi informacije o prostih omrežjih VLAN. Program požene program »dhcpstatus« in njegove informacije shrani v datoteko /home/radius/status. Iz nje prebere stanje strežnika DHCP in ugotovi, katera omrežja VLAN so prosta. Ta omrežja shrani v datoteko /home/radius/freevlans.txt. Programu nastavimo, katera omrežja VLAN bomo dodeljevali uporabnikom. Na primeru programa (Slika 52) imamo prikazano uporabo za omrežja VLAN 3, 4 in 5.

```
 GNU nano 2.2.6                    File: vlans.py

import os

#pozenemo program dhcpstatus in shranimo izpis
os.system("sudo dhcpstatus > /home/radius/status")
#definiramo, katera omrezja VLAN so uporabniska
vlanDict = {'10.10.13.0': 3, '10.10.14.0': 4, '10.10.15.0': 5}
subnet=""
freevlan=[]
#preberemo, kateri prosti VLAN-i so ze v datoteki "freevlans.txt"
with open("/home/radius/freevlans.txt") as vlani:
    for line in vlani:
        line=line.rstrip()
        freevlan.append(line)
#iz izpisa programa dhcpstatus preberemo, kateri VLAN-i
#nimajo zaasedenih naslovov IP
with open("/home/radius/status") as f:
    for line in f:
        if "Subnet:" in line:
            subnet=line[8:]
        if "IPS used: 0" in line:
            subnet=subnet.rstrip()
            if subnet in vlanDict:
                vlan=vlanDict[subnet]

                with open("/home/radius/freevlans.txt", "a") as pisi:
                        vlan=str(vlan)
                        if vlan not in freevlan:
                            vlan=vlan+"\n
                            pisi.write(vlan)
```

Slika 52: Program, ki iz izpisa »dhcpstatus« dobi podatke o omrežjih VLAN [1]

Program iz podatkov pridobljene informacije o prostih VLAN-ih shrani v datoteko freevlans.txt. Potreben je tudi program, ki podatke o prostih VLAN-ih posreduje strežniku FreeRadius.

```
 GNU nano 2.2.6                          File: setvlan.sh

#!bin/bash

#zaklenemo program
lockfile-create /home/radius/zakleni
#program prebere prvi zapis iz datoteke "freevlans.txt"
first=$(head -n 1 /home/radius/freevlans.txt)

#Ce je datoteka prazna (ni prostih VLAN-ov),
#FreeRadius posreduje VLAN 100
if [ -z $first]; then
        echo "100"
        rm -f /home/radius/zakleni.lock
else
        echo $first
        rm -f /home/radius/zakleni.lock
fi

#izbrise uporabljen VLAN iz datoteke "freevlans.txt"
sed -i '1d' /home/radius/freevlans.txt
```

Slika 53: Program setvlan.sh za posredovanje informacije o prostem omrežju VLAN strežniku FreeRadius [1]

Program setvlan.sh iz datoteke freevlans.txt prebere informacijo o prostem omrežju VLAN in jo izpiše (v nadaljevanju jo posreduje strežniku FreeRadius). Če ni prostih omrežij VLAN, bo za demonstracijo uporabljen privzeti VLAN 100. Vanj bomo v primeru zasedenosti vseh omrežij VLAN umestili uporabnike.

Nato je potrebno prilagoditi nastavitve strežnika FreeRadius, ki bo program setvlan.sh povprašal po prostem omrežju VLAN. V datoteki /etc/freeradius/sites-available/default moramo spremeniti nastavitve (Slika 54), da bo strežnik FreeRadius po uspešni avtentikaciji poklical skripto setvlans.sh in pridobil informacijo o prostem omrežju VLAN. Informacijo bo posredoval dostopni točki.

```
post-auth {
        update control {
                Tmp-Integer-0=`/home/radius/setvlan.sh`
        }
        update reply {

                Tunnel-Medium-Type = "IEEE-802"
                Tunnel-TYPE = "VLAN"
                Tunnel-Private-Group-ID = "%{control:Tmp-Integer-0}"
        }
}
```

Slika 54: Konfiguracija za dinamično dodeljevanje omrežij VLAN

Če poženemo FreeRadius z ukazom »freeradius -X« v razhroščevalnem načinu se ob avtentikaciji uporabnika opazi, da je FreeRadius poslal dostopni točki tudi informacijo o VLAN-u, ki ga bo uporabnik uporabljal (Slika 55).

```
++[control] returns noop
        expand: %{control:Tmp-Integer-0} -> 4
++[reply] returns noop
Sending Access-Accept of id 15 to 10.10.12.4 port 42318
        MS-MPPE-Recv-Key = 0x0d22e498a50e470f8f7b789c3432a2655f8e60
        MS-MPPE-Send-Key = 0xb4e2cf8d12bdc154764aed7eab82e4484089a1
        EAP-Message = 0x038f0004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "test"
        Tunnel-Medium-Type:0 = IEEE-802
        Tunnel-Type:0 = VLAN
        Tunnel-Private-Group-Id:0 = "4"
Finished request 3.
```

Slika 55: Prikaz posredovanega omrežja VLAN

Skripto, ki v datoteko shranjuje prosta omrežja VLAN, lahko na strežniku poganjamo vsako minuto. S tem dosežemo, da je datoteka »freevlanes.txt« vedno osvežena.

4.4.1 Pogajanje skripte

Pogajanje skripte za beleženje prostih VLAN-ov na strežniku v datoteko freevlans.txt bomo dosegli z uporabo programa »cronjob«. Ta skrbi za izvajanje skript in programov na strežniku ob določenih intervalih. V našem primeru bomo skripto vlans.py poganjali vsako minuto.

Na strežniku poženemo ukaz, s katerim dostopamo do nastavitev za zaganjanje skript (Slika 56).

```
root@diploma:~# crontab -e
```

Slika 56: Urejanje nastavitev programa "cronjob"

V datoteko dodamo nastavitve, ki jih želimo uporabiti za naš program. Kot prikazuje Slika 57, v datoteko zapišemo, kdaj bi radi, da se program izvede, in samo pot do programa. V našem primeru se program, zapisan v programskem jeziku Python, nahaja v datoteki /home/radius/vlans.py. Za zagon programa uporabimo absolutno pot do interpreterja /usr/bin/python. S tem dosežemo, da se program izvede vsako minuto in osvežuje datoteko, v kateri hranimo prosta omrežja VLAN.

```
  GNU nano 2.2.6                Datoteka: /tmp/crontab.I2HmoP/crontab

# m h  dom mon dow   command
*/1 * * * * /usr/bin/python /home/radius/vlans.py
```

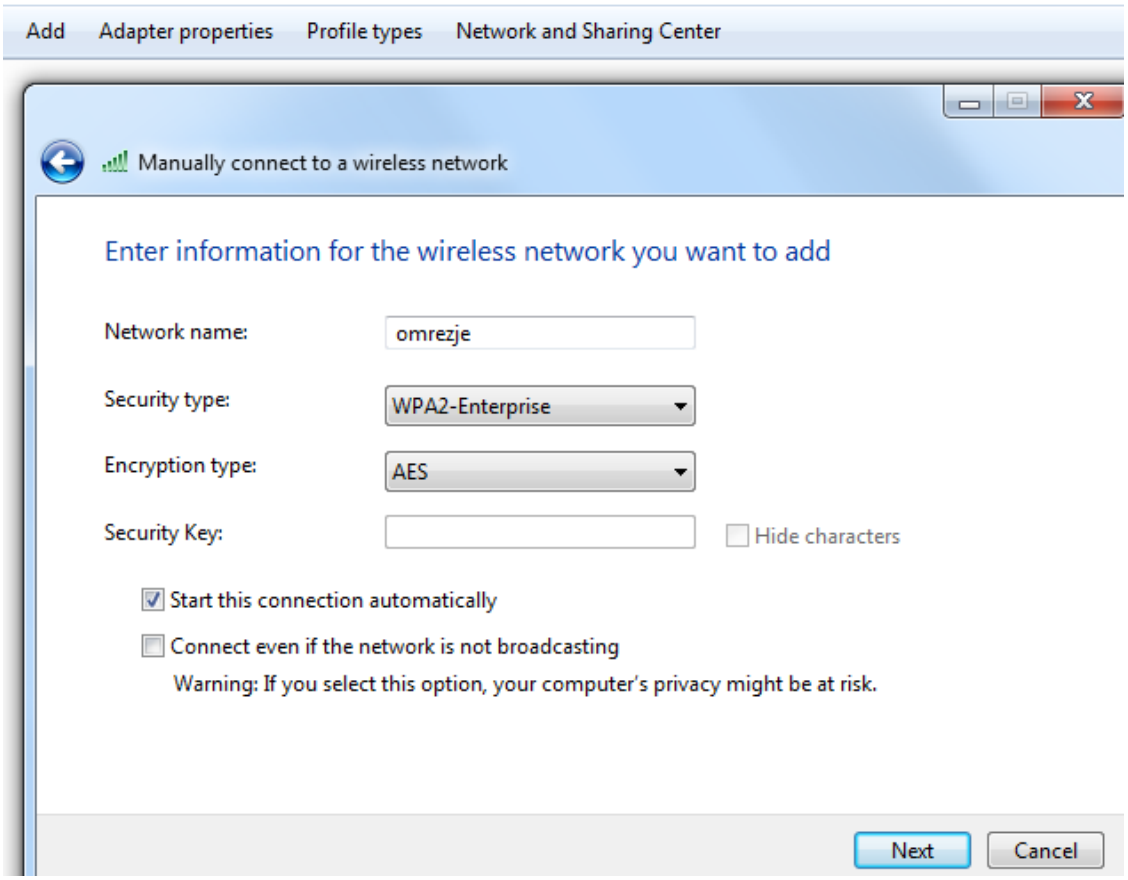
Slika 57: Nastavitve programa "cronjob"

Strežnik bo na tak način poskrbel za osvežene podatke o prostih omrežjih VLAN, ki jih bo strežnik FreeRadius nato posredoval dostopni točki. Ta bo uporabnike premaknila v prosta omrežja VLAN, ki so na voljo.

4.5 Nastavitve odjemalca

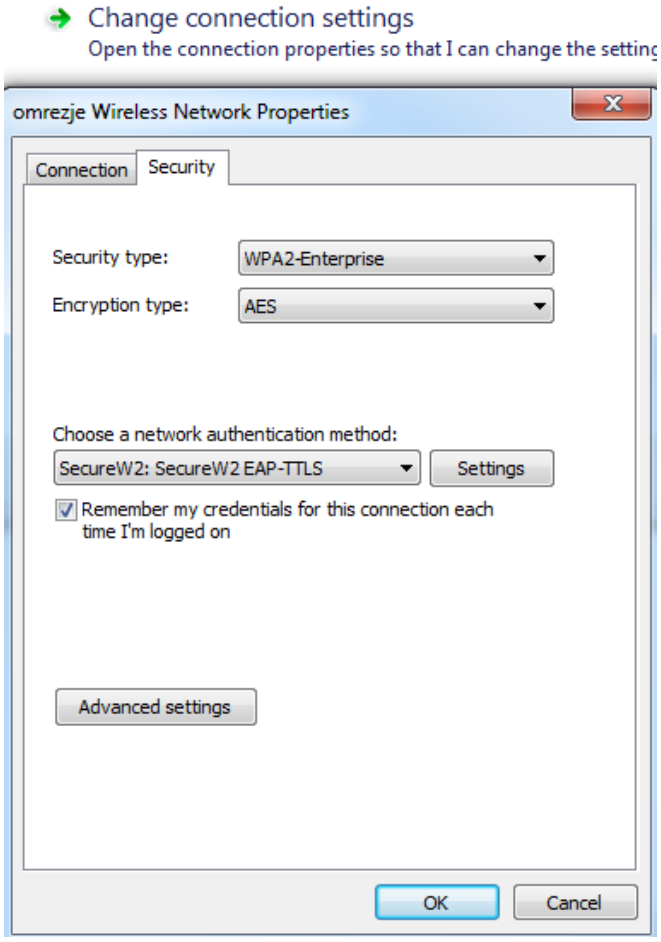
Za uporabo brezžičnega omrežja je potrebno nastaviti tudi pravilne nastavitve na računalniku, ki bo do omrežja dostopal. Če uporabljamo operacijski sistem Windows XP, Vista ali 7, je potrebno na odjemalca namestiti dodatno programsko opremo SecureW2, ki omogoča uporabo avtentikacije EAP-TTLS. Če imamo nameščen operacijski sistem Windows 8 je podpora vgrajena že v sam operacijski sistem.

Na računalniku dodamo novo brezžično omrežje (Slika 58). Izberemo vrsto zaščite »WPA2-Enterprise« in vrsto enkripcije »AES«.



Slika 58: Dodajanje novega brezžičnega omrežja

V naslednjem koraku omrežju nastavimo metodo za avtentikacijo SecureW2 EAP-TTLS in izberemo dodatne nastavitve (Slika 59).



Slika 59: Nastavljanje brezžičnega omrežja

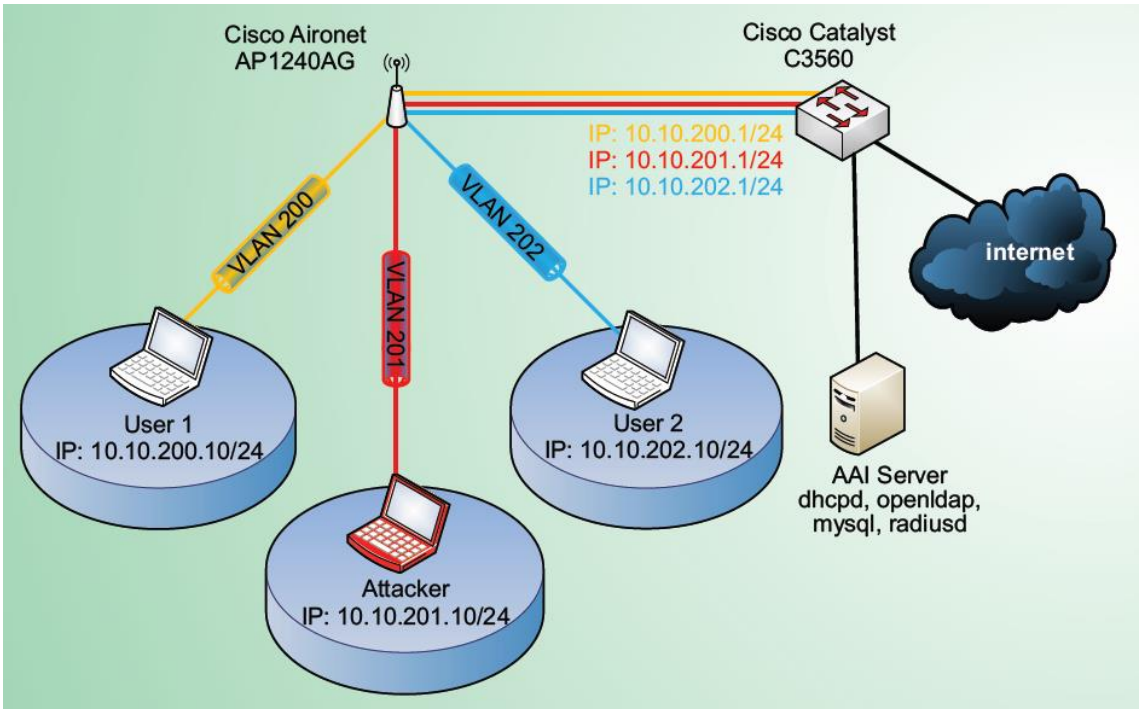
V dodatnih nastavitvah programa SecureW2 nastavimo uporabniško ime in geslo za dostop do brezžičnega omrežja (Slika 60).

Slika 60: Nastavljanje aplikacije SecureW2

Po uspešni namestitvi programa SecureW2 je naprava pripravljena za uporabo omrežja.

5 Sklepne ugotovitve

V diplomski nalogi nam je uspelo razviti sistem za ločevanje uporabnikov v omrežja VLAN na cenovno ugodni brezžični dostopni točki Raspberry Pi. Za razvoj omrežja smo potrebovali brezžično omrežje z enakimi lastnostmi, kot jih ima omrežje Eduroam. Postavili smo strežnik, na katerem smo namestili strežnik FreeRadius, DHCP, MySQL, nastavili stikalo za pravilno uporabo omrežij VLAN in brezžične dostopne točke. Namen zaščite uporabnikov pri uporabi brezžičnega omrežja na cenovno ugodni dostopni točki je bil uspešno dosežen. Odpravili smo nekatere pomanjkljivosti omrežja in s tem poskrbeli za boljšo varnost uporabnikov. Zaradi izolacije uporabnikov so tudi napadalci izolirani v ločeno omrežje VLAN, v katerem so sami. Zaradi tega ne morejo uporabiti napada, kot je zastrupljanje tabele ARP (Slika 61).



Slika 61: Preprečen napad zastrupljanja tabele ARP [1]

Za uporabnost sistema v večjih omrežjih bo potrebno v nadaljevanju opraviti še preizkuse zmogljivosti omrežja in se prepričati, da je dostopna točka res primerna za večje število uporabnikov. Potrebno bo tudi prilagoditi operacijski sistem Raspbian, da bo ta primeren za uporabo na dostopnih točkah. Za lažjo postavitev omrežja bo potrebno poenostaviti sam način nastavljanja dostopnih točk in omrežij VLAN in omogočiti enostavno vzdrževanje sistema. Za zadovoljitev pogojev, ki jih specificira omrežje Eduroam, bomo v nadaljevanju tudi vsako omrežje VLAN zunanjemu svetu predstavili z javnim naslovom IP (1:1 NAT). S tem bomo zagotovili manjšo porabo javnih naslovov IP, saj so za vsako omrežje VLAN trenutno potrebni vsaj štirje naslovi IP.

Literatura

[1] Marko Dolničar (2013) Layer 2 user isolation in Eduroam.si. Dostopno na: https://tnc2013.terena.org/core/poster/23

[2] Marko Dolničar (2013) Eduroam and IPv6. Dostopno na: https://tnc2012.terena.org/core/poster/20

[3] Jan Bočko Kuhar, Marko Dolničar (2013) Eduroam insecurities. Dostopno na: https://tnc2011.terena.org/core/poster/24

[4] (2013) Zavod Arnes. Dostopno na: http://www.arnes.si/zavod-arnes/predstavitev.html

[5] (2013) Eduroam. Dostopno na: http://aai.arnes.si/eduroam/index.html

[6] (2013) FreeRadius. Dostopno na: http://wiki.freeradius.org/guide/faq#FreeRADIUS-Overview

[7] (2013) 802.1X. Dostopno na: http://en.wikipedia.org/wiki/IEEE_802.1X

[8](2003) 802.1X Security, Dostopno na: http://www.sans.org/reading_room/whitepapers/firewalls/wired-8021x-security_1654

[9] (20013) FreeRadius, Dostopno na: http://freeradius.org/

[10] (2013) OpenWRT. Dostopno na: http://wiki.openwrt.org/toh/linksys/wrt54g

[11] (2013) DD-WRT. Dostopno na: http://www.dd-wrt.com/site/index

[12] (2013) RaspberryPi. Dostopno na: http://www.raspberrypi.org/

[13] (2013) Raspbian. Dostopno na: http://www.raspbian.org/

[14] (2013) Hostap. Dostopno na: http://hostap.epitest.fi/hostapd/

[15] (2013) Linux wireless drivers. Dostopno na: http://wireless.kernel.org/en/users/Drivers

[16] Alan Holt, Chi-Yu Huang, »802.11 Wireless Networks«, 2010, str. 101–110

[17] (2013) Iptables. Dostopno na: http://linux.die.net/man/8/iptables

[18] (2013) Suba Varadarajan, »Virtual Local Area Networks«. Dostopno na: http://www.cse.wustl.edu/~jain/cis788-97/ftp/virtual_lans/index.htm

[19] (2013) Linksys WRT54G series. Dostopno na: http://en.wikipedia.org/wiki/Linksys_WRT54G_series#WRT54GL

[20] (2013) Bob Fleck, Jordan Dimov, »Wireless Access Points and ARP Poisoning«, Dostopno na: http://bandwidthco.com/whitepapers/netforensics/arp-rarp/Wireless%20Access%20Points%20and%20ARP%20Poisoning.pdf

[21] (2013) Licia Florio, Klaas Wierenga, »Eduroam, providing mobility for roaming users«. Dostopno na: http://www.terena.org/activities/tf-mobility/docs/ppt/eunis-eduroamfinal-LF.pdf

[22] (2013) Licia Florio, Klaas Wierenga, »Eduroam: past, present and future«. Dostopno na: http://www.man.poznan.pl/cmst/www.old/papers/11_2/CMST11-11.pdf

[23] (2013) How to use IP helper-address to connect remote DHCP server. Dostopno na: http://cisconet.com/tcpip/dhcp/107-how-to-use-ip-helper-address-to-connect-remote-dhcp-server.html
[24] (2013) R. Droms, »Dynamic Host Configuration Protocol«. Dostopno na: http://www.ietf.org/rfc/rfc2131.txt
[25] (2013) Ethernet frame. Dostopno na: http://en.wikipedia.org/wiki/Ethernet_frame
[26] (2013) IEEE 802.1Q. Dostopno na: http://en.wikipedia.org/wiki/IEEE_802.1Q

Kazalo slik