Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Blaž Divjak

Vključitev lahkih dostopovnih točk v omrežje Eduroam

diplomsko delo

univerzitetni študijski program prve stopnje
računalništvo in informatika

Mentor: doc. dr. Mojca Ciglarič

Ljubljana 2012

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: 00023/2012
Datum: 10.04.2012

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

Kandidat: **BLAŽ DIVJAK**

Naslov: **VKLJUČITEV LAHKIH DOSTOPOVNIH TOČK V OMREŽJE EDUROAM**

INTRODUCING LIGHTWEIGHT ACCESS POINTS INTO EDUROAM NETWORK

Vrsta naloge: Diplomsko delo univerzitetnega študija prve stopnje

Tematika naloge:

Cilj diplomske naloge je uvedba lahkih brezžičnih dostopovnih točk s centralnim upravljanjem v omrežje Eduroam. Pripravite kratek pregled brezžičnih tehnologij IEEE 802.11. Opišite zgradbo omrežja Eduroam in tam uporabljene mehanizme za varnost in avtentikacijo. Pojasnite, kaj so lahke dostopovne točke. Na področju nadzora in upravljanja dostopovnih točk raziščite, kakšni krmilniki in kateri protokoli se lahko uporabljajo za ta namen ter predstavite njihove prednosti in slabosti, upoštevajte zlasti varnostni vidik.
Svoje ugotovitve preverite tudi v praksi. Postavite preizkusni poligon – maketo omrežja Eduroam, ki naj vključuje lahke dostopovne točke in centralno upravljanje. Ovrednotite spremembe v načinu upravljanja in varnostni nivo v primerjavi s klasično arhitekturo omrežja Eduroam. V zaključku komenitrajte, kakšen pomen imajo vaše ugotovitve za nadaljnji razvoj omrežja Eduroam.

Mentor:

M. Ciglarič

doc. dr. Mojca Ciglarič

Dekan:

prof. dr. Nikolaj Zimic

Fakulteta za računalništvo in informatiko
2
UNIVERZA V LJUBLJANI

Izjava o avtorstvu diplomskega dela

Spodaj podpisani Blaž Divjak, z vpisno številko **63080046**, sem avtor diplomskega dela z naslovom:

Vključitev lahkih dostopovnih točk v omrežje Eduroam

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.) identični s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki "Dela FRI".

V Ljubljani, dne 15. septembra 2012 Podpis avtorja:

Zahvaljujem se mentorici doc. dr. Mojci Ciglarič za pomoč pri izdelavi diplomskega dela. Zahvale gredo tudi vsem zaposlenim na Arnesu, ki so mi omogočili izdelavo diplomskega dela. Hvala Manji za odpravo slovničnih napak. Največja zahvala gre družini, ki mi je vsa leta študija stala ob strani in me podpirala.

Svoji dragi Katji.

Kazalo

Povzetek

Brezžična omrežja so bila na začetku priročna, danes pa so misijsko kritična. Potreba po mobilnosti zaposlenih v izobraževalni in raziskovalni sferi je leta 2003 na evropski ravni povzročila ustanovitev brezžičnega omrežja Eduroam. V začetku je omrežje pokrivalo majhne dele fakultet in šol, danes pa se je Eduroam razširil na celotne kampuse in študentske domove. Velika brezžična omrežja so vzdrževalce postavila pred nov izziv. Pojavila se je potreba po sistemu, ki omogoča hitrejšo distribucijo dostopovnih točk, kasneje pa lažji nadzor in oskrbo. V diplomskem delu smo predstavili delovanje brezžičnih omrežij in njihove varnostne mehanizme. Opisali smo težave, s katerimi se srečujejo vzdrževalci brezžičnih omrežij. Kot rešitev smo predstavili centralizirano brezžično arhitekturo in njene sestavne dele. Postavili smo preizkusni poligon - maketo omrežja Eduroam, z uporabo brezžične opreme za centralizirano upravljanje. Na podlagi preizkusov smo predlagali in ocenili možne načine uporabe opreme za centralizirano upravljanje v omrežju Eduroam. Preverili smo tudi njen doprinos k varnosti v primerjavi z običajnimi Eduroam omrežji.

Ključne besede:

Eduroam, brezžična omrežja, 802.11, 802.1x, RADIUS, dostopovni krmilnik, lahka dostopovna točka, CAPWAP, Cisco WLC

Abstract

In the begining wireless networks were convenient but now they are mission critical. Eduroam wireless network was launched in 2003. It enabled mobility in academic and educational sphere. At the begining Eduroam covered small parts of faculties and schools, but it evolved and is now covering large campuses and student dorms. Large wireless networks bring new challenges for their maintainers. For efficient control and provisioning of wireless access points a new solution was needed. In this thesis we presented centralized wireless architecture as the solution. We set up a test Eduroam lab with equipment for centralized wireless network management. We evaluated usability and recommended possible use cases of equipment for centralized management in Eduroam wireless network. We also tested security and compared it to autonomous Eduroam networks.

Key words:

Eduroam, WLAN, 802.11, 802.1x, RADIUS, access controller, lightweight acess point, CAPWAP, Cisco WLC

Poglavje 1

Uvod

Brezžična računalniška omrežja so se od leta 1997, ko so bili izdani prvi komercialni produkti, ki so temeljili na standardu IEEE 802.11, do danes močno razvila. Postala so pomemben del komunikacijske infrastrukture, tako doma kot tudi v večjih organizacijah, podjetjih, v mestih in na letališčih. K njihovi popularnosti je pripomoglo tudi to, da delujejo v nelicenciranem frekvenčnem spektru, imenovanem ISM - Industrial, scientific and medical, za katerega ni potrebno pridobiti licence. Omogočajo povezavo brez zamudnega postavljanja infrastrukture in vlečenja kablov, kot je to potrebno v primeru žičnih omrežij. Ena izmed njihovih glavnih prednosti pa je, da omogočajo večjo mobilnost uporabnikov in priklop na omrežje, ne glede na to, kje v prostoru se nahajamo.

S povečevanjem hitrosti in zanesljivosti brezžičnih omrežij se je povečevalo tudi število naprav in njihovih uporabnikov, ki takšna omrežja uporabljajo. Omrežni administratorji v večjih organizacijah so se tako srečali z načrtovanjem, nastavljanjem, nadzorovanjem in upravljanjem vse večjih brezžičnih omrežij. Zagotoviti je potrebno integriteto, zasebnost in stalno dosegljivost omrežja. S strani uporanikov je namreč brezžično omrežje enako zanesljivo kot žično, v resnici pa je za zanesljivo delovanje brezžičnega omrežja potrebno vložiti veliko več znanja in časa.

Potreba po mobilnosti zaposlenih v izobraževalni in raziskovalni sferi je leta 2003 na evropski ravni povzročila ustanovitev brezžičnega omrežja Eduroam, ki je podrobneje opisano v razdelku 2.3. Iz omrežja, ki je v začetku pokrivalo omejene dele fakultet in šol, se je Eduroam razširil na celotne kampuse in študentske domove. Število dostopovnih točk pod upravljanjem posamezne organizacije pa se je močno povečalo. S tem se je pojavila potreba po sistemu, ki bi omogočal hitrejšo distribucijo dostopovnih točk in kasneje njihovo lažje upravljanje.

V diplomskem delu bomo rešili problem nadzora, upravljanja in oskrbe velikih brezžičnih omrežij. Poiskali bomo arhitekturo brezžičnih omrežij in protokole, ki te naloge poenostavijo. Postavili bomo maketo omrežja Eduroam s predlagano arhitekturo. Na preizkusnem poligonu bomo preučili in preizkusili različne možnosti uporabe predlagane infrastrukture v izobraževalnih in raziskovalnih organizacijah, ki uporabljajo omrežje Eduroam. Raziskali in preizkusili bomo, kaj uporaba predlagane brezžične arhitekture pomeni za varnost v omrežju. Za primerjavo bomo vzeli varnost v običajnih Eduroam omrežjih.

Poglavje 2

Brezžična omrežja

Brezžična omrežja s seboj prinašajo najbolj očitno prednost - mobilnost uporabnikov. Namesto s kablom se lahko uporabniki v omrežje povežejo iz pisarne, knjižnice, konferenčne sobe ali celo kavarne čez cesto, če jih signal brezžične dostopovne točke tam doseže. Prav dostopnost prenosnega medija, vsem v dosegu brezžičnih signalov, zahteva dodatno pozornost pri zagotavljanju varnosti v omrežju. Ostale naprave, ki delujejo v frekvenčnem spektru ISM predstavljajo potencialne motnje delovanja brezžičnega omrežja. Za uspešno načrtovanje in upoštevanje vseh faktorjev, ki vplivajo na delovanje brezžičnega omrežja, je potrebno dobro poznati njegove sestavne dele.

V tem poglavju si bomo za začetek ogledali skupino brezžičnih standardov IEEE 802.11. V prvem delu bomo opisali lastnosti brezžičnih omrežij in njihove sestavne dele. V drugem pa se bomo posvetili v brezžičnih omrežjih uporabljenim varnostnim in avtentikacijskim metodam. Za konec bomo predstavili omrežje, ki te standarde uporablja in je poenostavilo mobilnost v raziskovalni in izobraževalni sferi, imenovano Eduroam.

2.1 IEEE 802.11

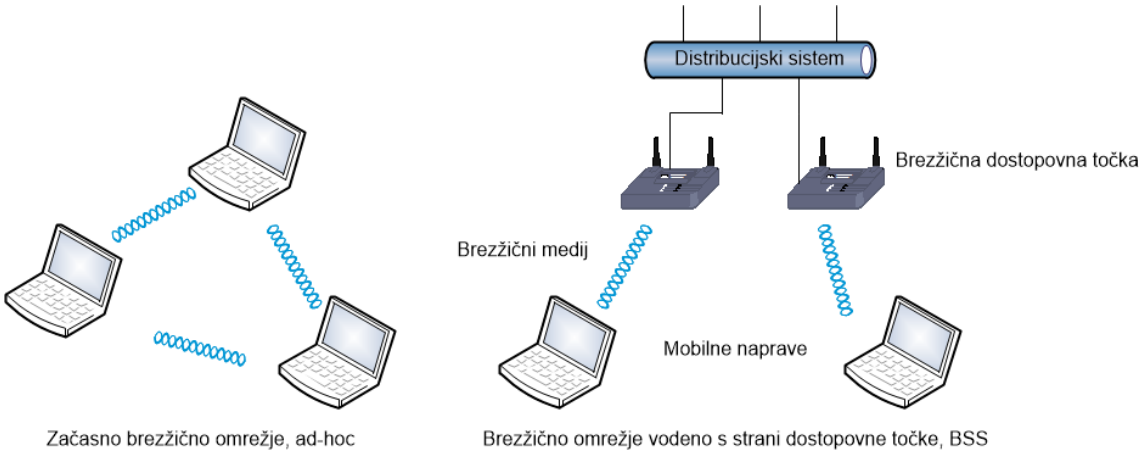
Skupina standardov IEEE 802.11 specificira brezžična lokalna omrežja, ki delujejo v 2.4 GHz, 3.6 GHz in 5 GHz [20] frekvenčnih področjih. Prvotni standard je vseboval tudi podporo infrardeči povezavi, ki pa ni bila veliko uporabljena. V tem delu bomo pozornost namenili predvsem omrežju, ki deluje na 2.4GHz in 5GHz. Uporaba 3.6GHz področja je namreč dovoljena le v ZDA.

2.1.1 Arhitektura brezžičnih omrežij

Standard IEEE 802.11 [3] definira brezžično komunikacijo med mobilnimi napravami in dostopovnimi točkami, imenovano BSS (*ang. Basic Service Set*). Standard omogoča tudi neposredno povezavo med mobilnimi napravami brez prisotnosti dostopovne točke. Takšen način povezave je pogosto imenovan tudi ad-hoc ali IBSS (*ang. Independant basic service set*). BSS in IBSS sta osnovni arhitekturi brezžičnih omrežij. V nadaljevanju se bomo osredotočili na arhitekturo, v kateri je omrežje vodeno s strani ene ali večih dostopovnih točk (BSS). V poglavju 3 bo predstavljena tudi arhitektura, ki poenostavi upravljanje in nadzor omrežja ter oskrbo dostopovnih točk, kadar je teh res veliko.

Omrežje se identificira z BSSID (*ang. Basic Service Set Identifier*) ali krajše SSID (*ang. Service set identification*), ki je pravzaprav ime omrežja. Ko je omrežje sestavljeno iz večih dostopovnih točk, ki oddajajo isti SSID, so lahko te dotopovne točke med seboj povezane prek distribucijskega sistema (DS). Več dostopovnih točk povezanih med seboj prek distribucijskega sistema imenujemo ESS (*ang. Extended Service Set*). Primarna naloga dostopovnih točk je posredovanje paketov med žičnim in brezžičnim omrežjem. Dostopovne točke so torej most, ki omogoča mobilnim napravam povezavo na distribucijski sistem in naprej v svet. V kakšni obliki mora biti distribucijski sistem standard ne določa, določa le storitve [3], ki jih mora zagotavljati. Storitve brezžičnih naprav so podrobneje opisane v razdelku 2.1.4. Običajno

se v komercialnih implementacijah za distribucijski sistem uporablja IEEE 802.3, znan tudi kot Ethernet. Možna je tudi uporaba brezžičnega distribucijskega sistema (WDS), ki pa se večinoma uporablja v mestnih omrežjih in omrežjih na prostem. Slika 2.1 prikazuje osnovni arhitekturi brezžičnih omrežij.



Slika 2.1: Omrežje vodeno s strani dostopovne točke in omrežje ad-hoc.

2.1.2 Frekvenčna področja

Na 2.4 GHz frekvenčnem območju imamo v Evropi 13 različnih kanalov širine 20 MHz. Sosednji kanali se med seboj prekrivajo, zato lahko naenkrat uporabljamo le do 4 neprekrivajoče kanale - 1, 5, 9 in 13. V 5 GHz omrežju je na voljo 19 neprekrivajočih kanalov, izbiro kanala pa je po predpisih Evropske unije potrebno prepustiti sistemu DFS (*ang. Dynamic Frequency selection*). V tem frekvenčnem območju namreč delujejo tudi vremenski radarji.

Prednost omrežja, ki deluje v 5 GHz frekvenčnem spektru je, da ima manj težav z interferencami, saj večina brezžičnih naprav, kot so Bluetooth naprave, brezžični telefoni in mikrovalovne pečice, deluje v 2.4 GHz frekvenčnem spektru. Slabost 5 GHz spektra je pol krajša valovna dolžina kot pri 2.4 GHz in posledično manjši domet omrežja. Stene, vrata in druge prepreke veliko lažje absorbirajo višje frekvence, kar je še ena omejitev 5 GHz brezžičnih omrežij. Priporočena je oprema, ki omogoča sočasno uporabo obeh frekvenčnih področij, saj to omogoča fleksibilnost, večjo kapaciteto in boljšo zanesljivost brezžičnega omrežja.

2.1.3 Upravljanje dostopa do skupnega medija

Prvotni brezžični standard 802.11 je za hkratni dostop do skupnega medija na fizičnem nivoju uporabljal multipleksiranji DSSS (*ang. Direct Sequence Spread Spectrum*) in FHSS (*ang. Frequency hopping Spread Spectrum*). Novejše verzije standarda, 802.11n in prihajajoči standard 802.11ac, pa uporabljata multipleksiranje OFDM (*ang. Orthogonal frequency-division multiplexing*). Dostop do medija se upravlja na povezavnem nivoju (MAC), kjer za izogibanje trkom skrbi mehanizem CSMA/CA.

2.1.4 IEEE 802.11 MAC

Standard IEEE 802.11 v podporo drugemu nivoju modela ISO/OSI, kasneje MAC, definira različne storitve [3], ki jih morajo opravljati naprave v brezžičnih omrežjih. Storitve so razdeljene v dve kategoriji - storitve po-

staj in storitve distribucijskega sistema. Storitve postaj izvajajo dostopovne točke in mobilne naprave. Storitve distribucijskega sistema pa skrbijo za povezavo dostopovnih točk na distribucijski sistem. Storitve prikazuje tabela 2.1.4.

Storitev	Tip storitve
distribucija	distribucijska storitev
integracija	distribucijska storitev
asociacija	distribucijska storitev
reasociacija	distribucijska storitev
deasociacija	distribucijska storitev
avtentikacija	storitev postaj
deavtentikacija	storitev postaj
zasebnost	storitev postaj
dostava MSDU-jev	storitev postaj

Tabela 2.1: Storitve postaj in distribucijskega sistema v standardu 802.11.

Poleg teh storitev brezžični standard definira tudi storitve MAC [12], ki jih opravljajo dostopovne točke. To so:

- generiranje upravljalskih okvirjev: beacon, probe request, probe response;
- procesiranje kontrolnih okvirjev;
- ponovni prenosi;
- sinhronizacija;
- nadzor hitrosti prenosa;
- kvaliteta storitev (802.11e);
- zagotavljanje zasebnosti z enkripcijo in dekripcijo.

Za opravljanje storitev so na voljo 3 vrste okvirjev MAC - upravljalski okvirji, kontrolni okvirji in podatkovni okvirji. Upravljalski okvirji (*association, authentication, beacon, probe request, probe response*) omogočajo sinhronizacijo, avtentikacijo in povezavo naprav v omrežju. Kontrolni okvirji (*RTS, CTS, ACK, PS-Poll, CF-End, CF-ACK*) služijo upravljanju dostopa do skupnega medija in potrditvam ob uspešno prejetih paketih. Podatkovni okvirji služijo za prenos podatkov. Ena izmed pomembnejših nalog dostopovnih točk in mobilnih naprav je tudi vzdrževanje zasebnosti, ki jo dosežeta z uporabo enkripcije in dekripcije. Varnostni mehanizmi v brezžičnih omrežjih so opisani v razdelku 2.2.

2.2 Varnostni in avtentikacijski mehanizmi

Brezžična komunikacija poteka prek radijskih valov, ki jih z ustrezno napravo lahko vsak posluša. Brez ustrezne preverbe pristnosti pa se v takšno omrežje lahko priključi vsaka brezžična naprava. V tem delu si bomo ogledali aktualna protokola, ki omogočata zagotavljanje mehanizmov, ki so v brezžičnih omrežjih potrebni za varnost [1]:

- obojestranska avtentikacija;
- nadzor dostopa;
- preprečevanje napada s ponavljanjem;
- zaznavanje ponarejenih sporočil;
- ohranjanje zasebnosti;
- zaščita ključev.

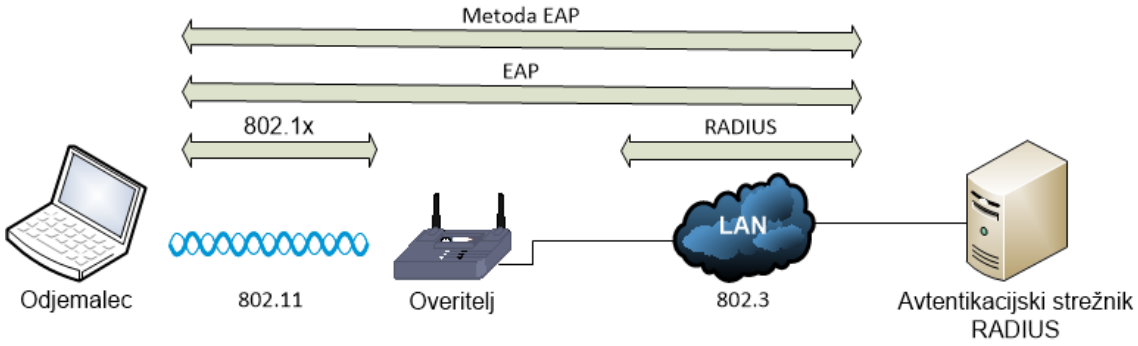
2.2.1 IEEE 802.11i

IEEE 802.11i je standard, ki specificira mehanizme za varnost v brezžičnih omrežjih. Uporablja enkripcijska mehanizma TKIP in CCMP. TKIP odpravlja pomankljivosti protokola WEP [2] in je zasnovan za kompatibilnost s starimi napravami, saj je za uporabo potrebna le nadgradnja programske opreme. CCMP pa temelji na AES-u. Standard uporablja dva načina avtentikacije uporabnikov, Pre-shared Key (PSK) ali protokol 802.1x z uporabo različnih metod EAP in avtentikacijskih strežnikov. Po uspešni avtentikaciji si dostopovna točka in odjemalec v 4-kratnem rokovanju izmenjata in nastavita sejne in skupinske ključe, ki jih uporabljata za šifriranje nadaljne komunikacije. V poglavju 2.2.2 si bomo ogledali delovanje protokola 802.1x, ko se za prenos avtentikacijskih sporočil uporablja RADIUS in močne metode EAP. Takšna uporaba je namreč običajna v večjih organizacijah in tudi omrežju Eduroam.

2.2.2 IEEE 802.1x

IEEE 802.1x je protokol, ki omogoča nadzor dostopa do omrežja. Uporablja se tako v žičnih kot v brezžičnih omrežjih. Entitete v omrežju razdeljuje na tri dele. Imenujemo jih:

- **odjemalec** (*ang. Supplicant*),to je tisti, ki se želi povezati v omrežje;
- **overitelj** (*ang. Authenticator*), ki nadzoruje dostop do omrežja;
- **avtentikacijski strežnik** (*ang. Authentication server*), ki odloči, kdo ima dostop do omrežja.



Slika 2.2: Prikaz komunikacije EAP v avtentikacijskem procesu 802.1x.

Dostop se omejuje na ravni vrat na primer na stikalu ali razdelilniku. V brezžičnih omrežjih fizične povezave med brezžično dostopovno točko (overiteljem) in mobilno napravo (odjemalcem) ni. Kot vrata se zato uporabi logična povezava. Logičnih povezav je na dostopovni točki toliko, kolikor je nanjo asociiranih mobilnih naprav. Vrata so na začetku v nenadzorovanem stanju, odjemalec pa ni avtenticiran. Takrat poteka prijava uporabnika v omrežje. Odjemalec in overitelj komunicirata s pomočjo sporočil EAP. Za prenos sporočil EAP se uporablja protokol EAPOL, ki skrbi za ovijanje metod EAP v Ethernet okvirje. Pogosto uporabljene metode EAP [18] so: EAP-TLS, EAP-TTLS, EAP-PEAP. Overitelj sporočila EAP nato prek protokola RADIUS [19] posreduje avtentikacijskemu strežniku. Komunikacijo EAP prikazuje slika 2.2.2. V tem procesu se lahko odjemalec in avtentikacijski strežnik obojestransko avtenticirata (strežnik preveri identiteto odjemalca in uporabnik identiteto strežnika). Šele po uspešni preverbi pristnosti na strani avtentikacijskega strežnika logična vrata spremenijo svoje stanje v nadzorovano in odjemalec pridobi možnost uporabe ostalih storitev v omrežju. V primeru brezžičnih omrežij na tem mestu avtentikacijski strežnik overitelju tudi posreduje potrebne sejne ključe. Ključe overitelj in odjemalec uporabita za generiranje začasnih ključev, ki so namenjeni šifriranju nadaljne komunikacije.

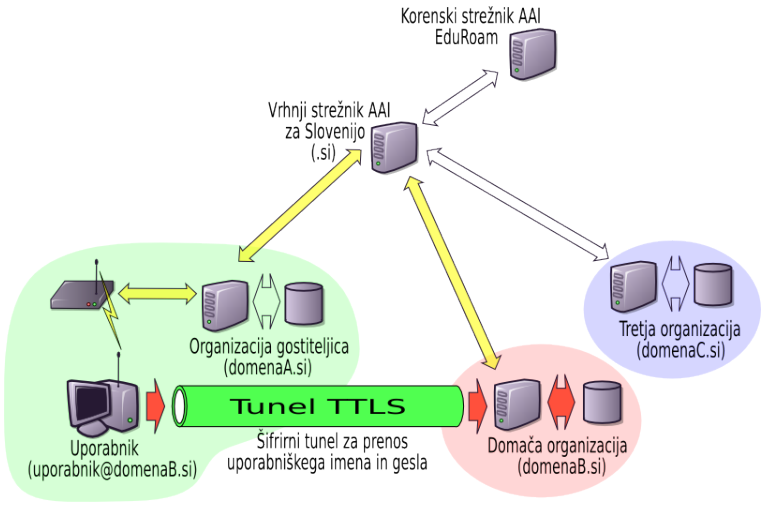
2.3 Omrežje Eduroam

Eduroam je sistem varnega mednarodnega gostovanja [6]. Temelji na pravnih in tehničnih dogovorih med člani konfederacije. Omrežje je sestavljeno iz avtonomnih brezžičnih omrežij izobraževalnih in raziskovalnih ogranizacij. Eduroam za prijavo uporabnikov uporablja AAI infrastrukturo, kar omogoča, da uporabniki do omrežja dostopajo z identiteto, pridobljeno na matični organizaciji (fakulteti, srednji šoli, inštitutu). Identitete so oblike uporabniško-ime@domena-organizacije. Domena organizacije služi usmerjanju uporabniških zahtevkov ob gostovanju. Preverba pristnosti uporabnika se tako vedno izvede na domači organizaciji, ne glede na to, ali uporabnik dostopa do omrežja na domači organizaciji ali katerikoli drugi organizaciji, ki ima vzpostavljen Eduroam.

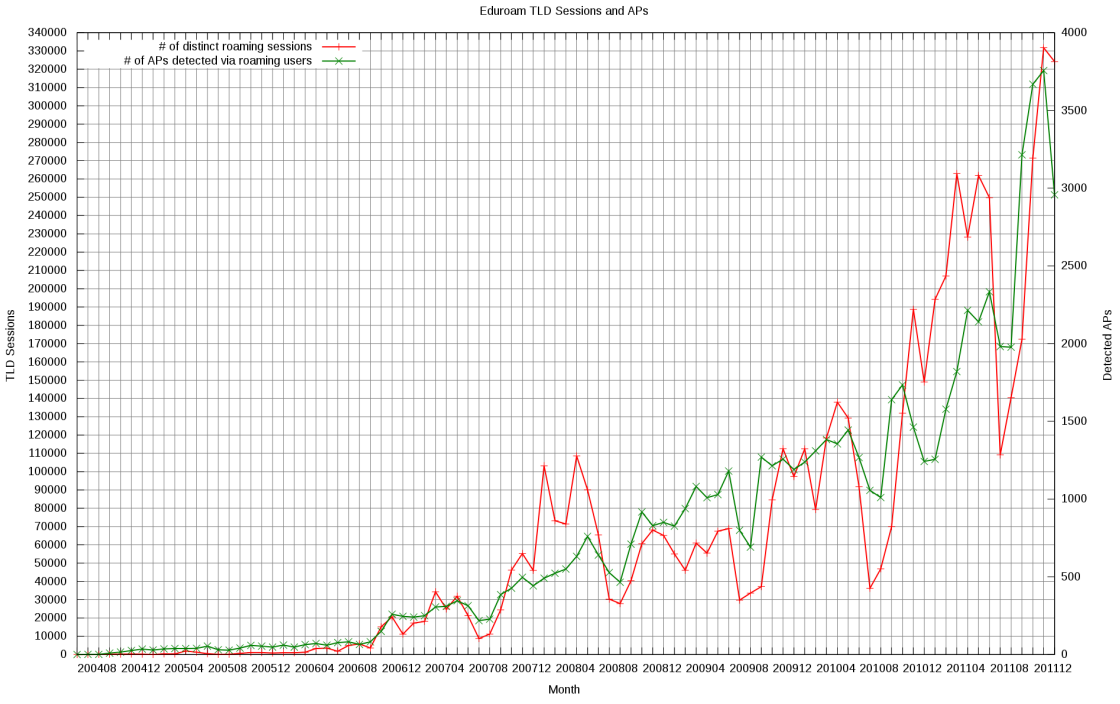
Uporabniki v omrežje lahko dostopajo z različnimi napravami (prenosniki, telefoni, tablični računalniki). Običajno povezava poteka prek brezžičnih dostopovnih točk, za varnost in anonimnost pa skrbita v razdelku 2.2 opisani tehnologiji 802.11i in 802.1x.

Slovensko omrežje Eduroam je sestavni del mednarodne infrastrukture, ki temelji na hierarhiji strežnikov RADIUS. Strežniki RADIUS skrbijo za posredovanje uporabniških avtentikacijskih zahtevkov med gostujočo in domačo organizacijo ter avtentikacijo uporabnikov. Arhitektura omrežja omogoča prožnost s poljubno izbiro centralizacije ali decentralizacije. Avtentikacijski strežnik in imenik uporabnikov sta lahko postavljena na ravni univerze, šolskega centra, fakultete ali šole [5]. Skrbnik slovenske konfederacijske infrastrukture in omrežja Eduroam je zavod Arnes.

Slika 2.3 prikazuje hierarhijo strežnikov RADIUS v omrežju Eduroam. Na sliki 2.4 pa je prikazano število dostopovnih točk in uporabniških sej, zaznanih med gostovanjem v omrežju Eduroam, od leta 2004 do leta 2011.



Slika 2.3: Prikaz hierarhije strežnikov RADIUS v omrežju Eduroam. Vir: [5]



Slika 2.4: Število dostopovnih točk in uporabniških sej, zaznanih pri gostovanju doma in v tujini. Vir: [5]

Poglavje 3

Nadzor in upravljanje brezžičnih dostopovnih točk

Brezžična omrežja so z razvojem pridobila na hitrosti in zanesljivosti. Posledično se je povečala tudi njihova popularnost in uporabnost. Povečano število mobilnih naprav in aplikacije, ki zahtevajo večjo pasovno širino in majhno zakasnitev, so povzročile povečanje brezžičnih omrežij, da so lahko leta zagotovila ustrezne kapacitete. Ob načrtovanju in upravljanju obsežnega števila dostopovnih točk so se pokazale slabosti trenutne arhitekture brezžičih omrežij, ki je podrobneje opisana v razdelku 2.1.1.

V tem poglavju bomo predstavili težave [9], ki se pojavijo pri upravljanju velikega števila dostopovnih točk in so vodile do razvoja arhitekture za centralizirano upravljanje omrežij. Ogledali si bomo centralizirano arhitekturo in predstavili lahke dostopovne točke (*ang. Wireless Termination Point*), ki si funkcionalnosti delijo z dostopovnim krmilnikom (*ang. Access Controller*). Predstavili bomo tudi varnostni vidik brezžičnih omrežij in preverili, kateri protokoli za centralizirano upravljanje omrežja obstajajo in izbrali najprimernejšega.

3.1 Težave pri upravljanju brezžičnih omrežij

Vsaka avtonomna dostopovna točka ima svojo IP številko in jo je običajno mogoče upravljati in konfigurirati prek ukazne vrstice, SNMP-ja, telnet-a, SSH-ja ali protokola HTTP. Upravljanje in nadzor brezžičnega omrežja, ki vsebujejo veliko dostopovnih točk, lahko tudi več 100 ali več 1000, je za omrežne administratorje zahtevna naloga.

Konfiguracije na dostopovnih točkah so si med seboj običajno zelo podobne. Na njih je potrebno nastaviti omrežja, ki jih dostopovna točka oglašuje, varnostne mehanizme in različne avtentikacijske parametre, povezavo dostopovne točke na distribucijsko omrežje, nastavitve radijskega dela ipd. Majhne razlike v konfiguracijah lahko vodijo v napake pri postavitvi omrežja in posledično nepravilno delovanje .

Nastavitve in programsko opremo na dostopovnih točkah je potrebno stalno vzdrževati in posodabljati. Dodajanje novih dostopovnih točk v omrežje in posodabljanje programske opreme na posameznih točkah lahko čez čas povzroči nekonsistentnost v nastavitvah omrežja.

Kot smo si ogledali v razdelku, 2.1.2 si brezžična omrežja medij delijo z veliko drugimi napravami in pogosto tudi sosednjimi brezžičnimi omrežji. Posledično je potrebno ob interferencah prilagajati kanale, na katerih dostopovne točke delujejo, da se lahko zagotovi optimalno delovanje. Načrtovanje in ročno popravljanje takšnih nastavitev je zahtevno, saj lahko popravek na eni dostopovni točki poslabša delovanje na sosednji.

Pomembna je tudi zagotovitev varnosti dostopovnih točk, saj v nastavitvah vsebujejo precej pomembnih skrivnosti, na primer gesla za dostop do strežnikov AAA ali kakšne druge opreme. Dostopovne točke morajo zato omogočati varno potrditev in zavarovanje s pomočjo ključavnice, saj bi kraja lahko omogočila nepooblaščen dostop v omrežje. Prav tako žica, s katero je dostopovna točka povezana v omrežje, predstavlja možnost za vdor v organizacijsko omrežje.

3.2 Varnostni vidiki nadzora brezžičnih omrežij

Pri načrtovanju brezžičnih omrežij je potrebno skrbno preučiti vse varnosne vidike. Pomembno je, da organizacije definirajo ustrezne varnostne politike in zagotovijo omejevanje dostopa v brezžično omrežje. Z uporabo varnostnih mehanizmov, ki smo jih opisali v poglavju 2.2, pa poskrbijo za zasebnost uporabnikov v brezžičnem omrežju. Delovanje omrežja je potrebno nadzorovati in se na morebitne napade ustrezno odzivati. Zaradi tesne prepletenosti žičnih in brezžičnih omrežij mora varnostna politika zajemati obe. Omrežje in njegovi uporabniki so namreč ranljivi z obeh strani.

Na žičnem delu je tako resna grožnja omrežju organizacije zlonamerna dostopovna točka. V omrežje jo lahko priključi zaposleni in zaradi pomankljive zaščite omogoči dostop do organizacijskega omrežja tudi napadalcu. Ta je lahko zaradi dosegljivosti brezžičnega signala tudi na parkirišču pred organizacijo. Nevarnost predstavljajo tudi običajno slabo zaščitena omrežja ad-hoc. Takšna omrežja lahko zaposleni postavijo za začasno povezljivost med mobilnimi napravami. Če je njihova mobilna naprava obenem priključena tudi v žični del organizacijskega omrežja, lahko napadalec pridobi dostop ne le do žrtvinih podatkov, ampak tudi do storitev organizacijskega omrežja.

V razdelku 2.2.2 smo poudarili pomen obojestranske avtentikacije v brezžičnih omrežjih. Neustrezno politiko organizacije in napačno konfiguracijo mobilnih naprav lahko napadalci izkoristijo z uporabo lažne dostopovne točke. Povezava mobilne naprave na takšno dostopovno točko lahko razkrije uporabniške podatke za dostop do organizacijskega omrežja. Prav tako omogoča napad "Mož v sredini"(*ang. Man in the middle attack*) in prestrezanje podatkov.

Zaščititi se je potrebno pred možnostjo kraje identitete uporabnika na omrežju. Z uporabo lažnega predstavljanja in uporabe lažnega naslova MAC lahko napadalec pridobi dostop do virov in storitev organizacijskega omrežja, do katerih mu dostop sicer ni dovoljen.

Doseg brezžičnega omrežja lahko brez težav seže tudi izven organizacijske zgradbe, kar omogoča zajem paketov in obdelava z orodji za razbija-

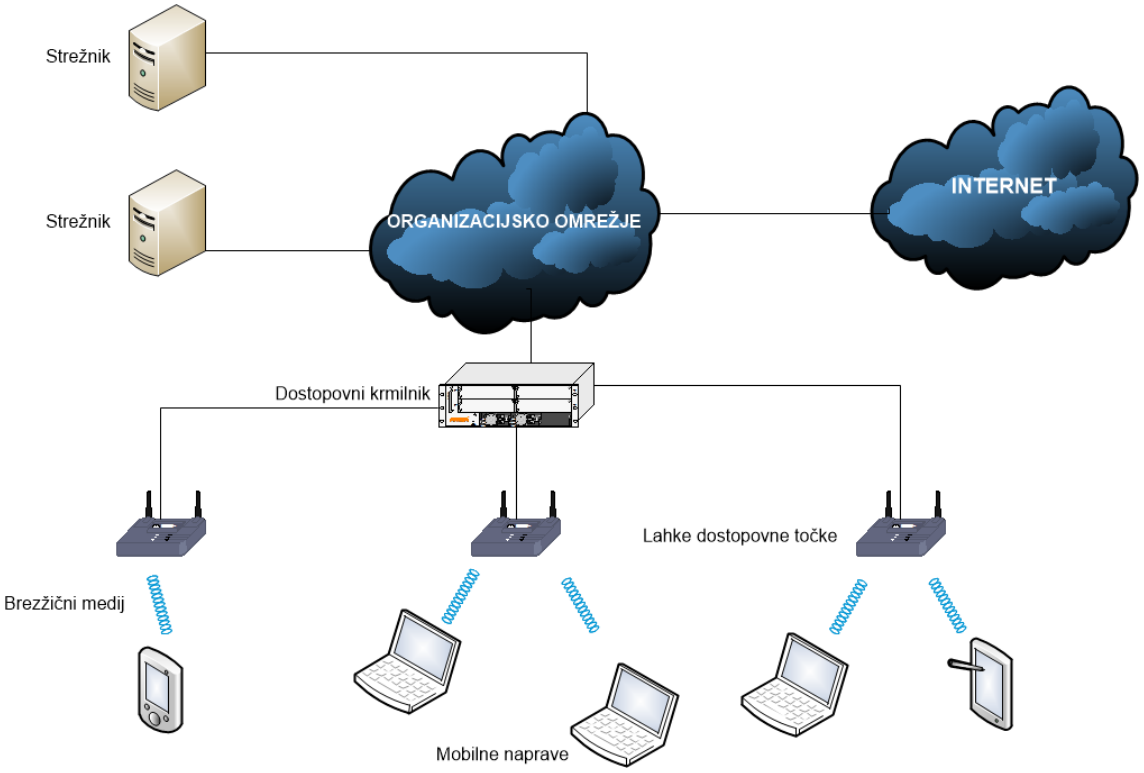
nje. Prav tako lahko napadalec uporabnikom dostop onemogoči z motenjem brezžičnega signala ali zasipanjem dostopovne točke z različnimi zlonamernimi paketi (*ang. Denial of Service attack*).

Čeprav se dostopovne točke običajno nahajajo v prostorih organizacije, jih je potrebno ustrezno zaščititi pred nepooblaščenim dostopom. Na stenah v organizacijskih prostorih dostopovne točke niso tako varne kot naprave v strežniški sobi. Žično omrežje, na katerega je dostopovna točka priključena, je mogoče izkoristiti za dostop do organizacijskega omrežja. Prav tako avtonomne dostopovne točke vsebujejo skrivnosti, ki lahko napadalcu omogočijo nepooblaščen dostop do omrežja.

To so le najpogostejše grožnje [17], ki lahko ogrozijo organizacijska omrežja. V rešitvi problema z upravljanjem in nadzorom velikega števila dostopovnih točk bomo preverili tudi kakšne prednosti prinaša centralizirano upravljanje in poskušali omrežje kar najbolje zaščititi.

3.3 Arhitektura za centralno upravljanje brezžičnih omrežij

V centralizirani omrežni infrastrukturi se izvajanje nalog v brezžičnem omrežju razdeli med dostopovne točke (*ang. Wireless termination point*) in dostopovni krmilnik (*ang. Access controller*). Razdelitev je podrobneje predstavljena v razdelku 3.3.1. Slika 3.1 prikazuje sestavne dele centralno upravljanega brezžičnega omrežja.



Slika 3.1: Centralno upravljano brezžično omrežje.

3.3.1 Vrste dostopovnih točk

Dostopovne točke v običajnih brezžičnih omrežjih imenujemo avtonomne dostopovne točke. O sestavi brezžičnega omrežja, ki vsebuje avtonomne dostopovne točke smo pisali v razdelku 2.1. Takšne dostopovne točke opravljajo vse funkcionalnosti, ki jih za njih specificira standard 802.11. Vsaka točko je potrebno nastavljati in upravljati posebej. To se lahko izvede z uporabo konzolskega vmestnika ali s pomočjo protokolov: SSH, SNMP in HTTP. V centralizirani brezžični infrastrukturi se naloge dostopovnih točk razdelijo med dostopovno točko in dostopovni krmilnik. Dostopovne točke uporabljene v centralizirani arhitekturi imenujemo nadzorovane dostopovne točke (*ang. controlled access points*). Delimo jih na lahke in tanke. Imeni izvirata iz tega, kako preprosti sta dostopovni točki. Preprostost je posledica prepustitve določenih funkcionalnosti 802.11 dostopovnemu krmilniku. Dostopovne točke lahko uvrstimo v 3 arhitekturne skupine, glede na to, koliko svojih funkcionalnosti si delijo z dostopovnim krmilnikom. Skupine imenujemo lokalni MAC (*ang. local MAC*), razdeljeni MAC (*ang. split MAC*) in oddaljeni MAC (*ang. remote MAC*).

Lahke dostopovne točke

Lahke dostopovne točke svoje funkcionalnosti 802.11 MAC delijo z dostopovnim krmilnikom. Omogočajo dve vrsti delitve [11], lokalni MAC in razdeljeni MAC. Pri razdeljenem MAC-u dostopovne točke opravljajo časovno krititične, realno časovne funkcionalnosti (*ang. real-time*), dostopovni krmilniki pa časovno neobčutljive, ne-realno časovne funkcionalnosti (*ang. non-real time*). Takšna razdelitev omogoča, da se dostopovne točke posvetijo nalogam, ki so specifične za območje, ki ga pokrivajo, dostopovni krmilnik pa poskrbi za naloge, ki niso občutljive na zakasnitev in pridobi boljši pregled nad celotnim omrežjem. Razdelitev funkcionalnosti omogoča tudi preprostejše in cenejše dostopovne točke. Ves promet z dostopovnih točk je tuneliran preko krmilnika, zato je pomembno, da je med njima dobra žična povezava. Takšne dostopovne točke brez krmilnika ne morejo delovati, saj skrbi tudi za njihovo

konfiguracijo, nadzor in jih oskrbuje s programsko opremo. Delitev na realno časovne in ne-realno časovne funkcionalnosti se od protokola do protokola nekoliko razlikujeje. Spodaj je prikazana delitev funkcionalnosti MAC [12], ki je skupna večini protokolov za centralizirano upravljanje brezžičnih omrežij.

Realno časovne funkcionalnosti 802.11 MAC, izvaja jih lahka dostopovna točka:

- generiranje okvirjev: beacon, probe request in probe response;
- procesiranje kontrolnih okvirjev;
- sinhronizacija;
- ponovni prenosi;
- nadzor hitrosti prenosa.

Ne-realno časovne funkcionalnosti 802.11 MAC, izvaja jih dostopovni krmilnik:

- avtentikacija in deavtentikacija;
- asociacija, deasociacija in reasociacija;
- integracijska in distribucijska storitev;
- zagotavljanje zasebnosti z enkripcijo in dekripcijo;
- fragmentacija in defragmentacija.

V razdelitvi lokalni MAC, dostopovne točke same opravljajo funkcionalnosti 802.11 MAC. Krmilniku le posredujejo nekatere okvirje (npr. asociacijo). Dostopovni krmilnik obdrži kontrolno vlogo. Skrbi za njihovo upravljanje, nadzor in oskrbo. Izbirno lahko v nekaterih implementacijah opravlja tudi avtentikacijo uporabnikov in skrbi za shranjevanje sejnih ključev, iz katerih dostopovne točke in odjemalci ustvarijo začasne ključe za šifriranje komunikacije. Odvisno od uporabljenega protokola in proizvajalca lahko dostopovne točke uporabniški promet usmerjajo lokalno ali ga centralno tunelirajo

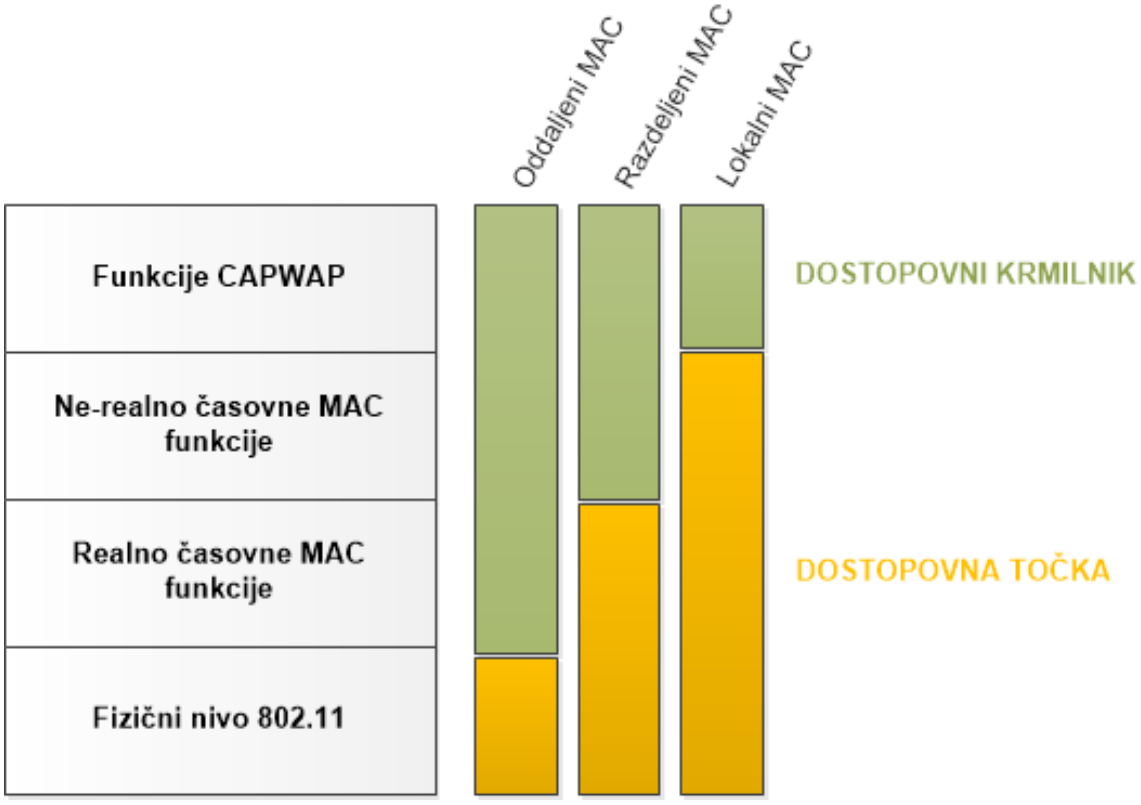
prek dostopovnega krmilnika. Tabela 3.1 prikazuje delitev [12] funkcionalnosti 802.11 med dostopovnim krmilnikom in lahko dostopovno točko.

Funkcija 802.11	razdeljeni MAC	lokalni MAC
distribucijska storitev	AC	WTP/AC
integracijska storitev	AC	WTP
generiranje okrivjev beacon	WTP	WTP
generiranje okrivjev probe response	WTP	WTP
upravljanje porabe energije	WTP	WTP
fragmentacija, defragmentacija	WTP	WTP
asociacija, deasociacija	AC	WTP/AC
kvaliteta storitev (QoS)		
razvrščanje v razrede	AC	WTP/AC
časovno razvrščanje	WTP/AC	WTP
čakalna vrsta	WTP	WTP
802.1X/EAP	AC	WTP/AC
Upravljanje sejnih ključev	AC	AC
Enkripcija in dekripcija	WTP/AC	WTPČ

Tabela 3.1: Razdelitev funkcionalnosti 802.11 med lahkimi dostopovnimi točkami (WTP) in dostopovnim krmilnikom (AC). AC pomeni, da se funkcija nahaja na dostopovnem krmilniku. WTP pomeni, da se funkcija nahaja na dostopovni točki.

Tanke dostopovne točke

Tanke dostopovne točke svoje funkcionalnosti 802.11 MAC povsem prepuščajo dostopovnemu krmilniku. Takšno delitev imenujemo oddaljeni MAC. Dostopovne točke delujejo kot pametne antene, ki imajo implementiran le fizični del standarda 802.11. Vse prejete pakete le posredujejo na brezžični krmilnik v obdelavo. Prednost takšnih dostopovnih točk je predvsem preprostost, saj se s tem zmanjša njihova cena in tudi potreba po nadgradnjah. Posebno pozornost je potrebno zagotoviti povezavi med dostopovno točko in krmilnikom, saj se na njem izvajajo tudi na zakasnitve občutljive storitve. Slika 3.2 prikazuje razdelitve funkcionalnosti MAC na primeru upravljalskega protokola CAPWAP.



Slika 3.2: Razdelitev funkcij MAC na primeru protokola CAPWAP.

3.3.2 Dostopovni krmilnik

Dostopovni krmilniki [11] so sestavni del centraliziranih brezžičnih omrežij. Z dostopovnimi točkami si delijo funkcionalnosti 802.11 MAC.

Njihova glavna prednost je poenostavitev nadzora in oskrbe dostopovnih točk v velikih brezžičnih omrežjih. Lahko upravljajo in oskrbujejo gručo dostopovnih točk. Glavne naloge dostopovnih krmilnikov so:

- **Odkrivanje dostopovnih točk**: Z njim krmilnik odgovarja na zahtevke za pridružitev (*ang. discovery request*), ki mu jih pošiljajo dostopovne točke;
- **Asociacija in avtentikacija dostopovnih točk**: Odkrita dostopovna točka in dostopovni krmilnik se s to funkcijo obojestransko avtenticirata;
- **Centralizirana konfiguracija**: Omogoča preprostejšo distribucijo enotnih nastavitev na pridružene dostopovne točke;
- **Uveljavljanje centralnih politik**: Omogoča definicijo varnostnih politik (npr. za določenega odjemalca) in njihovo distribuiranje;
- **Oskrba dostopovnih točk s programsko opremo**: Dostopovne točke se s tem ob pridružitvi posodobijo na verzijo programske opreme, s katero deluje dostopovni krmilnik. Na nekaterih protokolih je mogoče podatkovo opremo posodobiti tudi med delovanjem;
- **Nadzor omrežja**: Izvajanje nadzora in prilagajanje nastavitev, glede na statistične informacije, ki jih pošiljajo dostopovne točke (npr. prilagoditev radijskega dela);
- **Integracijska in distribucijska storitev**: Omogočata prenos podatkovnih paketov med napravami in premoščanje surovih 802.11 paketov, ki so tunelirani iz dostopovnih točk, na distribucijski sistem.

Dostopovne točke si s krmilnikom izmenjujejo kontrolni in podatkovni promet. Pri lokalnem in oddaljenem MAC-u si z dostopovnimi točkami krmilnik deli tudi funkcije 802.11 MAC. V primeru delitve lokalni MAC, krmilnik obdrži le kontrolno funkcijo. Nekateri proizvajalci brezžične opreme, so zato pričeli z nadomeščanjem dostopovnih krmilnikov. Nadomeščajo jih z upravljalskimi strežniki, ki služijo le za upravljanje lahkih dostopovnih točk. Kontrolno funkcionalnost pa distribuirajo med dostopovne točke. S tem želijo zmanjšati stroške, ki jih prinašajo dostopovni krmilniki, a ohraniti prednosti dostopovnih krmilnikov. Slabost centralizirane brezžične infrastrukture je, da morata biti za zagotavljanje redundance dostopovna krmilnika vsaj dva. Če si dostopovni krmilnik in dostopovna točka funkcionalnosti delijo po sistemu oddaljeni MAC ali razdeljeni MAC, odpoved krmilnika pomeni tudi prenehanje delovanja omrežja. Lokalni MAC omogoča tudi samostojno delovanje dostopovnih točk, če povezavo s krmilnikom izgubijo.

3.3.3 Pridružitev in avtentikacija dostopovne točke

V centralizirani brezžični arhitekturi se funkcionalnosti 802.11 nahajajo na dveh napravah, dostopovni točki in dostopovnem krmilniku. Napravi se morata za komunikacijo povezati prek žičnega omrežja. Dostopovne točke se lahko na dostopovni krmilnik priključijo z direktno povezavo točka v točko, povezavo prek stikala iz istega podomrežja ali pa s pomočjo usmerjanja, če se nahajajo v drugem podomrežju kot pa dostopovni krmilnik.

Ob začetku delovanja dostopovne točke pričnejo z odkrivanjem dostopovnih krmilnikov na omrežju. Brez povezave na krmilnik ne morejo pričeti z delovanjem. Dostopovne točke lahko dostopovni krmilnik odkrijejo s pomočjo protokola DHCP. To jim omogoča uporaba lastniških razširitev protokola DHCP (*ang. Vendor Specific Information*). Dostopovni krmilnik lahko odkrijejo tudi z oddajanjem poizvedb na lokalnem podomrežju. Naslov IP dostopovnega krmilnika se jim lahko vpiše tudi s statično konfiguracijo ali pa ga poiščejo z uporabo protokola DNS.

Ker se funkcije, ki so se prej nahajale znotraj avtonomne dostopovne točke, sedaj izvajajo na dveh napravah, je potrebno komunikacijo med njima ustrezno zaščititi. Pri pridružitvi je za varnost poskrbljeno z uporabo obojestranske avtentikacije, ki se izvede s pomočjo predhodno izmenjanih skrivnosti ali uporabo infrastrukture PKI. Za avtentikacijo dostopovnih točk je mogoče uporabiti tudi strežnik AAA. Obojestranska avtentikacija služi tudi kot izhodišče za vzpostavitev varnega tunela, ki ga različni upravljalski protokoli uporabljajo za zaščito kontrolne in podatkovne komunikacije.

3.4 Protokoli za upravljanje brezžičnih omrežij

3.4.1 Varnostni vidik

Nekateri proizvajalci zagovarjajo pristop, pri katerem dostopovnih točk pred prvo uporabo ni potrebno dodatno nastavljati (*ang. zero touch approach*). Težava s tem je, če na takšne dostopovne točke ne moremo namestiti certifikata ali vpisati skrivnosti za vzpostavitev varnega tunela z dostopovnim krmilnikom, protokol WiCoP na primer vzpostavitve varnega tunela sploh ne specificira. Vzpostavitev varnega tunela med dostopovnim krmilnikom in dostopovno točko je pomembno, ker so funkcije 802.11, ki se v avtonomni infrastrukturi nahajajo na eni napravi, tu razdeljene med dve napravi. Komunikacijo med dostopovnim krmilnikom in dostoponvo točko je zato potrebno zaščititi pred možnostmi potvarjanja paketov, napada s ponavljanjem, napada z možem v sredini in napada z onemogočanjem storitve. Zagotoviti je potrebno tudi obojestransko preverjanje pristnosti, kar preprečuje možnost lažnega predstavljanja, napade z možem v sredini in lahko omeji tudi napade z onemogočanjem storitve. Najbolje se pri tem obnese protokol DTLS [16], prvotno predstavljen v upravljalskem protokolu SLAPP. Kljub uporabi protokola DTLS pa se pred vsemi zlorabami ne da zaščititi. Še vedno ostaja možnost napada s preprečevanjem storitve, pred katero se upravljalski protokoli ne morejo zaščititi. Prav tako je potrebno zagotoviti varnost omrežja, na katerega so priključene lahke dostopovne točke, saj napadalec postavitev lažne omrežne infrastrukture (strežnika DHCP ali strežnika DNS) lahko izkoristi za preusmerjanje dostopovnih točk na lažni krmilnik.

3.4.2 Lastniški protokoli

Na trgu obstaja veliko rešitev za centralizirano upravljanje brezžičnih omrežij. Posamezni proizvajalci prodajajo svoje lastniške rešitve, ki pa omogočajo upravljanje le njihovih brezžičnih dostopovnih točk. Posamezne rešitve podpirajo različne razdelitve funkcionalnosti 802.11 MAC. Problem lastniških

rešitev je, da med seboj niso kompatibilne. Tako je potrebno za pravilno delovanje uporabjati krmilnik in dostopovne točke istega proizvajalca. Primeri lastniških protokolov za centralizirano upravljanje lahkih dostopovnih točk [13] so WiCoP, SLAPP, LWAPP, PAPI, SWAN. Za zagotavljanje združljivosti med proizvajalci in poenotenje komunikacije med dostopovnim krmilnikom in dostopovno točko je skupina znotraj IETF (*ang. Internet Engineering Task Force*) standardizirala protokol CAPWAP (*ang. Control And Provisioning of Wireless Access Points*) [14]. Kot osnovo za protokol so izbrali Ciscov lastniški protokol LWAPP, ki je najbolje ustrezal zahtevam [13]. Iz protokola SLAPP so vzeli njegovo dobro lastnost, in sicer šifriranje kontrolnega in podatkovnega kanala z uporabo DTLS [16].

Kot edini standardiziran protokol za komunikacijo med dostopovnim krmilnikom in dostopovno točko, ki omogoča centraliziran nadzor in upravljanje brezžičnih dostopovnih točk, bomo v naši rešitvi uporabili opremo, ki temelji na protokolu CAPWAP.

3.4.3 Protokol CAPWAP

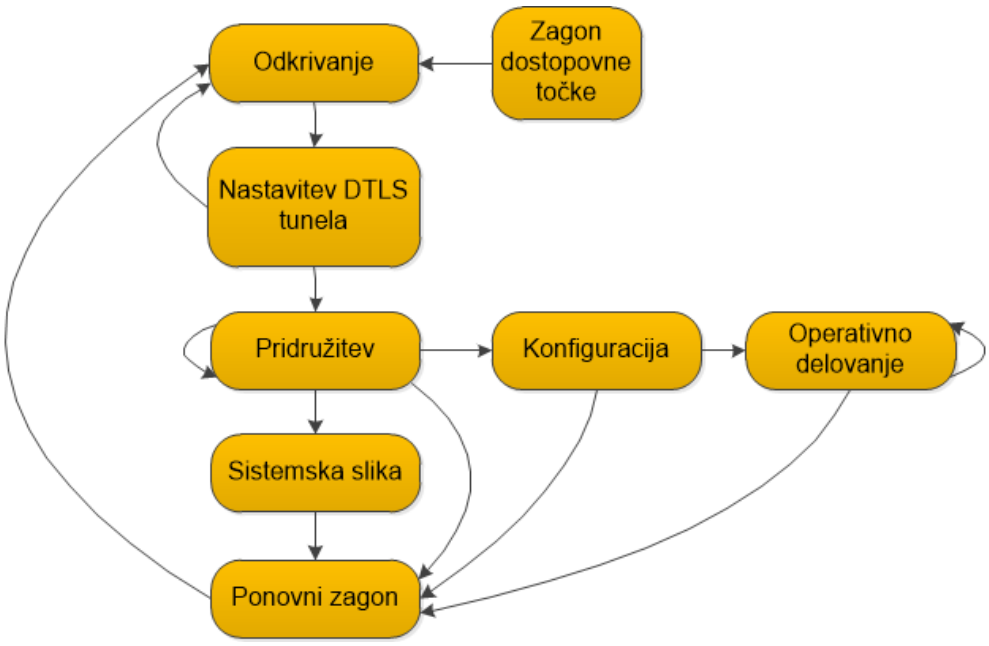
CAPWAP definira upravljanje in oskrbo dostopovnih točk s strani dostopovnega krmilnika. Protokol omogoča upravljanje različnih brezžičnih tehnologij. Delovanje s standardom 802.11 je posebej definirano v RFC-ju 5416 [15]. Podpira dve razdelitvi funkcionalnosti 802.11 MAC, lokalni MAC in razdeljeni MAC, ki sta podrobneje opisani v razdelku 3.3.1. Sporočila CAPWAP so razdeljena na kontrolna in podatkovna. Za pošiljanje se uporablja UDP, z uporabo vrat 5246 (kontrolna sporočila) in 5247 (podatkovna sporočila). Zanesljivost se zagotavlja z uporabo sistema zahteva - odgovor na zahtevo. Če poteče čas za prejem odgovora na poslano zahtevo, se ta še enkrat pošlje. Ves promet med dostopovnim krmilnikom in dostopovno točko je enkapsuliran v protokolu CAPWAP.

Za zagotavljanje varnosti se pred komunikacijo vzpostavi varni tunel, DTLS [16], ki se nato uporablja za zaščito kontrolnih in podatkovnih sporočil. Ob vzpostavitvi se dostopovna točka in dostopovni krmilnik obojestransko

avtenticirata z uporabo predhodno izmenjanih skrivnosti ali uporabo infrastrukture PKI.

Protokol omogoča upravljanje politik za mobilne naprave, ki so povezane na dostopovne točke in zbiranje statističnih informacij za uravnavanje radijskega dela ter upravljanje kvalitete storitev.

Ostali koncepti delovanja in razdelitve funkcionalnosti med dostopovni krmilnik in dostopovno točko, ki jih uporablja protokol CAPWAP, so podrobneje opisani v razdelku 3.3.1. Slika 3.3 prikazuje končni avtomat protokola CAPWAP.



Slika 3.3: Končni avtomat protokola CAPWAP.

Poglavje 4

Izvedba vključitve lahkih dostopovnih točk v Eduroam

Kot smo predstavili v prejšnjih poglavjih, se je v zadnjih letih zaradi zanesljivosti hitrosti in priročnosti brezžičnih omrežij povečala tudi njihova popularnost. Uporaba velikih brezžičnih omrežij pa je izpostavila težave pri nadzoru in upravljanju le-teh. Z istimi težavami se srečujejo večje organizacije (npr. univerze, fakultete, inštituti in šolski centri), pridružene v konfederacijo Eduroam.

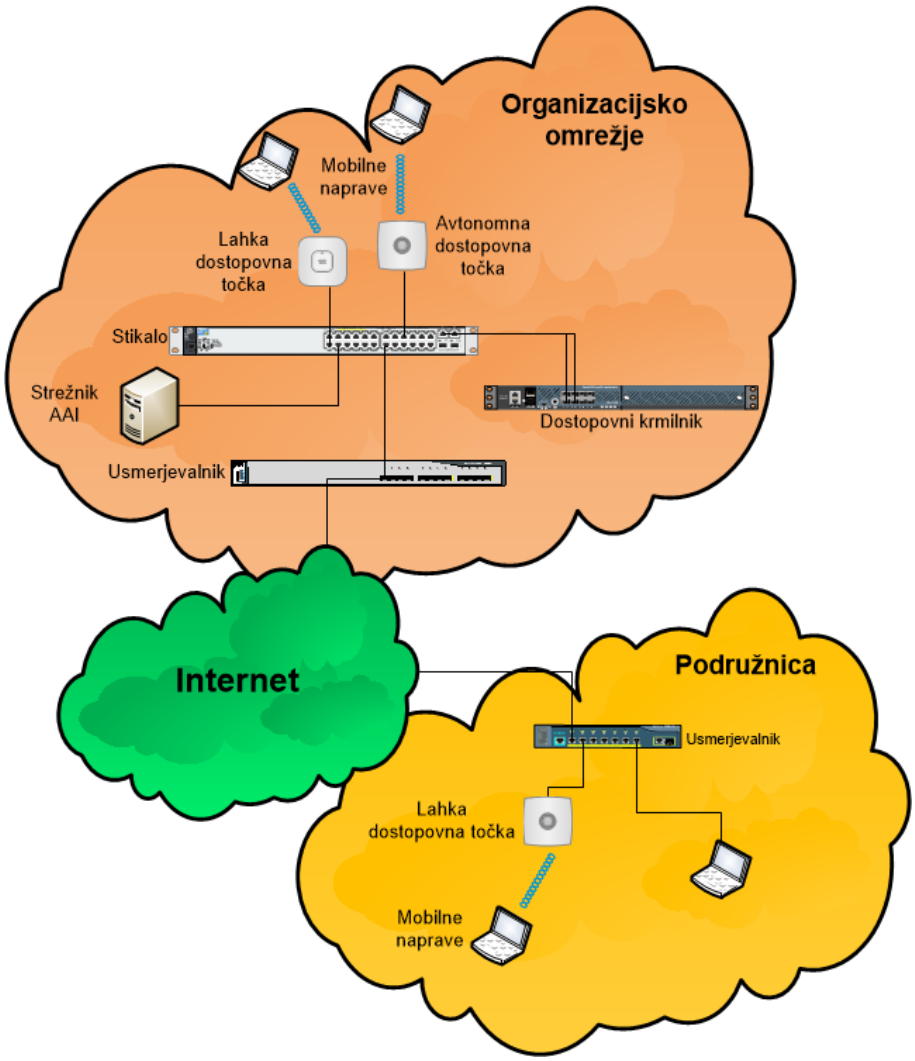
Kot možno rešitev težave smo v poglavju 3 izpostavili centralizirano omrežno infrastrukturo. V tem poglavju bomo z uporabo opreme za centralno upravljanje brezžičnih omrežij poiskali različne rešitve, ki bodo povečale enostavnost upravljanja brezžičnega omrežja Eduroam. Zasnovali bomo preizkusni poligon - maketo omrežja Eduroam. V njem bomo poskusili poenostaviti upravljanje in zagotoviti čim večjo varnost uporabnikov. V rešitvi bomo uporabili oba internetna protokola, trenutno aktualni IPv6 in stari IPv4.

4.1 Zasnova preizkusnega poligona

Poligon bo sestavljen iz dveh delov, brezžičnega omrežja znotraj organizacijskih prostorov in brezžičnega omrežja na oddaljeni lokaciji. S takšno situacijo se srečujejo različne organizacije vključene v Eduroam. S to zasnovo bomo lahko preizkusili vpliv na upravljanje, če organizacija deluje na večih lokacijah (npr. šola in več podružnic) ali pa če je omrežje razdeljeno med večimi zgradbami (npr. študentski domovi). Takšno porazdeljeno omrežje je težje dobro vzdrževati, saj se običajno, zaradi pomanjkanja človeških ali finančnih virov, tehnična ekipa, ki skrbi za upravljanje omrežja, nahaja na centralni lokaciji.

Na preizkusnem poligonu bomo preizkusili uporabo centralizirane brezžične arhitekture v centralnih organizacijskih prostorih in njen vpliv na enostavnost upravljanja ter varnost uporabnikov. Preučili bomo poenostavitev pogostega prilagajanja nastavitev dostopovnih točk ob različnih priložnostih ter poskusili centralizirati upravljanje dostopovnih točk v organizacijskih podružnicah. Izvedli bomo penetracijske teste in primerjali centralizirano infrastrukturo z avtonomno. Raziskali bomo tudi, kakšne možnosti za uporabo Edruoama v nestrukturiranih omrežjih in delo od doma prinaša takšna infrastruktura.

Slika 4.1 prikazuje topologijo preizkusnega poligona. V razdelku 4.2 so podrobneje predstavljeni sestavni deli preizkusnega poligona in njegova topologija na 2. nivoju modela ISO/OSI. Prikazuje jo slika 4.2.



Slika 4.1: Topologija preizkusnega poligona.

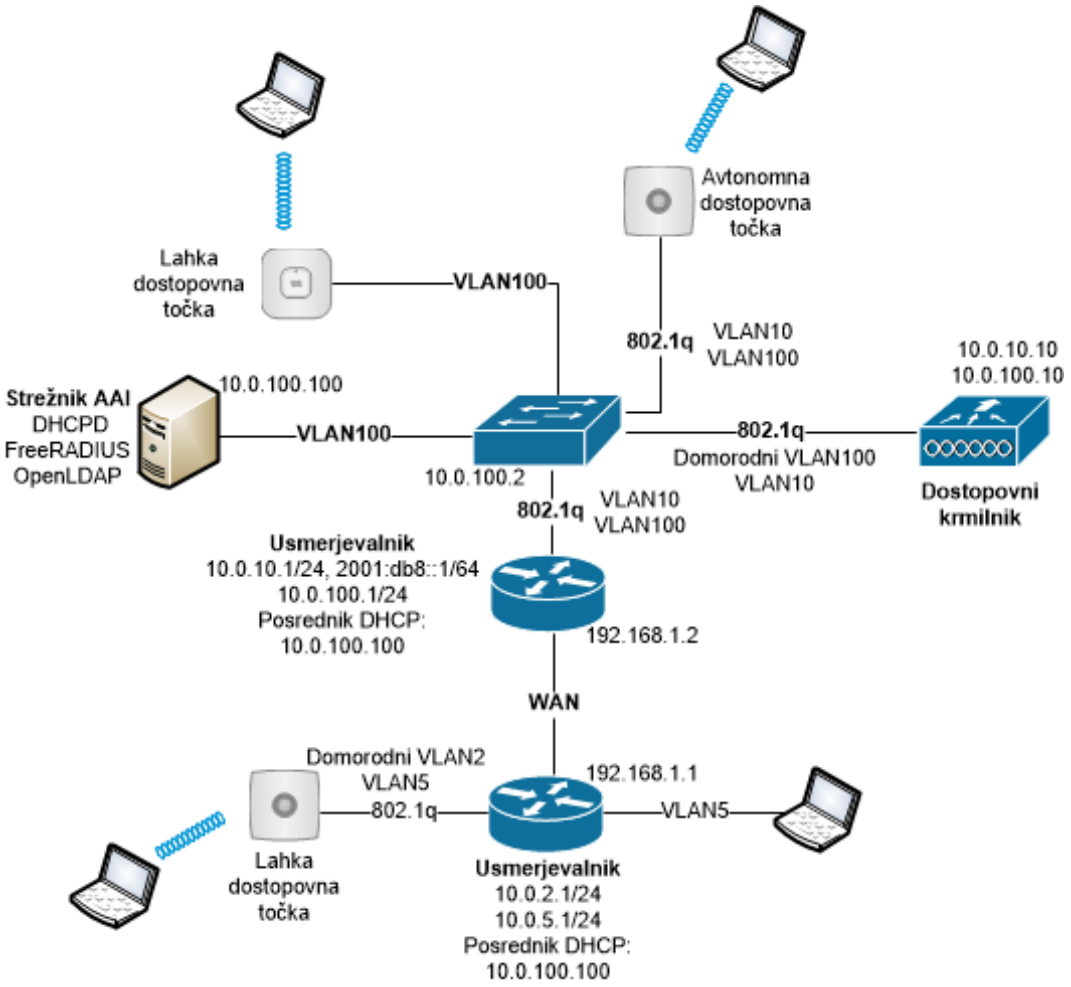
4.2 Postavitev preizkusnega poligona

4.2.1 Organizacijsko omrežje

V delu preizkusnega omrežja, ki se nahaja v glavni organizacijski zgradbi, je za usmerjanje prometa uporabiljeno stikalo L3 Cisco WS-C3750G-12S s programsko opremo verzije 12.2(55)SE1. Na njem je bilo potrebno aktivirati sistemsko sliko c3750-ipservicesk9-mz.122-55.SE1.bin, ki omogoča usmerjanje prometa in podpira oba internetna protokola, IPv4 in IPv6. Usmerjevalnik skrbi za usmerjanje v podomrežjih, ki se na njem zaključujejo, ter za povezavo prek interneta z oddaljeno podružnico. Podomrežji, ki smo ju nastavili sta:

- Upravljalsko podomrežje - VLAN 100 - 10.0.100.0/24;
- Uporabniško podomrežje - VLAN 10 - 10.0.10.0/24, 2001:db8::/64.

Usmerjevalnik služi tudi kot posrednik zahtevkov DHCP med uporabniškim omrežjem in strežnikom DHCP, ki se nahaja v upravljalskem omrežju. Na usmerjevalnik je povezano stikalo HP ProCurve 2610 s programsko opremo verzije R.11.72. Med stikalom in usmerjevalnikom smo speljali snop VLANov 802.1Q. V snopu sta VLAN-a 10 in 100. Kot je prikazano na sliki, 4.2 so nanj priključene vse naprave v centralnem organizacijskem omrežju. To sta obe dostopovni točki, strežnik AAI ter preizkusni računalniki. Slika 4.2 prikazuje topologijo preizkusnega poligona na povezavnem nivoju modela ISO/OSI.



Slika 4.2: Topologija preizkusnega poligona na 2. nivoju modela ISO/OSI.

4.2.2 Strežnik AAI

Za avtentikacijo uporabnikov in dodeljevanje številk IP v omrežjih smo uporabili virtualni strežnik, ki temelji na operacijskem sistemu Linux, distribucije CentOS6. Za dodeljevanje številk IP je skrbel servis ISC DHCP 4.2.4-P1. Avtentikacijo uporabnikov in obračunavanje prometa smo izvajali z uporabo strežnika FreeRADIUS 2.1.12. Na virtualnem strežniku je tekel tudi imenik OpenLDAP, v katerem so bili shranjeni uporabniški podatki za prijavo. Posebnost pri celotni konfiguraciji je uporaba lastniških razširitev DHCP . Dostopovne točke so dostopovni krmilnik poiskale s pomočjo podatkov pridobljenih v odgovoru DHCP. Spodnji izsek prikazuje nastavitev (*ang. Option 43*) za upravljalsko omrežje.

```
...
option space Cisco_CAPWAP;
option Cisco_CAPWAP.server-address code 241 = array of ip-address;
...
#Upravljalsko omrežje
shared-network "vlan100" {
    option Cisco_CAPWAP.server-address 10.0.100.10;
    ...
}
...
```

4.2.3 Dostopovne točke

Uporabili smo dostopovne točke proizvajalca Cisco, in sicer eno tipa AIR-AP1142N in dve tipa AIR-AP1131AG. Dostopovnim točkam je bilo pred uporabo potrebno zamenjati sistemsko sliko. Z zamenjavo avtonomne dostopovne točke pretvorimo v lahke. Z uporabo sledečega zaporedja ukazov novo sistemsko sliko prenesemo iz strežnika TFTP. Strežnik je v našem primeru tekel na računalniku z operacijskim sistemom Fedora 17.

```
ap(config)#interface bvi 1
ap(config-if)#ip address 10.0.0.2 255.255.255.0
ap#archive download-sw /overwrite /reload
tftp://10.0.0.1/c1140-rcvk9w8-tar.124-21a.JA2.tar
```

Obe dostopovni točki, ki smo ju pretvorili iz avtonomnih v lahki, podpirata oba načina podprta v protokolu CAPWAP. Razdeljeni MAC in lokalni MAC. Proizvajalec dostopovne točke v načinu lokalni MAC imenuje (*ang. Cisco FlexConnect, OfficeExtend*). Pretvorbo med različnimi načini je mogoče izvesti z ustrezno nastavitvijo na dostopovnem krmilniku. Na eni dostopovni točki smo ohranili avtonomno sistemsko sliko. Potrebovali jo bomo kot primerjavo v preizkusih.

4.2.4 Dostopovni krmilnik

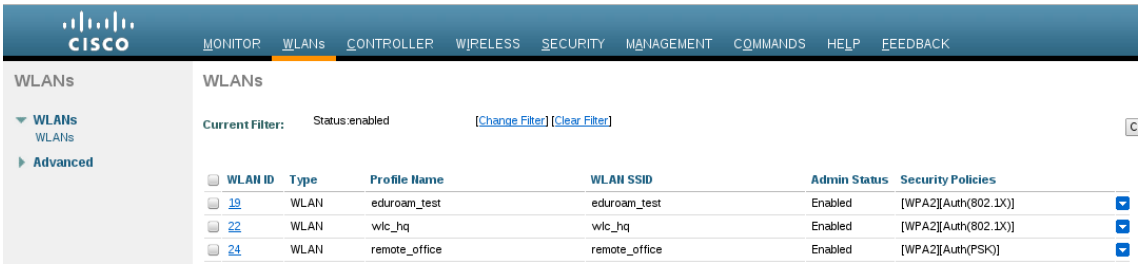
Dostopovni krmilnik je (*ang. Cisco Wireless Lan Controller (WLC) 5508*) s programsko opremo verzije 7.2.103.0 [4]. Med stikalom in dostopovnim krmilnikom smo speljali snop VLANov 802.1Q. Upravljalsko omrežje, v katerega je povezan dostopovni krmilnik, mora biti nastavljeno kot domorodni VLAN (802.1q).

V centralizirani omrežni arhitekturi dostopovni krmilnik služi kot overitelj v procesu 802.1x. V omrežju Eduroam se kot avtentikacijski strežnik uporablja RADIUS, zato smo na krmilniku nastavili strežnike RADIUS, ki skrbijo za avtenticiranje uporabnikov in obračunavanje prometnih podatkov.

Dostopovni krmilnik omogoča nastavitev več strežnikov RADIUS za zagotavljanje redundance.

Poleg tega dostopovni krmilnik v vseh omrežjih, v katerih so uporabniki, potrebuje vmesnik s številko IP. V avtonomni omrežni infrastrukturi je praksa, da ima dostopovna točka številko IP le v upravljalskem podomrežju. Takšna zahteva na krmilniku je posledica tega, da služi kot posrednik zahtevkov DHCP za uporabnike. Vmesnike lahko tudi združimo v skupine, kar omogoča, da je isto brezžično omrežje (*ang. WLAN*) pripeto na skupino vmesnikov. S tem dosežemo, da uporabniki istega brezžičnega omrežja lahko pridobijo naslov IP iz različnih podomrežij. Med podomrežji lahko izbiramo ciklično ali z uporabo direktive AAA v RADIUS Access-Accept paketu.

Vsa brezžična omrežja, ki jih bodo oglaševale dostopovne točke definiramo na enem mestu. Za posameznega nastavimo ime omrežja (*ang. SSID*), varnostne parametre in iz predhodno definiranih izberemo strežnike RADIUS. Posamezeno brezžično omrežje je nato potrebno pripeti vmesniku ali skupini vmesnikov. Slika 4.3 prikazuje brezžična omrežja, ki smo jih uporabili v preizkusnem poligonu. Wlc_hq se oddaja na centralni lokaciji, remote_office je lokalno usmerjano omrežje v podružnici, omrežje eduroam_test pa se oddaja na obeh lokacijah.



Slika 4.3: Brezžična omrežja nastavljena na dostopovnem krmilniku.

Dostopovne točke nato združujemo v skupine, kjer določimo, katera brezžična omrežja bo oglaševala katera izmed skupin. Posamezne skupine imajo lahko enako brezžično omrežje pripeto različnemu vmesniku oziroma skupini vmesnikov. To omogoča fleksibilnost pri vmeščanju uporabnikov v omrežje in porazdelitev bremena. Tako lahko dostopovne točke uporabnike istega brezžičnega omrežja v zgradbi A urvščajo v VLAN A, v zgradbi B pa jih dostopovne točke uvrščajo v VLAN B.

Dostopovne točke ob prvi pridružitvi padejo v privzeto skupino dostopovnih točk (*ang. default-group*), ki oglašuje brezžična omrežja z enoličnim identifikatorjem (ID) do vključno 16. Brezžičnih omrežij s takšnim identifikatorjem iz privzete skupine ni mogoče odstraniti. Med preizkušanjem funkcionalnosti se je izkazalo, da je lahko takšno delovanje nezaželjeno, saj je smiselno dobro definirati omrežno politiko in dostopovne točke dodajati v predefinirane skupine. Rešitev je, da je enolični identifikator brezžičnih omrežij, ki jih ustvarimo vedno večji od 16, brezžična omrežja pa ročno dodajamo skupinam dostopovnih točk. Privzeta skupina je služi kot čakalna vrsta za novo pridružene dostopovne točke.

Dostopovne točke so na brezžični opremi, ki smo jo uporabili v preizkusu, podpirale dve razdelitvi funkcionalnosti MAC, lokalni MAC in razdeljeni MAC. Pri razdeljenem MAC-u je ves uporabniški promet tuneliran do dostopovnega krmilnika. Proizvajalec dostopovno točko v takem načinu imenuje (*ang. local*). V načinu lokalni MAC (proizvajalec ga imenuje Flex-Connect) dostopovne točke omogočajo hibridno delovanje, promet določenih brezžičnih omrežij lahko tunelirajo do dostopovnega krmilnika, del pa lahko odlagajo na lokalno omrežje, na katerega so priključene. Tu se pojavi razlika v preprostosti konfiguracije med tipoma. (*Local*) dostopovna točka si preprosto prenese konfiguracijo, ki pripada skupini, v katero je vmeščena. Na stikalu, kamor je dostopovna točka priključena, ji le omogočimo dostop v podomrežje za dostopovne točke. Za pričetek delovanja potrebujejo s strani administratorja zelo malo pozornosti, kar je dobra lastnost, kadar je takšnih dostopovnih točk veliko. Vsaka dostopovna točka (*Flex-connect*) pa potrebuje ročno nastavi-

tev, v katero podomrežje bo uvrščala uporabnike brezžičnih omrežij, katerih promet odlaga na lokalno omrežje. To zahteva od administratorja poznavanje omrežja na oddaljeni lokaciji. Čeprav dostopovna točka (*Flex-connect*) uporabniški promet odlaga na oddaljeni lokaciji, mora biti na dostopovnem krmilniku vsakemu brezžičnemu omrežju, ki ga oglašuje, pripet vmesnik. Izkazalo se je, da je najbolje, če za ta namen ustvarimo "dummy vmesnik". To je vmesnik v podomrežju, ki na centralni lokaciji ne obstaja. Poimenovali smo ga črna luknja (*ang. blackhole*). Če takšnega omrežja ne bi bilo, bi bil ves promet v primeru napačne konfiguracije privzeto speljan v upravljalsko omrežje, v katerem se nahaja dostopovni krmilnik.

Privzeto je z uporabo DTLS [16] zaščiten le kontrolni promet med dostopovnimi točkami in krmilnikom. Za zagotavljanje večje varnosti je dobro vključiti tudi šifriranje podatkovnega prometa. Spodaj je prikazan ukaz, s katerim smo na dostopovnem krmilniku to vključili za vse pridružene dostopovne točke.

```
config ap link-encryption enable all
```

4.2.5 Omrežje podružnice

Omrežje oddaljene podružnice se v drugem podomrežju, s čimer simuliramo povezavo prek interneta (*ang. WAN*). Za vzpostavitev podružničnega omrežja pa smo kot preprost usmerjevalnik uporabili Cisco C2960G, ki z aktivacijo sistemske slike lanbase-routing omogoča osnovno usmerjanje paketov med podomrežji in nastavitev statičnih omrežnih poti. Stikalo služi kot usmerjevalnik za uporabniško in upravljalsko omrežje v oddaljeni podružnici.

- Upravljalsko podomrežje - VLAN 2 - 10.0.2.0/24,
- Uporabniško podomrežje - VLAN 5 - 10.0.5.0/24,

Usmerjevalnik omogoča tudi povezavo z centralnim organizacijskim omrežjem. Za ta namen ima vpisano statično pot, ki je prikazana spodaj. Deluje tudi kot posrednik zahtevkov DHCP. Posreduje jih strežniku DHCP, ki se nahaja v oblaku, na centralni lokaciji.

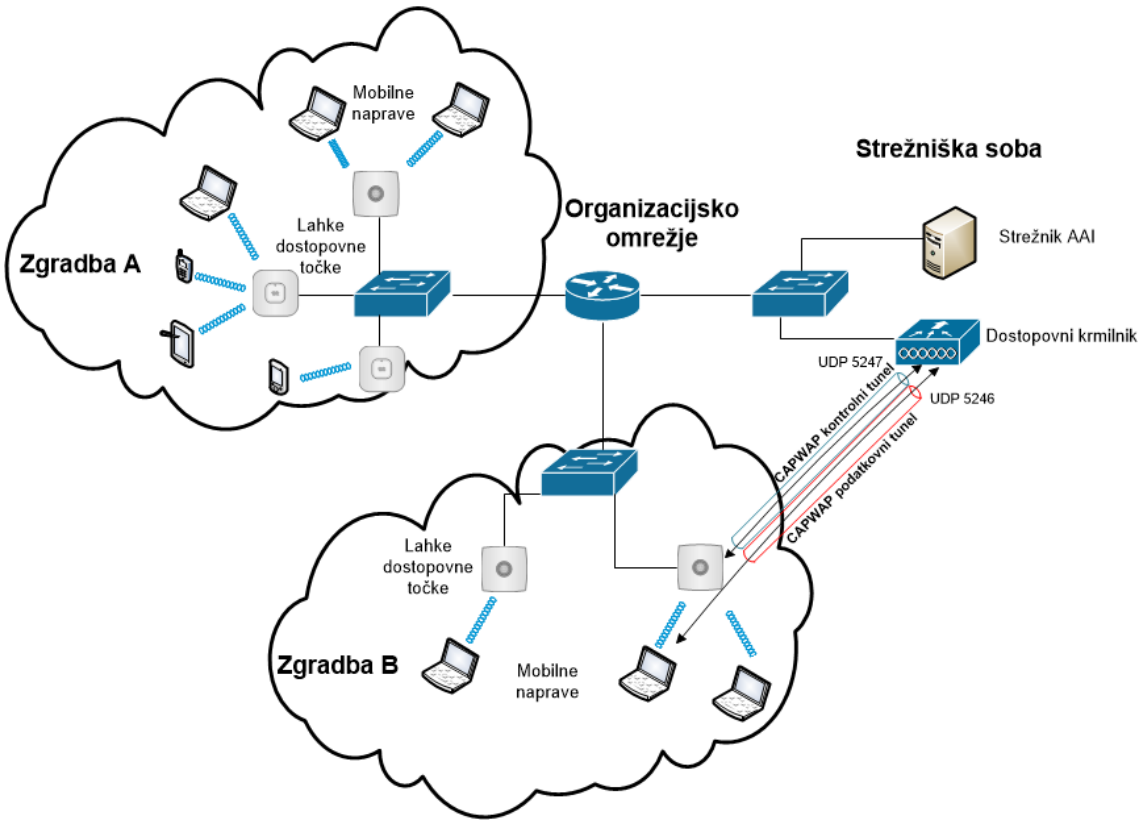
```
ip route 0.0.0.0 0.0.0.0 192.168.1.2
```

Nanj je priključena lahka dostopovna točka. Uporablja sistemsko sliko, ki uporablja razdelitev lokalni MAC. Na njej bomo preizkusili upravljanje iz centralne lokacije.

4.3 Uporabnost centralizirane brezžične infrastrukture

Preizkus dostopovnega krmilnika je pokazal, da je ena izmed glavnih prednosti konfiguracija vseh dostopovnih točk na enem mestu. Na dostopovnem krmilniku so nastavljena tako vsa brezžična omrežja, ki jih oglašujejo dostopovne točke, kot tudi vsi strežniki RADIUS, ki skrbijo za avtentikacijo uporabnikov. Ker pri uporabi lahkih dostopovnih točk kot overitelj v avtentikacijskem procesu 802.1x nastopa dostopovni krmilnik, nam strežnika RADIUS ni potrebno seznanjati z vsako dostopovno točko posebej, kot je to potrebno pri uporabi avtonomnih dostopovnih točk. Avtentikacijski strežnik (RADIUS) in overitelj za zaščito komunikacije uporabljata vnaprej izmenjano skrivnost. Z RADIUS-om seznanimo le dostopovni krmilnik.

Na dostopovnem krmilniku predhodno ustvarimo skupine dostopovnih točk, v katere, glede na organizacijsko politiko in namen delovanja, razvrstimo dostopovne točke. Dostopovne točke oglašujejo brezžična omrežja, ki so pripeta skupini, v katero spadajo. Delitev dostopovnih točk omogoča tudi, da različne skupine oglašujejo isto brezžično omrežje in obenem uporabnike uvrščajo v različa podomrežja (VLAN). Posamezna skupina lahko uporabnike določenega brezžičnega omrežja uvršča tudi v več različnih podomrežij, če je brezžično omrežje pripeto na skupino omrežnih vmesnikov. Oboje omogoča fleksibilnost pri načrtovanju omrežja. Slika 4.4 prikazuje centralizirano organizacijsko omrežje, ki se razteza čez dve zgradbi. Eduroam omrežje se lahko tako oddaja v obeh zgradbah, uporabniki pa so v različnih podomrežjih glede na zgradbo, v kateri se nahajajo. Takšna uporaba lahkih dostopovnih točk, s tuneliranjem uporabniškega prometa prek dostopovnega krmilnika, je mogoča na fakultetah ali v študentskih domovih. Z uporabo različnih podomrežij lahko uporabnike poljubno delimo med seboj in zmanjšamo kolizijsko domeno (*ang. broadcast domain*).

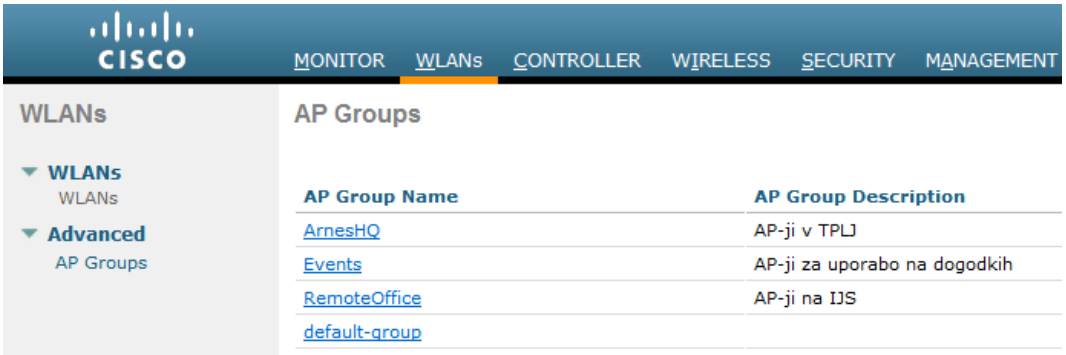


Slika 4.4: Organizacijsko omrežje pri uporabi lahkih dostopovnih točk.

Lažje in učinkovitejše je tudi upravljanje z radijskim delom dostopovnih točk. Avtonomnim dostopovnim točkam radijske kanale v 2.4 GHz frekvenčnem spektru običajno določamo na podlagi strokovnega ogleda območja, kjer se bo dostopovna točka nahajala. Izbira kanala lahko postane zelo zapletena v primeru področja, kjer je veliko sosednjih dostopovnih točk in druge interference. Na področjih, kjer je veliko uporabnikov, se za porazdelitev bremena postavi veliko dostopovnih točk. To lahko privede do fenomena blokirane celice (*ang. blocked cell*) [8]. Gre za dostopovno točko, ki se znajde med dvema dostopovnima točkama na ortogonalnih kanalih, ki se med seboj ne slišita. Blokirana dostopovna točka zaradi interferenc in uporabe CSMA/CA ves čas zaznava brezžični medij kot zaseden. V avtonomnih omrežjih se težavo rešuje s prilagajanjem izhodnih moči na dostopovnih točkah in spre-

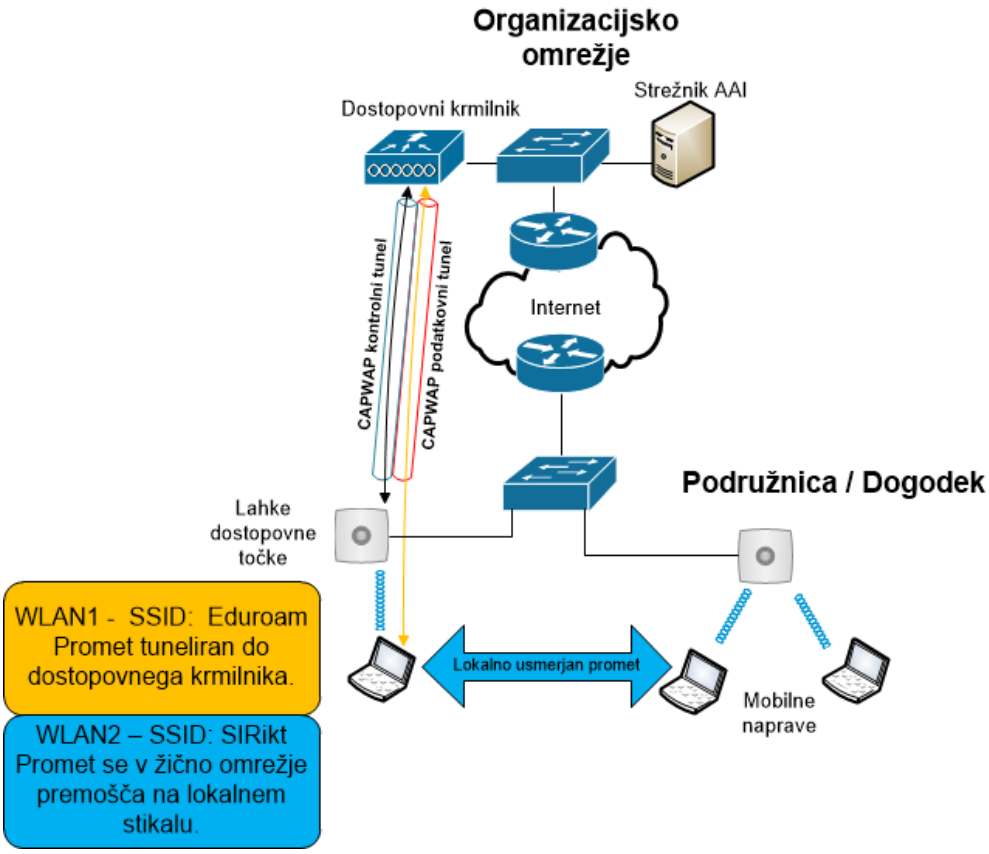
minjanjem kanalov na dostopovnih točka, kar pa je lahko ob velikem številu dostopovnih točk zahtevna naloga. V centraliziranem omrežju vse dostopovne točke pošiljajo podatke o moči signala in o razmerju signal-šum, kar dostopovnemu krmilniku omogoči izračun in prilagoditev nastavitev radijskega dela na področju celotnega omrežja.

Dodajanje novih dostopovnih točk v omrežje se prav tako poenostavi. Ker imamo vso konfiguracijo v naprej pripravljeno, je dostopovne točke ob prvi pridružitvi potrebno le uvrstiti v ustrezno skupino dostopovnih točk. V naprej pripravljene skupine smo preizkusili za primer Arnes-a, ki večkrat letno organizira različne konference in srečanja, kot so Sirikt, IPv6 Summit in različna izobraževanja. Ob takšnih priložnostih je potrebno določeno število dostopovnih točk prenastaviti za uporabo na dogodku. Dostopovne točke se pred dogodkom le priključi na krmilnik in se jim spremeni namembnost s spremembo skupine. Dostopovne točke prenesejo novo konfiguracijo in po ponovnem zagonu so pripravljene na delovanje. V primeru da je zaradi velikega števila uporabnikov dostopovnih točk premalo, lahko dodatne kapacitete zagotovimo zelo hitro. Slika 4.5 prikazuje nastavitev skupin na dostopovnem krmilniku.



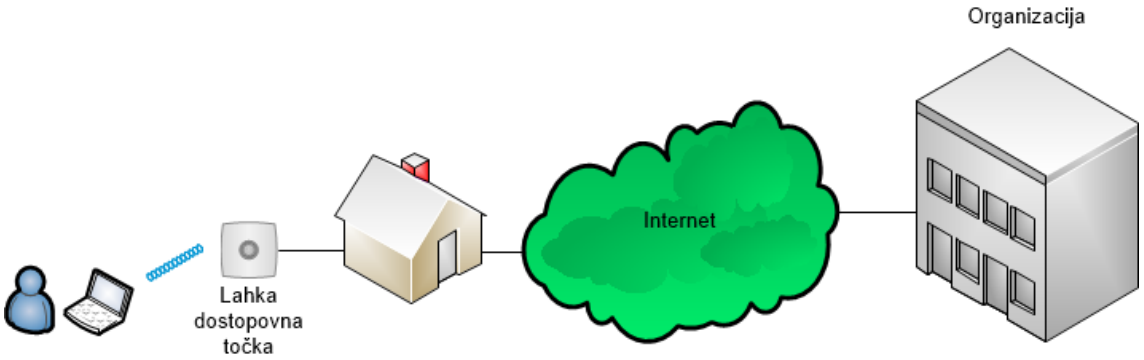
Slika 4.5: Skupine dostopovnih točk.

Dostopovne točke, ki smo jih preizkusili podpirajo dve različni razdelitvi funkcionalnosti MAC, lokalni MAC in razdeljeni MAC. Preobrazba dostopovne točke je mogoča z uporabo krmilnika. V obeh primerih so dostopovne točke upravljane s strani dostopovnega krmilnika. Razdelitev localni MAC (proizvajalec jo imenuje Flex-connect) na dostopovnih točkah omogoča poleg centralnega tuneliranja prometa tudi lokalno odlaganje prometa. Lokalno odlaganje pomeni, da promet odloži na omrežje, na katerega je priključena. Med centralnim tuneliranjem in lokalnim odlaganjem lahko izbiramo na ravni posameznega brezžičnega omrežja, ki ga dostopovna točka oglašuje. Takšen način je uporaben predvsem za upravljanje oddaljenih dostopovnih točk v podružnicah ali uporabo na dogodkih in ob priložnostih, kjer je potrebna pokritost z brezžičnim omrežjem. Slabost tuneliranja vsega prometa do dostopovnega krmilnika je namreč, da zahteva dobro povezavo med oddaljeno lokacijo in dostopovnim krmilnikom. V primeru optične povezave s tem ni težav, na počasnejših povezavah pa lahko pride do preobremenitve lokalne povezave v svet (internet). Najpočasnejša hitrost, ki še omogoča uporabo je 128kbps. Težava je lahko tudi velika zakasnitev, ali trpetanje zakasnitve. Flex-connect dostopovna točka omogoča nudenje storitev tudi, če izgubi povezavo z dostopovnim krmilnikom. Slika 4.6 prikazuje uporabo centralizirane brezžične arhitekture za podporo dogodkom in uporabo v oddaljenih podružnicah. Uporabljeni sta dve brezžični omrežji. Eno uporablja tuneliranje prometa v centralno organizacijsko omrežje, drugo pa lokalno usmerjanje.



Slika 4.6: Upravljanje omrežij za dogodke ali omrežij v podružnicah.

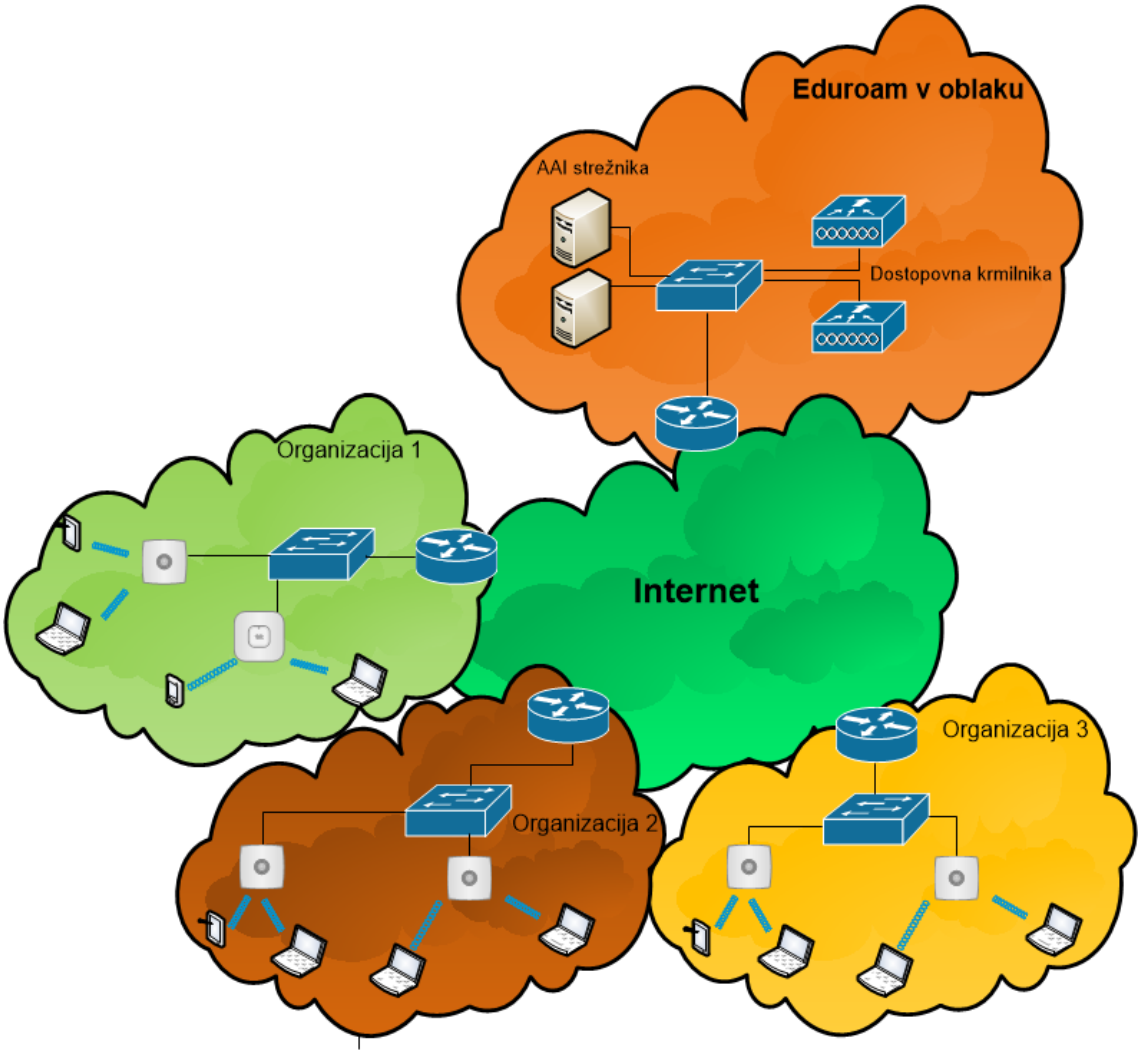
Med preizkusom smo preizkusili tudi možnosti, ki jih infrastruktura ponuja za uporabo Eduroama v nestrukturiranih omrežjih in delo od doma. Dostopovno točko smo do preizkusnega poligona povezali iz omrežja slovenskega komercialnega ponudnika internetnih storitev. Topologija preizkusa prikazuje slika 4.7. Proizvajalec način imenuje (*ang. Office Extend*), gre za nekoliko nadgrajeno verzijo programske opreme, prilagojeno posebej za ta namen. Način omogoča priklop dostopovne točke tudi v omrežju izven domače organizacije. Omrežju, v katerem izvedemo priklop, ni potrebno biti strukturirano na podomrežja. Edina zahteva je, da dostopovna točka pridobi številko IP, kar ji omogoči komunikacijo z dostopovnim krmilnikom. Kontrolni in podatkovni promet šifriramo v tunelu CAPWAP z uporabo DTLS in ga centralno usmerjamo, kar omogoča največjo varnost. V primeru Eduroam omrežja bi bila takšna uporaba primerna ob priložnostih, pri katerih je potreba po pokritju z brezžičnim signalom, a na mestu priklopa ni namenske infrastrukture, omrežje samo pa ni strukturirano na podomrežja. V primeru da zaposlenim s tem omogočimo delo od doma in dostop do omejenih virov v našem omrežju, je potrebno zagotoviti dobro avtentikacijo. Dobra izbira je na tem mestu uporaba močne avtentikacije, kot je 802.1x z avtentikacijskim strežnikom na centralni lokaciji.



Slika 4.7: Prikaz preizkusa uporabe Eduroama v nestrukturiranih omrežjih.

Ena od idej, preizkušenih na preizkusnem poligonu, je tudi možnost Eduroama v oblaku. Pred pridružitvijo v sistem gostovanja Eduroam morajo organizacije pri sebi vzpostaviti brezžično in avtentikacijsko infrastrukturo. S to infrastrukturo omogočijo uporabo brezžičnega omrežja Eduroam svojim in gostujočim uporabnikom. Za manjše organizacije je vzpostavitev takšne infrastrukture težka naloga, saj zato nimajo usposobljenega osebja. To jih lahko odvrne od vzpostavitve. Edina altenrativa za izvedbo je najem in plačilo zunanjih izvajalcev. Eduroam v oblaku bi vključeval vso avtentikacijsko infrastrukturo z imenikom uporabnikov, strežnik DHCP, za dodeljevanje naslovov IP in upravljanje z brezžičnim omrežjem. Izkazalo se je, da je konfiguracija lahkih dostopovnih točk s centralnim tuneliranjem na preizkusni opremi dovolj preprosta, da bi bila uporabna ob velikem številu gostujočih ogranizacij. Posameznih dostopovnih točk namreč ni potrebno dodatno nastavljati, dovolj je, da so pridružene ustrezni skupini dostopovnih točk in da je stikalo, na katerega so v organizaciji priključene skonfigurirano, tako da lahko pridobijo številko IP. V primeru gostovanja zaradi hitrosti prenosa in obremenitve organizacijske povezave v internet centralno tuneliranje vsega prometa ni dobra izbira. Slabost je prenos vse komunikacije prek dostopovnega krmilnika, tudi tiste, ki bi jo lahko opravili lokalno. V trenutni verziji programske opreme dostopovnega krmilnika (verzija 7.2) izbira, kateri promet je tuneliran in kateri ni, še ni mogoča. Zato smo preizkusili tudi možnost lokalnega usmerjanja prometa z dostopovnimi točkami v načinu (*ang. Cisco FlexConnect*), ki pa je na preizkusni opremi (Cisco WLC 5508) pokazala nekaj slabosti. Vsaka dostopovna točka ob konfiguriranju zahteva več pozornosti, kar je ob velikem številu dostopovnih točk nezaželjeno. Konfiguracija takšne točke je opisana v razdelku 4.2.4. Pomislek pri produkcijski implementaciji storitve na preizkusni opremi je tudi cena. Podprto število dostopovnih točk na krmilniku, ki smo ga preizkušali, je odvisno od kupljene licence, za zagotavljanje redundance pa bi morala biti krmilnika vsaj dva.

Slika 4.8 prikazuje dostopovna omrežja organizacij, katerih omrežje Eduroam je centralno upravljano.



Slika 4.8: Eduroam v oblaku.

4.4 Varnostni vidiki

V razdelku 3.2 smo predstavili najpogostejše nevarnosti, ki pretijo brezžičnim in žičnim omrežjem v organizacijah. V tem razdelku bomo opisali ugotovitve, pridobljene na podlagi preizkusne varnosti centralizirane brezžične infrastrukture. Penetracijske teste smo izvajali z uporabo Backtrack Linux-a 5 R3. Backtrack je distribucija Linux-a, ki omogoča penetracijske teste računalniških omrežij. Za primerjavo smo jih vedno izvedli tudi na avtonomni brezžični infrastrukturi oziroma na dostopovnih točkah vrste Flex-connect, ki so prav tako upravljane s strani dostopovnega krmilnika, a promet odlagajo na lokalno omrežje, v katerega so priključene (lokalni MAC). Dostopovne točke, ki uporabljajo takšno delitev funkcionalnosti MAC si varnostne lastnosti namreč delijo z običajnimi avtonomnimi dostopovnimi točkami, saj uporabniškega prometa ne tunelirajo do dostopovnega krmilnika, na katerem se nahajajo varnostni mehanizmi. Predstavili bomo tudi mehanizme za obrambo pred napadi, ki smo jih uporabili.

4.4.1 Vmestitev lahkih dostopovnih točk v omrežje

Lahke dostopovne točke, ki uporabniški promet tunelirajo preko dostopovnega krmilnika je najbolje vmesti v posebno omrežje (VLAN), ločeno od ostalih naprav v upravljalskem omrežju. Ker z dostopovnim krmilnikom komunicirajo le prek dveh vrat UDP, 5246 za kontrolni in 5247 za podatkovni promet, je lahko omrežje, v katerem se nahajajo povsem omejeno. Da jim omogočimo tudi pridružitev na dostopovni krmilnik, jim moramo omogočiti še dostop do strežnika DHCP in pošiljanje poizvedb DNS. S tem omrežje zaščitimo pred morebitnimi zlorabami. Ker se dostopovne točke običajno nahajajo na javnih mestih, bi lahko napadalci žično povezavo, na katero je priključena dostopovna točka, izkoristili za dostop v organizacijsko omrežje. To priporočilo pa se nanaša le na lahke dostopovne točke, ki uporabniški promet tunelirajo preko dostopovnegag krmilnika (razdeljeni MAC). Dostopovne točke, ki uporabljajo lokalni MAC pa se v omrežje vmesti na enak

način kot običajne avtonomne. Tudi pri uporabi avtonomnih dostopovnih točk je omrežje priporočljivo zaščititi s filtri, glede na politiko organizacije.

4.4.2 Zlonamerne dostopovne točke

Dostopovni krmilnik omogoča nadzor zračnega prostora v organizaciji in okolici. Dostopovne točke določen čas svojega delovanja, brez vpliva na uporabniško izkušnjo, namenijo zaznavanju potencialnih zlonamernih dostopovnih točk v in izven organizacije. Zaznati je mogoče tudi, če se dostopovne točke nahajajo v žičnem omrežju organizacije. Slika 4.9 prikazuje zaznane dostopovne točke v okolici preizkusnega omrežja. Če dostopovne točke spoznamo kot zlonamerne, lahko aktivno blokiramo njihovo delovanje. Dostopovni krmilnik lahko uporabi svoje dostopovne točke za pošiljanje deavtentikacijskih upravljalskih okvirjev napravam, ki so povezane na zlonamerno dostopovno točko. Vklop avtomatične blokade ni priporočen, saj so lahko zaznane tudi dostopovne točke drugih podjetij in organizacij. Ob takšni konfiguraciji bi jim onemogočili dostop do omrežja. Pred blokiranjem dostopovnih točk, ki jih sistem zazna, se je zato potrebno dobro prepričati, da so resnično zlonamerne.

Rogue APs

MAC Address	SSID	Channel	# Detecting Radios
00:10:7f:13:1d:37	Unknown	1	1
00:1e:c1:2e:b2:80	AudaxGuestWLAN	8	0
00:1f:d0:1d:70:33	Inkubattor	6	2
10:8c:cf:5e:86:a1	eduroam	36	2
84:c9:b2:6b:de:61	Centradesign	1	1
f8:d1:11:25:6d:ec	open.wlan-si.net	8	2

Slika 4.9: Zaznavanje zlonamernih dostopovnih točk.

Spodaj je prikazan izsek dnevniške datoteke dostopovnega krmilnika, ko

smo na Backtrack Linux-u zagnali skripto airbase-ng in vzpostavili zlobno dvojčico resnične Eduroam dostopovne točke. Takšne dostopovne točke so še posebej nevarne v primeru "HOTSPOT"omrežij, v katerih se pogosto ne uporablja šifriranja. Eduroam omrežje uporablja močno šifriranje 802.11i in avtentikacijo 802.1x, ki omogoča obojestransko preverjanje pristnosti, zato je možnost takšnega napada manjša. Do asociacije in avtentikacije na zlonamerno dostopovno točko, ki oglašuje omrežje Eduroam, lahko pride le v primeru, da odjemalec nima vključenega preverjanja strežniškega certifikata. Brez preverbe zaupa vsem strežnikom. Kot avtentikacijski strežnik za izvedbo zlorabe je mogoče uporabiti FreeRADIUS-WPE (*ang. Wireless Pwnage Edition*), ki je priložen Backtrack Linux-u.

```
Sat Sep 8 19:20:42 2012 Impersonation of AP with Base Radio MAC
10:8c:cf:39:d2:d0 using source address of 10:8c:cf:39:d2:d0
has been detected by the AP with MAC Address: 10:8c:cf:39:d2:d0
on its 802.11b/g radio whose slot ID is 0
```

Običajne avtonomne točke, uporabljene v večini slovenskih Eduroam omrežij, funkcionalnosti zaznavanja zlonamernih dostopovnih točk ne ponujajo.

4.4.3 Napadi na upravljalske okvirje

Z uporabo skripte aireplay-ng smo preizkusili, da lahko zloraba upravljalskih okvirjev omrežnim administratorjem povzroči velike preglavice. Mogoče je izvesti napad z onemogočanjem storitve (*ang. Denial of service attack*) in onemogočiti uporabnikom dostop do omrežja. Uporabili smo deavtentikacijski napad (*ang. deauth attack*). Podobni napadi na upravljalske okvirje so še napad z deasociacijo uporabnikov, avtentikacijski ali asociacijski napad in neveljavni probe odgovori (*ang. probe response*). Napasti je mogoče tudi kontrolne okvirje CTS/RTS.

Novejše dostopovne točke, tako avtonomne kot lahke, podpirajo zaščito uporabniških upravljalskih okvirjev (*ang. Management frame protection,*

IEEE 802.11w). Ti so pomembni predvsem za zaščito asociacije, avtentikacije, disasociacije in deavtentikacije. Okvirji so odjemalcem vedno posredovani v unicast obliki. Okvirji vsebujejo MIC (*ang. message integrity code*), ki odjemalcem omogoča, da prepoznajo veljavno dostopovno točko. MIC je zaščiten z začasnim šifrirnim ključem, tako kot ostala komunikacija ščitena s standardom 802.11i, ki smo ga podrobneje opisali v razdelku 2.2.1. Šifrirni ključ si z dostopovno točko izmenjajo v 4-kratnem rokovanju ob avtenitkaciji. Če odjemalec okvirjev ne more dešifrirati, jih zavrže. Prav tako tudi dostopovna, če prejme zahtevek za deavtentikacijo ali deasociacijo odjemalca, odjemalcu pošlje kriptirano poizvedbo. V kolikor od odjemalca dobi veljaven odgovor, prejeto zahtevo ignorira. V primeru centralizirane infrastrukture dostopovne točke nepravilnosti sporočijo krmilniku. Na končnih napravah je zaščita upravljalskih okvirjev podprta šele v verzijah CCXv5 [22] in višjih. Vse naprave, ki smo jih imeli v testnem okolju na voljo za preizkus, so bile največ verzije CCXv4. Za združljivost je bilo zato potrebno za posamezno brezžično omrežje nastaviti, da je uporaba zaščite upravljalskih okvirjev izbirna (*ang. optional*), sicer se nekompatibilne naprave na omrežje niso mogle povezati.

4.4.4 Zlonamerni strežnik DHCP

Napadi DHCP na brezžičnem omrežju so lahko izhodišče za napad moža v sredini (*ang. Man in the middle attack*) ali pa je njihov namen le napad z onemogočanjem storitve, ki s porabo vseh naslovov IP na strežniku DHCP onemogoči delovanje omrežja. Pri uporabi avtonomnih dostopovnih točk zahtevki DHCP, ki jih pošilja uporabnik, preplavijo podomrežje, v katerem se nahaja. Običajno se strežnik DHCP nahaja v drugem podomrežju, zato jih stikalo, ki služi kot posrednik, v unicast obliki posreduje do strežnika DHCP.

Preizkusili smo delovanje zlonamernega uporabnika, ki z uporabo skripte dhcpstarv porabi vse možne številke IP. Takšno delovanje je možno v nezaščitenem avtonomnem omrežju, saj dostopovne točke ne primerjajo izvornega

naslova MAC z naslovom CHADDR v zahtevku DHCP. Pomembno je, da dostopovne točke same zavržejo pakete iz naslovov MAC, ki nimajo veljavne asociacije. Torej poplavljanje z neveljavnimi naslovi MAC ni mogoče. S tem odpade tudi veliko skript za izvajanje napada, saj se poslužujejo ravno te tehnike. Kot zaščito smo na stikalu, na katerega je povezana dostopovna točka, uporabili mehanizem DHCP snooping, ki izvaja preverbo izvornega naslova MAC in naslova CHADDR v zahtevku DHCP. Spodaj je prikazan primer konfiguracije na stikalu HP ProCurve 2610.

```
switch1#(config)# no dhcp snooping information option 82
switch1#(config)# dhcp-snooping vlan 10
switch1#(config)# interface 13,24 dhcp-snooping trust
switch1#(config)# dhcp-snooping
```

Dostopovni krmilnik za ves promet, ki je tuneliran iz dostopovnih točk, izvaja pregled paketov DHCP. Vsebino paketov primerja s tabelo veljavnih asociacij za dostopovne točke pod svojim nadzorom. Vse neveljavne pakete odvrže. Spodaj je prikazan primer zavrženih paketov DHCP ob poskusu napada na centralizirani infrastrukturi. MSCB (*ang. Mobile Station Control Block*) je baza veljavnih naprav, ki imajo asociacije na dostopovnih točkah.

```
*DHCP Socket Task: 00:16:36:8d:06:09 DHCP dropping packet
(no mscb) found - (giaddr 0.0.0.0,
pktInfo->srcPort 68, op: 'BOOTREQUEST')
```

Na testnem poligonu smo preizkusili tudi zlonamerni strežnik DHCP, ki se nahaja na brezžičnem omrežju z ostalimi odjemalci (uporabniki). Na avtonomni omrežni infrastrukturi zaščite pred takšnim strežnikom ni. Čeprav uporaba DHCP snoopinga omogoča zaščito na drugih dostopovnih točkah v ESS, lahko zlonamerni strežnik DHCP brez težav dodeli naslov uporabniku, ki ima asociacijo na isti dostopovni točki. Takšni paketi namreč ne potujejo čez stikalo, ki izvaja DHCP snooping. Tak uporabnik nima veljavnega vnosa v DHCP snooping tabeli in zato stikalo njegove pakete odvrže, je pa možna zloraba za promet, ki ne potuje prek stikala.

Takšen napad na dostopovnem krmilniku ni mogoč, saj dostopovni krmilnik deluje kot posrednik zahtevkov DHCP za uporabnike. Paketov DHCP nikoli ne posreduje nazaj v brezžično omrežje, iz katerega jih je prejel. Poleg tega dovoljuje iz brezžičnih omrežij pošiljanje le zahtevkov DHCP, ostale pakete pa zavrže. V preizkusu se je pokazalo, da zlonamerni strežnik DHCP res ne prejme nobenega zahtevka, saj so bili vsi iz dostopovnega krmilnika posredovani na distribucijski sistem, kar je razvidno tudi iz dnevniške datoteke.

```
*DHCP Socket Task: 00:1d:e0:0a:fc:d3
DHCP successfully bridged packet to DS
```

4.4.5 Napad mož v sredini

Z uporabo zastrupljanja tabel arp lahko napadalec uporabniški promet v brezžičnem omrežju spelje preko svoje naprave. Promet lahko zajema in analizira, izvaja napad SSL strip ali pa ga aktivno spreminja. Z uporabo ettercap-a smo se postavili v vlogo napadalca. Brez ustreznih zaščit na stikalu, na katerega je priključena avtonomna dostopovna točka, je napad uspel brez težav. Slika 4.10 prikazuje prvotno in zastrupljeno tabelo arp na žrtvinem računalniku.

```
C:\Users\blaz>arp -a

Interface: 10.0.10.105 --- 0xd
  Internet Address      Physical Address      Type
  10.0.10.1             00-16-46-39-24-c2     dynamic
  10.0.10.255           ff-ff-ff-ff-ff-ff     static
C:\Users\blaz>arp -a

Interface: 10.0.10.105 --- 0xd
  Internet Address      Physical Address      Type
  10.0.10.1             00-1d-e0-0a-fc-d3     dynamic
  10.0.10.108           00-1d-e0-0a-fc-d3     dynamic
```

Slika 4.10: Zastrupljena tabela arp.

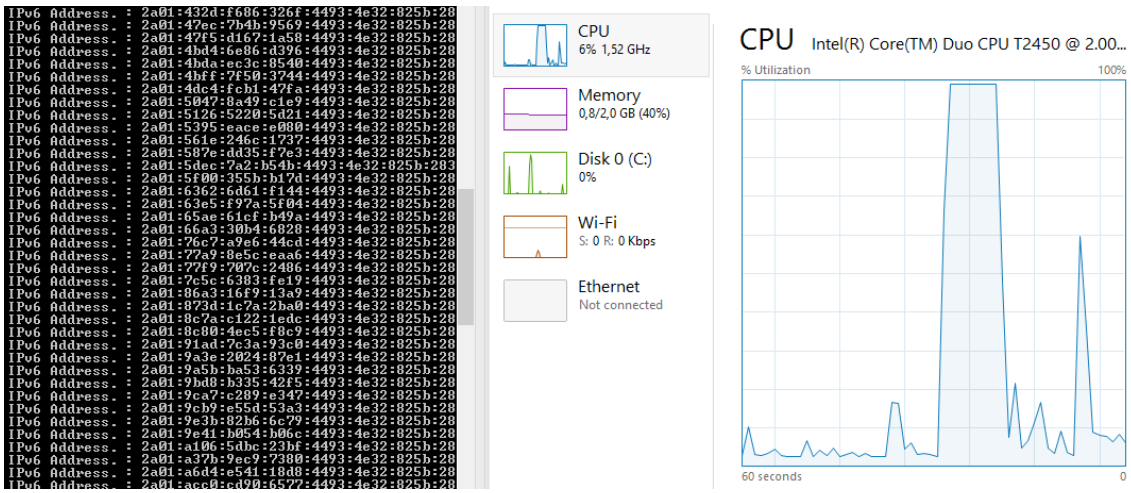
Zaščita pred takšnim napadom v avtonomnih omrežjih je mogoča z uporabo Arp inšpekcije (*ang. Arp inspection*), ki na podlagi statičnih vnosov in tabele, zgrajene z uporabo DHCP snoopinga, preverja zahtevke arp. Odvisno od nastavitev se lahko ob zaznani nepravilnosti vmesnik, na katerega je priključena dostopovna točka, izključi. Spodaj je prikazana nastavitev mehanizma na stikalu HP ProCurve 2610.

```
switch1#(config)# arp-protect vlan 10
switch1#(config)# arp-protect trust 13,24
switch1#(config)# arp-protect validate src-mac
switch1#(config)# arp-protect validate dest-mac
switch1#(config)# arp-protect validate ip
switch1#(config)# arp-protect
```

Dostopovni krmilnik izvaja arp inšpekcijo. Pregleduje zahtevke arp in jih primerja z bazo, ki jo ustvari z uspešnimi asociacijami. Dostopovni krmilnik služi kot posrednik paketov arp in ne dovoljuje pošiljanja le-teh med napravami na brezžičnem omrežju. Neveljavni paketi in paketi garp (*ang. Gratious Arp*) so zavrženi. S tem preprečuje arp zastrupljanje in posledično napade z možem v sredini. Isti napad z ettercapom je bil na lahkih dostopovnih točkah neuspešen.

4.4.6 Varnost IPv6

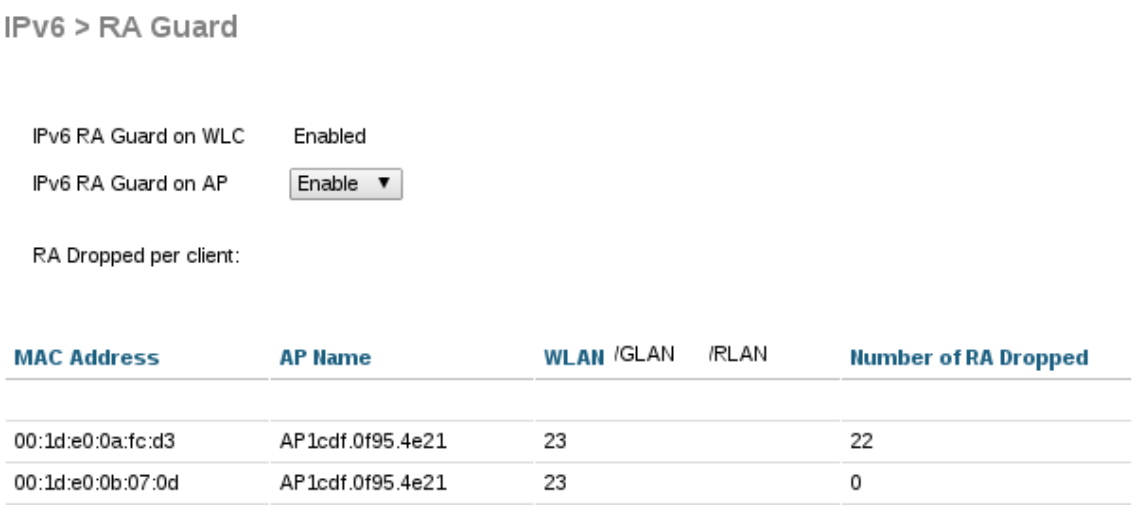
Za napadalce je zanimiv tudi trenutno aktualni internetni protokol IPv6. Zanj na večini trenutne omrežne opreme, uporabljene v Eduroam omrežjih v Sloveniji, primankujejo varnostni mehanizmi za protokol IPv6, kot sta na primer DHCP snooping in Arp inšpekcija v IPv4. Naše preizkusno omrežje je delovalo kot dvojni-sklad (*ang. dual-stack*). Na njem smo preizkusili napade na IPv6 omrežje [21]. Primer takšnega napada je, ko se uporabnik na omrežju lažno oglašuje kot usmerjevalnik. Brezžična oprema za centralizirano upravljanje omrežja, ki smo jo preizkusili, ima vgrajen mehanizem RA Guard, ki uporabnikom na brezžičnem omrežju dopušča le pošiljanje paketov, ki so končnim napravam v internetnem protokolu IPv6 dovoljeni. To jim prepreči, da bi se lažnivo predstavljali kot usmerjevalnik. Spodnja slika 4.11 prikazuje žrtev poplavljanja z lažnivimi usmerjevalniškimi oglasi (*ang. Rouge RA flood*).



Slika 4.11: Žrtvina mobilna naprava med poplavo lažnih IPv6 usmerjevalniških oglasov (*ang. Router Advertisment*).

Žrtev si zaradi privzeto uporabljenega mehanizma SLAAC glede na prejet RA nastavi globalni unicast naslov. V primeru poplave lažnih paketov RA si jih nastavi veliko, kar močno obremeni žrtvino mobilno napravo. Posledično ji

to prepreči dostop do omrežja (napad z onemogočanjem storitve). Slika 4.12 prikazuje števec zlonamernih RA paketov, ki jim je pot v omrežje preprečil RA Guard na dostopovnem krmilniku. Podobni mehanizmi za preprečevanje napadov so vgrajeni tudi v dragih stikalih, na katere lahko priključimo avtonomne dostopovne točke. Druga možnost je uporaba brezplačnih orodij, kot so NDPMon, 6mon, Arpwatch. Ta brezplačna orodja omogočajo le obveščanje o zlorabah, ne pa tudi preprečevanja napadov. Možna rešitev je tudi omejevanje prenosa paketa ICMP tipa 134 (Router Advertismet) iz določenih vmesnikov na stikalu, npr. iz omrežja, v katerem so uporabniki. S tem lahko zavarujemo uporabnike drugih dostopovnih točk, ki spadajo v isti ESS.



Slika 4.12: Mehanizem RA Guard na dostopovnem krmilniku in odvrženi lažni usmerjevalniški oglasi (*ang. Router Advertisment*).

4.5 Vrednotenje rezultatov

V tem poglavju smo na maketi brezžičnega omrežja Eduroam preizkusili centralizirano brezžično infrastrukturo. Preizkusili smo oba načina razdelitev funkcionalnosti MAC, ki jih podpirajo lahke dostopovne točke (lokalni MAC in razdeljeni MAC). V razdelku 4.3 smo predstavili možnosti uporabe centralizirane infrastrukture, v razdelku 4.4 pa smo na podlagi preizkusov opisali razlike v varnostnih vidikih lahkih in avtonomnih dostopovnih točk.

Preizkusi so pokazali, da lahke dostopovne točke, z uporabo razdelitve funkcionalnosti MAC - imenovane razdeljeni MAC, omogočajo enostavnejšo postavitev kompleksnih brezžičnih omrežij v organizacijah (npr. študentskih domovih, kampusih, fakultetah), ki potrebujejo veliko dostopovnih točk. Zaradi večje procesne moči dostopovni krmilniki vsebujejo varnostne mehanizme, ki so sicer prisotni na stikalih, na katera so priključene avtonomne dostopovne točke. Dostopovni krmilnik omogoča zagotavljanje večje varnosti, saj s pregledovanjem uporabniškega prometa preprečuje zlonamerno delovanje uporabnikov. Preprečuje tudi, da bi se uporabniki nelegalno predstavljali kot deli omrežne infrastrukture (npr. usmerjevalnik, strežnik DHCP, ipd.). Prednost varnostnih mehanizmov na dostopovnem krmilniku je tudi, da omogočajo pregled vsega prometa lahkih dostopovnih točk. V omrežjih z avtonomnimi dostopovnimi točkami lahko del zlonamernega prometa stikala, na katerem se izvajajo varnostni mehanizmi, ne doseže, zato ga posledično ni mogoče zaznati. Slabosti centralizirane infrastrukture z lahkimi dostopovnimi točkami so potencialna ozka grla, ki jih predstavljajo dostopovni krmilniki. Krmilnik, ki smo ga preizkusili lahko upravlja do 500 dostopovnih točk. Med dostopovnimi krmilniki in lahkimi dostopovnimi točkami mora biti zato speljano zanesljivo in zmogljivo žično omrežje. Za zagotavljanje redundance in porazdeljevanje bremena, ki ga predstavlja centralno tuneliranje prometa, morata biti dostopovna krmilnika vsaj dva. To močno poveča ceno celotnega omrežja.

Razširitev uporabnosti prinašajo lahke dostopovne točke, ki uporabljajo razdelitev funkcionalnosti MAC - imenovano lokalni MAC. V razdelku 4.3

smo predlagali možnosti za njihovo uporabo v omrežjih Eduroam. Prednost prinaša odlaganje uporabniškega prometa na lokalno omrežje, saj tuneliranje vsega prometa prek krmilnika, v primeru ko se omrežje razprostira čez več organizacijskih podružnic, ni smiselno. Težavo lahko predstavljajo tako počasne internetne povezave (npr. ADSL) kot tudi visoka zakasnitev in trepetanje zakasnitve. Ob uporabi razdelitve lokalni MAC dostopovni krmilnik obdrži le kontrolno CAPWAP funkcionalnost. Prednost te razdelitve je, da dostopovne točke lahko nadaljujejo z delovanjem, čeprav izgubijo povezavo z dostopovnim krmilnikom. Slabost takšnih dostopovnih točk, upravljanih s strani dostopovnega krmilnika, je predvsem v varnosti. Vsi varnostni mehanizmi so namreč prisotni na dostopovnem krmilniku. Varnost v takšnem omrežju je zato potrebno zagotoviti na stikalih, na katera so dostopovne točke priključene, tako kot v običajnih avtonomnih brezžičnih omrežjih.

Trenutno skoraj vsi izdelovalci brezžične opreme za centralno upravljanje podpirajo oba načina, podprta v protoklu CAPWAP. Centralno usmerjanje, z uporabo razdeljenega MAC-a, in odlaganje prometa na lokalno omrežje, z uporabo razdelitve lokalni MAC. Nekateri proizvajalci so razvili lastniške razširitve, s katerimi opuščajo dostopovni krmilnik in kontrolne CAPWAP funkcionalnosti porazdeljujejo med dostopovne točke. Upravljanje je tako mogoče prek upravljalskega strežnika. S tem želijo zmanjšati ceno brezžične opreme in obdržati vse funkcije, ki jih prinaša dostopovni krmilnik (upravljanje radijskega dela, upravljanje nastavitev, itd.).

Poglavje 5

Sklepne ugotovitve

V diplomskem delu smo spoznali brezžična omrežja, njihovo arhitekturo in sestavne dele. Predstavili smo omrežje Eduroam in težave upravljanja velikih brezžičnih omrežij Kot rešitev težave z upravljanjem velikih Eduroam omrežij smo predstavili centralizirano omrežno infrastrukturo in njene sestavne dele. Kot protokol, ki omogoča centralizirano upravljanje in oskrbo dostopovnih točko, smo izbrali protokol CAPWAP, saj ni lastniški kot njegovi ekvivalenti, ampak je standardiziran s strani IETF. Postavili smo preizkusni poligon - maketo omrežja Eduroam, v katerem smo uporabili lahke in avtonomne dostopovne točke. Lahke dostopovne točke smo upravljali z dostopovnim krmilnikom, preizkusili smo oba načina razdelitev funkcionalnosti MAC, ki jih podpirajo lahke dostopovne točke (lokalni MAC in razdeljeni MAC). Na preizkusnem poligonu smo ocenili in predstavili možnosti uporabe centralizirane brezžične infrastrukture za primer omrežja Eduroam. S penetracijskimi testi smo preverili spremembe v varnosnem vidiku in jih primerjali z običajnim avtonomnim Eduroam omrežjem. V razdelku 4.5 smo dodatno ovrednotili izsledke in podali mnenje o uporabnosti.

Arnes za raziskovalne in izobraževalne organizacije ureja dostopovna omrežja. Svetuje jim tudi pri implementaciji omrežja Eduroam ob njihovi pridružitvi. S priporočili za uporabo centralizirane brezžične infrastrukture in ocenami različnih možnosti uporabe, ki so bile predstavljene v tem diplom-

skem delu, bo mogoče večjim organizacijam svetovati tudi ob izbiri centralizirane infrastrukture. Podobno kot za avtonomne dostopovne točke bo na podlagi rešitev predstavljenih v diplomskem delu mogoče pripraviti navodila in priporočila za uporabo dostopovnega krmilnika tipa Cisco WLC z lahkimi dostopovnimi točkami.

Arnesovo brezžično omrežje Eduroam in omrežje za goste bo do konca leta prešlo na centralizirano brezžično infrastrukturo. Infrastruktura bo služila tudi za podporo dogodkom in delavnicam. Ugotovitve v diplomskem delu bodo koristile pri vzpostavitvi in zagotavljanju največje varnosti, ter uporabnosti produkcijskega omrežja.

Izhodišče za nadaljni razvoj Eduroama v Sloveniji je dodatna raziskava in preizkus možnosti gostovanja omrežja Eduroam v oblaku. Gostovanje Eduroam v oblaku bi omogočilo lažjo pridružitev manjših organizacij v mednarodni sistem gostovanja. Za pripravo ustreznega okolja bo potrebno dodatno raziskati možnosti razširitve funkcionalnosti na preizkušenem dostopovnem krmilniku (Cisco WLC 5508), ter preučiti delovanje brezžične opreme drugih proizvajalcev. Možnost je tudi izdelava lastne odprtokodne razširtive. Ta razširitev bi, kateremu od odprtokodnih operacijskih sistemov za dostopovne točke (npr. OpenWRT), dodala zmožnost delovanja s protokolom CAPWAP in komuniciranja z dostopovnim krmilnikom ali upravljalskim strežnikom.

Slike

Literatura

[1] J. Edney, W. A. Arbaugh. "Real 802.11 Security: Wi-Fi protected access and 802.11i". Boston: Addison-Wesley, Pearson Education, 2004

[2] F. Ohrtman, K. Roeder. "Wi-Fi HANDBOOK". ZDA: McGraw-Hill, pogl. 1-4, 2003

[3] M. S. Gast. "802.11 Wireless Networks, The Definitive Guide". Sebastopol, CA: O'Reilly Media, 2002

[4] Cisco Systems Inc. "Cisco Unified Wireless Networking". San Jose, CA: Cisco Systems Inc, 2011

[5] Arnes (2012) *Omrežje Eduroam*. Dostopno na: http://aai.arnes.si/eduroam

[6] M. Milinović, S. Winter (2012) *Eduroam Service Definition*. Dostopno na: http://www.eduroam.org/downloads/docs/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf

[7] T. C. Clancy (oktober, 2008) *Secure handover in Enterprise WLANS: CAPWAP, HOKEY, and IEEE 802.11R*. Wireless Communications, IEEE. Dostopno na: http://ieeexplore.ieee.org/Xplore/guesthome.jsp

[8] A. Levanti, F. Giordano, I. Tinnirello (november, 2007) *A CAPWAP-Compliant Solution for Radio Resource Management in Large-Scale*

802.11 WLAN. Wireless Communications, IEEE. Dostopno na: http://ieeexplore.ieee.org/Xplore/guesthome.jsp

[9] B. O'Hara, P. Calhoun, Airspace, J. Kempf, Docomo Labs USA (2005) *Configuration and Provisioning for Wireless Access Points (CAPWAP) Problem Statement*. Dostopno na: http://tools.ietf.org/html/rfc3990

[10] G. Conradi (2010) *Current Status and Overview of the CAPWAP Protocol*. Dostopno na: http://www.cse.wustl.edu/ jain/cse574-10/ftp/capwap/index.html

[11] T. Sridhar (2005) *Wireless LAN Switches — Functions and Deployment*. Dostopno na: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-3/wireless_lan_switches.html

[12] L. Yang, Intel Corp, P. Zerfos, UCLA, E. Sadot, Avaya (2005) *RFC 4118 - Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)*. Dostopno na: http://tools.ietf.org/html/rfc4118#page-3

[13] D. Loher, Envysion Inc., D. Nelson, Enterasys Networks Inc., O.volinsky, Colubris Networks Inc., B. Sarikaya, Huawei USA (2006) *RFC 4565 - Evaluation of Candidate Control and Provisioning of Wireless Access Points (CAPWAP) Protocols*. Dostopno na: http://grenache.tools.ietf.org/html/rfc4565

[14] P. Calhoun, Cisco Systems, M. Montemurro, Research in Motion, D. Stanley, Aruba Networks (2009) *RFC 5415 - Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification*. Dostopno na: http://www.ietf.org/rfc/rfc5415.txt

[15] P. Calhoun, Cisco Systems, M. Montemurro, Research in Motion, D. Stanley, Aruba Networks (2009) *RFC 5416 - Control and Provisioning of*

Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11. Dostopno na: http://tools.ietf.org/html/rfc5416

[16] E. Rescorla, RTFM Inc., Stanford University (2006) *RFC 4347 - Datagram Transport Layer Security.* Dostopno na: http://tools.ietf.org/html/rfc4347

[17] (2011) *Cisco Adaptive wIPS Enhanced Local Mode (ELM) Configuration and Deployment Guide.* Dostopno na: http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b82504.shtml#attacks

[18] (2012) *Extensible Authentication Protocol.* Dostopno na: http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP-TTLS

[19] (2012) *RADIUS.* Dostopno na: http://en.wikipedia.org/wiki/RADIUS

[20] (2012) *IEEE 802.11.* Dostopno na: http://en.wikipedia.org/wiki/IEEE_802.11

[21] Van Hauser (2005) *Attacking the IPv6 Protocol Suite.* Dostopno na: http://pacsec.jp/psj05/psj05-vanhauser-en.pdf

[22] (2011) *Cisco CCX Versions and Features.* Dostopno na: http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html