

UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Jan Blatnik

Analiza brezžičnih usmerjevalnikov

DIPLOMSKO DELO

UNIVERZITETNI ŠTUDIJSKI PROGRAM
PRVE STOPNJE
RAČUNALNIŠTVO IN INFORMATIKA

MENTOR: prof. dr. Nikolaj Zimic

Ljubljana, 2017

COPYRIGHT. Rezultati diplomske naloge so intelektualna lastnina avtorja in Fakultete za računalništvo in informatiko Univerze v Ljubljani. Za objavo in koriščenje rezultatov diplomske naloge je potrebno pisno privoljenje avtorja, Fakultete za računalništvo in informatiko ter mentorja.

Besedilo je oblikovano z urejevalnikom besedil L^AT_EX.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo: Analiza brezžičnih usmerjevalnikov.

Tematika naloge:

WiFi omrežja so danes široko uporabna, tako v domačih, kot tudi v poslovnih ter industrijskih okoljih. Standard WiFi natančno opredeljuje delovanje protokola, ne opredeljuje pa primera delovanja več vstopnih točk na istem kanalu.

V diplomski nalogi preverite delovanje več vstopnih točk na istem kanalu oziroma frekvenci. Preverite potek dostopa do medija ter vpliv oddaljenost na tekmovanje med vstopnimi točkami.

Raziščite tudi, ali se vstopne točke različnih proizvajalcev enako obnašajo. Glede na tekmo med proizvajalci vstopnih točk lahko pričakujemo, da so lahko nekatere vstopne točke bolj agresivne pri dostopu do medija.

Iskreno se zahvaljujem mentorju prof. dr. Nikolaju Zimicu za izjemno odzivnost, potrpežljivost, nasvete in usmerjanje pri pisanju diplomskega dela. Posebna zahvala gre družini za neprestano podporo, spodbudo in potrpežljivost. Zahvalil bi se tudi prijateljem, ki so mi krajšali čas tekom študija.

Kazalo

Povzetek

Abstract

1	Uvod	1
1.1	Cilji	1
1.2	Razdelitev na poglavja	2
2	Brezžično omrežje	3
2.1	Prenos signala	4
2.2	Kanali	5
2.3	Zgodovina brezžičnega omrežja in IEEE 802.11 standardi	7
2.4	Arhitektura brezžičnega omrežja	8
2.5	Okvirji MAC	11
3	Način dostopa do medija	17
3.1	Dostop do medija pri 802.11	18
3.2	Distributed Coordination Function	20
3.3	Point Coordination Function	21
3.4	Hybrid Coordination Function	22
4	Načrtovanje meritev	23
4.1	Opis opreme	23
4.2	Priprava scenarijev	26
4.3	Opravljanje meritev	30

5	Rezultati in analiza meritev	33
5.1	Anomalije pri opravljanju meritev	34
5.2	Rezultati pri scenariju 1	36
5.3	Rezultati pri scenariju 2	37
5.4	Rezultati pri scenariju 3	39
5.5	Rezultati pri scenariju 4	41
6	Zaključek	45
	Literatura	49

Seznam uporabljenih kratic

kratica	angleško	slovensko
OSI	Open Systems Interconnection	povezani odprti sistemi
IEEE	Institute of Electrical and Electronics Engineers	Inštitut inženirjev elektrotehnike in elektronike
MAC	Media Access Control	kontrola dostopa do fizičnega medija
LLC	Logical Link Control	krmiljenje logične povezave
ISM	Industrial, Scientific and Medical band	frekvenčno območje za industrijsko, znanstveno in medicinsko uporabo
WEP	Wired Equivalent Privacy	zasebnost enaka žični
CCK	Complementary Code Keying	komplementarna kodna modulacija
OFDM	Orthogonal Frequency Division Multiplexing	ortogonalno frekvenčno multipleksiranje
MIMO	Multiple Input Multiple Output	več vhodov, več izhodov
IBSS	Independent Basic Service Set	neodvisni nabor osnovnih storitev
BSS	Basic Service Set	nabor osnovnih storitev
ESS	Extended Service Set	razširjeni nabor storitev
SSID	Service Set Identifier	identifikator nabora storitev
DS	Distribution System	distribucijski sistem

CSMA	Carrier Sense Multiple Access	večkratni dostop s prepoznavanjem nosilca
CSMA/CD	Carrier Sense Multiple Access / Collision Detection	večkratni dostop s prepoznavanjem nosilca in zaznavanjem trkov
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance	večkratni dostop s prepoznavanjem nosilca in izogibanjem trkov
FDMA	Frequency-Division Multiple Access	frekvenčno porazdeljeni sodostop
TDMA	Time-Division Multiple Access	časovno porazdeljeni sodostop
CDMA	Code-Division Multiple Access	multipleksiranje s kodnim deljenjem
SIFS	Short Interframe Space	kratek prostor med okvirji
DIFS	PCF Interframe Space	prostor med okvirji pri PCF
PIFS	DCF Interframe Space	prostor med okvirji pri DCF
CW	Contention Window	tekmovalno okno
DCF	Distributed Coordination Function	funkcija s porazdeljeno koordinacijo
PCF	Point Coordination Function	funkcija s točkovno koordinacijo
HCF	Hybrid Coordination Function	funkcija s hibridno koordinacijo
PC	Point Coordinator	točkovni koordinator
QoS	Quality of Service	kvaliteta storitve
RTS	Request to Send	zahteva za pošiljanje podatkov
CTS	Clear to Send	odobritev zahteve za pošiljanje podatkov
NAV	Network Allocation Vector	vektor dodelitve omrežja
CFP	Contention Free Period	obdobje brez tekmovanja za dostop do medija

CP	Contention Period	obdobje tekmovanja za dostop do medija
TCP	Transmission Control Protocol	protokol za nadzor prenosa
UDP	User Datagram Protocol	protokol za uporabniška sporočila
AP	Access Point	dostopna točka
STA	Station	postaja
VM	Virtual Machine	navidezni stroj
IP	Internet Protocol	internetni protokol

Povzetek

Naslov: Analiza brezžičnih usmerjevalnikov

Avtor: Jan Blatnik

V diplomskem delu z naslovom Analiza brezžičnih usmerjevalnikov je analizirano sočasno delovanje dveh dostopnih točk na istem kanalu. Najprej je opisano, kaj je brezžično omrežje in kako deluje. Opisani so najpomembnejši protokoli, okvirji, zgodovina standarda 802.11 in kako brezžična omrežja prenašajo signal. V tretjem poglavju so navedeni in opisani načini dostopa do medija, ki so pomembni za brezžična omrežja.

V praktičnem delu je najprej navedena uporabljena strojna in programska oprema. Opisani so scenariji, v katerih smo opravili meritve, in sam potek meritev. V petem poglavju pa so navedeni rezultati meritev in njihova razlaga.

Ugotovljeno je bilo, da s sočasnim delovanjem dostopni točki medsebojno vplivata druga na drugo tako, da zmanjšata hitrost prenosa podatkov. Enaki dostopni točki si ob enakih pogojih pasovno širino razdelita enakomerno. Pri različnih dostopnih točkah lahko ena prevlada in začne uporabljati večji del pasovne širine. Med dvema dostopnima točkama, ki se razlikujeta zgolj v razdalji od postaje, uporabi večji del pasovne širine tista, ki je bližje.

Ključne besede: brezžični usmerjevalnik, dostopna točka, kanal, brezžično omrežje, wifi, wlan, 802.11, analiza, primerjava.

Abstract

Title: Wireless Router Analysis

Author: Jan Blatnik

Concurrent activity of two access points on the same channel is analyzed in this thesis titled Analysis of Wireless Routers. First, wireless network and its workings are described. Most important protocols, frames, the history of 802.11 standard and signal transmissions in wireless networks are described. The third chapter illustrates the Media Access Control techniques which are essential for wireless networks. Used hardware and software are initially described in the practical part of the study. Then scenarios of measurements and their executions are detailed. The fifth chapter lists the results of measurements with explanations. It has been established that access points which are concurrently active mutually influence each other in the way that reduces their throughput. The same access points used under the same conditions share the bandwidth equally. When different access points are used, there is a possibility that one becomes dominant using a larger share of the bandwidth. If there is only the difference of distance to the station between the two access points, the larger share of the bandwidth is used by the one which is closer to the station.

Keywords: wireless router, analysis, access point, channel, wireless network, wifi, wlan, 802.11, comparison.

Poglavje 1

Uvod

Dandanes je dostop do interneta izrednega pomena. Vedno bolj razširjena uporaba pametnih telefonov, prenosnih računalnikov in podobnih prenosnih naprav zahteva, da je dostop brezžičen. Zaradi tega so brezžična omrežja danes zelo pogosta in jih lahko najdemo v lokalih, javnih institucijah, podjetjih, gospodinjstvih, letališčih, in drugih tako javnih kot zasebnih okoljih. Tako pogosta uporaba brezžičnih omrežij privede do tega, da se ta med seboj prekrivajo. Vsako brezžično omrežje sicer uporablja enega od predpisanih frekvenčnih pasov oziroma kanalov, vendar je velikokrat omrežij toliko, da se uporabljanju istega kanala ne moremo izogniti. Kakršnokoli sočasno oddajanje signalov z enako frekvenco pa pogosto povzroča motnje, saj pride do interference, kar pri brezžičnih omrežjih pomeni izgubo podatkov.

Glede na to, da se sočasnemu oddajanju dostopnih točk na enakem kanalu velikokrat ne moremo izogniti, bi radi preverili, kako omenjena situacija v praksi vpliva na uporabo brezžičnih omrežij.

1.1 Cilji

Cilj diplomskega dela je proučiti medsebojni vpliv brezžičnih usmerjevalnikov oziroma dostopnih točk, ki sočasno oddajajo v istem frekvenčnem območju. S pomočjo izvajanja meritev pri različnih scenarijih želimo preveriti, ali ome-

njeno sočasno oddajanje vpliva na prepustnost omrežij in pri kakšnih obremenitvah se pojavijo težave. Zanima nas, ali se dostopni točki dogovorita in razdelita dostop do medija ali vsaka oddaja ne glede na aktivnost druge dostopne točke. Poleg tega opazujemo tudi, kako na prepustnost vpliva moč signala, ki jo zaznajo postaje, in model usmerjevalnika (oziroma dostopne točke).

1.2 Razdelitev na poglavja

Diplomsko delo je razdeljeno na več poglavij. V drugem poglavju razložimo, kaj je brezžično omrežje in kako deluje. Opišemo najbolj pomembne protokole, kako brezžična omrežja prenašajo signal in kratko zgodovino standarda 802.11. Navedemo tudi vrste brezžičnih omrežij in opišemo, kako so sestavljena. Na koncu poglavja omenimo vrste podatkov oziroma okvirjev, ki se prenašajo po brezžičnih omrežjih.

V naslednjem poglavju se osredotočimo na načine dostopa do medija. Navedemo načine, ki se uporabljajo pri brezžičnih omrežjih in jih nato tudi opišemo.

Četrto poglavje služi načrtovanju meritev. V tem poglavju opišemo strojno in programsko opremo, ki jo uporabimo pri izvajanju meritev. Navedemo scenarije, pri katerih bomo opravljali meritve, in vsakega tudi bolj podrobno opišemo. Scenariji predstavljajo pogoste situacije pri uporabi brezžičnih omrežij v vsakdanjem življenju. Za tem navedemo meritve, ki jih bomo opravili, in opišemo, kako bomo te meritve izvedli.

Naslednje poglavje vsebuje rezultate meritev za vsakega od scenarijev in obrazložitev oziroma komentar dobljenih rezultatov.

Zadnje poglavje pa služi sklepnim ugotovitvam in komentarju celotne naloge.

Poglavje 2

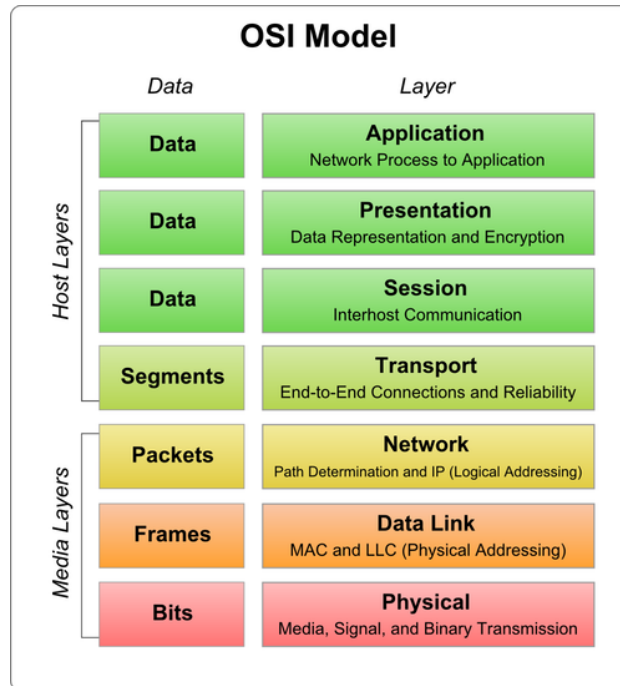
Brezžično omrežje

Brezžično omrežje 802.11 je računalniško omrežje, ki prenaša podatke s pomočjo radijskih valov. To nam omogoča, da lahko postaje komunicirajo, tudi če niso povezane s kablom. Delovanje omrežja 802.11 je zaradi prenosa podatkov z radijskimi valovi in pogostih motenj zapleteno. Zato sta pri 802.11 protokolih najbolj pomembni spodnji dve plasti modela OSI (*Open Systems Interconnection*) [11, 21] (glej sliko 2.1):

- fizična plast (angl. *physical layer*) – je zadolžena za prenos bitov po komunikacijskem kanalu [18]
- povezovalna plast (angl. *data link layer*) – je zadolžena za povezavo dveh naprav in zanesljiv prenos okvirjev [18]

Standard 802.11, ki definira brezžična lokalna omrežja, je del družine IEEE 802. Ta predstavlja specifikacije za tehnologije, ki se nanašajo na lokalna omrežja (glej sliko 2.2). IEEE 802 razdeli povezovalno plast še na dva dela) [11]:

- *Media Access Control* (MAC) – nadzoruje dostop do medija in pošiljanje podatkov [11]
- *Logical Link Control* (LLC) – skrbi za logično povezavo med napravami, ki med seboj komunicirajo [18]

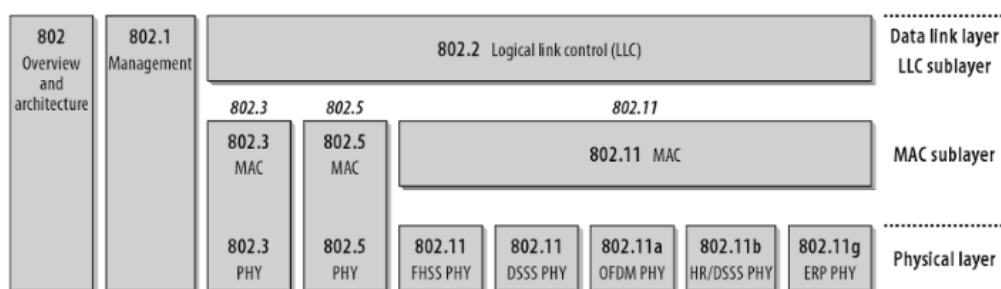


Slika 2.1: OSI model [18].

Ker je LLC enak za celoten IEEE 802, mora pri 802.11 MAC zapleteno delovanje brezžičnega omrežja predstaviti nivoju LLC, kot navadno lokalno omrežje. Zato MAC, poleg tradicionalnih zadolžitev, obravnava tudi mobilnost postaj. [13]

2.1 Prenos signala

Za brezžični prenos signala lahko uporabimo zvok, svetlobo, elektromagnetno indukcijo in radijske valove. Najbolj pogosto brezžično prenašamo signal s pomočjo radijskih valov. Nekatero bolj znane naprave, ki na takšen način prenašajo signal, so: AM in FM radio, televizija, mobilni telefoni, naprave *bluetooth*, brezžične tipkovnice in brezžične mrežne kartice [24]. Zaradi večje urejenosti, lažjega nadzora in izogibanju motnjam so organizacije, kot sta *Federal Communications Commission (FCC)* v ZDA in *European Conference of*



Slika 2.2: Družina IEEE 802 v povezavi z OSI modelom [11].

Postal and Telecommunications Administrations (CEPT) v Evropi, definirale frekvenčno območje, ki je namenjeno v industrijske, znanstvene in medicinske namene, imenovano ISM (*industrial, scientific and medical*). ISM določa tudi frekvenčna območja za uporabo brez licence, vendar je predpisana omejitev oddajne moči. Med njimi sta za prenos podatkov v računalništvu najbolj pogosti naslednji dve območji [11, 5]:

- 2,4 GHz (2,4 do 2,4835 GHz) in
- 5 GHz (5,15 do 5,35 in 5,725 do 5,825 GHz).

2.2 Kanali

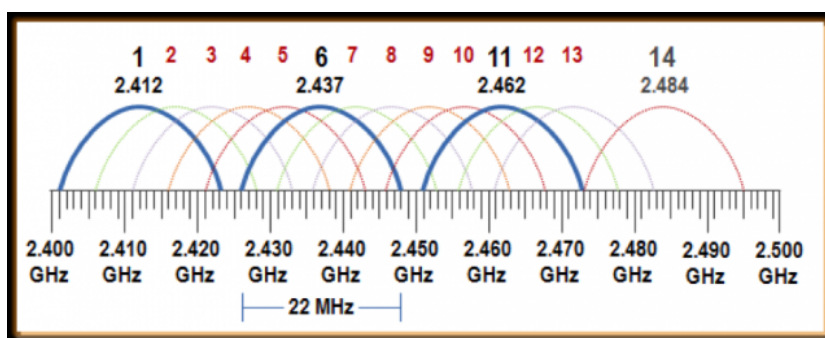
Standard IEEE 802.11 uporablja dve frekvenčni območji, ki jih ISM definira za uporabo brez uradnega dovoljenja, in sicer 2,4 GHz ter 5 GHz [21].

2.2.1 Frekvenčno območje 2,4 GHz

Najbolj pogosto uporabljen frekvenčni pas pri brezžičnih omrežjih je 2,4 GHz in je širok 100 MHz. Standard IEEE ga razdeli na 14 kanalov, ki so določeni z njihovo središčno frekvenco (glej sliko 2.3). Razdalja med središči je 5 MHz, širina vsakega kanala pa znaša 22 MHz, kar pomeni, da se kanali med seboj prekrivajo. Da ne prihaja do motenj, se večinoma uporabljajo kanali 1, 6 in

11, ki so edini kanali, katerih obseg frekvence se ne prekriva. Tudi kanal 14 se ne prekriva z drugimi kanali, vendar je dovoljen le na Japonskem [21].

Frekvenčno območje 2,4 GHz zaradi nižje frekvence omogoča boljši prenos signala skozi ovire. Vendar ta pas uporabljajo tudi mikrovalovne pečice, brezžični hišni telefoni in brezžične video kamere, kar lahko pri intenzivni uporabi povzroči tudi interferenco in napake pri prenosu podatkov. Dovoljeno je tudi združevanje dveh kanalov v frekvenčni pas velik 44 MHz. Širši kanali omogočajo večje hitrosti prenosa podatkov [21].

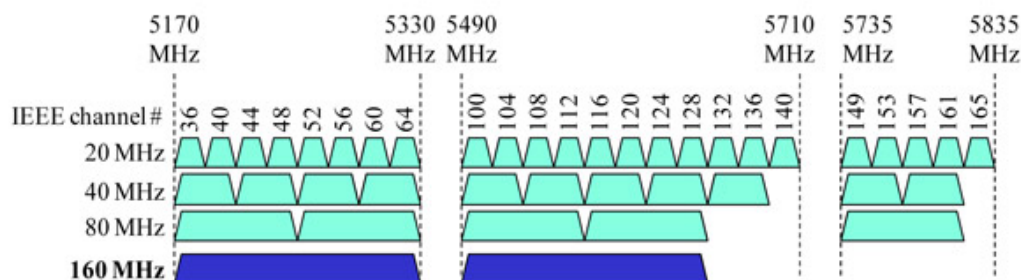


Slika 2.3: Kanali na frekvenčnem območju 2,4 GHz [12].

2.2.2 Frekvenčno območje 5 GHz

Standardi 802.11a, n in ac imajo definirano uporabo 5GHz frekvenčnega območja. Ta ima zaradi višje frekvence večje izgube skozi ovire. Območje je sestavljeno iz petindvajsetih 20 MHz kanalov, ki se med seboj ne prekrivajo (glej sliko 2.4) [12].

Zaradi večjega števila kanalov se promet lažje razporedi in zato težje pride do motenj. V tem frekvenčnem območju je omogočeno združevanje dveh, štirih in osmih kanalov, kar lahko privede do frekvenčnega pasu širokega tudi 160 MHz [12].



Slika 2.4: Kanali na frekvenčnem območju 5 GHz [1].

2.3 Zgodovina brezžičnega omrežja in IEEE 802.11 standardi

Brezžična omrežja imajo začetke že leta 1971, ko je havajska univerza povezala sedem računalnikov na štirih otokih z omrežjem imenovanim ALO-HAnet. Omrežje je bilo povezano s poceni komercialno radijsko opremo z osrednjo dostopno točko na otoku Oahu [26, 2].

V naslednjih desetletjih so se brezžične mrežne rešitve različnih proizvajalcev zelo razlikovale, zato med seboj niso bile združljive. V tem času so omrežja najbolj pogosto uporabljale univerze in deloma poslovna okolja [26].

Leta 1997 je inštitut IEEE (*Institute of Electrical and Electronics Engineers*) izdal standard 802.11, ki je nastajal sedem let in poskrbel za združljivost brezžičnih omrežij in naprav različnih izdelovalcev [26, 3]. V osnovi definira tri različne fizične sloje: infrardeči signal, razpršeni spekter s frekvenčnim skakanjem (angl. *Frequency hopping Spread Spectrum* — FHSS) in razpršeni spekter z neposrednim zaporedjem (angl. *Direct sequence Spread Spectrum* — DSSS). Definira tudi kontrolo dostopa do fizičnega medija (angl. *Media Access Control* — MAC) in algoritem za šifriranje in zagotavljanje integritete sporočil imenovan WEP (*Wired Equivalent Privacy*). Standard zagotavlja na fizičnem sloju 1 in 2 Mbit/s hitrost prenosa [3].

Dve leti kasneje sta bila sprejeta še dva standarda. Prvi je bil 802.11b, ki

deluje v 2,4 GHz frekvenčnem področju in uporablja na fizičnem sloju modula-
cijski postopek CCK (*Complementary Code Keying*), ki dodatno omogoča
še 5,5 in 11 Mbit/s hitrost prenosa [3].

Drugi standard, ki je bil sprejet leta 1999, je 802.11a, ki deluje v 5 GHz
frekvenčnem območju in uporablja modulacijo OFDM (*Orthogonal Frequency
Division Multiplexing*). Omogoča hitrost podatkov do 54 Mbit/s [3].

Leta 2003 je izšel standard 802.11g, ki uporablja modula-
cijski postopek OFDM in CCK. Poleg tega deluje v 2,4 GHz frekvenčnem območju, omogoča
hitrost prenosa podatkov do 54 Mbit/s in je navzdol združljiv s standardom
802.11b [3, 21].

Šest let kasneje je bil uradno sprejet standard 802.11n, ki je nadgradnja
prejšnjih standardov in lahko deluje tako v 2,4 kot tudi v 5 GHz frekvenčnem
območju. Omogoča uporabo več anten (MIMO), ki skupaj z modulacijo
OFDM poveča zanesljivost in hitrost prenosa podatkov ter izboljša do-
met. Omogoča tudi hitrost prenosa podatkov do 600 Mbit/s in združevanje dveh
frekvenčnih kanalov [15, 21].

Kot nadgradnja dotedanjih kanalov, je bil leta 2013 sprejet 802.11ac,
ki deluje samo na 5 GHz frekvenčnem območju. Z izboljšano modulacijo,
možnostjo uporabe do 8 anten (MIMO) in možnostjo združevanja po 4 ali 8
kanalov omogoča izjemno visoke hitrosti prenosa [21].

2.4 Arhitektura brezžičnega omrežja

Za brezžično omrežje 802.11 sta najbolj pomembna naslednja elementa (v
nadaljevanju ju skupno poimenujemo naprava) [17]:

- postaja (angl. *station* – STA) – oziroma odjemalec (angl. *client*) je
naprava v omrežju z vgrajeno ali zunanjo mrežno kartico, ki omogoča
povezovanje z brezžičnim omrežjem.
- brezžična dostopna točka (angl. *wireless access point* – AP) – je na-
prava, ki posreduje podatke med postajami in predstavlja povezavo
med brezžičnim in ožičenim omrežjem.

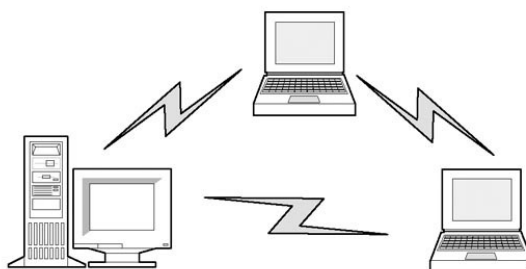
2.4.1 Topologija

Glede na način komuniciranja med postajami ločimo brezžična omrežja na tri osnovne topologije:

- IBSS

Independent Basic Service Set (IBSS) imenovan tudi *ad hoc* je najbolj enostavna postavitev sestavljena iz dveh ali več postaj, ki lahko neposredno, brez dostopne točke, komunicirajo med seboj in so si tako med seboj enakovredne (glej sliko 2.5) [20].

Ker ne potrebuje dostopne točke, so začetni stroški takšne postavitve majhni, vendar morajo biti postaje dovolj blizu, da se med seboj dosežejo [20, 26].



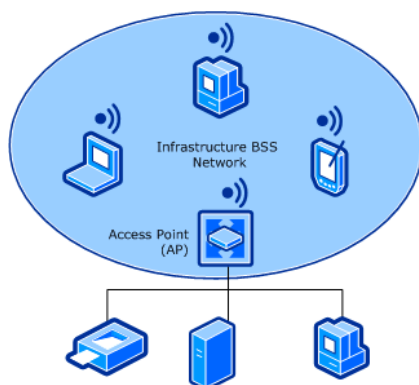
Slika 2.5: Primer topologije IBSS, kjer naprave neposredno komunicirajo med seboj [26].

- BSS

Basic Service Set (BSS) topologija je sestavljena iz ene brezžične dostopne točke in vsaj ene postaje (glej sliko 2.6). Ves promet in komunikacija odjemalcev v takšnem omrežju poteka preko dostopne točke [17].

Dostopna točka je zadolžena za oglaševanje omrežja, vzpostavljanje povezave z napravami ter povezavo med brezžičnim in ožičenim omrežjem

[11, 20]. Komunikacija preko dostopne točke omogoča večji obseg omrežja, saj odjemalca lahko komunicirata, čeprav se neposredno ne dosežeta. Število postaj v takšnem omrežju s standardom 802.11 ni omejeno, vendar se v praksi pri večjem številu odjemalcev pojavi nizka prepustnost omrežja [11]. (vir: 802.11 Wireless Networks: The Definitive Guid)

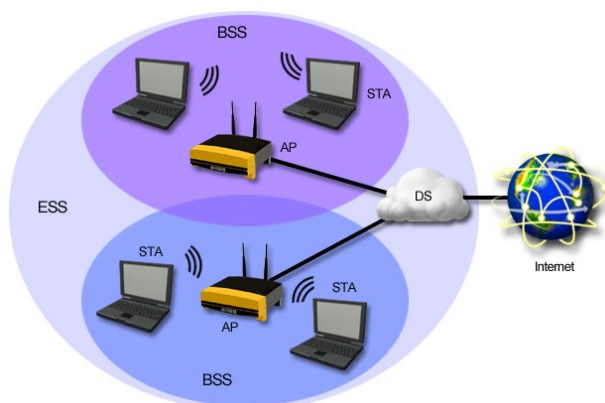


Slika 2.6: Primer topologije BSS, kjer naprave komunicirajo preko dostopne točke [4].

- ESS

Extended Service Set (ESS) je sestavljen iz dveh ali več dostopnih točk oziroma BSS-jev, ki imajo enako ime SSID (*service set identifier*) in so med seboj žično povezane (glej sliko 2.7) [11].

Delovanje posamezne dostopne točke je podobno kot pri osnovni postavitvi, le da žična povezava, imenovana tudi *Distribution System* (DS), med dostopnimi točkami ustvari most (angl. *bridge*). Ta omogoča enostaven prehod med dostopnimi točkami povezanimi v isto omrežje in komunikacijo postaj, ki so povezane na različne dostopne točke. Kot pri BSS, ves promet pri ESS poteka preko dostopnih točk [11].



Slika 2.7: Primer topologije ESS, kjer sta v skupno omrežje povezani dve dostopni točki [10].

2.5 Okvirji MAC

V nasprotju z ožičenim omrežjem, je protokol pri brezžičnem omrežju veliko bolj zapleten [20]. Brezžični prenosni medij zahteva številne kontrolne in vzdrževalne naloge, ki pri ožičenem omrežju niso bile potrebne. Standard 802.11 določa tri različne okvirje, ki se razlikujejo glede na nalogo, ki jo upravljajo [11]:

- kontrolni okvirji (angl. *control frames*) – se uporabljajo za zagotavljanje uspešnega prenosa podatkov,
- upravljalni okvirji (angl. *management frames*) – omogočajo postajam, da se povežejo in vzdržujejo povezavo z omrežjem,
- podatkovni okvirji (angl. *data frames*) – se uporabljajo za prenos podatkov z višjih nivojev.

2.5.1 Kontrolni okvir

Kontrolni okvir je skupaj s podatkovnim okvirjem zadolžen, da se podatki zanesljivo prenesejo od postaje do postaje. Kontrolni okvirji vsebujejo le

glavo (angl. *header*) okvirja v velikosti 16 bitov [11, 23].

Da vse naprave zaznajo, da gre za kontrolni okvir, so vsi biti, razen podtipa (angl. *Sub type*), fiksno nastavljeni (glej sliko 2.8). Podtip pove napravi, kateri od kontrolnih okvirjev je prispel, da ta lahko ustrezno ukrepa [23].

bits		2		4				1	1	1	1	1	1	1	1
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Protocol		Type = control		Sub type				ToDS	FromDS	More Frag	Retry	Pwr Mgmt	More data	Protected Frame	Order
0	0	1	0					0	0	0	0	0	0	0	0

Slika 2.8: Zgradba kontrolnega okvirja [23].

Vrste kontrolnih okvirjev [6]:

- *Control wrapper* – se uporablja za prenos drugih kontrolnih okvirjev z dodanim kontrolnim poljem HT (*High Throughput*).
- *Block ACK request* (BAR) – preden naprava pošlje blok podatkov (pogosto so to QoS podatki) v načinu *Block ACK*, mora preveriti, da postaja to omogoča. Nato lahko pošlje blok podatkov in zahtevo *Block ACK request*, ki zahteva, da prejemnik pošlje le *Block ACK*, ki naenkrat potrdi celoten blok podatkov.
- *Block ACK* – s tem prejemnik potrdi celoten blok prejetih podatkov, namesto da potrjuje vsak okvir posebej.
- *Power Save – Poll* (PS-Poll) – postaja, ki ima omogočen način varčevanja z energijo, pošlje PS-Poll do dostopne točke, ki ji nato odgovori s podatki, ki so namenjeni tej postaji in so bili v čakalni vrsti.
- *Request to Send* (RTS) – RTS/CTS je mehanizem za izogibanje trkom. V tem načinu mora postaja, preden pošlje želene podatke, opraviti izmenjavo RTS/CTS. Z okvirjem RTS postaja pove, koliko časa bo pošiljala podatke.

- *Clear to Send* (CTS) – ko naprava prejme RTS, odgovori z okvirjem CTS, s katerim pove, koliko časa bo potekal prenos, rezervira medij in dovoli postaji, ki je poslala RTS, da pošilja podatke.
- *Acknowledge* (ACK) – ko naprava uspešno prejme podatke, to potrdi s pošiljanjem okvirja ACK napravi, ki je podatke poslala.
- *Contention Free-End* (CF-End) – način PCF (angl. *Point Coordinated Function*), pomeni, da je omrežje upravljano z ene točke (angl. *Point Coordinator* – PC) – navadno je to dostopna točka. Okvir CF-End pošlje dostopna točka in z njim označi konec periode CFP (angl. *Contention Free Period*), oziroma čas, v katerem ni tekmovanj za omrežje.
- *Contention Free-END + Contention Free-ACK* (CF-End + CF-ACK) – ta okvir se uporablja za sočasno označevanje konca periode CFP in potrjevanje prispelega okvirja.

2.5.2 Upravljalni okvir

Obstaja več upravljalnih okvirjev, ki se uporabljajo za vzdrževanje na povezovalni plasti [11].

- *Beacon*

Okvirji *beacon* oznanjajo obstoj omrežja in so del mnogih njegovih vzdrževalnih nalog. Oddajani so v rednih intervalih in omogočajo postajam, da zaznajo in identificirajo omrežje, ter uskladijo parametre za povezovanje v omrežje. Vsebujejo interval *beacon* znan kot TBTT (*Target Beacon Transmission Time*), ki pove, kakšen je interval pošiljanja okvirjev *beacon*. Uporablja se tudi za sinhronizacijo naprav v omrežju. Za razliko od BSS in ESS, kjer jih oddaja dostopna točka, jih pri IBSS oddajajo kar postaje same. Ker znotraj BSS poteka ves promet skozi dostopno točko, morajo biti vse postaje dovolj blizu dostopne točke, da zaznajo okvirje *beacon*.

- *Probe request*

Postaje uporabljajo te okvirje za iskanje obstoječih 802.11 omrežij. Okvir vsebuje ime SSID in hitrosti, ki jih podpira. Naprava, ki prejme *probe request*, preveri ali postaja zadostuje kriterijem za pridružitev omrežju.

- *Probe response*

Če *probe request* najde omrežje s kompatibilnimi parametri, naprava, ki je zadnja poslala okvir *beacon* — pri splošni postavitivi je to dostopna točka, odgovori z okvirjem *probe response*. *Probe response* vsebuje enake parametre kot okvir *beacon*, kar omogoči postaji, ki ga prejme, da uskladi parametre in se pridruži omrežju.

- *IBSS announcement traffic indication map (ATIM)*

Ker *ad hoc* omrežje nima dostopne točke, ta ne more hraniti podatkov v čakalni vrsti za naprave v načinu nizke porabe energije. Zato naprave, ki imajo okvirje pripravljene v čakalni vrsti, pošljejo okvir ATIM, da obvestijo prejemnika o podatkih pripravljenih na pošiljanje.

- *Association request*

Ko postaja zazna kompatibilno omrežje in se mu overi (angl. *Authenticate*), se mu lahko poskusi pridružiti s pošiljanjem okvirja *association request*. Preden dostopna točka dovoli pridružitev omrežju, preveri, ali se parametri v okvirju, kot so tip omrežja (angl. *Compatibility Info*), SSID in podprte hitrosti (angl. *Supported Rates*) ujema s parametri omrežja.

- *Reassociation request*

Če prehaja med BSS znotraj enega ESS ali začasno zapusti BSS in se nato vrne, se mora ponovno asociirati z omrežjem. *Reassociation request* se od *association request* razlikuje le v tem, da vsebuje naslov dostopne točke, s katero je trenutno povezan. S pomočjo tega naslova,

lahko dostopna točka, s katero se poskuša povezati, zaprosi trenutno dostopno točko za podatke o asociaciji. Prenesejo se lahko tudi podatki, namenjeni omenjeni postaji, ki jih je imela prejšnja dostopna točka v čakalni vrsti.

- *Association response* in *Reassociation response*

Kadar se postaja poskuša povezati z omrežjem in se njuni parametri ujemajo, dostopna točka odgovori z enim od teh okvirjev. Okvirja se razlikujeta le v polju *Frame Control*. Kot del odgovora, dostopna točka dodeli *Association ID*.

- *Authentication*

Okvir *authentication* se uporablja za overjanje oziroma potrjevanje verodostojnosti postaje in omrežja. Ker se lahko uporabljajo različni algoritmi, je eden izmed njih določen v polju *The Authentication Algorithm Number*.

- *Disassociation* in *Deauthentication*

Okvirji *disassociation* se uporabljajo za razveljavitev asociacije postaje. Okvir *deauthentication* pa razveljavi overitev postaje. Oba okvirja vsebujeta fiksno polje s šifro razloga (angl. *Reason code*).

- *Action*

Ta okvir je bil dodan s 802.11h in se ga uporablja za proženje meritev.

2.5.3 Podatkovni okvir

Podatkovni okvirji so okvirji, ki v telesu prenašajo podatke iz višjih nivojev. Zaradi potreb protokolov, obstajajo tudi nekateri podatkovni okvirji, ki ne vsebujejo podatkov. Glede na vsebino in funkcijo jih lahko razvrstimo v skupine na več načinov prikazanih na sliki 2.9. Ena od možnih delitev v skupine je glede na uporabo storitve na podlagi tekmovanja (angl. *Contention-based service*) ali storitve brez tekmovanja (angl. *Contention-free service*). Druga

možna delitev je med okvirji, ki prenašajo (angl. *Carry data*) in ne prenašajo (angl. *Does not carry data*) podatkov [11].

Frame type	Contention-based service	Contention-free service	Carries data	Does not carry data
Data	✓		✓	
Data+CF-Ack		✓	✓	
Data+CF-Poll		AP only	✓	
Data+CF-Ack+CF-Poll		AP only	✓	
Null	✓	✓		✓
CF-Ack		✓		✓
CF-Poll		AP only		✓
CF-Ack+CF-Poll		AP only		✓

Slika 2.9: Kategorizacija podatkovnih okvirjev [9].

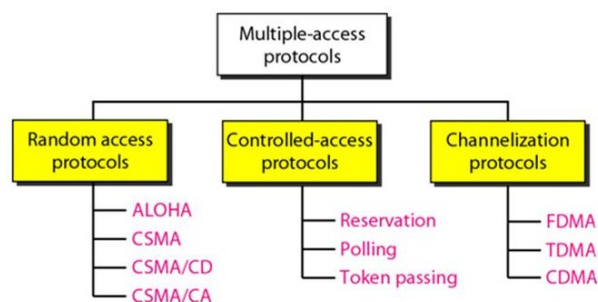
Poglavje 3

Način dostopa do medija

Kadar dve ali več naprav, ki si delijo medij (pri brezžičnih omrežjih to pomeni, da oddajajo na isti frekvenci), oddaja hkrati, lahko zaradi motenj pride do napak pri sprejemu podatkov. Da se temu izognemo, poskrbi nivo MAC, ki upravlja skupinski dostop do media. Protokole, ki določajo, kako poteka skupinski dostop, delimo v tri skupine, prikazane na sliki 3.1: protokoli za naključni dostop, protokoli za izmenični dostop in protokoli za delitev kanala [19].

- Protokoli za naključni dostop (angl. *Random access protocols*) so protokoli, kjer se naprave borijo za medij in vsaka oddaja, kadar želi. Če pri prenosu pride do kolizije, se jo razrešuje. Najbolj pogosti so ALOHA, CSMA (*Carrier Sense Multiple Access*), CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*) in CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*).
- Protokoli za nadzorovan dostop (angl. *Controlled-access protocol*) napravam dodeljujejo pravice do pošiljanja. Naprava ne sme poslati, dokler ne dobi dovoljenja. Najbolj znani so *reservation*, *polling* in *token passing*.
- Protokoli za delitev kanala (angl. *Channelization protocols*) razdelijo medij na kanale. Najbolj znani so FDMA (*Frequency-division multiple*

access), ki razdeli na podlagi frekvence, TDMA (*Time-division multiple access*), ki razdeli medij na podlagi časa, in CDMA (*Code-division multiple access*), ki omogoča souporabo medija s pomočjo kodiranja.



Slika 3.1: Protokoli za skupinski dostop [19].

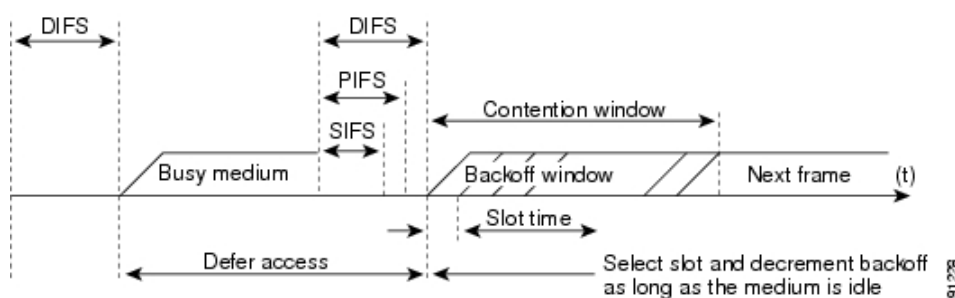
3.1 Dostop do medija pri 802.11

Za dostop do medija je pri 802.11 najbolj pomemben protokol CSMA/CA, saj deluje tako, da pred pošiljanjem preveri, ali je medij prost in se poskuša trkom izogniti [23]. V grobem pri brezžičnih omrežjih ločimo načine dostopa do medija na nekoordinirane in koordinirane s strani dostopne točke.

Za razumevanje načinov dostopa do medija so pomembni naslednji elementi (glej sliko 3.2) [8, 13]:

- SIFS (*Short interframe space*) – predstavlja najkrajši prostor med okvirji. Uporablja se za prenos okvirjev z najvišjo prioriteto (na primer okvirjev CTS in ACK).
- PIFS (*PCF interframe space*) – predstavlja prostor med okvirji v načinu *Point Coordination Function*. Uporablja ga točkovni koordinatorski (angl. *Point Coordinator*) za dostop do medija med obdobjem *Contention Free Period*.

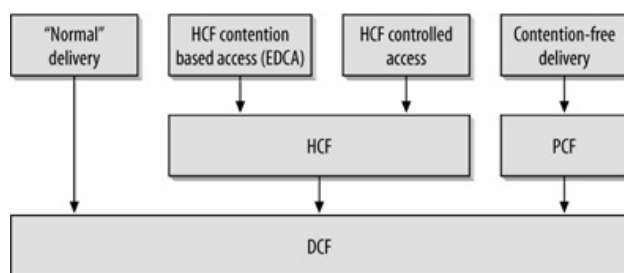
- DIFS (*DCF interframe space*) – predstavlja prostor med okvirji v načinu *Distributed Coordination Function*. Uporablja se za prenos upravljalnih in podatkovnih okvirjev.
- CW (*Contention Window*) – je okno, znotraj katerega se izbere naključen časovni interval, ki ga mora naprava počakati pred oddajo paketa.



Slika 3.2: Prikaz prostorov med okvirji [14].

Standard 802.11 uporablja naslednje načine dostopa do medija (glej sliko 3.3) [11]:

- DCF (*Distributed Coordination Function*) – je najbolj osnoven način dostopa. Ko postaja želi oddajati, počaka neki vnaprej določen čas (DIFS), nato še naključen časovni interval in začne z oddajanjem.
- PCF (*Point Coordination Function*) – je način, v katerem točkovni koordinator (angl. *Point Coordinator*) vodi komunikacijo v omrežju. Ta čaka manjši časovni interval (PIFS) kot postaja (DIFS), zato ima vedno prednost.
- HCF (*Hybrid Coordination Function*) – je način, ki se uporablja le v omrežjih z omogočeno kvaliteto storitev. Je hibriden način, ki združuje načina DCF in PCF, z dodanimi mehanizmi za zagotavljanje kakovosti storitve (QoS) [13].



Slika 3.3: Načini dostopa do medija pri 802.11 [11].

3.2 Distributed Coordination Function

Kot je s slike 3.3 razvidno, je način DCF najbolj osnoven in temeljni način dostopa do medija, na katerem temeljita tudi načina PCF in HCF. Ko je naprava, ki uporablja način DCF, pripravljena na pošiljanje, gre skozi naslednje korake [7]:

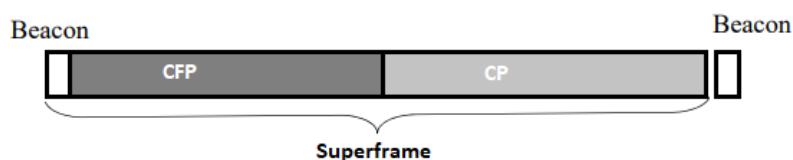
1. generira naključen časovni interval od 0 do CW,
2. počaka vnaprej določen časovni interval DIFS,
3. če je medij ves ta čas prazen, začne z odštevanjem naključnega časovnega intervala,
4. če je medij kadarkoli med čakanjem zaseden, se ponovijo koraki od 2 do 4 in
5. če je po naključnem časovnem intervalu medij še vedno prost, naprava lahko začne z oddajo.

S pomočjo naključnega časovnega intervala se naprave, ki bi želele hkrati pošiljati podatke, lažje izognejo trkom. Če vseeno pride do trka, se jim podvoji vrednost okna CW. Način DCF se lahko uporablja tako pri BSS kot IBSS, saj za delovanje ne potrebuje točkovnega koordinatorja oziroma dostopne točke. Poleg omenjenega načina preverjanja medija in izogibanja trkom, DCF omogoča tudi dostop z rokovaljem, ki odpravlja težavo skritega

vozljšča (angl. *Hidden Node problem*)¹. Pri tem mu pomagata kontrolna okvirja RTS in CTS, ki vsebujeta vektor NAV (*Network Allocation Vector*). Vektor NAV predstavlja čas, ki ga okvir potrebuje za prenos in napravam pove, koliko časa bo medij zaseden. Vsaka naprava, ki dobi okvir RTS ali CTS, ki ni namenjen njej, preveri NAV in za toliko časa preneha z oddajanjem na mediju, saj bo ta zaseden [11].

3.3 Point Coordination Function

Point Coordination Function (PCF) je način, pri katerem omrežje upravlja točkovni koordinator (angl. *Point Coordinator* – PC). Ta način ni možen v IBSS, saj potrebuje dostopno točko, ki bi opravljala nalogo PC. Čas med dvema okvirjema *beacon* se imenuje *Superframe* in je razdeljen na dva dela (glej sliko 3.4): *Contention Free Period* (CFP) in *Contention Period* (CP). Takoj ko dostopna točka odda okvir *beacon*, se začne perioda CFP. V tem času dostopna točka zasede omrežje in nadzira njegovo delovanje. Ker je interval PIFS krajši od intervala DIFS, bo dostopna točka vedno imela prednost. Dostopna točka z okvirjem CF-Poll sprašuje postaje, ali želijo poslati podatke. Če ne želijo, morajo odgovoriti z okvirjem *null*. Ko je konec periode CFP, dostopna točka drugim napravam to sporoči z okvirjem CF-end in s tem se začne perioda CP. To je čas, ko naprave enakovredno dostopajo do medija na podlagi DCF [8, 13].



Slika 3.4: Superframe razdeljen na CFP in CP.

¹https://en.wikipedia.org/wiki/Hidden_node_problem

3.4 Hybrid Coordination Function

Kot je bilo že omenjeno, je HCF hibridni način, ki združuje načina DCF in PCF. Omogoča prioriteten prenos podatkov, kjer natančno časovno usklajevanje pri načinu PCF ni potrebno [11]. Namenjen je omrežjem, ki ponujajo kakovost storitve (angl. Quality of Service – QoS). Ta nudijo prednost pri prenosu bolj pomembnim podatkom oziroma okvirjem z višjo prioriteto [13]. To pomeni, da lahko poleg prioritete postaj določa tudi prioriteto posameznih sej znotraj ene postaje.

Poglavje 4

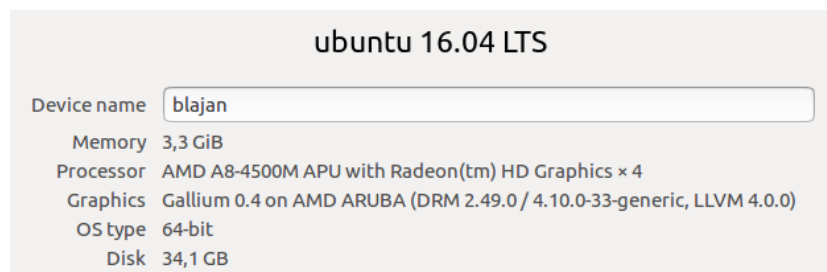
Načrtovanje meritev

Standardi 802.11 nimajo eksplicitno definirano, kako naj si dostopne točke (AP) razdelijo dostop do medija in pošiljanje prometa pri sočasnem delovanju na istem kanalu. Da bi preverili njihovo delovanje, bomo pripravili različne scenarije delovanja dostopnih točk in opravili meritve.

4.1 Opis opreme

Za postavljanje zelenih scenarijev potrebujemo opremo, s katero bomo vzpostavili omrežje. Uporabili bomo naslednje naprave:

- Prenosni računalnik (v nadaljevanju PC-1) s specifikacijami predstavljenimi na sliki 4.1.



Slika 4.1: Specifikacije prenosnega računalnika.

- Namizni računalnik (v nadaljevanju STA-S) z mrežno kartico *Broadcom NetLink BCM5786 Gigabit Ethernet PCI Express* in drugimi specifikacijami na sliki 4.2.

ubuntu 16.04 LTS	
Device name	sta-s
Memory	980,9 MiB
Processor	Intel® Pentium(R) D CPU 2.80GHz × 2
Graphics	Intel® 946GZ
OS type	64-bit
Disk	38,8 GB

Slika 4.2: Specifikacije namiznega računalnika.

- Trije USB brezžični vmesniki *D-Link DWL-G122*¹.
- Dva brezžična usmerjevalnika *Linksys WRT54GL 1.1*² z naloženo strojno-programsko opremo *OpenWRT*³ *10.03.1 Backfire* s privzetimi nastavitvami in vključenim brezžičnim omrežjem (v nadaljevanju AP-A in AP-B).
- Brezžični usmerjevalnik *NETGEAR WNR854T*⁴ s privzetimi nastavitvami (v nadaljevanju imenovan NETGEAR).
- Brezžični usmerjevalnik *NETGEAR MR814v2*⁵ s privzetimi nastavitvami, ki ga bomo uporabljali zgolj kot stikalo za žično povezovanje

¹<https://www.amazon.com/D-Link-DWL-G122-Compact-Wireless-Adapter/dp/B0002DQUHC>

²https://wikidevi.com/wiki/Linksys_WRT54GL_v1.1

³<https://wiki.openwrt.org/toh/linksys/wrt54g>

⁴<https://www.netgear.com/support/product/wnr854t.aspx>

⁵<https://www.netgear.com/support/product/MR814v2.aspx>

dostopnih točk in STA-S (v nadaljevanju bo omenjeni usmerjevalnik imenovan stikalo).

V pomoč pri povezovanju naprav, generiranju prometa in izvajanju meritev nam bo različna programska oprema. Za realizacijo scenarijev je ključna naslednja programska oprema:

- Virtualbox [22]

Virtualbox je brezplačna in odprtokodna programska oprema, ki omogoča ustvarjanje in uporabljanje navideznih strojev (angl. *virtual machines*; v nadaljevanju VM). Uporabili bomo *Virtualbox 5.0.40* s pripadajočim razširitvenim paketom (angl. *expansion pack*) za ustvarjanje dveh VM z enakimi okolji.

- Wireshark [25]

Wireshark je brezplačen in odprtokoden program, ki omogoča analizo paketov. Uporablja se za odpravljanje motenj in analizo omrežja, razvijanje programske opreme in komunikacijskih protokolov ter izobraževanje. Za analiziranje paketov v omrežju bomo v nalogi uporabili *Wireshark 2.2.7*.

- Iperf [16]

Iperf je programska oprema, ki se uporablja za merjenje zmogljivosti omrežja. S programom nastavimo strežnik in odjemalca, med katerima pošlje tok podatkov in opravi meritve. Omogoča protokola TCP (angl. *Transmission Control Protocol*) in UDP (angl. *User Data Protocol*). Protokol TCP s pomočjo potrjevanja zagotavlja uspešen prenos in vrstni red podatkov. UDP ne preverja uspešnega prenosa podatkov, zato se pojavijo izgube paketov (angl. *packet loss*), vendar to omogoča večjo hitrost prenosa. Med uporabljanjem protokola UDP imamo možnost nastavljanja zelene pasovne širine ter merimo dejansko pasovno širino s katero so potovali podatki, spreminjanje zakasnitve paketov (angl. *jit-*

ter) in izgubo paketov. Program zaženemo v terminalu z ukazom *iperf* in zelenimi opcijami. Za nas so pomembne opcije:

- *-s*, definira strežnik,
- *-c [IP strežnika]*, definira odjemalca in določi, na kateri strežnik se poveže; naslov IP strežnika je lokalni naslov IP postaje, na kateri deluje strežnik,
- *-t [čas]*, definira čas ustvarjanja prometa v sekundah,
- *-l [velikost medpomnilnika]*, definira velikost medpomnilnika, ki se uporablja za zapisovanje oziroma branje podatkov,
- *-u*, definira uporabo protokola UDP,
- *-b [hitrost prenosa podatkov]M*, definira hitrost v Mbit/s, s katero odjemalec generira podatke.

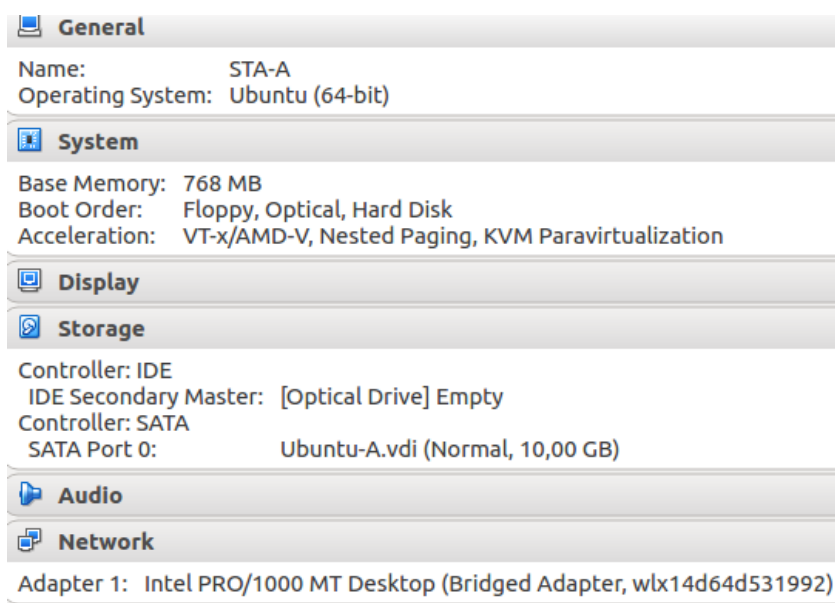
4.2 Priprava scenarijev

Zanima nas, kako se dostopne točke (AP) odzovejo na sočasno uporabljanje istega kanala. Da bi to preverili, moramo izvesti meritve pri različnih scenarijih. Merili bomo dejansko pasovno širino, *jitter* in izgubo paketov pri protokolu UDP. Poleg tega bomo opazovali tudi vsebino in vrstni red paketov v omrežju.

Da zagotovimo veljavne meritve, moramo imeti enake pogoje pri pošiljanju podatkov preko vsake AP. Zato s pomočjo programa *Virtualbox* ustvarimo dve VM z enakimi specifikacijami in konfiguracijo. To dosežemo z ustvarjanjem prve VM (v nadaljevanju imenovana STA-A) z ustreznimi specifikacijami predstavljenimi na sliki 4.3 in ustrezno konfiguracijo programske opreme (naložimo *Virtualbox Guest Additions* in *Iperf*). S slike 4.3 je razvidno, da VM uporablja za povezovanje z omrežjem *bridged* način s svojim USB brezžičnim vmesnikom. Nato kloniramo STA-A v novo VM (v nadaljevanju imenovano STA-B), kar nam zagotovi popolnoma enake pogoje. Pri STA-B

spremenimo ime iz STA-A v STA-B za lažje prepoznavanje in izberemo drugi brezžični vmesnik.

Vsaka AP ima svoje omrežje z različnim imenom SSID. Vse AP pa so nastavljene na kanal 11 in uporabljajo standarda 802.11g in 802.11b (zaradi omejenosti drugih naprav to pomeni, da bo v uporabi standard 802.11g).

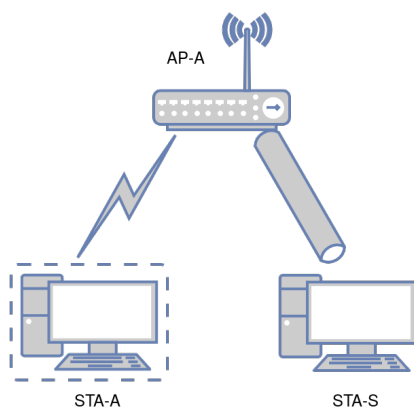


Slika 4.3: Specifikacije VM STA-A.

4.2.1 Scenarij 1

Pri scenariju 1 imamo eno brezžično postajo (STA-A), eno dostopno točko (AP-A) in eno žično povezano postajo (STA-S). Vse so v istem omrežju. Kot je razvidno s slike 4.4, sta STA-A in AP-A povezani brezžično, ter STA-S in AP-A povezani z žico.

To je kontrolni scenarij, kjer pošiljanje prometa poteka v idealnih pogojih, brez motenj drugih AP. Rezultati teh meritev bodo izhodiščna točka za opazovanje sprememb in vpliv delovanja več AP na istem kanalu.



Slika 4.4: Postavitev pri scenariju 1.

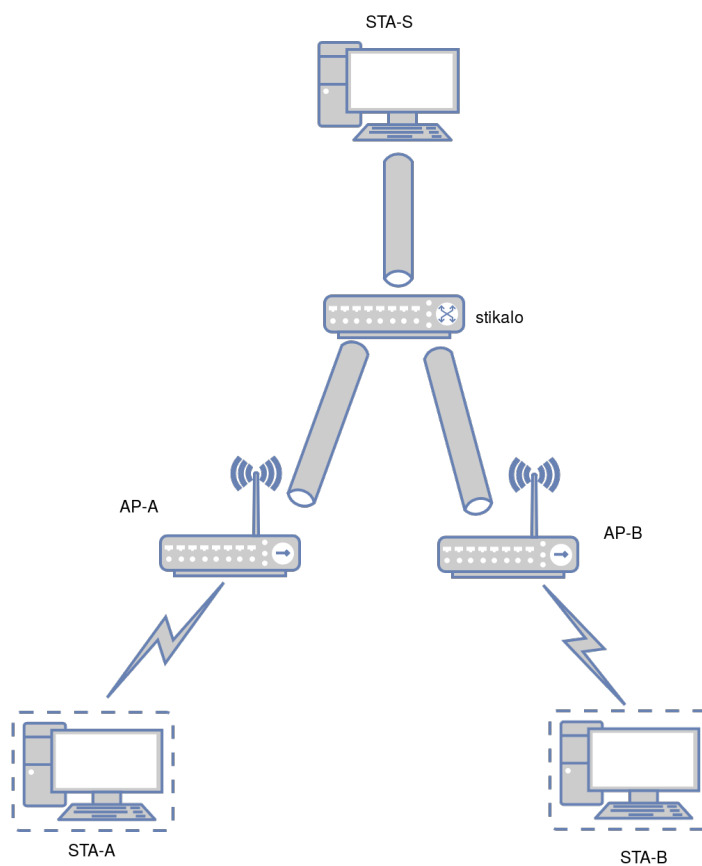
4.2.2 Scenarij 2

Scenarij 2 sestavljata dve AP (AP-A in AP-B), dve brezžični postaji (STA-A in STA-B), stikalo in žično povezana postaja STA-S. S slike 4.5 je razvidno, da so naprave AP-A, AP-B in STA-S žično povezane s stikalom. Ta omogoči, da se povezane naprave med seboj vidijo, kar pripomore k enostavnemu komuniciranju s pomočjo lokalnih naslovov IP. Obe AP imata v svoje omrežje povezano še brezžično postajo, in sicer je z AP-A povezana STA-A in z AP-B povezana STA-B.

V tem scenariju imata obe omrežji enake pogoje, enako postavitev in enako opremo. Zato sta omrežji enakovredni in scenarij predstavlja testni primer za opazovanje medsebojnega vpliva AP, ki delujejo na istem kanalu.

4.2.3 Scenarij 3

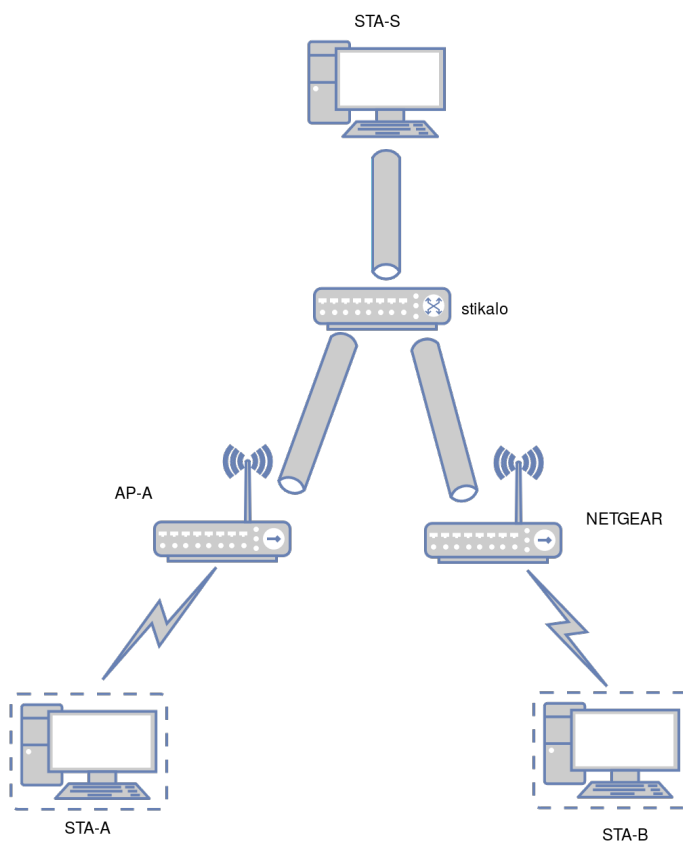
Na sliki 4.6 lahko vidimo, da je postavitev v scenariju 3 enaka kot pri scenariju 2, le da namesto AP-B uporabimo NETGEAR. Ta predstavlja starejšo in nekoliko slabšo AP. V tem scenariju preverimo, ali na tekmovanje za dostop oziroma kvaliteto prenosa podatkov vpliva model AP.



Slika 4.5: Postavitev pri scenariju 2.

4.2.4 Scenarij 4

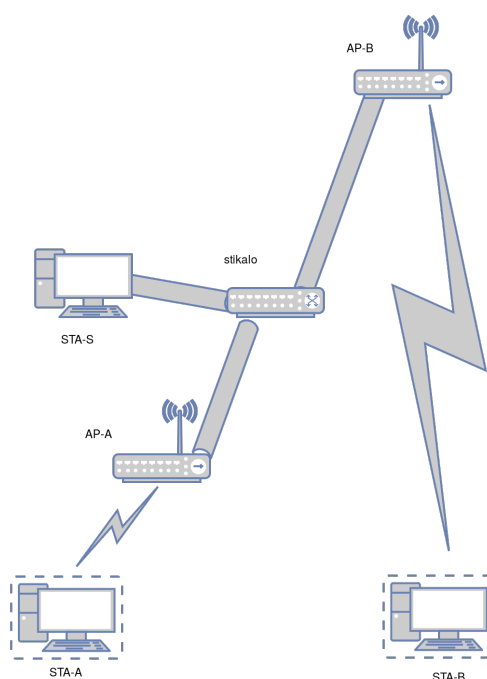
S slike 4.7 je razvidno, da ima scenarij 4 enako opremo in je enako povezan kot scenarij 2. Razlikuje se zgolj v oddaljenosti AP-B od STA-B. AP-B odmaknemo za približno pet metrov zračne razdalje od STA-B z vmesno opuščno steno. To povzroči, da ima AP-B slabši signal od AP-A. S tem preverimo, ali kvaliteta signala ene AP vpliva na kvaliteto oziroma hitrost prenosa druge AP.



Slika 4.6: Postavitev pri scenariju 3.

4.3 Opravljanje meritev

Pri vsakem scenariju opravimo meritve za promet od brezžične postaje proti AP in od AP proti brezžični postaji pri naslednjih generiranih hitrostih podatkov ($-b$): 5, 10, 20, 30, 40, 50 in 100 Mbit/s. Pri vsaki meritvi pošljemo podatke 30 sekund ($-t\ 30$) in z vsakim paketom pošljemo 1464 B ($-l\ 1464$) podatkov. Ustvarjanje in merjenje prometa opravimo s pomočjo programa *Iperf*. Med izvajanjem meritev s pomočjo orodja *Wireshark* opazujemo pakete na določenem kanalu. To storimo tako, da imamo v eno od postaj (PC-1) vključen brezžični vmesnik nastavljen na *monitor mode*, kar pomeni, da lahko vidi ves promet v omrežju na določenem kanalu.



Slika 4.7: Postavitev pri scenariju 4.

Za meritve protokola UDP v smeri od brezžične postaje do AP (oziroma postaje STA-S, ki je žično povezana z AP) najprej postavimo strežnik na STA-S z ukazom `iperf -s -u`. Preden začnemo z ustvarjanjem prometa, začnemo zajemati promet z orodjem *Wireshark*. Nato z ukazom `iperf -c [IP strežnika] -u -l1464 -t30 -b [pasovna širina]` zaženemo ustvarjanje prometa in meritev. Po koncu meritev se rezultati izpišejo v terminalu. Takrat tudi ustavimo zajemanje v *Wiresharku* in preverimo zajete pakete. Nato postopek ponovimo še v smeri od STA-S do brezžične postaje. To storimo s postavitvijo strežnika na brezžični postaji in zaženemo odjemalca na STA-AP.

Če imamo v scenariju dve AP, moramo biti pozorni na ustvarjanje prometa s STA-S. V terminalu napišemo ukaz, s katerim bi zagnali promet za vsak strežnik posebej in ju združimo z znakom `&`. Primer ustvarjanja podatkov UDP bi bil `iperf -c 192.168.0.4 -u -l1464 -t 30 -b 5M & iperf -c 192.168.0.5 -u -l1464 -t 30 -b 5M`. Pri meritvah podatkov od brezžične po-

staje proti STA-S posebne nastavitve strežnika niso potrebne, saj lahko *Iperf* strežnik meri podatke od različnih virov. Pozorni moramo biti, da ukaza za zagon meritev poženemo istočasno. Za zajem prometa v orodju *Wireshark* je dovolj zajem preko enega brezžičnega vmesnika, saj zajame ves promet na določenem kanalu.

Poglavje 5

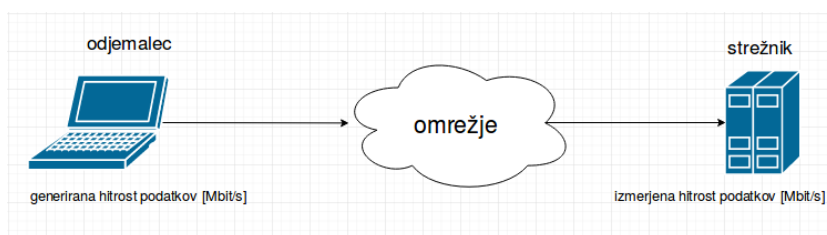
Rezultati in analiza meritev

V tem poglavju prikažemo rezultate meritev, opišemo, kaj prikazujejo, in razložimo kaj pomenijo za vsakega od scenarijev.

Meritve izvedemo tako, da zaženemo strežnik in izberemo odjemalca. Kot je prikazano na sliki 5.1, sta strežnik in odjemalec povezana v isto omrežje. V programu *Iperf* izberemo želeno hitrost prenosa podatkov, s katero odjemalec pošilja podatke proti strežniku. To smo v tabelah poimenovali generirana hitrost prenosa podatkov. Strežnik opravlja meritve nad prejetimi podatki in meri čas prenosa posameznega podatkovnega paketa, število prejetih paketov in količino prejetih podatkov. S pomočjo izmerjenega časa prenosa posameznega paketa izračuna spremembo v zakasnitvi prejetih paketov, ki je predstavljena kot *jitter*. Glede na število prejetih paketov izračuna odstotek izgubljenih podatkovnih paketov (angl. *datagram loss*). Izmerjena hitrost prenosa podatkov pa predstavlja hitrost, s katero je strežnik prejel podatke. Strežnik po opravljenih meritvah odjemalcu pošlje dobljene rezultate, ki jih nato oba prikažeta na zaslonu (glej sliki 5.2 in 5.3).

Meritve smo opravili z generirano hitrostjo prenosa podatkov 5, 10, 20, 30, 40, 50 in 100 Mbit/s. Za vsako od teh vrednosti smo izvedli pet meritev. Rezultate petih meritev za posamezno generirano hitrost smo povprečili in dobljeno povprečno vrednost vstavili v tabelo.

Ker smo v nekaterih scenarijih pri meritvi pošiljali in prejeli podatke



Slika 5.1: Povezava odjemalca in strežnika pri izvajanju meritev s programom *Iperf*.

```

Client connecting to 192.168.0.7, UDP port 5001
Sending 1464 byte datagrams
UDP buffer size: 208 KByte (default)
-----
[ 3] local 192.168.0.10 port 59205 connected with 192.168.0.7 port 5001
[ ID] Interval      Transfer    Bandwidth
[ 3] 0.0-30.0 sec  17.9 MBytes 5.00 Mbits/sec
[ 3] Sent 12811 datagrams
[ 3] Server Report:
[ 3] 0.0-27.2 sec  16.4 MBytes 5.06 Mbits/sec  0.120 ms 1073/12810 (8.4%)
[ 3] 0.0-27.2 sec  1 datagrams received out-of-order

```

Slika 5.2: Primer izpisa meritev na odjemalcu, ki jih je opravil program *Iperf*.

z dvema brezžičnima postajama, smo podatke označili z oznakama A in B. Oznaka A tako označuje podatke, ki se nanašajo na postajo STA-A, in oznaka B podatke, ki se nanašajo na postajo STA-B.

Po pregledu zajetih paketov v vsakem izmed omrežij smo ugotovili, da v nobenem omrežju niso prisotni okviri značilni za PCF, kar pomeni, da vsa omrežja delujejo v načinu DCF, kjer vse postaje vedno tekmujejo za dostop do medija.

5.1 Anomalije pri opravljanju meritev

Med opravljanjem meritev smo zasledili nekaj anomalij oziroma posebnosti. Najprej bi omenil *jitter*. Tako kot na izgubo paketov in izmerjeno hitrost prenosa podatkov, tudi na njega vpliva faktor naključnosti, vendar se pri njem ta pojav pozna bolj izrazito. Medtem ko je odstopanje deležev izgube

```
-----  
Server listening on UDP port 5001  
Receiving 1470 byte datagrams  
UDP buffer size: 208 KByte (default)  
-----  
[ 3] local 192.168.0.7 port 5001 connected with 192.168.0.10 port 59205  
[ 3] 0.0-27.2 sec 16.4 MBytes 5.06 Mbits/sec 0.121 ms 1073/12810 (8.4%)  
[ 3] 0.0-27.2 sec 1 datagrams received out-of-order
```

Slika 5.3: Primer izpisa meritev na strežniku, ki jih je opravil program *Iperf*.

paketo in hitrosti prenosa podatkov pri ponovitvah ene meritve majhno, je odstopanje *jitterja* v nekaterih primerih zelo veliko. To ima pri povprečenju zgolj petih meritev še vedno velike posledice. Po pregledu vseh meritev lahko vidimo vzorec, da se z večanjem generirane hitrosti prenosa podatkov večja tudi *jitter*, vendar je zaradi opisanega pojava preveč odstopanj, zato smo pri nadaljnji analizi rezultatov *jitter* izpustili.

Anomalije se opazijo tudi pri rezultatih merjenj deleža izgubljenih paketov in hitrosti prenosa podatkov, kadar strežnik prejema podatke z enako hitrostjo, kot jih generira odjemalec. V omenjenem primeru je izmerjena hitrost prenosa podatkov celo večja kot generirana hitrost prenosa podatkov. Pojav je prikazan na sliki 5.2 in označen v tabelah z zvezdico (*) ob vrednosti. Na sliki 5.2 vidimo, da je čas generiranja podatkov enak 30 s, čas prejemanja podatkov pa le 27,2 s. Ker je hitrost prenosa podatkov obratno sorazmerna s časom prenosa podatkov, je zaradi krajšega časa na strežniku izmerjena hitrost prenosa podatkov večja kot generirana hitrost. Zaradi enakega razloga zaznamo izgubljene pakete, čeprav sta generirana in izmerjena hitrost prenosa podatkov enaki (ali pa je izmerjena celo višja). Glede na to, da se pri nizkih generiranih hitrostih prenosa podatkov (pri katerih se opazita omenjena pojava) prenese manj podatkov oziroma paketov, odstopanja toliko bolj pridejo do izraza.

Opozoriti je treba, da je pri scenariju 3 in scenariju 4 program *Iperf* kljub ukazu *-b100M* generiral podatke proti brezžični postaji s hitrostjo 50 Mbit/s, zaradi česar smo rezultate iz tabel 5.6 in 5.8 umaknili. Najverjetneje je do tega prišlo zaradi prevelike izgube podatkov.

	generirana hitrost prenosa podatkov [Mbit/s]						
	5	10	20	30	40	50	100
izm. hitr. pod. [Mbit/s]	5,03*	10,03*	20,1*	29,9	33,3	33,3	33,2
jitter [ms]	0,05	0,08	0,04	0,12	0,13	0,25	0,49
izgubljeni paketi [%]	0	0,01	0,11	0,07	16	30	62

Tabela 5.1: Rezultati meritev prometa UDP od STA-A proti STA-S pri scenariju 1. Z zvezdico (*) so označene anomalije, ki so opisane v podpoglavju 5.1.

	generirana hitrost prenosa podatkov [Mbit/s]						
	5	10	20	30	40	50	100
izm. hitr. pod. [Mbit/s]	5,02*	10,1*	20,1*	28,7	28	27,6	28,1
jitter [ms]	0,11	0,07	0,21	0,12	0,32	5,87	2,76
izgubljeni paketi [%]	0,16	0,21	0,17	3,2	29	43	71

Tabela 5.2: Rezultati meritev prometa UDP od STA-S proti STA-A pri scenariju 1. Z zvezdico (*) so označene anomalije, ki so opisane v podpoglavju 5.1.

5.2 Rezultati pri scenariju 1

S tem scenarijem želimo preveriti delovanje dostopne točke v idealnih pogojih, brez motenj preostalih dostopnih točk.

Tabela 5.1 prikazuje rezultate, ki smo jih dobili ob pošiljanju podatkov od brezžičnega omrežja (STA-A) proti ožičenemu omrežju (STA-S).

Iz tabele 5.1 je razvidno, da program brez težav pošilja podatke proti ožičenemu omrežju do generirane hitrosti 30 Mbit/s. Pri višjih generiranih hitrostih začne izgubljati podatke. Opazimo, da se izmerjena hitrost prenosa podatkov ustali pri 33,3 Mbit/s, kar prikazuje pasovno širino našega omrežja.

Tabela 5.2 prikazuje rezultate, ki smo jih dobili ob pošiljanju podatkov od ožičenega omrežja (STA-S) proti brezžičnemu omrežju (STA-A).

Opazimo, da se pri pošiljanju podatkov proti postaji v brezžičnem omrežju

	generirana hitrost prenosa podatkov [Mbit/s]						
	5	10	20	30	40	50	100
izm. hitr. pod. A [Mbit/s]	4,81	5,89	6,1	6,07	5,57	6,33	5,86
izm. hitr. pod. B [Mbit/s]	4,91	6,13	6,06	6,12	6,25	5,89	6,08
jitter A [ms]	2	1,19	0,89	0,98	2,17	0,97	3,13
jitter B [ms]	1,28	3,17	0,96	0,10	3,01	3,01	1,74
izgubljeni paketi A [%]	2,6	37	65	79	85	87	94
izgubljeni paketi B [%]	1,8	33	65	79	83	90	93

Tabela 5.3: Rezultati meritev prometa UDP proti STA-S pri scenariju 2.

(STA-A) pojavijo nekoliko večje izgube paketov (3,2 %) že pri generirani hitrosti 30 Mbit/s. Izmerjena hitrost prenosa podatkov je tako ustaljena pri 28,1 Mbit/s, kar je 5,2 Mbit/s (15,6 %) manj kot pri pošiljanju podatkov v drugo smer. S tem smo dobili izhodiščne rezultate, na podlagi katerih bomo lahko opazovali vpliv preostalih dostopnih točk.

5.3 Rezultati pri scenariju 2

S tem scenarijem opazujemo vpliv sočasnega delovanja dveh dostopnih točk na istem kanalu na prepustnost posameznega omrežja.

Tabela 5.3 prikazuje rezultate meritev od brezžičnega proti ožičenemu omrežju (STA-S). Rezultati obeh omrežij (A in B) so si zelo podobni. Kar pomeni, da dostopni točki do medija dostopata enakomerno. Ob podrobnejši analizi opazimo, da se izgube paketov pojavijo že pri generirani hitrosti podatkov 5 Mbit/s. Poleg tega se skupna izmerjena hitrost prenosa podatkov (vsota izmerjene hitrosti podatkov A in B) ustali pri povprečno 12,05 Mbit/s. To je samo 36,2 % izmerjene hitrosti pri scenariju 1. Iz tega lahko sklepamo, da sočasno oddajanje dveh dostopnih točk zmanjša prepustnost pri pošiljanju podatkov proti ožičenemu omrežju.

Ob pregledu rezultatov v tabeli 5.4, ki prikazuje meritve pri prometu

	generirana hitrost prenosa podatkov [Mbit/s]						
	5	10	20	30	40	50	100
izm. hitr. pod. A [Mbit/s]	5.02*	9.88	12.8	14	13,4	12,9	14,6
izm. hitr. pod. B [Mbit/s]	5.00	10	13.66	12,7	13,4	13,47	12,99
jitter A [ms]	0.13	0,17	1,43	0,56	1	1,8	1,01
jitter B [ms]	0.14	0,11	4,86	1,22	0,89	1,64	4,11
izgubljeni paketi A [%]	0.58	1.72	35.00	49	66	72	81
izgubljeni paketi B [%]	1.57	0,41	30.14	54	66	70	86

Tabela 5.4: Rezultati meritev prometa UDP od STA-S pri scenariju 2. Z zvezdico (*) so označene anomalije, ki so opisane v podpoglavju 5.1.

proti brezžični postaji, zopet opazimo, da so si rezultati obeh postaj (A in B) zelo podobni. S tem potrdimo, da dostopni točki enakomerno dostopata do medija oziroma, da si pasovno širino enakomerno razdelita. To je bilo tudi pričakovano, saj sta dostopni točki enaki in delujeta ob enakih pogojih.

Iz tabele 5.4 razberemo tudi, da se izgubljeni paketi pojavijo šele pri generirani hitrosti 20 Mbit/s in da se skupna izmerjena hitrost prenosa podatkov ustali pri 26,78 Mbit/s. To je 95,3 % izmerjene hitrosti prenosa proti brezžični postaji pri scenariju 1. Kar pomeni, da ima sočasna aktivnost dveh postaj na istem kanalu vpliv tudi na prepustnost proti brezžični postaji, vendar je ta veliko manjši kot pri meritvah podatkov poslanih žično povezani postaji.

Po pregledu rezultatov pri scenariju 2 smo ugotovili, da si enaki dostopni točki, ki sočasno oddajata na istem kanalu, razpoložljivo pasovno širino enakomerno razdelita. Ugotovili smo tudi, da ima ta scenarij občutno večji vpliv na skupno prepustnost obeh omrežij pri prometu proti žično povezani postaji, kot pri prometu proti brezžični postaji.

	generirana hitrost prenosa podatkov [Mbit/s]						
	5	10	20	30	40	50	100
izm. hitr. pod. A [Mbit/s]	4,89	4,8	5,34	5,73	5,47	5,11	6,11
izm. hitr. pod. B [Mbit/s]	5,01*	5,13	5,27	5,18	5,51	6,96	5,61
jitter A [ms]	0,67	0,62	1,31	1,29	0,98	2,96	2,24
jitter B [ms]	1,00	0,13	1,87	3,29	1,62	1,72	1,89
izgubljeni paketi A [%]	1,4	51	73	78	86	89	93
izgubljeni paketi B [%]	0,06	49	73	81	86	85	94

Tabela 5.5: Rezultati meritev prometa UDP proti STA-S pri scenariju 3. Z zvezdico (*) so označene anomalije, ki so opisane v podpoglavju 5.1.

5.4 Rezultati pri scenariju 3

Z uporabo različnih dostopnih točk želimo v scenariju 3 opazovati, ali na delitev razpoložljive pasovne širine med dostopni točki vpliva njun model.

Rezultati meritev v tabeli 5.5 so podobni rezultatom iz tabele 5.3, kar pomeni, da si dostopni točki zopet enakomerno razdelita razpoložljivo pasovno širino. Podobno je tudi povprečje skupne izmerjene hitrosti podatkov, pri kateri se ustalijo meritve, in sicer 10,89 Mbit/s. Rezultati nam ne povedo nič novega in z njimi zgolj potrdimo opažanja pri tabeli 5.3.

Veliko bolj nepričakovani pa so rezultati v tabeli 5.6, saj že na prvi pogled opazimo prevlado dostopne točke NETGEAR, ki je povezana z napravo STA-B. Poleg tega se je nekoliko povišala tudi skupna izmerjena hitrost prenosa podatkov, ki v povprečju znaša 29,37 Mbit/s, kar je za 9,6 % več kot v tabeli 5.4. Razlika sicer ni zelo velika, vendar dovolj, da smo jo lahko zabeležili.

Zanimivo je tudi videti, da si pasovno širino pri nizki obremenitvi enakomerno razdelita. Pri generiranih hitrostih 5 in 10 Mbit/s, ko skupno še ne presežeta razpoložljive pasovne širine, je to pričakovano. Vendar si enakomerno razdelita tudi pri generirani hitrosti 20 Mbit/s, ko skupna generirana hitrost prenosa podatkov skozi obe omrežji (40 Mbit/s) preseže najvišjo sku-

	generirana hitrost prenosa podatkov [Mbit/s]						
	5	10	20	30	40	50	100
izm. hitr. pod. A [Mbit/s]	4,99	9,98	9,25	4,1	4,2	4,7	/
izm. hitr. pod. B [Mbit/s]	4,99	10,1*	8,99	25,2	25,4	24,5	/
jitter A [ms]	0,13	0,32	1,85	2,5	3,5	2,22	/
jitter B [ms]	0,09	0,37	1,39	0,25	0,3	6,41	/
izgubljeni paketi A [%]	0,32	0,4	53	86	89	90	/
izgubljeni paketi B [%]	0,06	0,2	56	15	35	48	/

Tabela 5.6: Rezultati meritev prometa UDP od STA-S pri scenariju 3. Z zvezdico (*) so označene anomalije, ki so opisane v podpoglavju 5.1.

pno izmerjeno hitrost, pri kateri se ustalijo meritve (29,36 Mbit/s) za več kot 30 %. Izredno velike razlike pa se pojavijo pri večjih obremenitvah, pri katerih je izmerjena hitrost prenosa podatkov skozi omrežje NETGEAR v povprečju kar 25,03 Mbit/s, medtem ko ta v omrežju AP-A v povprečju znaša zgolj 4,3 Mbit/s. Po bolj natančnem pregledu zajetih paketov s programom *Wireshark* opazimo, kako se spreminja hitrost podatkov (angl. *data rate*) posameznih paketov. Na sliki 5.4 lahko vidimo, da se je v omrežju AP-A hitrost podatkov enega od paketov spustila do 18 Mbit/s, medtem ko je na sliki 5.5 razvidno, da je v omrežju NETGEAR (kamor je povezana STA-B) še vedno na privzeto nastavljenih 54 Mbit/s. Po pregledu preostalih zajetih podatkov (glej sliko 5.6) smo ugotovili, da se od časa do časa spremeni tudi podatkovna hitrost posameznega paketa v omrežju NETGEAR, vendar je ta pojav veliko redkejši in manj izrazit kot v omrežju AP-A. To pomeni, da omrežje NETGEAR prenaša podatke z večjo hitrostjo in prevzame večji delež pasovne širine.

S pomočjo scenarija 3 smo ugotovili, da ima model dostopne točke velik vpliv na zasedanje pasovne širine. Vendar se ta vpliv pozna zgolj pri prenosu podatkov od brezžične postaje proti žično povezani. Čeprav je model NETGEAR nekoliko starejši, ima drugačne privzete nastavitve ter drugačno

81...	0.000014002	192.168.0.10	192.168.0.6	UDP	1542 40445 → 5001 L...
81...	0.000008800		Cisco-Li_c1:e8:18 ...	802.11	28 Acknowledgemen...

▶ Present flags
 ▶ Flags: 0x00
 Data Rate: 18,0 Mb/s
 Channel frequency: 2462 [BG 11]
 ▶ Channel flags: 0x00c0, Orthogonal Frequency-Division Multiplexing (OFDM), 2 GHz spectru

Slika 5.4: Hitrost podatkov pri paketu, ki potuje skozi AP-A, prikazana v programu *Wireshark*.

81...	0.000351023	192.168.0.10	192.168.0.7	UDP	1544 33656 → 5001 L...
81...	0.000007334		Netgear_24:09:23 (...)	802.11	28 Acknowledgemen...
81...	0.000014002	192.168.0.10	192.168.0.6	UDP	1542 40445 → 5001 L...
81...	0.000008800		Cisco-Li_c1:e8:18 ...	802.11	28 Acknowledgemen...

▶ Present flags
 ▶ Flags: 0x00
 Data Rate: 54,0 Mb/s
 Channel frequency: 2462 [BG 11]
 ▶ Channel flags: 0x00c0, Orthogonal Frequency-Division Multiplexing (OFDM), 2 GHz spec

Slika 5.5: Hitrost podatkov pri paketu, ki potuje skozi NETGEAR, prikazana v programu *Wireshark*.

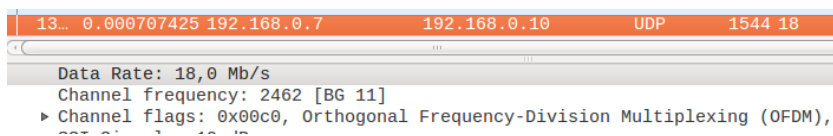
programsko in strojno opremo, kar privede do prevlade v omrežju in zasedanje večjega dela pasovne širine.

5.5 Rezultati pri scenariju 4

S scenarijem 4 skušamo ugotoviti, ali na prenos podatkov, pri sočasnem oddajanju dveh enakih dostopnih točk, vpliva oddaljenost dostopne točke oziroma moč signala, s katero brezžični vmesnik zazna dostopno točko.

Rezultati v tabeli 5.7 so zopet podobni rezultatom v tabelama 5.3 in 5.5. S tem lahko sklepamo, da moč signala ne vpliva na tok podatkov od brezžične do žično povezane postaje.

Iz tabele 5.8 je razvidno, da se pozna vpliv moči signala, saj je pri večjih obremenitvah delež uporabljene pasovne širine veliko bolj v prid omrežju dostopne točke AP-A (ki je bližje brezžičnim postajam). Povprečna skupna izmerjena hitrost prenosa podatkov znaša 25,31 Mbit/s, kar je zelo podobno scenariju 3 in scenariju 2. Vendar se v povprečju podatki do postaje STA-A



Slika 5.6: Ena od nizkih hitrosti podatkov pri paketu, ki potuje skozi AP-B, prikazana v programu *Wireshark*.

	generirana hitrost prenosa podatkov [Mbit/s]						
	5	10	20	30	40	50	100
izm. hitr. pod. A [Mbit/s]	4,8	5,39	5,6	5,55	5,78	5,65	5,91
izm. hitr. pod. B [Mbit/s]	5	6,55	6,23	5,31	5,05	5,65	5,49
jitter A [ms]	0,1	1,8	1,38	2,69	1,38	1,67	1,24
jitter B [ms]	1,14	1,1	1,98	1,58	3,99	0,84	2,41
izgubljeni paketi A [%]	4	47	72	80	85	88	93
izgubljeni paketi B [%]	0,01	35	70	86	87	88	94

Tabela 5.7: Rezultati meritev prometa UDP proti STA-S pri scenariju 4.

prenašajo s hitrostjo 18,52 Mbit/s, do postaje STA-B pa le s 6,78 Mbit/s.

Znova smo pregledali zajete pakete in opazili, da je hitrost podatkov (angl. *data rate*) posameznih okvirjev manjša od privzete 54 Mbit/s, pri večini paketov v omrežju postaje AP-B. Iz tega lahko sklepamo, da je postaja AP-B, katere signal je pri postaji šibkejši, zaradi povečane izgube podatkov zmanjšala hitrost pošiljanja podatkov po omrežju. S tem pa omogoči drugi dostopni točki, da uporabi večji delež pasovne širine.

S tem smo ugotovili, da tudi oddaljenost dostopnih točk od brezžičnih postaj vpliva na delitev uporabljene pasovne širine. Tako kot pri scenariju 3, se vpliv pozna le pri pošiljanju podatkov od ožičene proti brezžični postaji.

	generirana hitrost prenosa podatkov [Mbit/s]						
	5	10	20	30	40	50	100
izm. hitr. pod. A [Mbit/s]	4,98	9,83	20,1	20,8	14,1	19,1	/
izm. hitr. pod. B [Mbit/s]	4,87	10,05*	5,3	6,88	9,45	5,5	/
jitter A [ms]	0,61	0,54	4,41	1,42	0,64	1,62	/
jitter B [ms]	0,79	0,87	1,29	2,94	2,92	3,26	/
izgubljeni paketi A [%]	0,4	2,7	0,29	30	64	59	/
izgubljeni paketi B [%]	11	0,01	73	76	76	88	/

Tabela 5.8: Rezultati meritev prometa UDP od STA-S pri scenariju 4. Z zvezdico (*) so označene anomalije, ki so opisane v podpoglavju 5.1.

Poglavje 6

Zaključek

V sklopu diplomske naloge smo najprej razložili, kaj je brezžično omrežje, kako je sestavljeno in kako deluje. Opisali smo tudi načine dostopa do medijev, ki se uporabljajo pri brezžičnem omrežju.

V praktičnem delu diplomske naloge je bil cilj opazovati medsebojni vpliv brezžičnih usmerjevalnikov oziroma dostopnih točk, ki sočasno delujejo v istem frekvenčnem območju. V različnih scenarijih, ki predstavljajo situacije iz vsakdanjega življenja, smo opravljali meritve z uporabo protokola UDP s programom *Iperf*. Ob posebnih rezultatih meritev smo pregledali tudi pakete v omrežju, ki smo jih zajeli s programom *Wireshark*.

Najprej smo opazili, da se medsebojne točke ne dogovarjajo oziroma si ne rezervirajo medija, temveč za dostop do medija tekmujejo.

Nato smo ugotovili, da pri sočasnem delovanju dveh dostopnih točk na istem kanalu ti dve medsebojno vplivata druga na drugo. Hitrost, s katero lahko pošiljata podatke po omrežju, se obema zniža, saj si morata razdeliti razpoložljivo pasovno širino medija. Delež pasovne širine, ki jo dostopna točka uporablja, je odvisen tako od modela dostopne točke kot od moči signala dostopne točke, ki ga zazna povezana postaja. Z večjim deležem pasovne širine se v omrežju poveča hitrost prenosa podatkov in zmanjša delež izgubljenih paketov. V smeri pošiljanja podatkov od brezžične postaje do ožičene se je v vseh scenarijih skupna hitrost pošiljanja podatkov znižala za

več kot polovico izmerjene v scenariju 1, medtem ko je pri pošiljanju v drugo smer ostala enaka oziroma sprememba ni tako opazna. Dejavnika, kot sta model dostopne točke in zaznana moč signala, pri pošiljanju proti ožičeni postaji ne vplivata na hitrost prenosa. Močno pa vplivata pri prenosu podatkov od ožičene postaje proti brezžični. Pri različnih modelih se je ena od dostopnih točk (*Linksys WRT54GL 1.1*), zaradi velikih izgub v omrežju, podredila oziroma znižala hitrost podatkov (*data rate*), medtem ko je druga ostala pri privzeti hitrosti in tako uporabljala večji del pasovne širine. Enako se je zgodilo tudi pri sočasnem delovanju dveh enakih dostopnih točk, s tem da je bila ena bolj oddaljena in je zato postaja zaznala bolj šibek signal. V tem primeru se je podredila dostopna točka s šibkejšim signalom. Če sta dostopni točki enaki in delujeta pod enakimi pogoji, si pasovno širino razdelita enakomerno.

Ugotovili smo tudi, da so pri sočasnem pošiljanju podatkov proti ožičeni postaji s hitrostjo 10 Mbit/s izgube paketov že višje od 30 %, kar pomeni, da je omrežje neučinkovito. Pri pošiljanju podatkov v drugo smer se meja pri, kateri postane omrežje neučinkovito, premakne na 20 Mbit/s. Izjema je dostopna točka, ki je bližje postaji pri scenariju 4, kjer je delež izgube paketov pri generirani hitrosti prenosa podatkov 20 Mbit/s proti ožičeni postaji manjši od 1 %.

Cilj diplomskega dela je bil s tem dosežen, vendar bi se dalo raziskavo tudi izboljšati. Glede na to, da so bile meritve izrazito statistične, bi lahko opravili več meritev in jih izvajali dalj časa. Ena od izboljšav bi bila tudi uporaba dveh enakih računalnikov namesto virtualnih strojev ali boljšega računalnika, ki bi poganjal virtualne stroje. Namreč lahko se pojavijo odstopanja zaradi preobremenitve uporabljenega prenosnega računalnika, ki poganja dva virtualna stroja in program *Wireshark*. Možne so bile tudi motnje s signali drugih naprav, ki uporabljajo 2,4 GHz frekvenčno območje.

Poleg tega obstaja še veliko situacij iz vsakdanjega življenja, ki vplivajo na sobivanje dostopnih točk na istem kanalu. Zanimivo bi bilo primerjati še več različnih modelov dostopnih točk, raziskati, kako sobivajo dostopne točke,

ki uporabljajo PCF, kako sobivajo dostopne točke, ki omogočajo kakovost storitve (QoS), ter kako na sobivanje vplivajo različni standardi in frekvenčno območje 5 GHz.

Literatura

- [1] Dosegljivo: <http://www.hadyaiinternet.com/images/5ghz.jpg>. [Dostopano: 20. 8. 2017].
- [2] Norman Abramson. Ieee transactions on information theory. *Development of the ALOHANET*, 31(2):119–123, 1985.
- [3] Klemen Albret, Rudolf Sušnik, Jaka Sodnik, and Sašo Tomazič. Wlan - brezžična lokalna omrežja. Technical report, Fakulteta za elektrotehniko, Univerza v Ljubljani.
- [4] Introduction to wireless lan networks. Dosegljivo: <https://docs.microsoft.com/en-us/windows-hardware/drivers/network/introduction-to-wireless-lan-networks>, 2017. [Dostopano: 20. 8. 2017].
- [5] The european table of frequency allocations and applications in the frequency range 8.3 khz to 3000 ghz (eca table). Dosegljivo: <http://www.erodocdb.dk/docs/doc98//official/pdf/ERCREP025.PDF>, 2016. [Dostopano: 20. 8. 2017].
- [6] Cwap – 802.11 control frame types. Dosegljivo: <https://mrnciew.com/2014/10/02/cwap-802-11-control-frame-types/>. [Dostopano: 7. 7. 2017].
- [7] Enterprise Mobility 4.1 Design Guide. Dosegljivo: <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/>

- Mobility/emob41dg/emob41dg-wrapper.pdf, 2008. [Dostopano: 13. 7. 2017].
- [8] Certified wireless analysis professional official study guide. Dosegljivo: https://www.cwnp.com/wp-content/uploads/pdf/CWAP_WLAN_ANALYSIS.pdf, 2004. [Dostopano: 5. 8. 2017].
- [9] Dosegljivo: http://masters.donntu.org/2008/kita/handildi/library/oreilly/ch4_t1.png. [Dostopano: 25. 8. 2017].
- [10] Wireless network structure. Dosegljivo: <https://sites.google.com/a/ppcare.vn/it/security-pages/wireless-network-structure>. [Dostopano: 25. 8. 2017].
- [11] M.S. Gast. *802.11 Wireless Networks: The Definitive Guide: The Definitive Guide*. O'Reilly Media, 2005.
- [12] Alexandra Gunther. GETTING FAMILIAR WITH WI-FI CHANNELS? WLAN BACK TO BASICS. Dosegljivo: <https://boundless.aerohive.com/experts/WLAN-Channels-Explained.html>, 2015. [Dostopano 2. 7. 2017].
- [13] 802.11-2016. Dosegljivo: <https://standards.ieee.org/findstds/standard/802.11-2016.html>, 2016. [Dostopano: 5. 7. 2017].
- [14] Cisco unified wireless qos. Dosegljivo: <https://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/WANQoS.html>. [Dostopano: 25. 8. 2017].
- [15] Different Wi-Fi Protocols and Data Rates. Dosegljivo: <https://www.intel.com/content/www/us/en/support/network-and-i-o/wireless-networking/000005725.html>, 2017. [Dostopano: 9. 7. 2017].
- [16] Iperf. Dosegljivo: <https://openmaniak.com/iperf.php>, 2010. [Dostopano: 4. 8. 2017].

- [17] How 802.11 Wireless Works. Dosegljivo: [https://technet.microsoft.com/en-us/library/cc757419\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx), 2003. [Dostopano: 10. 7. 2017].
- [18] The OSI Model – What It Is; Why It Matters; Why It Doesn't Matter. Dosegljivo: <http://www.tech-faq.com/osi-model.html>, 2016. [Dostopano: 10. 8. 2017].
- [19] Multiple access. Dosegljivo: <http://onlinenotesandlectures.blogspot.si/2013/02/multiple-access.html>. [Dostopano: 25. 8. 2017].
- [20] P. Roshan and J. Leary. *802.11 Wireless LAN Fundamentals*. Cisco Press fundamentals series. Cisco Press, 2004.
- [21] Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements. Dosegljivo: <http://www.nortelcoelectronics.se/document-file5116?lclid=1053&pid=Native-ContentFile-File>, 2013. [Dostopano: 12. 7. 2017].
- [22] Virtualbox. Dosegljivo: <https://en.wikipedia.org/wiki/VirtualBox>, 2017. [Dostopano: 20. 8. 2017].
- [23] D.A. Westcott, D.D. Coleman, B. Miller, and P. Mackenzie. *CWAP Certified Wireless Analysis Professional Official Study Guide: Exam PW0-270*. IT Pro. Wiley, 2011.
- [24] Wireless. Dosegljivo: <https://en.wikipedia.org/wiki/Wireless>, 2017. [Dostopano: 5. 7. 2017].
- [25] Wireshark. Dosegljivo: <https://en.wikipedia.org/wiki/Wireshark>, 2017. [Dostopano: 3. 9. 2017].
- [26] Peter Šepetavc. Omrežje brez žic. Dosegljivo: <http://www.monitor.si/clanek/omrezje-brez-zic/121845/>, 2005. [Dostopano 2. 7. 2017].