

Dr Nataša Nešković

# **LOKALNE BEŽIČNE MREŽE**

AKADEMSKA MISAO  
Beograd 2017.

Dr Nataša Nešković

## LOKALNE BEŽIČNE MREŽE

prvo izdanje

*Recenzenti*

Prof. dr Irini Reljin  
Prof. dr Đorđe Paunović

*Izdavač*

AKADEMSKA MISAO  
Beograd

---

Odlukom Nastavno-naučnog veća Elektrotehničkog fakulteta u Beogradu broj 1456/3 od 05.03.2016. godine ova knjiga je odobrena kao nastavni materijal na Elektrotehničkom fakultetu u Beogradu.

---

*Štampa*

Akademski misao, Beograd

*Tiraž*

300 primeraka

ISBN 978-86-7466-641-8

---

NAPOMENA: Fotokopiranje ili umnožavanje na bilo koji način ili ponovno objavljivanje ove knjige u celini ili u delovima - nije dozvoljeno bez saglasnosti i pismenog odobrenja izdavača.

---

# SADRŽAJ

<b>1. UVOD</b> .....	<b>1</b>
<b>2. TOPOLOGIJA IEEE 802.11 MREŽE</b> .....	<b>3</b>
2.1. NEZAVISNI <i>BASIC SERVICE SET</i> .....	4
2.2. INFRASTRUKTURNI <i>BASIC SERVICE SET</i> .....	4
2.2.1. <i>Extended Service Set (ESS)</i> .....	5
2.3. QoS MREŽA.....	6
2.4. <i>MESH BASIC SERVICE SET</i> .....	7
2.5. WLAN MREŽA BAZIRANA NA KONTROLERU.....	8
2.6. LOGIČKA ARHITEKTURA IEEE 802.11 STANDARDA.....	8
<b>3. IEEE 802.11 MEDIUM ACCESS CONTROL SLOJ</b> .....	<b>10</b>
3.1. FORMAT MAC OKVIRA.....	12
3.2. PRIDRUŽIVANJE WLAN MREŽI I SINHRONIZACIJA.....	14
3.3. PRISTUP BEŽIČNOM MEDIJUMU.....	15
3.3.1. <i>Distributed Coordination Function (DCF)</i> .....	16
3.3.1.1. <i>Carrier Sense mehanizam</i> .....	17
3.3.1.2. <i>Inter Frame Space periodi</i> .....	19
3.3.1.3. <i>Collision Avoidance</i> .....	21
3.3.1.4. <i>Post backoff</i> .....	23
3.3.1.5. <i>Procedura oporavka i retransmisije</i> .....	24
3.3.2. <i>Point Coordination Function (PCF)</i> .....	24
3.3.3. QoS ograničenja 802.11 MAC.....	26
3.3.3.1. <i>QoS ograničenja DCF</i> .....	27
3.3.3.2. <i>QoS ograničenja PCF</i> .....	27
3.3.4. <i>Hybrid Coordination Function (HCF)</i> .....	28
3.3.4.1. <i>Enhanced Distributed Channel Access (EDCA) mehanizam</i> .....	28
3.3.4.2. <i>HCF Controlled Channel Access (HCCA)</i> .....	36
3.3.4.3. <i>Kontrola pristupa</i> .....	39
3.4. FRAGMENTACIJA PAKETA.....	41
3.5. POTVRĐIVANJE OKVIRA - <i>BLOCK ACKNOWLEDGMENT</i> .....	42
3.6. <i>ROAMING</i> .....	43
3.6.1. Proces <i>roaming</i> -a u IEEE 802.11 mrežama.....	44
3.6.1.1. <i>Probe kašnjenje (kašnjenje usled otkrivanja)</i> .....	47
3.6.1.2. <i>Kašnjenje prilikom autentifikacije</i> .....	48
3.6.1.3. <i>Kašnjenje usled reasocijacije</i> .....	48
3.6.2. Šeme za brzi <i>roaming (fast handoff)</i> .....	48
3.6.2.1. <i>Smanjenje probe kašnjenja</i> .....	48
3.6.2.2. <i>Smanjenje kašnjenja usled reautentifikacije</i> .....	52
3.6.2.3. <i>Kvalitativna analiza</i> .....	54
3.6.3. Problemi <i>roaming</i> -a.....	57
3.7. KONTROLA SNAGE.....	57
3.8. KONTROLA GREŠKI I DETEKCIJA DUPLIKATA.....	58

<b>4. IEEE 802.11 FIZIČKI SLOJ .....</b>	<b>59</b>
4.1. FHSS SPECIFIKACIJA FIZIČKOG SLOJA .....	60
4.2. DSSS SPECIFIKACIJA FIZIČKOG SLOJA .....	62
4.2.1. 802.11 DSSS .....	63
4.2.2. 802.11b standard - HR/DSSS .....	64
4.3. OFDM SPECIFIKACIJA FIZIČKOG SLOJA .....	65
4.3.1. 802.11g standard - <i>Extended Rate PHY</i> .....	65
4.3.2. 802.11a standard .....	67
<b>5. IEEE 802.11n STANDARD.....</b>	<b>69</b>
5.1. POBOLJŠANJA NA FIZIČKOM SLOJU .....	71
5.1.1. MIMO koncept .....	71
5.1.1.1. <i>Predajni beamforming</i> .....	72
5.1.1.2. <i>Prostorno multipleksiranje</i> .....	73
5.1.2. <i>Channel Bonding</i> .....	73
5.1.3. Kodno-modulacione šeme .....	74
5.1.4. Kraći zaštitni interval .....	74
5.1.5. Interoperabilnost 802.11a/g i 802.11n uređaja .....	75
5.2. POBOLJŠANJA NA MAC SLOJU .....	77
5.2.1. Agregacija .....	81
5.2.1.1. <i>MAC Service Data Units agregacija</i> .....	81
5.2.1.2. <i>MAC Protocol Data Unit agregacija</i> .....	83
5.2.2. <i>Block Acknowledgement</i> .....	84
5.2.3. <i>Reverse direction</i> protokol.....	85
5.2.4. Ušteda energije .....	85
5.2.4.1. <i>Spatial Multiplexing Power Save</i> .....	86
5.2.4.2. <i>Power Save Multi-Poll</i> .....	86
5.2.5. <i>Phased coexistence operation</i> .....	87
<b>6. IEEE 802.11ac STANDARD .....</b>	<b>89</b>
6.1. ORGANIZACIJA KANALA .....	90
6.1.1. Statički i dinamički pristup kanalu .....	92
6.1.2. RTS/CTS mehanizam .....	93
6.2. MIMO TEHNOLOGIJA .....	94
6.2.1. <i>Single-User MIMO</i> .....	94
6.2.2. <i>Multi-User MIMO</i> .....	95
6.2.3. <i>Predajni beamforming</i> .....	96
6.3. DODATNA POBOLJŠANJA NA FIZIČKOM I MAC SLOJU .....	97
6.3.1. Kodno-modulacione šeme .....	97
6.3.2. Agregacija okvira .....	98
<b>7. IEEE 802.11ad STANDARD.....</b>	<b>99</b>
7.1. IEEE 802.11ad USMERENE KOMUNIKACIJE .....	101
7.2. IEEE 802.11ad FIZIČKI SLOJ .....	102
7.3. IEEE 802.11ad ARHITEKTURA MREŽE .....	103
7.3.1. <i>Beacon</i> interval.....	103
7.3.2. <i>Personal Basic Service Set (PBSS)</i> .....	105
7.4. 802.11AD <i>MEDIA ACCESS CONTROL</i> SLOJ.....	105
7.4.1. Pristup medijumu na principu „takmičenja“ .....	106
7.4.2. Dinamička dodela resursa .....	106
7.4.3. Raspodela resursa po TDMA principu .....	108
7.5. 802.11AD <i>BEAMFORMING</i> KONCEPT .....	108
7.5.1. <i>Sector Level Sweep</i> faza .....	108
7.5.2. <i>Beam Refinement Procedure (BRP)</i> faza.....	111
7.5.3. 802.11ad <i>beamforming</i> protokol.....	112
7.5.3.1. <i>Association beamforming trening</i> .....	113
7.5.3.2. <i>Beamforming trening u Data Transmission Interval-u</i> .....	114

<b>8. WLAN MESH MREŽE.....</b>	<b>115</b>
8.1. ARHITEKTURA IEEE 802.11s MREŽE.....	115
8.2. FORMAT MAC OKVIRA.....	116
8.2.1. <i>Frame Control</i> polje.....	117
8.2.2. <i>Mesh Control</i> polje.....	118
8.2.2.1 <i>Mesh Flags</i> polje.....	118
8.2.2.2 <i>Mesh Address Extension</i> polje.....	119
8.3. MCF KOORDINACIONA PROCEDURA.....	119
8.3.1. MCCA mehanizam pristupa.....	120
8.3.1.1. <i>MCCA Access Fraction (MAF)</i> vrednost.....	121
8.3.1.2. <i>MCCA Setup Request</i> okvir.....	121
8.3.1.3. <i>MCCA Setup Reply</i> okvir.....	122
8.3.1.4. <i>MCCAOP Advertisement</i> okvir.....	123
8.3.1.5. <i>MCCAOP Advertisement Request</i> okvir.....	125
8.3.1.6. <i>MCCA Teardown</i> okvir.....	126
8.3.1.7. <i>Rezervisanje MCCAOP intervala (MCCAOP setup procedura)</i> .....	126
8.3.1.8. <i>Oglašavanje MCCAOP parametara (MCCAOP Advertisement)</i> .....	128
8.3.1.9. <i>Poništavanje rezervacije MCCAOP intervala (MCCAOP teardown procedura)</i> .....	129
8.3.1.10. <i>Pristup bežičnom medijumu</i> .....	130
8.4. SINHRONIZACIJA I UŠTEDA ENERGIJE U MESH MREŽAMA.....	134
8.5. KONTROLA ZAGUŠENJA.....	134
8.6. BEZBEDNOST U MESH MREŽAMA.....	134
8.7. ODABIR PUTANJA U 802.11s MREŽAMA.....	135
<b>9. WLAN MREŽE SA KONTROLERIMA.....</b>	<b>137</b>
9.1. PREDNOSTI MREŽA BAZIRANIH NA WLC.....	139
9.1.1. Centralizovano postavljanje parametara AP uređaja.....	139
9.1.2. Sigurnost.....	139
9.1.3. Podešavanja u mreži - snage predajnika i radio kanali.....	140
9.2. CONTROL AND PROVISIONING OF WIRELESS ACCESS POINTS PROTOKOL.....	140
9.2.1. Osnove CAPWAP protokola.....	141
9.2.1.1. <i>CAPWAP kontrolne poruke</i> .....	142
9.2.1.2. <i>Korisničke poruke i njihova enkapsulacija</i> .....	142
9.2.1.3. <i>Dijagram stanja CAPWAP protokola</i> .....	142
9.2.1.4. <i>Prenos CAPWAP poruka</i> .....	143
9.2.1.5. <i>Modovi procesiranja: SPLIT MAC i LOCAL MAC</i> .....	144
9.3. ARHITEKTURA MREŽA BAZIRANIH NA WLC.....	144
9.3.1. Arhitektura CUWN mreže.....	145
9.3.2. Fleksibilnost CUWN mreža.....	145
9.3.3. Robusnost CUWN mreža.....	145
9.3.3.1. <i>N:1 redundantna konfiguracija</i> .....	146
9.3.3.2. <i>N:N redundantna konfiguracija</i> .....	147
9.3.3.3. <i>N:N:1 redundantna konfiguracija</i> .....	147
9.3.4. Skalabilnost CUWN mreža.....	148
9.3.4.1. <i>Mobilnost u CUWN mrežama</i> .....	148
9.3.4.2. <i>Mobilne grupe</i> .....	149
9.5. WIRELESS CONTROL SYSTEM.....	152
9.6. ASPEKTI PROJEKTOVANJA MODERNIH WLAN MREŽA.....	153
9.6.1. 100 procentni bežični pristupni sloj.....	153
9.6.2. Potreba za većim zonama pokrivanja WLAN mreža.....	154
9.6.3. Stalna dostupnost i planiranje za slučaj kvara na nekom od uređaja.....	154
9.6.4. Ušteda potrošnje energije u WLAN mrežama.....	156
<b>10. SIGURNOST U WLAN MREŽAMA.....</b>	<b>157</b>
10.1. MEHANIZMI TAJNOSTI.....	157
10.1.1. Simetrično šifrovanje.....	158
10.1.2. Asimetrično šifrovanje.....	162
10.2. MEHANIZMI ZA OSTVARIVANJE INTEGRITETA.....	167
10.2.1. <i>Hash</i> funkcije.....	167
10.2.2. <i>Message Authentication Codes (MACs)</i> .....	167
10.2.3. Digitalni potpisi.....	169

10.3. UPRAVLJANJE KLJUČEVIMA .....	170
10.3.1. Digitalni sertifikati.....	171
10.4. AUTENTIFIKACIJA I PRIVATNOST.....	171
10.4.1. <i>Wired Equivalent Privacy</i> protokol.....	172
10.4.2. Standardizovani načini WEP autentifikacije .....	176
10.4.2.1. Open System autentifikacija .....	176
10.4.2.2. Autentifikacija korišćenjem deljenog ključa.....	177
10.5. ASOCIJACIJA.....	178
10.6. PROŠIRIVI AUTENTIFIKACIONI PROTOKOL.....	178
10.6.1. Tipovi autentifikacije.....	181
10.6.1.1. Lightweight Extensible Authentication Protocol ( <i>LEAP</i> ).....	184
10.6.1.2. Flexible Authentication via Secure Tunneling ( <i>EAP-FAST</i> ).....	185
10.6.1.3. Transport Layer Security ( <i>EAP-TLS</i> ).....	186
10.6.1.4. Autentifikacija lozinkom.....	186
10.6.1.5. Subscriber Identity Module ( <i>EAP-SIM</i> ).....	189
10.6.1.6. Message Digest 5 ( <i>EAP-MD5</i> ).....	190
10.7. GENERISANJE KLJUČEVA.....	190
10.7.1. Uspostava master ključa.....	190
10.7.2. Generisanje <i>Pairwise Transient Key</i> .....	191
10.7.2.1. Four-way handshake.....	191
10.7.3. Generisanje <i>Group Transient Key</i> .....	193
10.7.3.1. Group Transient Key two-way handshake.....	194
10.8. PROŠIRENJE IEEE 802.11 STANDARDA SA STANOVIŠTA SIGURNOSTI.....	195
10.8.1. <i>Temporal Key Integrity Protocol</i> (TKIP).....	195
10.8.2. <i>Counter Mode/CBC-MAC Protocol</i> (CCMP).....	197
10.8.3. <i>Wireless Protected Access</i> (WPA).....	198
10.8.4. <i>Wireless Protected Access 2</i> (WPA2).....	199
10.9. AUTORIZACIJA ADMINISTRATORA MREŽE.....	199
10.10. BRZI <i>ROAMING</i> .....	199
10.10.1. <i>Over-the-air</i> osnovni FT protokol.....	201
10.10.1. <i>Over-the-DS</i> osnovni FT protokol.....	202
<b>11. LITERATURA.....</b>	<b>204</b>

## 1. UVOD

Bežične lokalne računarske mreže (*Wireless Local Area Network*, WLAN) predstavljaju segment telekomunikacione industrije koji se razvija izuzetnom brzinom. Slično kao u slučaju standardnog LAN-a, bežična LAN tehnologija ima osnovnu namenu da obezbedi pristup servisima prenosa podataka na ograničenom prostoru. WLAN mreže su inicijalno razvijene kao alternativa za relativno visoke troškove instalacije i održavanja u žičanim LAN infrastrukturama (uzrokovane neprestanim proširivanjima i rekonfiguracijama sistema). Vremenom se pokazalo da bežični pristup pruža ogromne mogućnosti koje su se izuzetno dopale, kako privatnim, tako i poslovnim korisnicima. Kao dopuna fiksnim mrežama, prvenstveno omogućavaju mobilnost korisnika uz izuzetnu produktivnost i efikasnost u radu. Omiljena su opcija kada treba sačuvati lepotu enterijera starih građevina u kojima je polaganje kablova izuzetno otežano. Sve prethodno navedeno uslovalo je nagli razvoj WLAN mreža, tako da su u periodu od svega desetak godina zauzele značajno mesto u svetu modernih telekomunikacija.

Uzimajući u obzir usluge koje treba obezbediti, zahtevi korisnika bežičnih LAN mreža nisu ništa blaži nego što je to slučaj u žičanim LAN mrežama. Uspešno ispunjavanje tih zahteva zasnovano je, pre svega, na već postojećim protokolima i procedurama primenjenim u fiksnim mrežama, ali je upotpunjeno novim standardima baziranim na karakteristikama specifičnim za bežičnu tehnologiju. Neke od najvažnijih osobina WLAN mreža su:

- Prenos podataka vrši se bežično, korišćenjem radio talasa. Shodno tome, radio interfejs podrazumeva rad u odgovarajućem frekvencijskom opsegu.
- Obezbeđuju se veliki protoci podataka (od nekoliko desetina do nekoliko stotina Mb/s).
- Tipična zona koju pokriva jedna pristupna tačka WLAN mreže prečnika je od 100 do 300 m (u uslovima direktne optičke vidljivosti, pri čemu prepreke značajno smanjuju domete).
- Obezbeđuje se mobilnost korisnika uz kontinuitet ostvarene veze.
- Podržava se *roaming* između različitih delova mreže.
- Na strani mobilnih terminala zahteva se adekvatno baterijsko napajanje uz intenzivnu primenu tehnika kontrole snage.
- WLAN mreže su podložne interferencijama različitih tipova i izvora.
- Sigurnosna zaštita WLAN mreža je problem koji zahteva posebnu pažnju, jer su WLAN mreže veoma osetljive na narušavanje tajnosti i integriteta podataka.

IEEE 802.11 standard je donet 1997. godine kao rezultat rada 802 radne grupe. Standard specificira fizički sloj i *Medium Access Channel* (MAC) podsloj bežičnih lokalnih mreža. Podsloj kontrole logičkog linka, *Logical Link Control* (LLC), zajednički je za sve LAN mreže, što omogućava njihovu međusobnu povezanost.

Originalna verzija standarda propisala je primenu *Frequency Hopping Spread Spectrum* (FHSS) i *Direct Sequence Spread Spectrum* (DSSS) tehnika proširenog spektra, kao i rad u 2.4 GHz *Industrial, Scientific and Medical* (ISM) frekvencijskom opsegu, pri čemu je omogućen protok od 1-2 Mb/s.

Nakon dve godine (1999.), usvojene su dve nove verzije IEEE 802.11 standarda: IEEE 802.11b i IEEE 802.11a. Dok IEEE 802.11b standard podrazumeva primenu DSSS tehnike proširenog spektra, kao i rad u 2.4 GHz ISM frekvencijskom opsegu, IEEE 802.11a standard se bazira na *Orthogonal Frequency Division Multiplexing* (OFDM) tehnici i funkcionise u frekvencijskom opsegu oko 5 GHz. Pri tome, IEEE 802.11b standard omogućava maksimalni protok od 11 Mb/s, dok u slučaju IEEE 802.11a standarda maksimalni teorijski protok iznosi 54 Mb/s.

2003. godine usvojena je i treća modifikacija IEEE 802.11 standarda, IEEE 802.11g standard. Kao i IEEE 802.11b standard, navedeni standard koristi 2.4 GHz ISM frekvencijski opseg, ali se bazira na OFDM tehnici. IEEE 802.11g standard definiše maksimalni protok na fizičkom sloju od 54 Mb/s.

Sledeća verzija IEEE 802.11 standarda, IEEE 802.11n, usvojena je 2009. godine, pri čemu je u okviru nje uvedena i primena *Multiple Input Multiple Output* (MIMO) tehnologije. IEEE 802.11n standard koristi kako 5 GHz, tako i 2.4 GHz, frekvencijski opseg i u potpunosti je kompatibilan sa prethodnim verzijama standarda, IEEE 802.11a i IEEE 802.11b. IEEE 802.11n standard omogućava maksimalni teorijski protok od 600 Mb/s, dok se u praksi može postići protok koji je nešto veći od 100 Mb/s.

Ideja o bežičnim aplikacijama koje zahtevaju protoke do 1 Gb/s dovela je do razvoja novih amandmana IEEE 802.11 standarda, 802.11ac i 802.11ad. Maksimalni teorijski protoci koji su prema ovim standardima ostvarivi veći su i od protoka raspoloživih u žičanim *gigabit Ethernet* mrežama. Cilj IEEE 802.11ac standarda bio je dostići maksimalne protoke od najmanje 1 Gb/s na frekvencijskim opsezima ispod 6 GHz, isključujući opseg 2.4 GHz, dok je IEEE 802.11ad prvi standard u kome je predviđeno korišćenje frekvencijskog opsega 60 GHz sa ciljem ostvarivanja komunikacija u tzv. milimetarskom opsegu.

Mogućnost da dve mobilne stanice u okviru WLAN mreže, koje su međusobno van dometa, mogu da razmenjuju podatke preko jedne ili više bežičnih međustanica, koje imaju relejnu ulogu u prosleđivanju podataka, ostvarena je razvojem IEEE 802.11s standarda.

Sve veća primena WLAN mreža dovela je do potrebe za boljim radio pokrivanjem, sigurnošću i pouzdanošću. Kao i sa svakom drugom savremenom tehnologijom, primenjeni su brojni različiti pristupi radi unapređenja sveukupne funkcionalnosti WLAN mreža. Verovatno najbitniji napredak na ovom polju ostvaren je uvođenjem *Wireless LAN Controller*-a (WLC) koji su omogućili centralizaciju brojnih WLAN funkcija, čime je stvoren znatno fleksibilniji jedinstveni WLAN sistem, nasuprot prethodnih sistema sačinjenih od velikog broja samostalnih elemenata.

U toku višegodišnjeg razvoja IEEE 802.11 standarda i uređaja za realizaciju bežičnih mreža posebna pažnja posvećena je razvoju sigurnosnih procedura. Ostvareni nivo zaštite u lokalnim bežičnim mrežama može varirati od potpuno nezaštićene mreže do mreže koja je podložna samo najsofisticiranijim metodama narušavanja tajnosti i integriteta.

Svi prethodno navedeni standardi i specifikacije predstavljeni su u ovoj knjizi sa ciljem da se objasne osnovni principi funkcionisanja ovih danas veoma popularnih i važnih mreža.