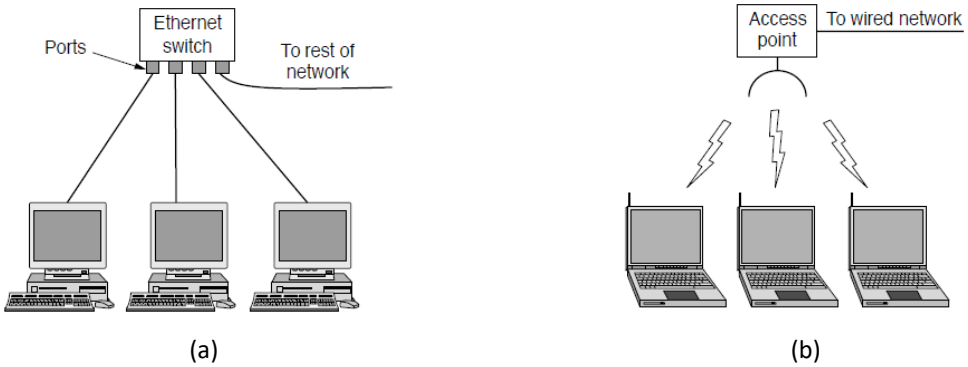
6 WLAN

Lokalna računarska mreža, ili LAN (*Local Area Network*) je privatna mreža koja pokriva manji, obično zatvoreni prostor, kao što je stan, kuća, zgrada, kancelarija ili fabrika (ili fakultet). Široko se koristi za povezivanje personalnih računara i drugih elektronskih uređaja, omogućavajući im da dele resurse (npr. štampače), razmenjuju informacije i pristupaju Internetu. Postoje dva načina izvođenja LAN mreže: žičani i bežični (WLAN). Ethernet mreža je danas najzastupljeniji žičani LAN (Sl. 1(a)). Najčešći način organizacije je zvezdasta topologija, sa centralnim uređajem tipa Ethernet *switch*, koji je *point-to-point* kablovima povezan sa ostalim uređajima u mreži (stanicama). Uloga *switch*-a je da usmerava saobraća između lokalnih stanica i ostvaruje vezu sa ostatkom mreže.

Bežična lokalna računarska mreža, ili WLAN (*Wireless Local Area Network*), je vrsta LAN mreže koja omogućava bežičnu komunikaciju između uređaja unutar ograničenog geografskog područja. U odnosu na žičani LAN, ulogu uređaja *switch* sada ima uređaj tipa *Access Point* (AP), a žičani kablovi su zamenjeni *point-to-point* bežičnim linkovima između AP i ostalih umreženih uređaja (Sl. 1(b)). Ova, danas sveprisutna tehnologija koristi bežične komunikacione protokole, kako bi omogućila povezivanje različitih uređaja, poput računara, pametnih telefona, i drugih, na lokalnom nivou bez potrebe za fizičkim kablovima. WLAN pruža fleksibilnost i mobilnost korisnicima, omogućavajući im, između ostalog, da se povezuju s Internetom bez fizičkog priključivanja na žičanu infrastrukturu. U većini slučajeva, WLAN mreža je zvezdaste topologije, sa AP-om u centru. Uloga AP je da prenosi pakete kako između samih bežičnih uređaja, tako i između bežičnih uređaja i Interneta.



Sl. 1 LAN: (a) žičani; (b) bežični, ili WLAN

Najzastupljeniji WLAN standard danas nosi oznaku IEEE 802.11. To je zapravo obiman set standarda, razvijen od strane međunarodne organizacije za standardizaciju IEEE, koji definiše specifikacije za implementaciju bežičnih lokalnih mreža. U širokoj upotrebi je skraćenica WiFi (*wireless fidelity*), koja zapravo prestavlja komercijalni naziv za bežične mreže koje su usklađene sa standardnom IEEE 802.11. WiFi mreže su u toj meri rasprostranjene da se skraćenica „WiFi“ često poistovećuje sa „WLAN“. Imajući u vidu značaj ovog standarda, u ovom poglavlju biće predstavljene samo osnovna funkcionalnost i karakteristike WiFi mreža.

Standard 802.11 pokriva dva najniža sloja OSI modela: fizički sloj (*Physical Layer*) i sloj veze (*Data Link Layer*). Fizički sloj obuhvata aspekte vezane za bežični prenos podataka, uključujući način na koji se podaci modulišu i prenose kroz bežični kanal. Sloj veze obuhvata specifične protokole koji se koriste

za upravljanje bežičnim vezama, uključujući MAC i LLC (*Logical Link Control*) protokole. Reč je o veoma kompleksnom standardnu koji ne samo što obuhvata mnoštvo funkcionalnosti, već i neprekidno evoluira prilagođavajući se tehnološkom napretku u oblasti bežičnih komunikacija. U tabeli ispod navedeno je nekoliko ključnih standarda u okviru 802.11 porodice (uz napomenu da su date približne vrednosti brzina prenosa podataka, jer stvarne mogu zavisiti od mnogo faktora, uključujući udaljenost od AP-a, prisustvo prepreka, broj uređaja na mreži i druge smetnje).

Oznaka	**Godina**	**Max. brzina**	**Opis**
802.11a	1999	54 Mbps	Definiše bežične mreže koje koriste frekvencije od 5 GHz. Pruža visoke brzine prenosa podataka, ali ima kraći domet u poređenju s nekim drugim standardima.
802.11b	1999	11 Mbps	Koristi frekvencije od 2.4 GHz i podržava niže brzine prenosa podataka u poređenju s 802.11a. Međutim, ima bolji domet.
802.11g	2003	54 Mbps	Funkcioniše na frekvencijama od 2.4 GHz i kombinuje elemente 802.11a i 802.11b. Pruža veće brzine od 802.11b.
802.11n	2009	od 72 od nekoliko stotina Mbps	Predstavlja unapređenje prethodnih standarda, podržava više antena i Multiple Input Multiple Output (MIMO) tehnologiju, obezbeđujući veće brzine i stabilniju vezu.
802.11ac	2013	nekoliko stotina Mbps do nekoliko Gbps	Radi na 5 GHz i donosi još veće brzine od 802.11n. Takođe podržava MIMO tehnologiju.
802.11ax	2021	nekoliko Gbps	Noviji standard koji donosi poboljšanja u efikasnosti mreže, upravljanju uređajima i povećava kapacitet WLAN-a.

6.1 Fizički sloj

U vezi fizičkog sloja, ovde će biti date samo osnovne informacije. Standard 802.11 ne definiše samo jedan, već nekoliko alternativnih fizičkih slojeva, koji se razlikuju prema frekventnom opsegu i tipu modulacije koja se koristi. Već u prvobitnoj specifikaciji standarda 802.11, predviđena su tri fizička sloja:

- Frequency-hopping spread-spectrum (FHSS) radio PHY
- Direct-sequence spread-spectrum (DSSS) radio PHY
- Infrared light (IR) PHY

U prethodnom nabrajanju, dati su originalni nazivi na engleskom jeziku, ali ipak lako možete prepoznati pojmove i tehnike koje su uvedene u poglavlju o MAC protokolima (PHY znači *Physical Layer* – fizički sloj). Izuzetak je treća opcija, IR, koja omogućava komunikaciju putem infracrvenog svetala (što, inače, u praksi nije ni zaživelo). Primera radi, kod FHSS, frekventni opseg širine $83.5\ MHz$ u bandu 2.4GHz podeljen je na 79 frekventnih kanala širine $1\ MHz$ (sa odgovarajućim razmakom). Reč je o sporom frekventnom skakanju, sa frekvencijom skakanja od samo $1Hz$ (frekventni kanal se menja svake sekunde). Sekvencu skakanja određuje AP i distribuira je svim uređajima, koji onda menjaju radnu frekvenciju u sinhronizmu sa AP. Ovaj standard koristi CSMA za kontrolu pristupa medijumu, pri čemu se sama procedura obavlja na trenutnom frekventnom kanalu. U novijim revizijama standarda 802.11, FHSS, kao i DSSS, je zamenjen naprednijim tehnikama koje omogućavaju brži prenos podataka uz smanjenu interferenciju, kao što su:

- 802.11a: Orthogonal Frequency Division Multiplexing (OFDM) PHY
- 802.11b: High-Rate Direct Sequence (HR/DS or HR/DSSS) PHY
- 802.11g: Extended Rate PHY (ERP)
- 802.11n: MIMO PHY (or the High-Throughput PHY)

6.1.1 OFDM

OFDM (*Orthogonal Frequency Division Multiplexing*) predstavlja osnovnu tehniku modulacije kod većine savremenih 802.11 standarda i ključnu je za postizanje visokih brzina prenosa podataka u WiFi mrežama. OFDM je napredna varijanta FDMA (prethodno poglavlje) tehnike, kod koje se široki frekventni opseg razlaže na veliki broj užih frekventnih podopsega, tzv. podnosioca (*subcarriers*). U svakom podopsegu se istovremeno emituje poseban noseći signal modulisan podacima. Umesto da se podaci prenose velikom brzinom na jednoj nosećoj frekvenciji, oni se dele na više paralelnih tokova koji se istovremeno prenose manjom brzinom na različitim nosećim frekvencijama, tj. podnosiocima. Ključna karakteristika OFDM-a je ortogonalnost između podnosioca. To znači da su frekvencije podnosioca matematički precizno razmešten tako da ne interferiraju jedan sa drugim, iako su frekvencijski vrlo blizu, što omogućava efikasno iskorišćenje dostupnog spektra.

Osnovne prednosti OFDM su: *a*) otpornost na interferencije, jer interferencija od drugih bežičnih ili elektronskih uređaja utiče samo na pojedinačne podnosioce, ali ne na sve. Čak i ako se neki podnosioce oštete, ostatak podataka može biti uspešno prenesen preko neoštećenih podnosioca; *b*) veća ukupna propusnost, jer istovremeno emitovanje na više frekventnih podnosioca omogućava značajno veću ukupnu propusnost u odnosu na tradicionalne tehnike sa jednim nosiocem; *c*) otpornost na feding, jer je intersimbolska interferencija manje izražena pri manjim brzinama prenosa. Primera radi, kod 802.11g, umesto da se prenosi jedan tok podataka brzinom $54\ Mbps$, prenos se deli na 48 podnosioca sa brzinom prenosa od oko $1.1\ Mbps$ preko svakog podnosioca. Zbog manje brzine prenosa, simboli traju duže, pa je time i intersimbolska interferencija manje izražena.

Prelaskom na OFDM brzina prenosa podataka u WiFi mreži je povećana sa maksimalno $11\ Mbps$, kod starijih na $54\ Mbps$ pa čak i više stotina $Mbps$, kod novijih varijanti. Međutim, OFDM je značajno složenija tehnika u poređenju sa recimo FHSS i DSSS, što znači da su potrebni sofisticiraniji RF transiveri. Uz to i utrošak energije je značajno veći.

6.1.2 MIMO

MIMO (*Multiple-Input Multiple-Output*) je još jedan koncept koji je bitan za poboljšanje performansi (brzina prenosa i otpornost na interferencije) fizičkog sloja savremenih 802.11 mreža. MIMO funkcioniše tako što koristi više antena za slanje i prijem signala na oba kraja komunikacije - i na predajniku i na prijemniku. Postoji nekoliko standardnih konfiguracija antena, označenih kao 2x2, 3x3, 4x4, itd., gde prvi broj označava broj predajnih antena, a drugi broj prijemnih antena. U konfiguraciji 2x2, moguće je istovremeno prenositi dva toka podataka između predajnika i prijemnika, što praktično udvostručuje brzinu prenosa u odnosu na sistem sa jednom antenom. U konfiguraciji 4x4, moguće je uporedo prenositi četiri toka podataka, što omogućava još veće brzine. Bitno je razumeti da svi MIMO tokovi koriste istu frekvenciju istovremeno. Ovo je moguće jer se koristi prostorno razdvajanje signala umesto frekventnog. Različiti tokovi podataka se razlikuju po prostornoj poziciji antena i prostornim kanalskim karakteristikama, što omogućava prijemniku da matematički izdvoji pojedinačne tokove iz "mešavine" signala.

MIMO može da radi u dva osnovna režima: prostorno multipleksiranje (*spatial multiplexing*) i prostorna raznovrsnost (*spatial diversity*). U režimu prostornog multipleksiranja, različiti i nezavisni tokovi podataka se prenose istovremeno preko različitih antena. Ovaj režim se koristi kada su uslovi prostiranja dobri (jak signal, malo smetnji) i prioritet je postizanje maksimalne brzine prenosa. Na primer, kod 2x2 MIMO konfiguracije, jedna antena šalje tok podataka A, dok druga antena istovremeno šalje potpuno različit tok podataka B. U režimu prostorne raznovrsnosti, isti podaci se prenose preko više antena istovremeno. Ovaj pristup se koristi kada su uslovi kanala loši (slab signal, puno smetnji) i prioritet je pouzdanost prenosa. Ako jedan signal stigne oslabljen zbog prepreka, drugi

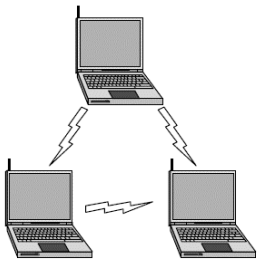
putevi mogu da kompenzuju, čime se poboljšava ukupna pouzdanost komunikacije. WiFi sistemi ne koriste oba režima istovremeno na istim podacima, već adaptivno biraju koji pristup da koriste na osnovu trenutnih uslova kanala. Sistem kontinuirano procenjuje kvalitet kanala i automatski menja strategiju u realnom vremenu. Kada su uslovi dobri koristi se prostorno multipleksiranje za maksimalnu brzinu; kada su uslovi loši, koristi se prostorna raznovrsnost za veću pouzdanost. MIMO u kombinaciji sa OFDM, omogućava veoma velike brzine prenosa podataka, koje dostižu $600\ Mbps$ (kod 802.11n), nešto preko $1\ Gbps$ (kod 802.11ac), do čak nekoliko $Gpbs$ (kod 802.11ax).

6.2 Arhitektura 802.11 mreže

Arhitektura 802.11 mreže je veoma fleksibilna i omogućava značajni nivo mobilnosti umreženih bežičnih uređaja i transparentu integraciju u žičanu LAN mrežu. Transparentnost je posledica stroge separacije između nižih nivoa protokol steka, fizički i sloj veze, koji su obuhvaćeni standardom 802.11, i viših nivoi (mrežni, transportni i viši). Uz to, 802.11 koristi istu 48-bitnu šemu adresiranja (MAC adrese) koja važi i za Ethernet LAN. Standard 802.11 predviđa dva načina povezivanja uređaja u bežičnu mrežu, ili dva režima rada: *ad hoc* režimi infrastrukturni režim. Pojmovi infrastrukturne i *ad hoc* mreže su uvedene u poglavlju o arhitekturama bežičnih mreže.

***Ad hoc* režim**

Ad hoc mreže (Sl. 2) su korisne za brzo i lako uspostavljanje bežične mreže svuda tamo gde mrežna infrastruktura (žičana ili bežična) nije dostupna ili nije praktična. Nalaze primenu u oblastima poput vojnih operacija, oporavka od katastrofa, hitna komunikacija i direktna komunikacije između uređaja. Nedostatak *ad hoc* mreža je taj što komunikacija ograničena samo na povezane uređaje, odnosno ne postoji mogućnost pristupa npr. Internetu. Podrška za formiranje *ad hoc* bežične mreže kod 802.11 je poznata kao IBSS (*Independent Basic Service Set*) i tipično se koristi za uspostavljanje direktne veze između uređaja, poput pametnih telefona, tableta, laptopova i štampača, radi deljenja fajlova, strimovanja audio/video sadržaja i drugih zadataka koji uključuju saradnju između više lokalnih uređaja. U slučaju kada IBSS sadrži više od dva uređaja, topologija formirane mreže je tipa *peer-to-peer* („svako sa svakim“) – podržana je samo *single-hop* komunikacija, odnosno rutiranje nije podržano. Ovo, naravno, podrazumeva da svi uređaji umreženi u IBSS, koliko god da ih je, moraju biti jadan drugom u radio dometu.



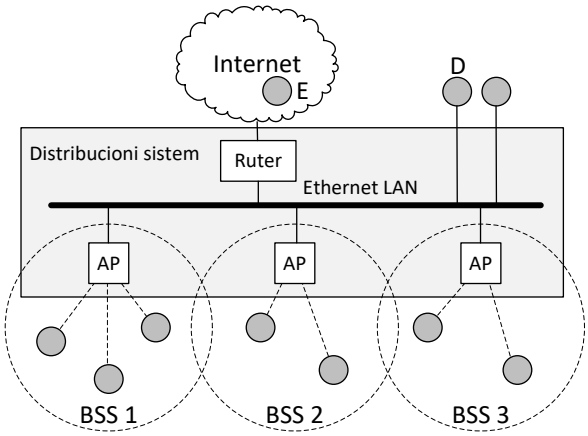
Sl. 2 *Ad hoc* WiFi mreža. Napomena: ilustrativniji primer je dat na Sl. 4 iz poglavlja 4

Infrastrukturni režim

Infrastrukturni režim, ili BSS (*Basic Service Set*) je najčešće korišćeni režim rada 802.11 mreže, koji omogućava povezivanje mrežnih uređaja (poput laptopova i pametnih telefona) sa drugom mrežom, kao što je LAN ili Internet (Sl. 1(b)). U ovom režimu, svaki mrežni uređaj (klijent) je pridružen jednom AP-u, preko koje se odvija sva komunikacija. BSS može biti izolovan, ili, posredstvom AP, povezan na pozadinsku mrežu (LAN), koja se u terminologiji standarda 802.11 naziva *distribucioni sistem* (*DS* –

Distribution System). Uređaji u okviru istog BSS ne komuniciraju direktno, već posredstvom AP. Ako uređaj A želi da pošalje paket uređaju B u istom BSS, uređaj A šalje paket AP-u, a AP prosleđuje paket uređaju B. Kada uređaj iz BSS šalje poruku udaljenom odredištu (npr. server na Internetu), uređaj šalje paket AP-u, koji ovaj, posredstvom DS, upućuje krajnjem odredištu. Slično, za komunikaciju u suprotnom smeru, paket koji udaljeni server šalje bežičnom uređaju, isporučuje se AP-u preko DS, a onda, AP, bežičnim putem, paket prosleđuje uređaju.

Bežična komunikacija je ograničenog dometa, što znači da jedna AP može da pokrije samo ograničeni fizički prostor, odnosno sa AP-om mogu da se povežu samo oni uređaji koji su u dometu radio komunikacije (npr. jedna ili nekoliko susednih prostorija u stanu/zgradi). Standard 802.11 takođe pruža mogućnost formiranja proširene 802.11 mreže (*ESS – Extended Service Set*), koja objedinjuje više BSS putem žičane mreže, tj. distribucionog sistema (Sl. 3). Distribucioni sistem je, po pravilu, Ethernet LAN mreža. Proširena 802.11 mreža omogućava komunikaciju između uređaja pridruženih različitim AP-ovima. Praktično, svi uređaji su deo iste mreže (istog LAN) iako je svaki uređaj povezan sa jednim, obično najbližom, AP-om. U ovakvom sistemu, svaki prenos paketa između uređaja iz različitih BSS, podrazumeva tri „skoka“: od izvornog uređaja do lokalne AP, između dve AP preko distribucionog sistema i između AP u drugom BSS i odredišnog uređaja.



Sl. 3 802.11 ESS (*Extended Service Set*). Mrežni uređaji su bežično povezani sa lokalnim AP-ovima; AP-ovi su međusobno umreženi putem LAN, koji između ostalog obezbeđuje pristup Internetu. *Napomena*: jedina razlika u odnosu na Sl. 3a iz poglavlja 4 je u tome što je pojam „infrastruktura bežične mreže“ zamenjen pojmom „distribucioni sistem“, zato što je ovo drugo usklađeno sa terminologijom iz standarda 802.11

Svaki mrežni uređaj ima svoju jedinstvenu 48-bitnu fizičku, tj. MAC adresu, koje se koriste kao identifikatori uređaja u komunikaciji na MAC nivou. MAC adrese su iste one koje se koriste kod Ethernet LAN, nepromenljive su i globalno jedinstvene. U suštini MAC adresa se dodeljuje mrežnom interfejsu uređaja. AP, po pravilu, ima dva mrežna interfejsa, jedan za bežičnu komunikaciju, i drugi, za Ethernet LAN. Ova dva interfejsa imaju svoje nezavisne MAC adrese. Uređaj koji ima samo interfejs za bežičnu komunikaciju, ima jednu MAC adresu.

Svaka infrastrukturna 802.1 mreža, bilo da je BSS ili ESS, ima svoj identifikator, tj. SSID (*Service Set Identifier*) – obično je to niz alfa-numeričkih znakova (tekst). Ovaj identifikator omogućava uređajima da prepoznaju i povežu se sa određenom bežičnom mrežom. SSID se definiše prilikom instalacije mreže, konfiguracijom AP-a (ili AP-ova, u slučaju ESS). U ESS mreži, svi AP-ovi, povezeni preko distribucionog sistema, su konfigurisani istim SSID.

Takođe, svaka AP ima svoj identifikator, tzv. BSSID (*Basic Service Set Identifier*), koji se koristi kao jedinstveni identifikator AP-a u okviru bežične mreže. BSSID se formira kombinovanjem MAC adrese bežičnog interfejsa AP-a i SSID mreže kojoj AP pripada. Na primer, ako je MAC adresa AP-a

01:23:45:67:89:AB, a SSID je *MyNetwork*, onda BSSID izgleda ovako: 01:23:45:67:89:AB_MyNetwork. Dakle, 801.12 bežična mreža (BSS ili ESD) ima svoj SSID, a svaki AP u toj mreži ima svoj BSSID.

6.3 Access Point

Uloga AP-a u infrastrukturnoj 802.11 mreži je višestruka i ključna za njeno funkcionisanje. Primarna funkcija AP je da premosti jaz između žičane i bežične mreže i omogući pridruženim bežičnim uređajima da, posredstvom žičane mreže komuniciraju sa udaljenim odredištima. Uz to AP organizuje komunikaciju uređaja u okviru mreži, upravlja pristupom medijumu i protokom podataka. Takođe, AP je odgovorna za sprovođenje bezbednosnih mera radi zaštite od neovlašćenog pristupa mreži, kao i zaštite samih podataka koji se prenose u mreži. U nastavku su detaljnije objašnjenje glavne funkcije AP-a.

6.3.1 Alokacija kanala

Savremene 802.11 mreže podržavaju rad u dva frekventna opsega, $2.4\ GHz$ i $5\ GHz$. U okviru svakog opsega postoji određeni broj frekventnih kanala, 14 u opsegu $2.4\ GHz$ i 20 u opsegu $5\ GHz$, mada precizan broj kanala može zavisiti od regulative u određenoj zemlji. Takođe, zbog preklapanja kanala, u opsegu $2.4\ GHz$ se, po pravilu, koriste samo tri: 1, 6 i 11. Izbor, ili alokacija kanala, je u nadležnosti AP-a. AP uvek radi na jednom kanalu, koji može biti podešen manuelno ili se bira automatski tokom inicijalizacije AP-a. U automatskom režimu izbora, AP analizira bežični medijum, detektuje prisustvo drugih 802.11 mreža i bira najmanje opterećeni kanal, kako bi se minimizovala potencijalna interferencija. Uz to, neki AP podržavaju i opciju dinamičke alokacije kanala, kada periodično, tokom rada, a ne samo tokom inicijalizacije, analiziraju bežični medijum i eventualno menjaju frekventni kanal.

6.3.2 Emitovanje bikona

U 802.11 bežičnim mrežama, bikon (*beacon*) predstavlja posebnu vrsta paketa koji AP periodično emituje (na primer, svakih $100\ ms$) kako bi okolnim uređajima oglasilo svoje prisustvo i preneo im osnovne sistemske parametre, o sebi i mreži. Drugim rečima, bikoni pomažu uređajima da otkriju prisustvo AP-a u svojoj okolini i pridruže se bežičnoj mreži. Format bikon paketa je definisan standardom 802.11 i tipično sadrži sledeće podatke (veoma skraćeni spisak):

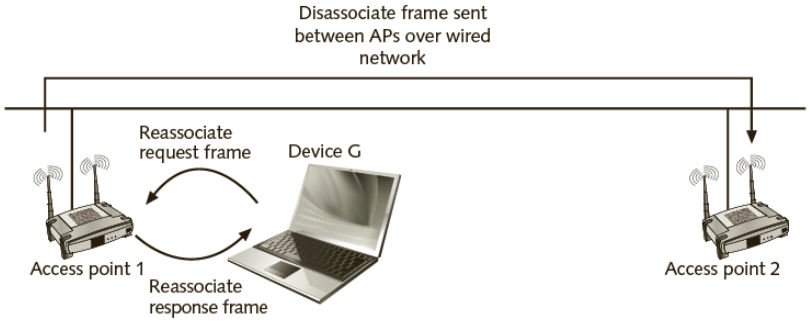
- *Timestamp*: vreme kada je bikon emitovan.
- *Bikon-interval*: perioda emitovanja bikona.
- *Karakteristike mreže*: Sadrži informacije o mogućnostima AP-a, podržanim standardima (npr. 802.11.ac), sigurnosnim merama, opcijama za uštedu energije, podršci za kvalitet servisa i drugim karakteristikama koje uređaji mogu koristiti za odabir optimalne mreže.
- *SSID*: identifikator bežične mreže.
- *BSSID*: identifikator AP-a
- *Frekventni kanal i vremenski parametri*: informacije o kanalu na kojem radi AP, kao i vremenskim parametrima za koordinaciju pristupa medijumu.
- *Bežična sigurnost*: informacije o podržanim tipovi enkripcije i autentifikacije
- *Energetska efikasnost*: informacije o metodama energetske efikasnosti i mogućnostima za uštedu energije koje podržava AP.

6.3.3 Asocijacija, reasocijacija, deasocijacija

Servis *asocijacije*, ili *pridruživanja* (*association*) omogućava mrežnim uređajima da se povežu sa AP-ovima. Uređaj koji nije povezan na mrežu, neprekidno skenira 802.11 frekventne kanale radi prijema bikona koje emituje obližnji AP, ili AP-ovi. Tokom skeniranja, uređaj povremeno menja frekventni kanal koji osluškuje (jer ne može unapred znati na kom kanalu radi AP). Servis asocijacije se pokreće odmah nakon što se uređaj nađe unutar radio dometa AP-a i primi AP-ov bikon. Putem bikona, uređaj saznaje identitet i mogućnosti AP-a, a nakon toga šalje zahtev za pridruživanje AP-u, koji ovaj može da prihvati ili odboje.

Servis *reasocijacije*, ili ponovnog pridruživanja, omogućava mrežnom uređaju da promeni AP. Ova mogućnost je korisna, pre svega, za mobilne uređaje i funkcioniše poput *handover* servisa u celularnim mrežama. Uređaj koji je pridružen nekom AP-u, neprekidno prati nivo (jačinu) signala koji AP emituje. Kada nivo signala padne ispod određenog praga, što ukazuje na to da se uređaj pomerio dalje od AP-a, uređaj počinje proces skeniranja, kako bi otkrio da li u okolini postoje drugi dostupni AP-ovi, beležeći pri tom njihove nivoe signala. Na osnovu rezultata skeniranja kao i nekih dodatnih kriterijuma (npr. trenutno opterećenje AP-ova i podržane brzine prenosa podataka), uređaj bira novi AP kome će se pridružiti. Uređaj šalje zahtev za reasocijaciju (*reassociate request frame*) izabranom AP, koji nakon toga odgovara potvrdom pridruživanja (*reassociate response frame*). Reasocijacija je transparentna za mobilni uređaj, u smislu da se obavlja u pozadini, automatski, i ako je korektno sprovedena, neće prouzrokovati gubitak podataka koji se, tokom ovog procesa, prenose ka ili od realociranog mrežnog uređaja.

Mrežnom uređaju je takođe na raspolaganju servis *deasocijacije*, ili razdruživanja, kojim raskida vezu sa AP-om. Uređaj bi trebalo da inicira deasocijaciju uvek pre nego što započne proces sopstvenog gašenja (*shutdown*), ili na zahtev korisnika koji želi da prekine mrežnu konekciju (npr. korisnik mobilnog telefona). Takođe, i AP bi trebalo da pre svog isključenja izvrši deasocijaciju svih trenutno pridruženih uređaja. Deasocijacija se, uz to, dešava i pri svakoj reasocijaciji, kada uređaj iz domena jednog prelazi u domen drugog AP u okviru istog ESS. Međutim, ovde postoji jedan problem, jer se može desiti da uređaj više nije u radio dometu AP od koje treba da se deasocira. Zbog toga zahtev za deasocijacju ne šalje sam uređaj, već AP s kojim se uređaj upravo asocirao i to preko distribucionog sistema (Sl. 4).



Sl. 4 Procedura reasocijacije. Uređaj koji je asociran sa AP2, traži reasocijaciju na AP1; AP1 potvrđuje zahtev i šalje zahtev za deasocijaciju AP1 (zato što uređaja više nije u radio dometu AP1)

6.3.4 Prenos podataka

AP aktivno učestvuje u prenosu podataka (to je zapravo njegov glavni zadatak), odnosno obezbeđuje servis *isporuke podataka* za pridružene uređaje. Uvek kada primi paket podataka od pridruženog uređaja, AP, u zavisnosti od krajnjeg odredišta paket, reemituje paket ka nekom drugom pridruženom uređaju, ili paket prosleđuje dalje preko distribucionog sistema. Takođe, AP emituje svaki paket koji

primi preko distribucionog sistema, a namenjen je nekom od pridruženih uređaja. Na primer, ako uređaj A želi da pošalje paket uređaju B, i oba su pridruženi istom AP-u, ova komunikacija se ostvaruje u dva koraka (skoka). Prvo, uređaj A šalje paket AP-u, a zatim AP prosleđuje paket uređaju B. Ako uređaj A šalje podatke nekom odredištu na Internetu, tada A šalje paket AP-u, a zatim AP, putem recimo LAN mreže, paket prosleđuje odredištu. U slučaju da udaljeno odredište šalje paket uređaju A, paket se isporučuje AP-u, a AP ga, bežičnim putem, prosleđuje uređaju A.

Treba istaći da 802.11 ne garantuje ispravan prenos (kao što to ne garantuje ni npr. Ethernet LAN). Servis isporuka podataka je, kaže se, *best effort service* (usluga maksimalnog napora) - raspoloživi resursi se koriste kako bi se obezbedila najbolja moguća usluga, ali bez garancije određenog nivoa performansi, pouzdanosti ili kvaliteta. Odgovornost za detekciju i ispravljanje grešaka u prenosu su odgovornost viših nivoa protokol steka (npr. TCP).

6.3.5 Sigurnost i privatnost

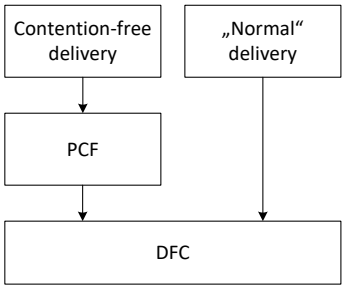
Mrežni uređaj, prilikom pridruživanja mreži, mora da dokaže svoj identitet AP-u, prolazeći kroz proces autentifikacije. Procedura autentifikacije nije jedinstvena, već zavisi od toga koja od više alternativnih sigurnosna šema se koristi u konkretnom sistemu. Standard 802.11 dopušta preskakanje ovog koraka, što mrežu čini otvorenom za sve zainteresovane korisnike (uređaje). Međutim, ako je autentifikacija uključena, tada uređaj (korisnik) mora da dostavi AP-u svoje podatke za pristup da njegov zahtev za pridruživanje ne bi bio odbijen.

Poseban deo standarda 801.11, poznat pod skraćenicom WPA2 (*Wi-Fi Protected Access* 2), posvećen je sigurnosti bežične mreže. Ovim delom standarda obuhvaćena je ne samo autentifikacija korisnika, već i zaštita od mrežnih napada i sigurnost u vezi integriteta podataka.

Ovde se nećemo dalje baviti ovom širokom i kompleksnom problematikom.

6.4 MAC

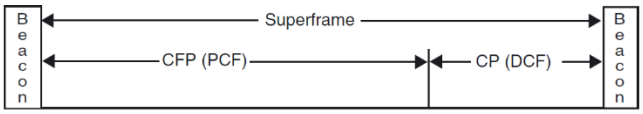
MAC sloj standarda 802.11 zasnovan je klasičnom CSMA/CA protokolu sa podrškom za RTS/CTS proceduru i NAV, uz brojna proširenja koja su doprinose većoj pouzdanosti prenosa podataka, manjoj potrošnji energije i obezbeđivanju zahtevanog kvaliteta servisa. Neka od ovih proširenja biće obrađena kasnije u okviru ove sekcije. Za CSMA/CA, sa svim ovim proširenjima, u standardu 802.11 se koristi naziv DCF (*Distributed Coordination Function*). DCF je zapravo podrazumevani režim rada 802.11 mreže, koji omogućava uređajima da deluju nezavisno, bez potrebe za bilo kakvim centralizovanim upravljanjem, tj. da se kroz nadmetanje stiču pravo pristupa medijumu. Standard takođe predviđa i opcioni režim rada – PCF (*Point Coordination Function*), kod koga pristupna tačka, tj. AP, upravlja svim aktivnostima u svojoj ćeliji, poput bazne stanice u celularnoj mreži. PCF se oslanja na DFC i obezbeđuje beskonfliktnu komunikaciju (Sl. 5), ali pošto ovaj način rada dobro može da funkcioniše samo u kontrolisanim uslovima, bez interferencije sa drugim mrežama, ipak se retko koristi u praksi.



Sl. 5 MAC sloj standarda 802.11. DCF je CSMA/CA sa RTS i NAV; PFC je nadogradnja DFC

Koegzistencija DCF i PCF

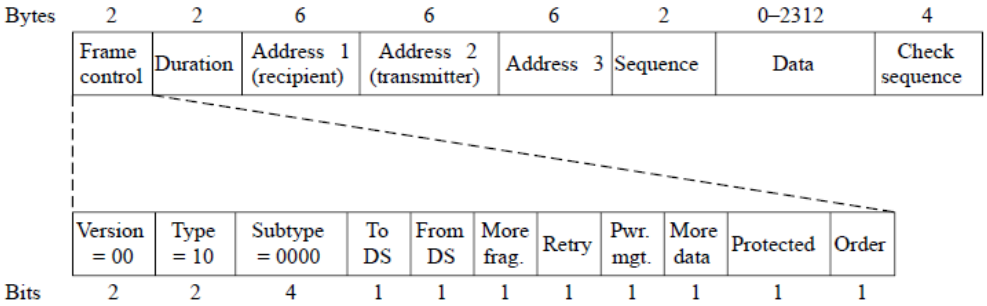
Standard 802.11 omogućava koegzistenciju DCF i PFC u istoj mreži. U tom slučaju, AP uspostavlja tzv. superfrejm (*superframe*). Superfrejm počinje bikon porukom, koju šalje AP, i sadrži dva vremenska intervala: period bez nadmetanja (*CFP - contention-free period*) i period za nadmetanje (*CP - contention period*), Sl. 6. U bikon poruci je sadržana informacija o trajanju CFP i CP intervala, tako da uređaji znaju kada koji interval počinje. Za kontrolu pristupa medijumu tokom CFP, koji je opcioni, koristi se PCF, dok se tokom CP koristi DFC (tj. CSMA/CA). PCF predstavlja režim rada gde AP preuzima punu kontrolu nad kontrolom pristupa medijumu. To znači da AP određuje redosled pristupa i vreme slanja za sve umrežene bežične uređaje. Naime, tokom CFP intervala, AP se sukcesivno obraća svim uređajima. U tom obraćanju, AP može uređaju da pošalje poruku podataka (ako ima takvu poruku) ili poruku prozivke (kojom pita uređaj da li ima poruku za slanje). Ako uređaj ima poruku za slanje, iskoristiće priliku da na nakon primljene prozivke to poruku i pošalje. Ovo omogućava pouzdaniji i deterministički pristup mreži za određene aplikacije koje zahtevaju nisku latenciju i stabilnost. PCF može da poboljša propusnost u mrežama sa velikim brojem uređaja; da smanji latenciju za uređaje sa strogim *real-time* zahtevima i da lako uvodi prioritete u komunikaciji. Međutim, iako pruža određene prednosti u smislu koordinacije pristupa, PCF nije u širokoj upotrebi i nije uključen u sve bežične mreže. Razlozi za to su složenost implementacije i ograničenja u smislu skalabilnosti i prilagodljivosti, a posebno nije efikasan u malim mrežama.



Sl. 6 Struktura superfrejma kod 802.11

6.4.1 Format paketa

Standard 802.11 definiše posebne tipove paketa za prenos podataka, upravljanje i menadžment mrežom. Paket bilo kog tipa se sastoji iz zaglavlja i tela. Zaglavlje obično sadrži mnoštvo polja od kojih svako nosi neki specifičan tip informacije. Kao primer, na Sl. 7 je prikazan format paketa podataka. Paket počinje zaglavljem koje sadrži šest polja ukupne dužine 24 bajta. Podaci koji se prenose su smešteni u delu „Data“. Kao što vidimo, paket može da prenosi najviše 2312 bajta podataka. Paket se završava 4-bajtnim poljem za proveru (CRC).



Sl. 7 Format paketa podataka kod 802.11

Značenje pojedinačnih polja u paketu podataka je sledeće:

- Polje „*Frame control*“: zaglavlje paketa podataka počinje poljem „*Frame control*“, koje je dalje podeljeno na 11 pod-polja:
  - Prvo pod-polje, „*Version*“, sadrži oznaku verzije formata. Aktuelna verzija je „00“.

- Polje „*Type*“ sadrži identifikaciju tipa paketa (da li je to paket podataka, upravljanja ili menadžmenta), a polje „*Subtype*“ identifikator pod-tipa u okviru izabranog tipa. Na primer, za regularne pakete podataka, u polju *Type* je binarna vrednost 10, a u polju *Subtype* vrednost 0000.
- Bitovi u poljima „*To DS*“ i „*From DS*“ predstavljaju indikaciju o tome da li paket dolazi iz distribucionog sistema (žičana mreža na koju je povezan AP), ili se šalju ka distribucionom sistemu. „*To DS*“ postavljeno na 1 znači da je paket namenjen uređaju van BSS-a i da AP treba paket da prosledi distribucionom sistemu; 0 znači da je paket namenjen uređaju u okviru BSS-a. Vrednost 1 u bit-polju „*From DS*“ znači da paket potiče od uređaja koji je van BSS-a, odnosno dolazi preko distribucionog sistema; 0 znači da paket potiče od uređaja iz BSS-a.
- Standard 801.11 podržava fragmentaciju (tj. podelu) veće poruke na više paketa (fragmenata) manje dužine, koji će se sukcesivno prenositi. Bit-polje „*More fragments*“, postavljeno na 1, predstavlja indikaciju da dati paket nije poslednji fragment u nizu fragmentiranih paketa. Vrednost 0 u ovom polju znači da je paket ili poslednji fragment u nizu, ili da je reč o nefragmentiranom paketu.
- Bit-polje „*Retry*“ označava da li je dati paket ponovno poslat (retransmitovan) ili ne. Ako je vrednost ovog polja postavljena na 1, to znači da je isti paket već jednom emitovan (ali bezuspešno). Vrednost 0 znači da je ovo prvi pokušaj slanja paketa.
- Bit-polje „*Power management*“, kada je postavljeno na vrednost 1, ukazuje da pošiljalac paketa ulazi u režim smanjene potrošnje.
- Bit-polje „*More data*“, ako je njegova vrednost 1, ukazuje na to da pošiljalac paketa ima još paketa za slanje istom primaocu.
- Bit-polje „*Protected Frame*“, ako je postavljeno na vrednost 1, ukazuje da je sadržaj datog paketa šifrovan radi sigurnosti.
- Bit-polje „*Order*“ ukazuju primaocu datog paketa da viši nivou protokol steka očekuju da im paketi iz niza paketa koji sledi budu isporučeni u striktnom redosledu kako su poslati.

- Polje „*Duration*“ sadrži informaciju o tome koliko će trajati transmisija paketa i njegove potvrde (ACK). Ovde je vreme izraženo u mikrosekundama. Polje „*Duration*“ je prisutno u svim tipovima paketa koje definiše standard 802.11. Informacija o vremenu transmisije se koristi za implementacije NAV mehanizma.
- Paket podataka sadrži tri adresna polja, svako dužine 6 bajta. Tumačenja adresa zavisi od konteksta, tj. od tipa paketa i vrednosti bit-polja „To DS“ i „From DS“ u polju „*Frame control*“, prema tabeli na Sl. 8.

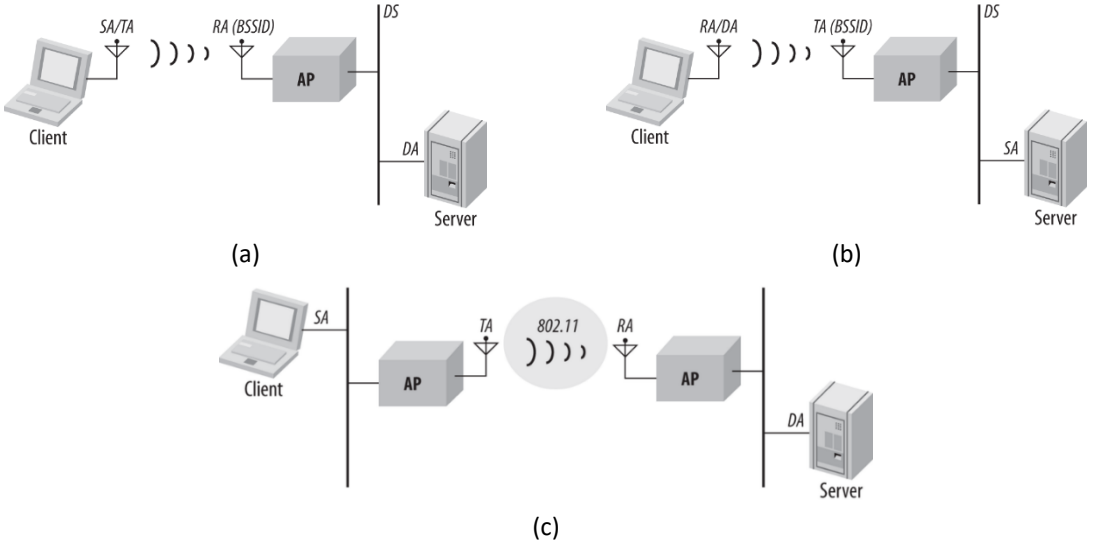
Bits: 2	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	Prot. Frame	Order

Frame Control field

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA = DA	TA = SA	BSSID	N/A
0	1	RA = DA	TA = BSSID	SA	N/A
1	0	RA = BSSID	TA = SA	DA	N/A
1	1	RA	TA	DA	SA

Sl. 8 Tumačenje adresnih polja u MAC paketu podataka u zavisnosti od flegova „To DS“ i „From DS“ iz polja „*Frame control*“. SA – MAC adresa izvora paketa; DA – MAC adresa odredišta paketa; TA – MAC adresa predajnika; RA – MAC adresa prijemnika; BSSID – MAC adresa AP-a

Polje *„Address 1“* sadrži adresu prijemnika paketa (RA), odnosno MAC adresu uređaja koji bežičnim putem treba da primi paket. Polje *„Address 2“* nosi adresu predajnika (TA), odnosno bežičnog uređaja koji emituje paket. Polje *„Address 3“* sadrži adresu izvora ili krajnjeg odredišta paketa. Na primer, na Sl. 9(a) i (b) je prikazana jednostavna mreža u kojoj bežični klijent komunicira sa serverom preko 802.11 mreže. Pretpostavimo da klijent šalje paket serveru (treća vrsta u tabeli). U ovom slučaju (Sl. 9(a)), klijent je ujedno i izvor paketa i predajnik paketa (jer emituje paket), AP prijemnik (prima paket i putem distribucionog sistema ga prosleđuje server) i server je odredište paketa. To znači da polje *„Address 1“* sadrži MAC adresu bežičnog interfejsa AP-a (BSSID), polje *„Address 2“* MAC adresu klijenta, a polje *„Address 3“* MAC adresa servera. Za suprotan smer prenosa (Sl. 9(b)), kada server šalje paket klijentu (druga vrsta u tabeli), izvor paketa je server, AP je predajnik, a klijent prijemnik i odredište paketa. U ovom slučaju, *„Address 1“* sadrži MAC adresu klijenta (jer je on sada prijemnik), polje *„Address 2“* MAC adresu AP-a (igra ulogu predajnika), i polje *„Address 3“* MAC adresu servera. Prva vrsta u tabeli se odnosi na *ad hoc* mreže, gde ne postoji AP, već mrežni uređaji direktno komuniciraju. U ovom slučaju, jedan uređaj je izvor i predajnik, a drugi odredište i prijemnik paketa. Pojedini paketi imaju i četvrto adresno polje, koje se koristi u specifičnom slučaju kada 802.11 mreža igra ulogu mosta između dva distribuciona sistema. U primeru na Sl. 9(c), izvor paketa je klijent, a odredište server; AP na strani klijenta je predajnika, a AP na strani servera prijemnik paketa.



Sl. 9 Tri scenarija za objašnjenje adresiranja u infrastrukturnoj 802.11 mreži: (a) klijent iz bežične mreže šalje paket serveru u žičanoj mreži (DS); (b) server iz žičane mreže šalje paket klijentu u bežičnoj mreži i (c) konfiguracija u kojoj dva AP premošćavaju dve žičane mreže

- Polje *„Sequence“* dužine dva bajta se koristi za brojanje, odnosno numeraciju paketa, kako bi se izbegli duplikati i omogućila rekonstrukcija fragmentiranih paketa na prijemnoj strani. Od 16 bita u ovom polju, prva 4 (*Fragment number*) identifikuju fragment, odnosno sadrže redni broj fragmenta, dok preostalih 12 nose ceo broj (*Sequence number*) koji se inkrementira za 1 sa svakim prenosom novog paketa. Dakle, ako je, na primer, duži paket podeljen na četiri kraća fragmenta, onda će u pod-poljima *„Fragment number“* fragmentiranih paketa biti redom upisane vrednosti: $0,1,2,$ i 3, dok će pod-polje *„Sequence number“* svih fragmenata nositi istu vrednost, npr. 2345. Sadržaj pod-polja *„Sequence number“* narednog paketa koji će emitovati taj isti uređaj imaće vrednost 2346. U slučaju retransmisije, sadržaj polja *„Sequence“* ostaje isti kao u originalnom paketu.

Potreba za fragmentiranjem postoji npr. kada treba preneti paket protokola višeg nivoa (recimo, IP datagram) koji je duži maksimalne dužine paketa koju podržava MAC sloj 802.11 mreže. Drugi razlog za fragmentaciju je u povećanju pouzdanosti prenosa (vidi sledeću sekciju).

- Polje „*Data*“ sadrži korisne podatke (*payload*), odnosno, tu je smešten paket protokola višeg nivoa. Maksimalna dužina polja „*Data*“ je 2312 bajta, uz napomenu da se prva 4 bajta u ovom polju koriste kao identifikacija protokola višeg nivoa kome su podaci namenjeni.
- Paket se završava 32-bitnim poljem za proveru, „*Check sequence*“. U ovo polje se smešta 32-bitna vrednost dobijena primenom CRC algoritma na celokupan sadržaj paketa. Prijemnik izračunava CRC primljenog paketa i upoređuje ga sa onim iz polja „*Check sequence*“. Podudarnost ove dve vrednosti ukazuje da je paket, sa veoma velikom verovatnoćom, primljen bez grešaka. U tom slučaju, prijemnik ima obavezu da pošalje predajniku ACK paket kao potvrdu uspešnog prijema. U suprotnom, ako primenjeni i izračunati CRC-ovi nisu isti, prijemnik zaključuje da u paketi ima grešaka i takav paket, prosto odbacuje (uništava), a o tome čak ni ne obaveštava više slojeve protokol steka, niti šalje ACK predajniku. Zbog izostanka ACK paketa, predajnik će ponoviti slanje istog paketa.

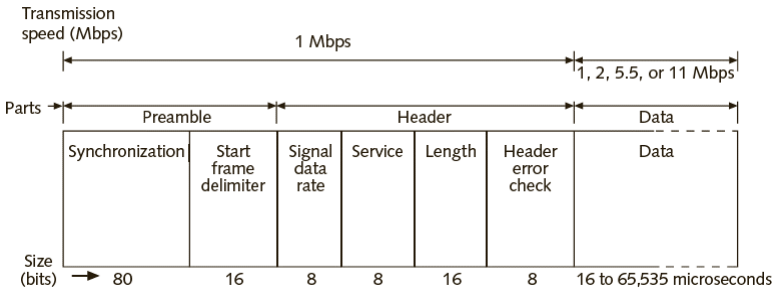
Prethodno je predstavljen format MAC paketa za prenos podataka. Paketi za menadžment mreže imaju sličan format u smislu da počinju zaglavljem nakon kojeg sledi polje za podatke. Neka polja u zaglavlju imaju isto, a neka različito značenje u odnosu na polja u paketu podatka. Primer menadžment paketa je bikon paket. Upravljački paketi (poput RTS, CTS i ACK) su kratki. I ovi paketi sadrže polja poput „*Frame control*“, „*Duration*“ i „*Check sequence*“, ali zato ne nose podatke i većina njih ima samo jedno polje za adresu.

Potrebno je još napomenuti da MAC paket nije i paket koji će se emitovati, već je on upakovan u paket fizičkog sloja. Paket fizičkog sloja ima svoje zaglavlje, a u njegovom delu za podatke je smešten MAC paket. Zaglavlje paketa fizičkog sloja nije univerzalno i zavisi od verzije 802.11 standarda. Na Sl. 10 je prikazano „fizičko“ zaglavlje po standardu 802.11b.

- Paket počinje tzv. preambulom koja se sastoji iz polja za sinhronizaciju, „*Synchronization*“ i polja za indikaciju početka paketa, „*Start frame delimiter*“. Sadržaj ova dva polja je uvek isti. Polje „*Synchronization*“ sadrži naizmenični niz 0 i 1, dok je u polju „*Start frame delimiter*“ prisutna bit-sekvenca „1111001110100000“. Naizmenični niz 0 i 1 služi prijemniku da sinhroniše svoj oscilator za frekvencijom dolaznog signala. Fiksna bit sekvenca u polju „*Start frame delimiter*“ označava početak paketa.
- Polje „*Signal data rate*“ sadrži informaciju o brzini prenosa kojom će se prenositi paket.
- Većina bita u polju „*Service*“ su rezervisana, tj. ne koriste se u trenutnim verzijama 802.11.
- Polje „*Length*“ sadrži informaciju o trajanju transmisije dela za podatke datog paketa. Vreme se izražava brojem vremenskih slotova trajanja 1 mikrosekunde. Opseg vrednosti u ovom polju je od 16 do 65535.
- „*Header error check*“ je polje za proveru. Vrednost u ovom polju se izračunava na osnovu sadržaja zaglavlja i ne obuhvata deo za podatke (koji ima svoje polje za proveru).
- U polju „*Data*“ smešteni su podaci koje se prenose datim paketom (MAC paket). Maksimalna dužina ovog polja 4095 bajta.

Bitno je istaći da se zaglavlje fizičkog paketa uvek prenosi brzinom od $1\ Mbps$, dok se deo za podatke može prenositi i višom brzinom, onom koja je navedena u polju „*Signal data rate*“. Na ovaj način, zaglavlje paketa će moći da prime svi uređaji u mreži, što je ključno za izbegavanje kolizija. Nedostatak je taj što uređaji koji podržavaju više brzine prenosa moraju stalno da menjaju podešavanja svojih

primopredajnika: $1\,Mbps$ dok se čeka na pojavu novog paketa u bežičnom medijumu, a onda prebacivanje na veću brzinu, ukoliko je paket namenjen tom uređaju.



Sl. 10 Paket fizičkog sloja po standardu 802.11

6.4.2 Pouzdanost prenosa

Bežični medijum, za razliku od žičanog, je u mnogo većoj meri podložan dejstvu šuma i interferencije od drugih uređaja, što značajno utiče na pouzdanost komunikacije. Upotreba paketa potvrde (ACK) i retransmisije nepotvrđenih paketa je od male pomoći ukoliko je verovatnoća prijema paketa sa greškom velika. Glavna strategija za povećanje stope uspešnosti prenosa je smanjenje brzine prenosa podataka. Pri manjoj brzini prenosa, energija po simbolu je veća, pa je veća i izvesnost da će, pri istom odnosu signal-šum, poslata informacija biti korektno primljena. Dakle, jedna strategija za povećanje pouzdanosti prenosa bi bila da mrežni uređaj, nakon što uoči veću stopu izgubljenih paketa, prosto, smanji brzinu prenosa podataka. Ukoliko se, u datim uslovima, paketi isporučuju bez grešaka, mrežni uređaj može, povremeno, da testira prenos pri većim brzinama prenosa i poveća brzinu ukoliko se test pokaže uspešnim.

Alternativna strategija za povećanje pouzdanosti prenosa je prenos u manjim paketima. Treba naglasiti da će paket biti odbačen na prijemu čak iako je greška u prenosu nastupila na samo jednom bitu. Pri istoj bitskoj stopi grešaka (BER), verovatnoća za gubitak paketa je manja što je paket kraći. Standard 802.11 omogućava fragmentaciju paketa, odnosno podelu paketa na manje delove fragmente. Fragmenti se prenose sukcesivno, jedan za drugim, kao posebni paketi, koji imaju svoje polje za proveru ispravnosti prenosa. Fragmenti se numerišu i nezavisno potvrđuju (ACK). U slučaju greške u prenosu, ponovo se prenosi samo fragment pogođen greškom. Naravno, fragmentacijom se povećavaju režijski troškovi (zato što svaki paket-fragment ima svoje zaglavlje), pa je s tim u vezi bitan kompromis između pouzdanosti prenosa, s jedne i potrošnje energije i žrtvovanja dela komunikacionog kapaciteta s druge strane.

Uticaj fragmentacije paketa na pouzdanost prenosa
Pretpostavimo da je verovatnoća da bit informacije bude prenet sa greškom jednaka p=10^{-4} (BER). To znači da će na prijemu, u proseku, svaki 10.000-ti bit biti pogrešan. Pretpostavimo da se prenose paketi najveće dužine koja je dozvoljene 802.11 standardom, tj. $N_{max} = 2384$ bajta. Verovatnoća da se ni na jednom bitu paketa ne pojavi greška jednaka je $(1-p)^{N_{max}} = 0.15$, odnosno, samo 15% paketa će se preneti bez greške, dok će preostalih 75% morati ponovo da se šalje. Međutim, ukoliko se paket podeli na četiri fragmenta, dužine 596 bajta, i svaki fragment se nezavisno prenosi, verovatnoća ispravno prenetog fragmenta će biti $(1-10^{-4})^{2384/4} = 0.94$, odnosno čak 94% svih fragmenat će biti ispravno preneto, dok će samo 4% morati ponovo da se šalje.

6.4.3 Upravljanje potrošnjom energije

Racionalno korišćenje raspoložive energije u savremenim komunikacionim sistemima je često u prvom planu, pre svega u mrežama mobilnih uređaja i distribuiranim embeded sistemima gde se uređaji

napajaju baterijom. Kod bežičnih uređaja, najveći potrošač energije je, po pravilu, upravo RF primopredajnik, koji troši energiju ne samo tokom emitovanja, već i dok je u režimu prijema i to bez obzira da li aktivno prima RF signal ili samo osluškuje kanal i čeka na početak transmisije. Uvođenje primopredajnika u režim smanjene potrošnje, kaže se i u režim spavanje, je jedini način kako se značajno može smanjiti njegova potrošnja energije. Međutim, u režimu spavanja, primopredajnik je praktično isključen, što znači da se može desiti da propusti paket koji mu se šalje. Rešenje ovog problema je u implementaciji mehanizama za upravljanje potrošnjom (*power management*), koji će omogućiti uređaju da smanjuju utrošak energije povremenim isključivanjem primopredajnika, ali na način da to ne dovede do propuštanja transmisija koje su njemu namenjene.

Standard 802.11 predviđa dva *power management* mehanizma. Zajedničko za oba mehanizma je da uređaj koristi bit "*Power Management*" iz polja "*Frame Control*" u MAC paketu kako bi obavestio AP o svom statusu, odnosno da li se nalazi u režimu smanjene potrošnje ili ne. Takođe, u oba slučaja, AP vodi evidenciju o tome koji uređaji su u stanju smanjene potrošnje i za sve takve uređaje privremeno baferuje pakete koji im stižu preko distribucionog sistema. U prvom mehanizmu, AP utiskuje u bikone (koje inače periodično emituje) tzv. mapu saobraćaja (*TIM - traffic indication map*) koja sadrži identifikatore (MAC adrese) svih uređaja za koje čuva pristigle pakete. S druge strane, uređaj, iako je u režimu smanjene potrošnje, budi se na kratko za prijem svakog bikona i proverava mapu saobraćaja. Ukoliko u mapi saobraćaja pronađe svoju adresu, uređaj šalje AP-u zahtev za isporuku baferovanih paketa. Nakon što primi pakete, uređaj ponovo uspavljuje svoj primopredajnik.

Drugi mehanizam za upravljanje potrošnjom, tzv. APSD (*Automatic Power Save Delivery*), veoma je sličan prethodnom. Razlika je samo u tome što AP umesto da baferovane pakete isporučuje uređaju na njegov (eksplicitni) upit, on mu ih isporučuje automatski, odmah nakon što od uređaja primi bilo koji paket. Ovo podrazumeva da uređaj, nakon slanja paketa, ostane još neko kraće vreme na prijemu kako bi primio paket koji će mu AP, eventualno, poslati. S obzirom da u ovoj šemi uređaj ostaje u stanju mirovanja sve dok ne dobije potrebu da pošalje (ili primi) podatke, ona je efikasna u primenama kada postoji učestali saobraćaj u oba smera (kao što je *VoIP – Voice over IP*).

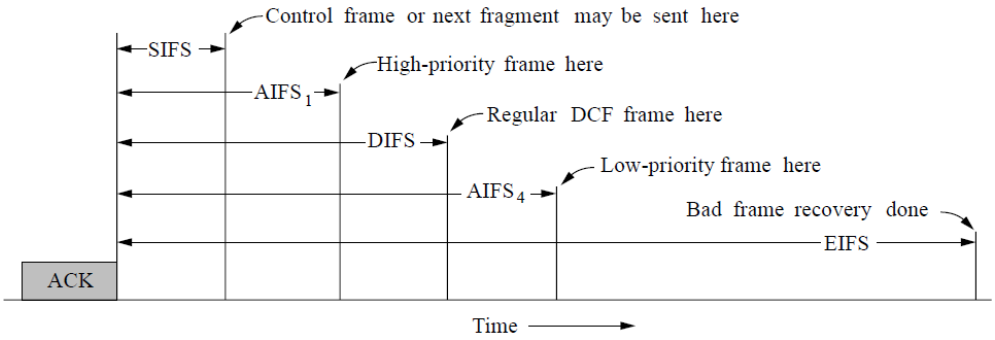
6.4.4 Upravljanje kvalitetom servisa

Kvalitet servisa (*QoS - Quality of Service*) je generalni pojam koji se odnosi na skup tehnika koji se koriste za pružanje određenog nivoa usluge ili kvaliteta u komunikacionim mrežama. Ovaj koncept fokusira se na garantovanje i poboljšanje karakteristika prenosa podataka, kao što su propusnost, kašnjenje, pouzdanost i druge, kako bi se ispunile specifični zahtevi aplikacija ili korisničkih usluga. Na primer, QoS je posebno bitan u primenama koje uključuju reprodukciju multimedijalnog sadržaja tokom preuzimanja (*streaming*).

U okviru standarda 802.11, podrška za QoS dolazi kroz mogućnost davanja višeg prioriteta u nadmetanju za pristup bežičnom medijumu paketima koji prenose kritične podatke. Mehanizam je veoma jednostavan i oslanja se na kašnjenja predviđena protokolom CSMA/CA nakon detekcije slobodnog kanala, tzv. IFS (*InterFrame Spacing Intervals*). Kao što znamo, uređaj, nakon što detektuje slobodan medijum, obavezno nastavlja s osluškivanjem medijuma tokom fiksnog vremena DIFS. Tek nakon što medijum ostane slobodan i nakon isteka ovog dodatnog osluškivanja, uređaj ulazi u *backoff* period. Takođe, prijemni uređaj ima obavezu da nakon prijema paketa podataka čeka obavezno fiksno vreme, odnosno SIFS, pre nego što pošiljaocu paketa pošalje ACK potvrdu.

Osim DIFS-a i SIFS-a, standard 802.11 uvodi još dva IFS-a, od kojih se jedan, AIFS (*Arbitration InterFrame Spacing*) koristi za regulisanje prioriteta u nadmetanju. Trajanje intervala AIFS nije fiksno već zavisi od konfiguracije mreže i specifičnih zahteva implementacije. Mrežni uređaji mogu da koriste

AIFS različitog trajanja, koje ne bi trebalo da bude kraće od SIFS[1]. Što je AIFS kraće, to će i prioritet uređaja u nadmetanju biti viši. Na primer, interval $AIFS_1$ na Sl. 11 je duži od SIFS, ali kraći od DIFS[2]. Mrežni uređaj koji, prilikom slanja podataka visokog prioriteta, umesto DIFS koristi $AIFS_1$ imaće veće šanse da dobije pravo pristupa medijumu od uređaja koji prenose redovni saobraćaj koristeći DIFS interval. Na primer, ako uređaj A koristi AIFS1, a uređaj B DIFS, A će prvi ući u *backoff* period i imaće veće šanse da dobije pristup medijumu od uređaja B. S druge strane, AIFS intervali koji su duži od DIFS-a (poput $AIFS_4$ na Sl. 11) namenjeni su uređajima koji prenose pozadinski saobraćaj niskog prioriteta, odnosno nižeg od prioriteta redovnog saobraćaja. U slučajevima kada se nadmeće više uređaja, oni koji koriste DIFS imaće veću šansu da prvi pošalju svoje podatke u odnosu na uređaje koji koriste $AIFS_4$. Interval EIFS (*Extended InterFrame Spacing*) nije u vezi sa QoS, već pomaže da se efikasnije prevaziđu situacije nakon prijema paketa sa greškom. Naime, kada uređaj primi paket sa greškom (CRC provera), on ne zna da li je taj paket bio paket podataka, ACK, RTS ili nešto drugo. Zbog toga ne može da odluči kada je bezbedno da ponovo pokuša slanje. Kako bi se izbegle kolizije sa odgovorom nekog drugog uređaja koji je ipak uspešno primio paket, uređaj tada koristi EIFS, koji je duži od uobičajenog DIFS-a.



Sl. 11 IFS (*Inter-Frame Spacing*) intervali kod 802.11

[1] SIFS (*Short InterFrame Spacing*) je najkraći vremenski interval između dva uzastopna prenosa. Koristi se kada nema nadmetanja, tj. kada je poznato da sledeći prenos treba da se desi odmah. Primer: kada prijemnik odgovara na paket slanjem ACK-a, ili šalje sledeći fragment. SIFS omogućava da odgovor (npr. ACK) stigne što je to brže moguće, bez čekanja, i ima prioritet nad ostalim saobraćajem. Uređaji koji samo pasivno slušaju medijum neće smeti da šalju ništa dok traje SIFS.

[2] DIFS (*Distributed InterFrame Spacing*) je duži vremenski interval i koristi se kada uređaj želi da inicira novu transmisiju. Nakon što detektuje da je medijum slobodan, uređaj mora da sačeka DIFS pre nego što krene u *backoff* proceduru. DIFS služi za pravljenje razmaka između nezavisnih prenosa u mreži i obezbeđuje da se SIFS-prioritetni odgovori završe pre nego što novi uređaj pokuša da šalje.

6.5 Vodič za učenje

- Pojam LAN-a. Razlike između žičanog i bežičnog LAN (WLAN) – Sl. 1
- Uopšteno o IEEE 802.11. Nije potrebno da pamtite podatke iz tabele, već samo da imate uopštenu predstavu o evoluciji ovog standarda i napretku u brzini prenosa

Fizički sloj

- Nije potrebno pamtiti nazive fizičkih slojeva i revizije standarda u kojima su uvedeni. Takođe, opisa FHSS nije potrebno detaljno učiti (to je samo informativno).
- Potrebno je znati šta je to OFDM i MIMO, ali samo do nivoa koji je dat u materijalu.

Arhitektura 802.11 mreže

- IBSS (*ad hoc*), BSS i ESS konfiguracije. Princip, osnovne karakteristike, ograničenja i mogućnosti svake konfiguracije. Uloga distribucionog sistema kod BSS i ESS.
- SSID i BSSID

Access Point

- Alokacija kanala. Kako AP bira frekventni kanal.
- Emitovanje bikona. Nije neophodno da pamtite sve podatke koji su sadržani u bikon poruci, ali bi trebalo da znate koja je uloga bikon poruke i koju vrstu informacija nosi.
- Asocijacija, reasocijacija, deasocijacija. Trebalo bi da znate generalne procedure koje su vezane za ova tri servisa. Reasocijacija u ESS mreži (Sl. 4)
- Prenos podataka, sigurnost i privatnost. Samo informativno. (Prenos podataka je obuhvaćen prethodnim tekstom)

MAC

- DFC i PCF, generalno.
- Koegzistencija DCF i PCF. Superfrejm. Osnovni način rada PCF.
- Napomena: DCF je zasnovan na CSMA/CA sa RTS/CTS i NAV, što bi trebalo da se zna iz prethodnog poglavlja
- Format MAC paketa
    - Nije potrebno da pamtite detalje formata (Sl. 7), odnosno dužine polja i njihov redosled u paketu.
    - Potrebno je da znate značenja i uloge pojedinih polja, kao i prateće mehanizme: adresiranje (Sl. 9 i prateća objašnjenja), fragmentacija paketa, CRC
    - Format paketa fizičkog sloja. Značenje pojedinih polja, ali ne i njihove dužine i redosled. Napomena o brzini prenosa podataka.
- Pouzdanost prenosa. Dva načina za povećanje brzine prenosa.
- Upravljanje potrošnjom energije. Princip rada *power management* mehanizma kod 802.11.
- Upravljanje kvalitetom servisa. Šta je to QoS. Koji mehanizam za QoS se primenjuje na MAC nivou - AIFS.

- ♦ ♦ ♦ -