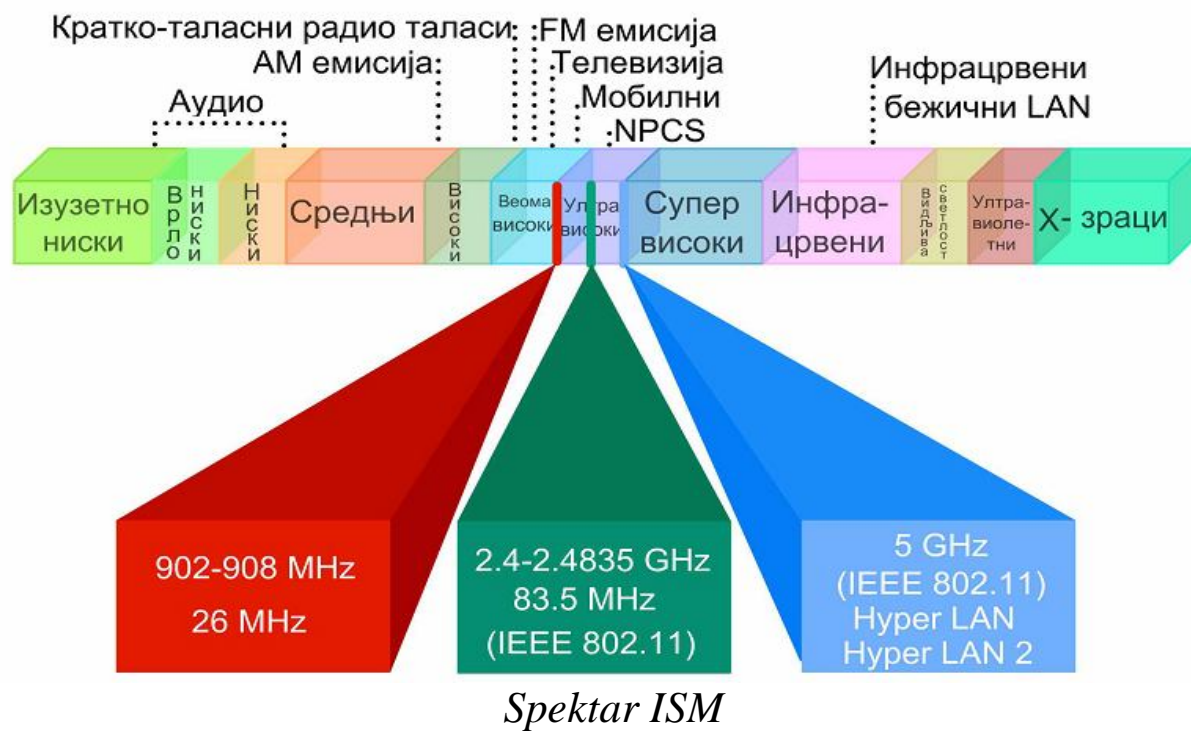


Bežične mreže: IEEE 802.11 standard

Prvi eksperiment bežičnog povezivanja računara realizovan je 1970. godine u laboratorijama IBM-a u Švajcarskoj. Ta računarska mreža zasnivala se na prenosu u infracrvenom delu spektra. Iste godine i Hewlett-Packard oformio je svoju bežičnu računarsku mrežu koristeći radio-talase. Brzine koje su dostignute bile su 100 kb/s, ali nijedan od tih proizvoda nije doživeo komercijalnu primenu. Razvoj bežičnih mreža nastavlja se 1985. godine pošto je FCC odobrio korišćenje opsega radio-frekvencijskog spektra bez posebnih dozvola za potrebe industrije, naučnih istraživanja i medicine (ISM- *Industrial Scientific Medical*). Ovaj frekvencijski opseg obuhvata tri grupe frekvencija:

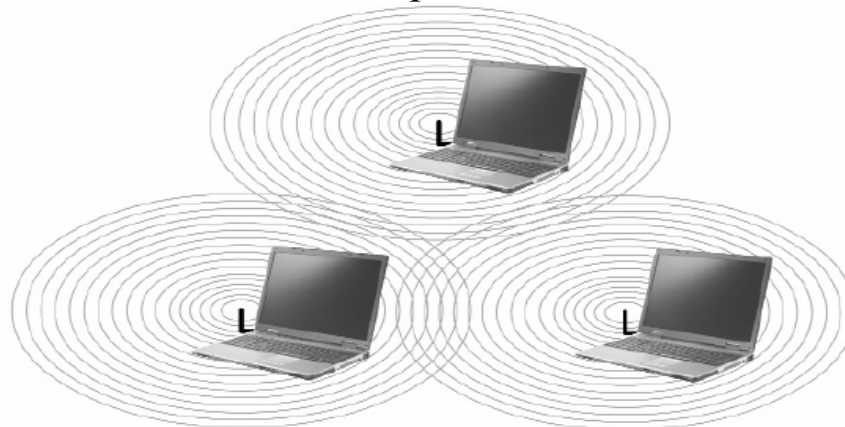
- 902 - 928MHz;
- 2,4 - 2,4835GHz
- 5,725 - 5,875GHz.



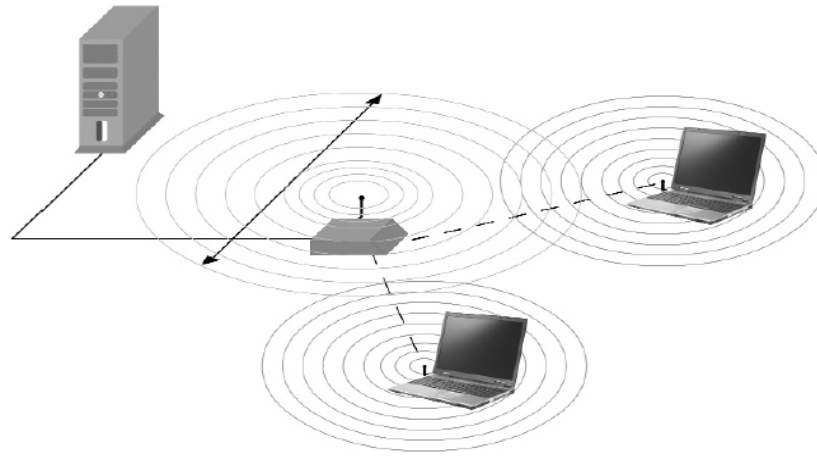
Modularnost i fleksibilnost bežičnih lokalnih računarskih mreža čini ih dobrim rešenjem za pojedine objekte kao na primer: povezivanje računara na sajmovima, u bolnicama, bibliotekama, povezivanje zgrada koje su razdvojene prometnim saobraćajnicama ili rekom, u zgradama od istorijske vrednosti u kojima nije dozvoljena promena izgleda zgrade, ali i kao dopuna ili proširenje kablovskih mreža. Bežične mreže pružaju veliku fleksibilnost i mogućnost kombinovanja različitih načina povezivanja. Iskristalisale su se sledeće topologije: *samo za ovu priliku(ad hoc), infrastrukturna i tačka-tačka.*

Topologije bežičnih lokalnih računarskih mreža

Ad hok lokalne računarske mreže omogućavaju korisnicima uspostavljanje veze „svako sa svakim” bez uređaja za pristup (AP) . Kao takve pogodne su za komunikaciju između manjih grupa korisnika na malom rastojanju i uglavnom se primenjuju tamo gde je potrebno brzo uspostaviti privremenu mrežu (sajmovi, skupovi). Da bi mogla da se ostvari međusobna komunikacija potrebno je da svaki računar bude u dometu svih ostalih računara, što ograničava pokretljivost korisnika na relativno mali prostor.



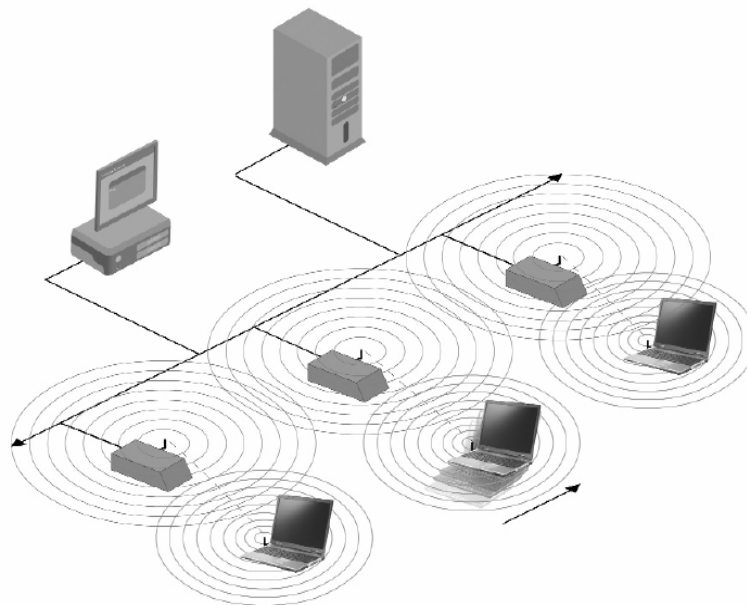
Ukoliko stanice nisu u stanju da komuniciraju bez posredstva uređaja za pristup AP onda se primenjuje način rada koji zahteva odgovarajuću infrastrukturu. Sve stanice koje se nalaze u zoni pokrivanja uređaja za pristup međusobno komuniciraju preko njega.



Infrastrukturni način povezivanja

Domet jednog uređaja za pristup zavisi od primene i kreće se od 100m u zatvorenim prostorima do 300m na otvorenom. Broj korisnika koje može da opsluži jedan uređaj za pristup zavisi od proizvođača i kreće se od 15 do 50.

U slučaju da se želi povećati pokrivenost može se instalirati više uređaja za pristup i formirati ćelijska (celularna) mreža.



Ćelijski način povezivanja

U takvoj mreži stanice ne mogu da komuniciraju direktno među sobom već isključivo posredstvom uređaja za pristup, međusobno povezanih kablovima u računarsku mrežu. Određenim brojem pristupnih stanica može se pokriti određeno područje, pri čemu se zone pokrivanja pojedinih stanica, tzv. ćelije, mogu međusobno delimično i preklapati. U slučaju da je u određenoj ćeliji velika gustina saobraćaja moguće je istu površinu pokriti sa više pristupnih stanica, koje međusobno dele mrežni saobraćaj i na taj način omogućavaju opsluživanje većeg broja korisnika. Karakteristika ćelijskih mreža je da korisnici mogu biti pokretljivi u toku rada, menjajući pristupne stanice preko kojih komuniciraju sa ostatkom mreže. Uređaji za pristup AP vezuju se na ožičenu mrežu. Takođe se po potrebi mogu i bežičnim putem povezati na ostatak mreže.

U određenim situacijama pogodne su i mreže tipa tačka-tačka, na primer za povezivanje dve udaljene lokalne mreže. Najčešće se izvode korišćenjem usmerenih radio-veza ako su van objekata, ili upotrebom infracrvene tehnologije ako su veze unutar jedne prostorije. Ove veze najčešće su fiksnog karaktera, odnosno njihovi korisnici ne mogu biti mobilni.

Tehnologije bežičnih lokalnih računarskih mreža

Bežične lokalne računarske mreže WLAN prema tehnici prenosa generalno se mogu podeliti na sledeće kategorije:

- tehnike prenosa u infracrvenom delu spektra (IR),
- tehnike proširenog spektra (SS) i
- uskopojasne mikrotalasne tehnike

Infracrveni i radio talasi su deo elektromagnetnog talasnog spektra. Infracrveni uređaji su opremljeni sa LED i laserskim diodama koje emituju infracrvene svetlosne talase. Ovi talasi mogu da se usmere direktno ka prijemniku (point-to-point) ili mogu da se reflektuju od zidova ili tavanice (difuzno). Implementiranje point-to-point infracrvenog LAN-a je mnogo teže, jer predajni i prijemni uređaji moraju da budu poravnati.

Postoje neke prednosti infracrvenih sistema. Infracrvene signale nije regulisao FCC kao što je to slučaj sa radio signalima. To znači da za

- opremu koja se zasniva na infracrvenim talasima nisu neophodne licence.
- Sledeća prednost je što infracrveni talasi ne prodiru kroz čvrste objekte, tako da su sigurniji od neovlašćenog prisluškivanja spolja.
- Na infracrvene talase ne utiče radio interferenca.

Korišćenje radio talasa je nešto složenije i razlikuje se od konvencionalnog radija kod koga se signal emituje na datoj nosećoj frekvenciji i vi podešavate radio aparat za njegov prijem. Javlja se problem interference od drugih uređaja, prisluškivanje signala, ometanje prenosa. Da bi se rešili ovi problemi, 802.11 standard koristi **široki sprektar (spread spectrum)**, tehnologiju koja se koristi ne samo za bežične LAN mreže, već i za bežične i mobilne telefone. Umesto da koristi uski frekventni opseg, prenosi u širokom spektru emituju energiju signala preko šireg opsega frekvencija (tj većeg propusnog opsega). To ih čini manje sklonim interferencama i obezbeđena je bolja zaštita. 802.11 standard definiše dva tipa tehnologija širokog spektra za WLAN fizički sloj: **direct-sequence spread spectrum i frequency-hopping spread spectrum**.

Principi na kojima se zasniva FHSS (frequency-hopping spread spectrum) je sledeći: uređaj koji koristi FHSS definiše niz frekvencija $f_1, f_2, f_3, \dots, f_n$ koje se nalaze u emisionom opsegu. Uređaj za prenos u određenom periodu koristi frekvenciju f_1 , pa prelazi na frekvenciju f_2 . I na toj drugoj frekvenciji vrši prenos za određeni vremenski period i onda prelazi na f_3 . Ovaj šablon se nastavlja sve dok uređaj vrši prenos preko frekvencija u fiksnom periodu. Kada završi prenos preko frekvencije f_n , ponovo počinje od f_1 . Svako ko pokuša da prisluškuje na konkretnoj frekvenciji čuće periodične nailaske signala koji se razlikuju od šuma. Uređaj utvrđuje ove frekvencije pomoću pseudonasumičnog generatora brojeva. Prijemni uređaj koristi isti algoritam i generiše isti set frekvencija.

FHSS komunikacije za bežične LAN mreže obično funkcionišu između 2,4 i 2,483 GHz i koriste do 79 zasebnih kanala, čime su obezbeđena 22 različita šablona (redosled frekvencija). Učestalost sa kojom uređaj menja frekvencije menja se u skladu sa komunikacionim polisama uspostavljenim u konkretnoj zemlji.

DSSS (direct-sequence spread spectrum) tehnologija funkcioniše na nešto drugačiji način. U kraćim periodima FHSS koristi uskopojasne prenose, ali u dužim periodima koristi široki propusni opseg. DSSS proširuje jedan bit podataka na više njih. Sledeći koraci ilustruju kako ovo funkcioniše:

- Predajni uređaj startuje sa stringom podataka
- Za svaki bit podataka generiše pseudonasumično izabrani niz bitova, nazvan **chipping sekvenca**, sa n bitova
- Kombinuje svaki bit podataka i odgovarajuću chipping sekvencu za kreiranje chip koda dužine n bitova
- Proces izvodi operaciju isključivo ILI između bitova podataka i svakog bita u chipping sekvenci.
- Rezultat je sekvenca 4-bitnih chip kodova (ako se izvodi primer sa 4 bita u sekvenci), po jedan za svaki bit

0	1	0	1	niz podataka
0010	1101	1000	1101	chipping sekvenca
0010	0010	1000	0010	rezultat

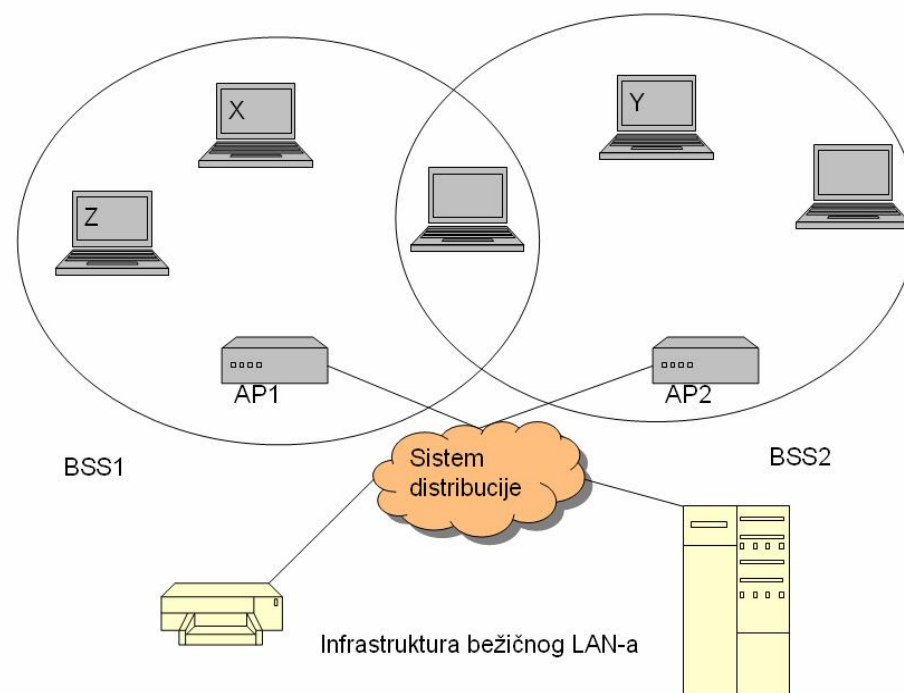
(802.11 standard koristi 11-bitnu chipping sekvenca koja se naziva **Barkerov kod** za generisanje chip kodova.) Ovde predajnik mora da prenese n bitova za svaki bit podatka. Npr da bi se postigla brzina od 1 Mbps, uređaj mora da ima mogućnost prenosa n Mbps. Sa druge strane, veća bitska brzina zahteva signale iz većeg propusnog opsega. Tu se dešava rasipanje signala preko šireg opsega. 802.11 standard primenjuje binarni metod faznog pomeranja za chip kod kako bi se postigla bitska brzina od 1 Mbps i kvadraturni metod faznog pomeranja za postizanje bitske brzine od 2 Mbps. Nakon toga se signal moduliše na nosećoj frekvenciji od 2,4 do 2,483 GHz pre prenosa.

Uskopojasni radio-sistemi koriste se za prenos podataka od ranih 80-ih. Korisnicima se dodeljuju uski frekvencijski opsezi, o čemu vode računa posebna tela na nivou države. Korisnici šalju i primaju podatke na tačno određenoj učestanosti. Širina frekvencijskog opsega je što je moguće uža.

Neželjena preslušavanja između kanala izbegavaju se frekvencijskim planiranjem, a sigurnost i izbegavanje interferencije postižu se upotrebom posebnih radio- frekvencija. Filter na prijemniku odstranjuje sve signale osim željenog. Prvi proizvođač koji je napravio uskopojasnu bežičnu računarsku mrežu u nelicenciranom frekvencijskom opsegu je RadioLAN 1995. godine.

Adresiranje

802.11 protokol definiše 4 različita adresna polja za svaki okvir.



Skup bežičnih uređaja sa jednim AP uređajem označen je kao BSS (basic service set – osnovni servisni skup – tačnije, to su svi uređaji koji se nadmeću za pristup istom medijumu tj. koriste istu frekvenciju). Pošto je moguće da postoji više AP uređaja, moguće je da postoji više BSS-ova. Osim toga, više BSS-ova može da se poveže preko sistema distribucije (DS-distribution system). Kada uređaj pošalje, postoje četiri različite mogućnosti.

Opis	Adresa1 (prijemnik)	Adresa2 (predajnik)	Adresa3	Adresa4
1. X šalje okvir do Z (okvir ostaje u BSS1)	Z	X	BSS1	-
2. X šalje okvir do Z (okvir ide do AP1)	AP1	X	Y	-
3. AP1 šalje okvir do AP2 preko DS	AP2	AP1	Y	X
4. AP2 šalje okvir koji potiče od X do Y	Y	AP2	X	-

1. slučaj

X šalje okvir do Z. Oba se nalaze u istom BSS-u i AP nije uključen u prenos. Adresa1 označava odredište okvira, a Adresa2 označava izvor. Ovde nismo napravili razliku između „izvora“ i „predajnika“ (oba su X), niti između „prijemnika“ i „odredišta“ (oba su Z). Adresa3 predstavlja ID BSS-a, a Adresa4 se ne koristi.

2. slučaj

X šalje okvir namenjen uređaju Y. Pošto se X i Y nalaze u različitim BSS-ovima, protokol je složeniji. U ovom slučaju Adresa1 definiše AP1, a Adresa2 označava izvor. Razlika je u tome što ovde prijemnik (AP1) nije i eventualno odredište. Polje Adresa3 definiše Y kao odredište. Ovo je neophodno kako bi AP1 rutirao okvir.

3. slučaj

Treći slučaj se primenjuje ako sistem distribucije sledi i bežični standard. U tom slučaju, AP1 (polje Adresa2) prenosi okvir, a AP2 (polje Adrese1) treba da primi taj okvir. Međutim, ni jedan njih nije niti originalni izvor, niti eventualno odredište. Polja Adresa3 i Adresa4 naznačavaju X i Y, respektivno.

4. slučaj

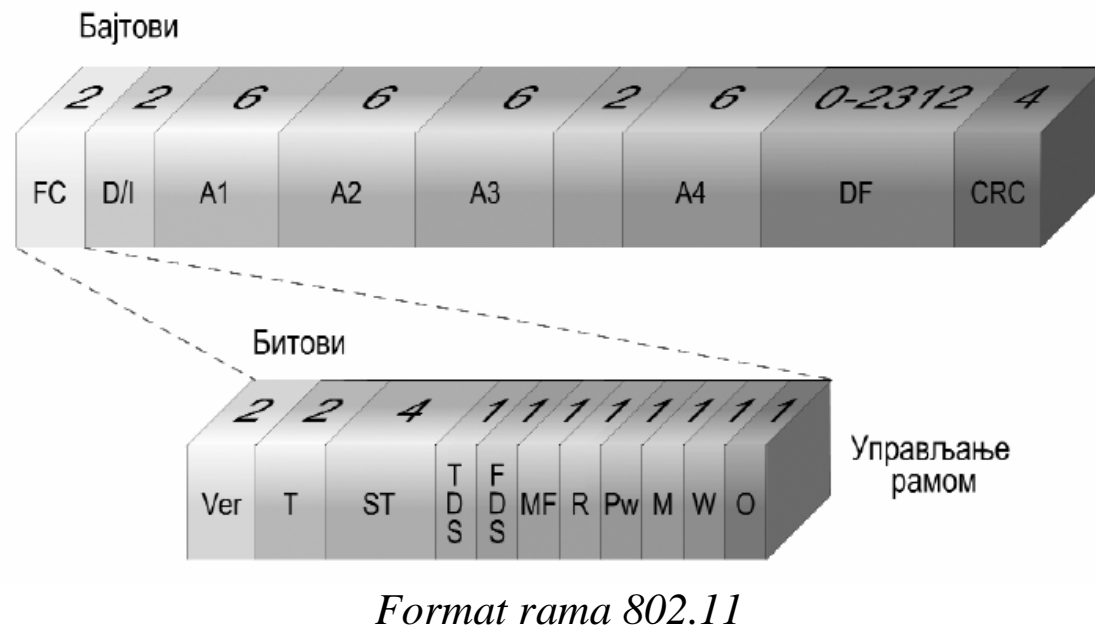
Poslednji slučaj se primenjuje kada okvir napušta DS dok ga AP2 prenosi do Y. U tom slučaju, odredište i prijemnik su isti (Y), ali su predajnik (AP2) i izvor (X) različiti.

Sva četiri slučaja imaju nešto zajedničko. Adresa1 uvek definiše uređaj koji treba da primi okvir. Dakle, dok uređaj prati radio signale od kojih se okvir sastoji, dovoljno je samo da proveri polje Adresa1 kako bi video da li treba da reaguje. Drugo, polje Adrese2 uvek definiše uređaj koji prenosi okvir. Ovo je neophodno zbog ACK okvira koji treba da se pošalje nakon uspešnog prijema. Prijemni uređaj mora da zna gde da pošalje ACK okvir. Glavne razlike se ogledaju u sadržaju polja Adresa3 i Adresa4.

Format okvira

Standard IEEE 802.11 definiše 3 različite klase ramova: **podatak, upravljanje i nadzor**. Za svaki od ovih ramova definisana su polja unutar MAC podsloja. Prvo polje za upravljanje ramom (FC – frame control) sadrži 11 potpolja:

1. **Ver** – verzija protokola – definiše tekuću verziju protokola
2. **T (type field)** – tip – ukazuje da li je ram podataka, upravljanja, ili nadzora. (upravljački okviri se koriste za konfigurisanje mreže, kontrolni okviri se koriste za pristup medijumu)
3. **ST (Subtype)** – podtip – ukazuje da li je ram RTS ili CTS ili ACK
4. **TDS (To DS)** – ka DS – ukazuje da ram ide ka distribucionom sistemu. (1 u slučajevima 2 i 3)
5. **FDS (From DS)** – od DS – ukazuje da ram ide od distribucionog sistema (1 u slučajevima 3 i 4)
6. **MF (More Fragment)** – ukazuje da postoji više fragmenata
7. **R (Retry)** – označava retransmisiju ramova koji su već ranije poslani (npr, nije stigla potvrda o prijemu)
8. **Pw (Power management)** – koristi bazna stanica za postavljanje mobilne stanice u mirno ili aktivno stanje
9. **M (More)** – ukazuje da pošiljalac planira da pošalje još ramova primaocu
10. **W (Wired Equivalent Privacy)** – ukazuje da je sadržaj rama šifrovan koristeći WEP algoritme
11. **O (Order)** – ukazuje primaocu da ramovi sa postavljenim bitom na 1 treba da budu obrađeni redosledom kojim su primljeni



Primeri korišćenja upravljačkih okvira:

- **Konfiguracija BSS-a**

Slučaj kada se dva BSS-a preklapaju. To znači da uređaj mora da se pridruži AP uređaju ako mu je neophodan pristup sistemu distribucije. Da bi se to izvelo, uređaj šalje **Association Request** okvir do naznačenog AP uređaja. Ako AP prihvati pridruživanje, reaguje slanjem okvira **Association Response**.

- **Pronalaženje AP uređaja**

Kako uređaj zna koji AP postoje? Da bi detektovao i identifikovao AP uređaje, svaki uređaj šalje **Probe Request** okvir. Svaki AP detektuje okvir i reaguje slanjem **Probe Response** okvira. Uređaj koji je inicirao ispitivanje, nakon toga može da selektuje AP (možda onaj sa najjačim signalom) i može da mu se pridruži, kao što je objašnjeno u prethodnom koraku.

- **Roaming**

Uređaji su mobilni, što znači da mogu da prelaze iz jednog BSS-a u drugi. Kada se to desi, uređaj može da pošalje **Reassociate Request** okvir do novog AP uređaja. AP može da reaguje sa **Reassociate Response** okvirom. **Disassociation** okvir razdružuje uređaj od prethodno pridruženog AP-a. Međutim, mobilni uređaj se možda više ne nalazi u domenu starog AP-a. Zato je novi AP odgovoran za slanje **Disassociation** okvira do starog AP-a u ime mobilnog uređaja. Ponovo pridruživanje treba da se izvrši automatski. Ako se uređaj pomeri i detektuje oslabljeni signal iz postojećeg AP-a, mora da pronade AP sa jačim signalom i da mu se pridruži. Ovo je analogno funkcionisanju mobilnih telefona kada korisnik prelazi iz jedne ćelije u drugu, osim što je ovde reč o mnogo manjim razmerama.

- **Bezbedne komunikacije**

Uređaj može da se uključi u bezbednu slanjem **Authenticate** okvira. Nakon toga, dva uređaja mogu da razmenjuju informacije u skladu sa pravilima bezbednih komunikacija. Kada se bezbedna komunikacija završi, okončava se slanjem **Deauthentication** okvira.

Polje (**D/I – Duration/Connection ID**) – ukazuje na to koliko će dugo (izraženo u milisekundama) ram i njegova potvrda zauzeti kanal. Ovo polje postoji i u upravljačkim ramovima tako da na osnovu njega stanice mogu da postave svoje indikatore NAV. Duration polje ukazuje na period u kome se odvija razmena RTS/CTS.

Zaglavlje rama sadrži četiri adrese (A1-A4). Sve adrese su standardnog IEEE802 formata. Dve adrese su izvorišna i odredišna adresa mobilnih stanica. Preostale dve adrese su izvorišna i odredišna adresa baznih stanica kada se saobraćaj odvija između ćelija.

Polje za sekvencne brojeve (**SC – sequence control**) koristi se za obeležavanje fragmenata. Od 16 bitova koji su na raspolaganju 12 bitova se koristi za obeležavanje ramova a 4 bita za obeležavanje delova ramova (fragmenata).

Polje podataka (**DF – Data Field**) sadrži korisne podatke od 0 do 2312 bajtova

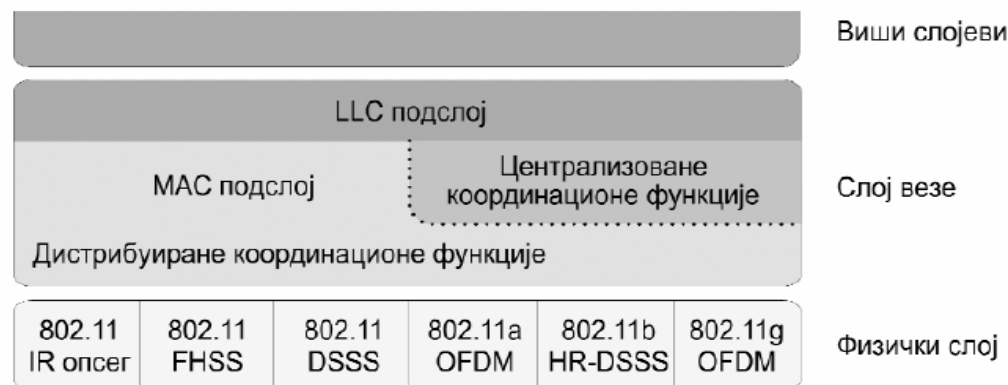
Polje kontrolnog zbira (**CRC – Cyclic Redundancy Check**) ima uobičajenu namenu da otkrije greške u prenosu.

Ramovi za nadzor imaju format sličan formatu ramova podataka osim broja adresa. Pošto se ramovi nadzora razmenjuju isključivo unutar jedne ćelije adresa bazne stanice nije potrebna.

Upravljački ramovi su kraći i imaju samo jednu ili dve adrese. Ne sadrže polje za podatke ni polje za sekvencne brojeve. Ključne informacije u ovim ramovima nalaze se u podpolju podtip koje ukazuje da li je ram zahtev za uspostavom veze (RST), potvrda o uspostavi veze (CST) ili potvrda o uspešnom prijemu rama podataka (ACK).

Arhitektura IEEE 802.11

Protokoli koji se koriste u seriji IEEE 802.11 imaju zajedničku strukturu. Standard se odnosi na prva dva sloja OSI arhitekture: fizički sloj i sloj veze. Podslaj MAC (sloja veze) određuje način dodele kanala. A podslaj LLC (sloj veze) ima zadatak da zaštiti više slojeve od različitih tehnika IEEE 802.11 serije.



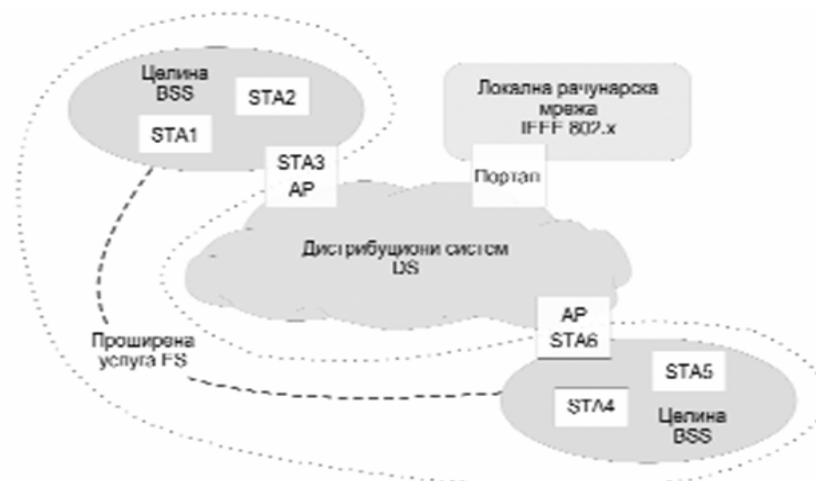
Slojevita arhitektura protokola u bežičnim lokalnim računarskim mrežama

U opštem slučaju mreža IEEE 802.11 sastoji se od jedne ili više celina sa osnovnom (baznom) uslugom (BSS – Basic Service Set), koje su povezane sa distribucionim sistemom (DS). Obično je distribicioni sistem ožičena lokalna računarska mreža koja ima funkciju okosnice ali može da bude i bilo koja druga komunikaciona mreža. Celina sa baznom uslugom (BSS) je osnovna gradivna celina arhitekture IEEE 802.11. Grupa stanica koja je pod direktnim upravljanjem jedne koordinacione funkcije formira celinu sa osnovnom uslugom (BSS).

Ad-hok mreža predstavlja grupisanje stanica u jednu celinu sa osnovnom uslugom (BSS). Standard IEEE 802.11 koristi naziv nezavisna BSS celina (IBSS). Bilo koja stanica u celini sa osnovnom uslugom može da komunicira sa bilo kojom drugom stanicom bez uređaja za pristup (AP).

Kada se za komunikaciju između stanica koristi uređaj za pristup (AP) onda standard IEEE 802.11 za takvu mrežu koristi termin **infrastrukturna mreža**. Uređaj za pristup omogućava proširenje opsega i mogućnost komunikacije više celina sa osnovnom uslugom. Proširena usluga (ESS) sastoji se od dve ili više celina sa osnovnom uslugom, međusobno povezanih distribucionim sistemom.

Za integraciju IEEE 802.11 arhitekture sa tradicionalnim lokalnim računarskim mrežama sa žičanim transmisionim medijumima, ili povezivanje na internet, koristi se **portal**. Logika portala se ugrađuje u uređaje kao što su mostovi ili ruteri koji su deo kablovske računarske mreže i koji su priključeni na distribicioni sistem.



Arhitektura 802.11

Protokol MAC podsloja IEEE802.11

Protokol na MAC podsloju standarda IEEE 802.11 značajno se razlikuje od protokola na MAC podsloju standarda IEEE 802.3, zbog veće složenosti bežičnih u odnosu na kablovske sisteme. Kod IEEE 802.3 sistema stanica čeka dok se transmisioni medijum ne oslobodi i tek onda počinje sa slanjem. Ukoliko ne primi signal koji ukazuje da je došlo do kolizije skoro je sigurno da je ram uspešno isporučen. Kod bežičnih sistema situacija je drugačija. Postoji problem nevidljive stanice: sve stanice nisu jedna drugoj u radio-dometu pa se može desiti da se predaja u jednom delu ćelije ne može detektovati u drugom delu iste ćelije.

Broj mobilnih korisnika koji koriste i telefone i računare u stalnom je porastu. Da bi se postigla potpuna mobilnost pokretni računari treba da koriste radio ili infracrveni signal za komunikaciju. Sistem sa pokretnim računarem koji komunicira radio-putem smatra se bežičnom lokalnom računarskom mrežom. Ove lokalne računarske mreže imaju različite osobine u odnosu na standardne lokalne mreže i zahtevaju specijalan podsloj (MAC)

Standardna konfiguracija za bežične mreže je sa baznim stanicama (pristupna tačka, AP) raspoređenim po zgradi. Sve bazne stanice su povezane međusobno optičkim vlaknima ili bakarnim kablovima. Ukoliko je predajna snaga bazne stanice predviđena da pokriva razdaljinu od 3 do 4m, svaka soba postaje jedna ćelija. Zgrada postaje veliki ćelijski sistem, kao što je standardni sistem mobilne telefonske mreže.

Višestruki pristup sa izbegavanjem kolizije (*MACA Multiple Access with Collision Avoidance*) prvi je protokol projektovan za bežične lokalne računarske mreže. Osnovna ideja je da pošiljalac šalje primaocu kratak ram, tako da ga stanice koje su u blizini mogu da detektuju i „izbegnu“ slanje za vreme slanja dolazećeg, velikog rama podataka.

Wired Equivalent Privacy (WEP) protokol

Bezbednost je problem bežičnih okruženja, posebno kada se koriste niskofrekventni radio talasi. 802.11 standard uključuje bezbednosni protokol poznat pod nazivom *Wired Equivalent Privacy (WEP)*.

- WEP obezbeđuje autentifikaciju i šifrovanje komunikacije između uređaja i AP-a. Algoritam za šifrovanje koristi 40-bitni tajni ključ i dodaje 24-bitni vektor inicijalizacije kako bi se kreirao 64-bitni ključ. Za svaki okvir se koristi drugačiji vektor inicijalizacije, tako da se dobijaju različiti ključevi šifrovanja svakog okvira. Novija oprema omogućava šifrovanje i sa 128-bitnim ključem.
- Protokol ne definiše algoritam koji se koristi za razmenu ključeva. Pretpostavlja se da su ključevi ugovoreni pre bilo kakve razmene. Skoro polovina WLAN mreža koja implementira WEP koristi podrazumevani ključ za šifrovanje.
- Metod za šifrovanje koristi algoritam poznat kao RC4. 40-bitni ključ i 24-bitni vektor inicijalizacije su ulazne vrednosti za algoritam koji generiše sekvencu pseudonasumičnih ključeva. Svaki od tih ključeva se propušta kroz operacije EXILI sa sekcijom običnog teksta iz okvira. Svaki vektor inicijalizacije je poslat u sklopu okvira. Prijemni uređaj koristi vektor inicijalizacije i 40-bitni ključ za generisanje iste sekvence ključeva i izvodi se operacija EXILI sa dolazećim šifrovanim tekstom za ponovno kreiranje originalnog teksta

Varijacije standarda 802.11

Originalni 802.11 standard koristi jedan od tri fizička sloja: infracrveni, DSSS, FHSS. Svi mogu da se izvršavaju brzinom od 1 Mbps ili 2 Mbps, što je veoma sporo u poređenju sa današnjim protokolima za kablirana LAN okruženja. Postoji nekoliko verzija standarda 802.11 kako bi se obezbedile brže komunikacije. To su 802.11a, 802.11b i 802.11g. Sve su zasnovane na CSMA/CA i imaju velike razlike u fizičkim slojevima. Npr. 802.11b, koji je poznat kao Wi-Fi (wireless fidelity) koristi radio talase iz opsega od 2,4GHz i postiže brzine od 11 Mbps. Koristi samo DSSS, jer veće brzine ne mogu da se postignu sa FHSS. 802.11a funkcioniše u opsegu od 5 GHz i teorijski može da postigne bitske brzine od 54 Mbps. 802.11g funkcioniše u opsegu od 2.4 GHz i postiže bitske brzine od 54 Mbps.

Standard IEEE 802.11a

Prvi u nizu standarda većih brzina u bežičnim sistemima je IEEE 802.11a. Koristi se ISM frekvencijski opseg 5,4GHz i ortogonalni frekvencijski multipleks OFDM1. Ne koristi se tehnika proširivanja spektra već potkanali sa nosiocima na različitim međusobno ortogonalnim učestanostima. Podaci se dele u više tokova a svaki se prenosi pomoću svog podnosioca, kroz svoj potkanal. Moguće brzine su: 6, 9, 12, 18, 24, 36, 48 i 54Mb/s. Koriste se do 52 nosioca koji su modulisani sa BPSK, QPSK, 16QAM, 64QAM u zavisnosti od brzine koja se zahteva.

Standard IEEE 802.11b

Cilj je bio ponuditi standard IEEE 802.11b koji podržava brzine prenosa podataka kao i (tadašnji) IEEE 802.3 standard. Ponuđene su brzine 5,52 Mb/s i 11 Mb/s i rad u ISM frekvencijskom opsegu od 2,4 GHz do 2,4835 GHz. Samo povećanje brzine prenosa na 11Mb/s omogućeno je upotrebom CCK (complementary code keying) modulacije, ili takozvane modulacije sa komplementarnim kodovima. CCK se koriste kao kodna sekvenca pri procesu širenja spektra DSSS tehnikom. Ulazni podaci se posmatraju kao blokovi od po 8 (odnosno 4 bita) brzine 1,375 MHz. Šest od osam bitova povezuje se jednom od 64 kodne sekvence i moduliše sa QPSK. Da li će protok biti 11 Mb/s ili 5,5 Mb/s zavisi od stanja u kanalu, a uređaj se sam tome prilagođava.

Standard IEEE 802.11g

Standard IEEE 802.11g je poboljšana verzija 802.11b. Koristi OFDM modulaciju ali radi u 2,4GHz frekvencijskom opsegu. Teoretski može da dostigne brzine od 54Mb/s.

Standard IEEE 802.11e

U standardu IEEE 802.11e unapređene su koordinacione funkcije MAC podsloja (distribuirane DCF i centralizovane PCF) uvođenjem nove hibridne koordinacione funkcije (HCF). U okviru hibridne koordinacione funkcije definisana su dva metoda za pristup kanalu (slična originalnom IEEE 802.11 MAC standardu): poboljšani distribuirani pristup (EDCA) i kontrolisani pristup (HCCA). Oba metoda definišu klase saobraćaja, tako da se na primer e-pošti može dodeliti najniži prioritet, a govoru najviši. Kod metoda sa poboljšanim distribuiranim pristupom (EDCA) stanica sa većim prioritetom u proseku čeka malo manje, pre nego što pošalje svoj ram, od stanice nižeg prioriteta. Svakom od nivoa prioriteta dodeljen je period vremena (TXOP) u kome stanica ili uređaj za pristup mogu da pošalju odjednom više ramova. Uređaji za pristup sa WMM sertifikatom moraju da imaju ovu opciju (ostale ne moraju).

Kod načina rada sa kontrolisanim pristupom (HCCA) interval između ramova- farova, koje PCF šalje stanicama, podeljen je u dva dela. U prvom delu koriste se centralizovane koordinacione funkcije. U drugom delu može se koristiti poboljšani distribuirani pristup (EDCA). U zavisnosti od prioriteta nekim stanicama može se dodeliti češći pristup medijumu. Stanicama se u zavisnosti od klase usluga dodeljuje i različita dužina njihovog pristupa. Kvalitet usluga (QoS) može se podešavati prema zahtevima korisnika. Na taj način su obezbeđeni uslovi za kvalitetan prenos govora i videa.

Standard IEEE 802.11i

IEEE 802.11i (poznat i kao WPA2) je proširenje IEEE 802.11 standarda koji specificira sigurnost u Wi-Fi mrežama. Prethodna specifikacija (WEP) pokazala se nedovoljno sigurnom. Specifikacija WPA2 primenjuje AES standard za šifrirawe. Pored toga moguća je i primena drugih metoda zaštite kao što su provera pristupa na osnovu portova, RADIUS ili virtuelne privatne mreže.

Standard IEEE 802.11n

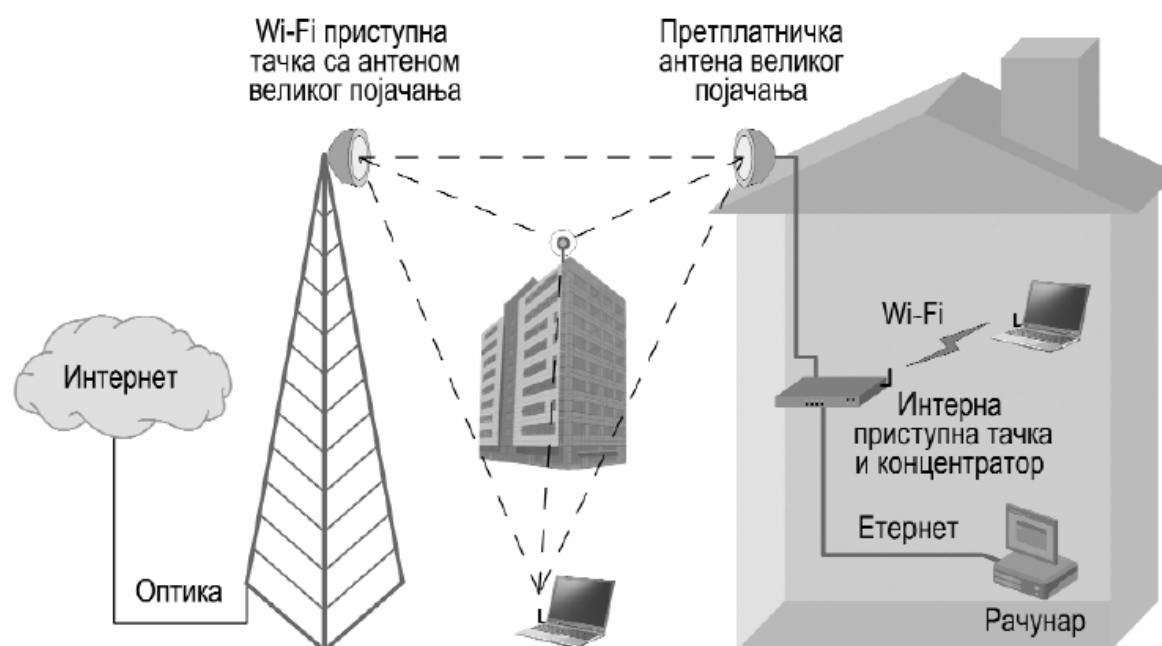
U januaru 2005. godine IEEE je formirao radnu grupu 802.11TG čiji je zadatak da razvije proširenje IEEE 802.11 standarda za bežične lokalne računarske mreže. Očekuje se da će se dostići brzine veće od 100Mb/s. Predviđa se korišćenje OFDM i MIMO prenosa. Tehnologija MIMO koristi više antena (prostorno raspoređenih) i multiputno prostiranje signala. Koristi QAM sa 64 i 256 konstelacionih tačaka. Potkanali su širine 40MHz u odnosu na sadašnjih 20MHz (u državama u kojima regulatorska tela to dozvoljavaju).

Standard IEEE 802.11p

Standard IEEE 802.11p označava se i kao standard za bežični pristup pokretnih vozila WAVE. Namena mu je da obezbedi bežičnu vezu između vozila u pokretu i uređaja na putevima. Vozila mogu dobiti informacije o uslovima na drumu (meteorološki pregled, saobraćaj) ili neku od naprednih usluga npr. inteligentno navođenje vozila. Domet je oko 300m i radi u licenciranom frekvencijskom opsegu od 5,96GHz, a brzine je 6Mb/s. Realizacija je složena pošto se vozila brzo kreću.

Standard IEEE 802.11s

Međusobno povezane mreže postaju sve popularnije u velikim gradovima pošto je moguće povezati lokalne računarske mreže bez postavljanja dodatnih kablova. Da bi se isporučio saobraćaj koji je na drugom kraju mreže predlaže se rutiranje i na MAC i na IP sloju.



Međusobno povezane mreže