

OFDM OFDMA

Sadržaj

OFDM
OFDMA

OFDM (*Orthogonal Frequency Division Multiplexing*).

(ortogonalni frekvencijski multipleks)

- OFDM se bazira na principu prenosa sa više nosilaca, odnosno, tok korisničkih podataka se deli na nekoliko delova (podkanala), od kojih svaki ima mnogo manju bitsku brzinu nego tok od koga je nastao
- podkanali modulišu podnosioce koji su međusobno ortogonalni
- zbog svoje ortogonalnosti, podnosioci mogu da budu veoma blizu jedan drugom u frekvencijskom domenu, a da se pri tome međusobno ne ometaju
- s obzirom da se radi o maloj bitskoj brzini ovih podkanala, njihovi bitski intervali su veliki, pa nema intersimbolske interferencije

OFDM (*Orthogonal Frequency Division Multiplexing*).

Koristi se kod

- DAB
- DVB
- 802.11a
- 802.11g
- LTE
- ADSL
- Prenosa podataka kod elektroenergetskih vodova

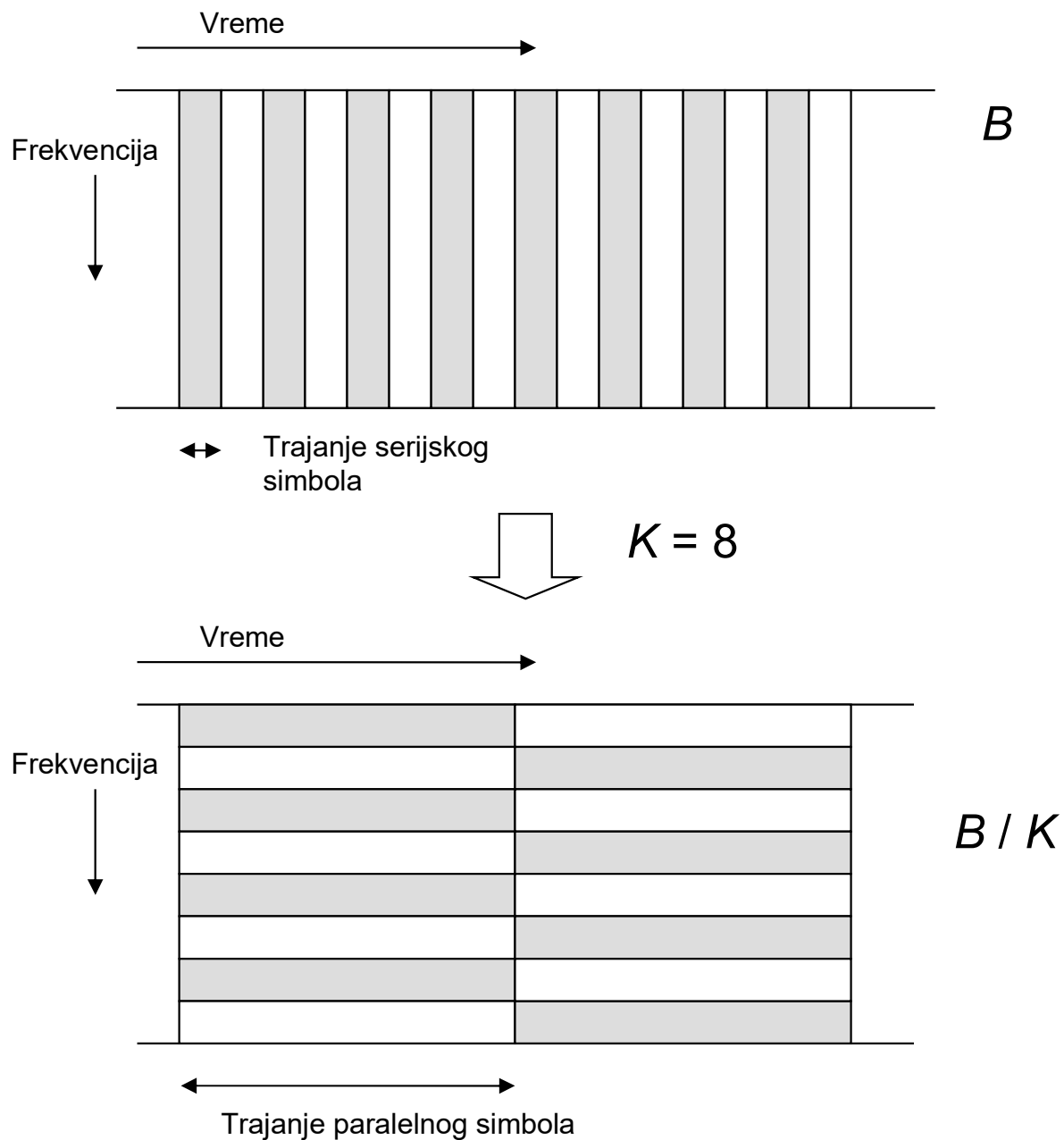
Za:

- Efikasno korišćenje spektra: ortogonalni podnosioci mogu da budu veoma blizu jedan drugom
- Otpornost na uskopojasnu smetnju
- Otpornost na smetnju koja se javlja usled prostiranja signala po više putanja

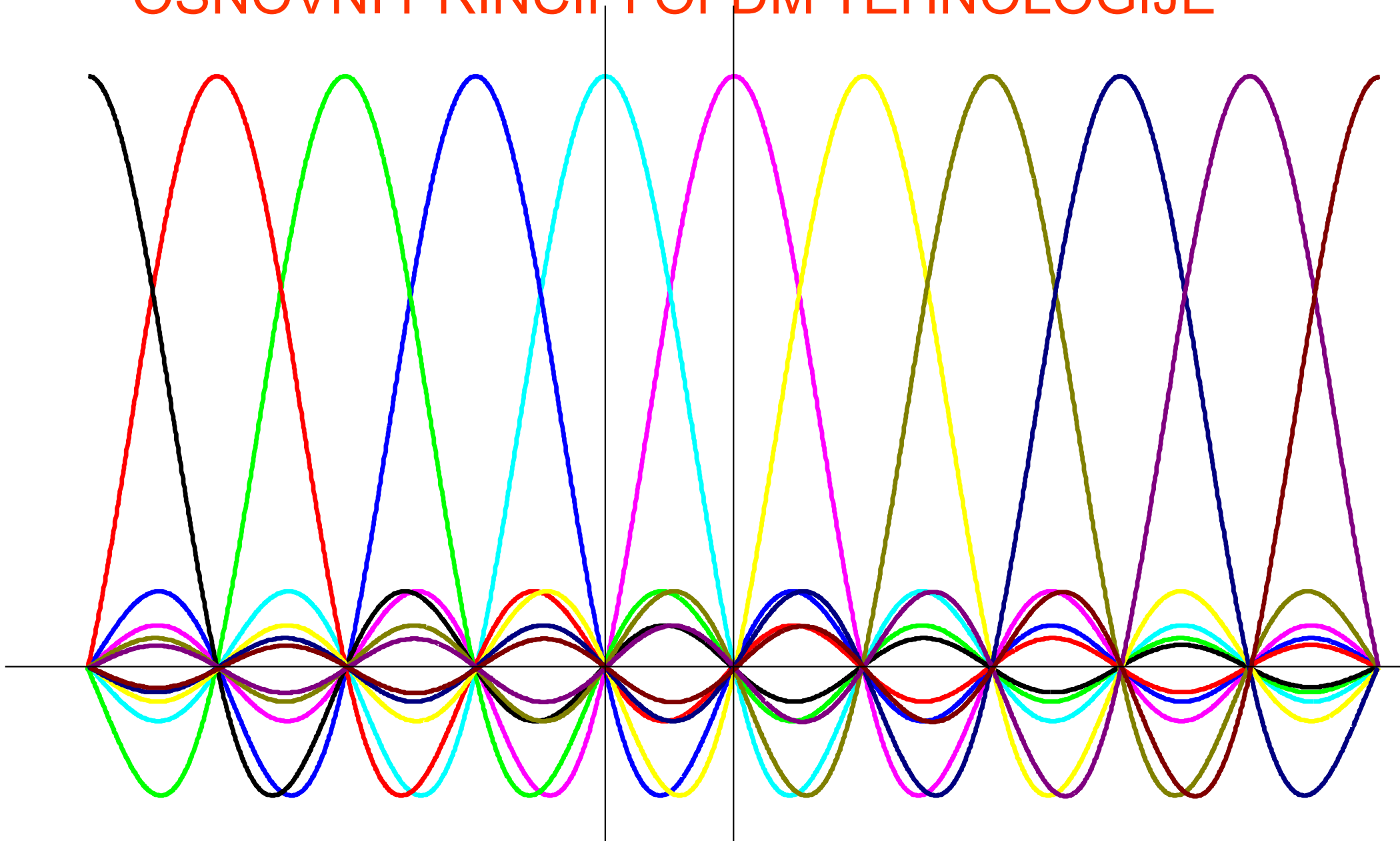
Protiv:

- veliki odnos maksimalne trenutne snage i srednje snage

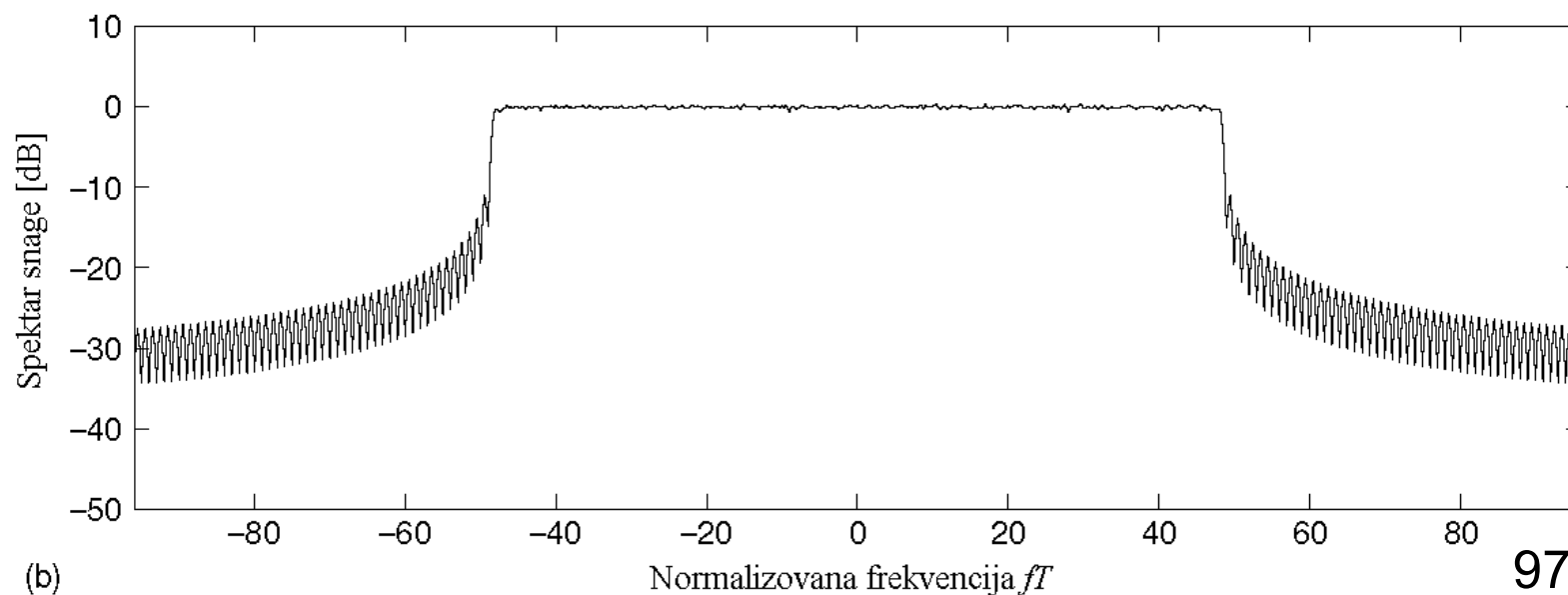
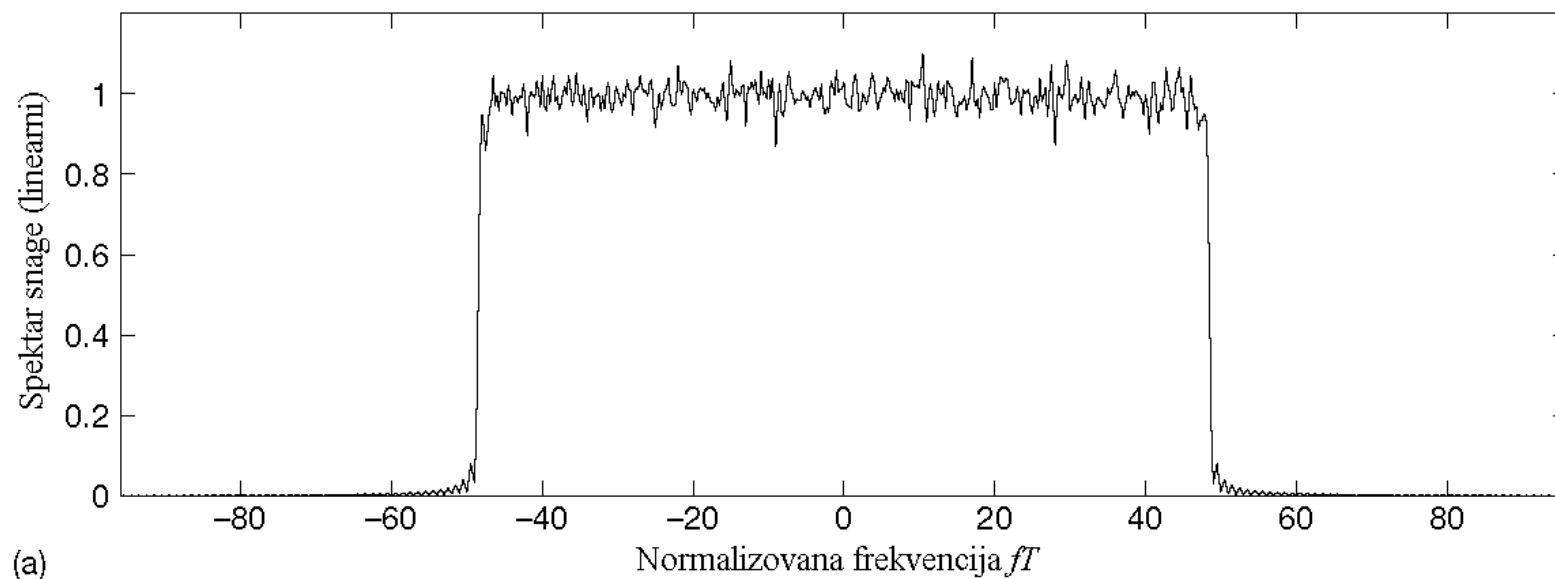
OSNOVNI PRINCIPI OFDM TEHNOLOGIJE

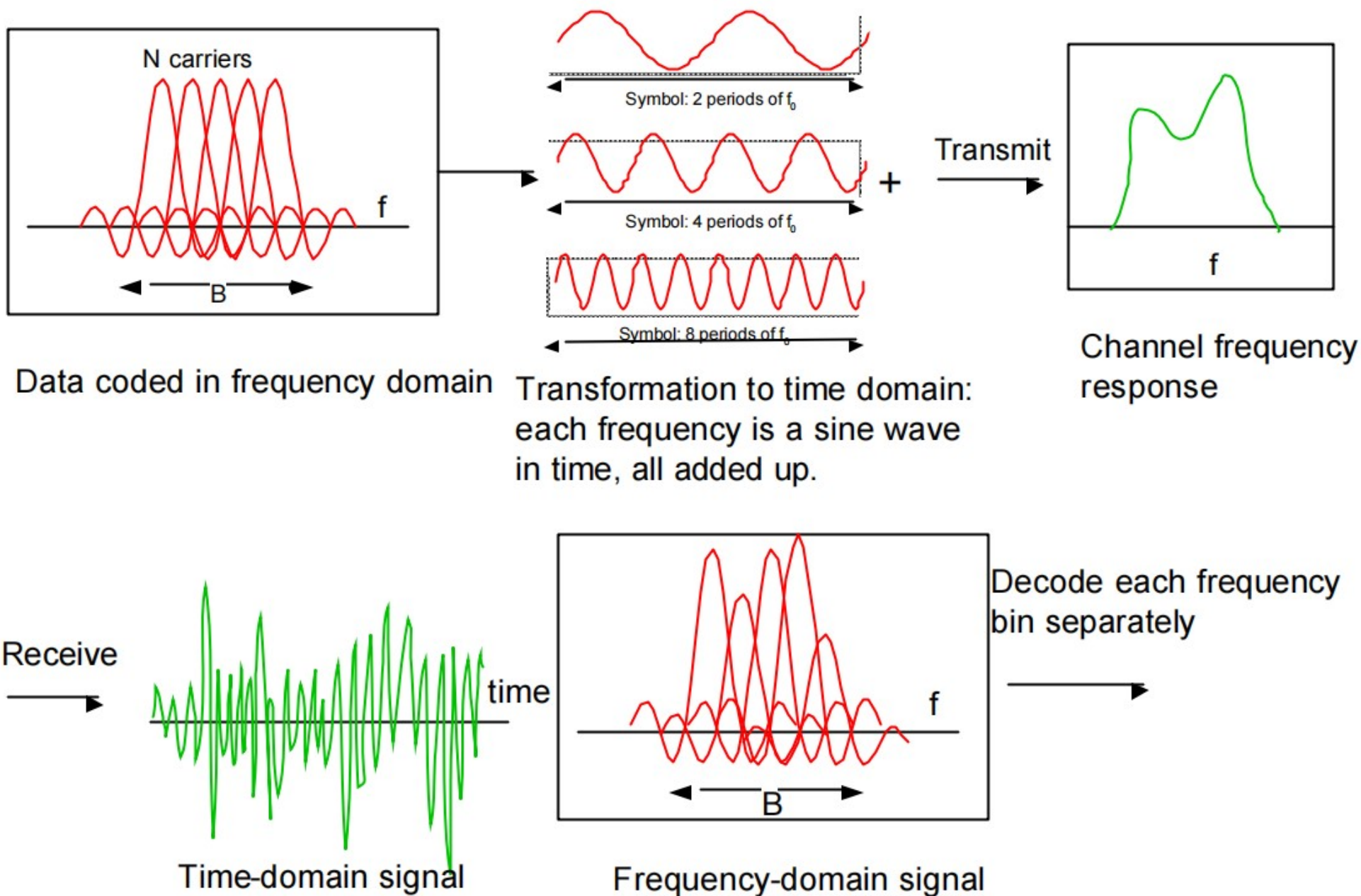


OSNOVNI PRINCIPI OFDM TEHNOLOGIJE

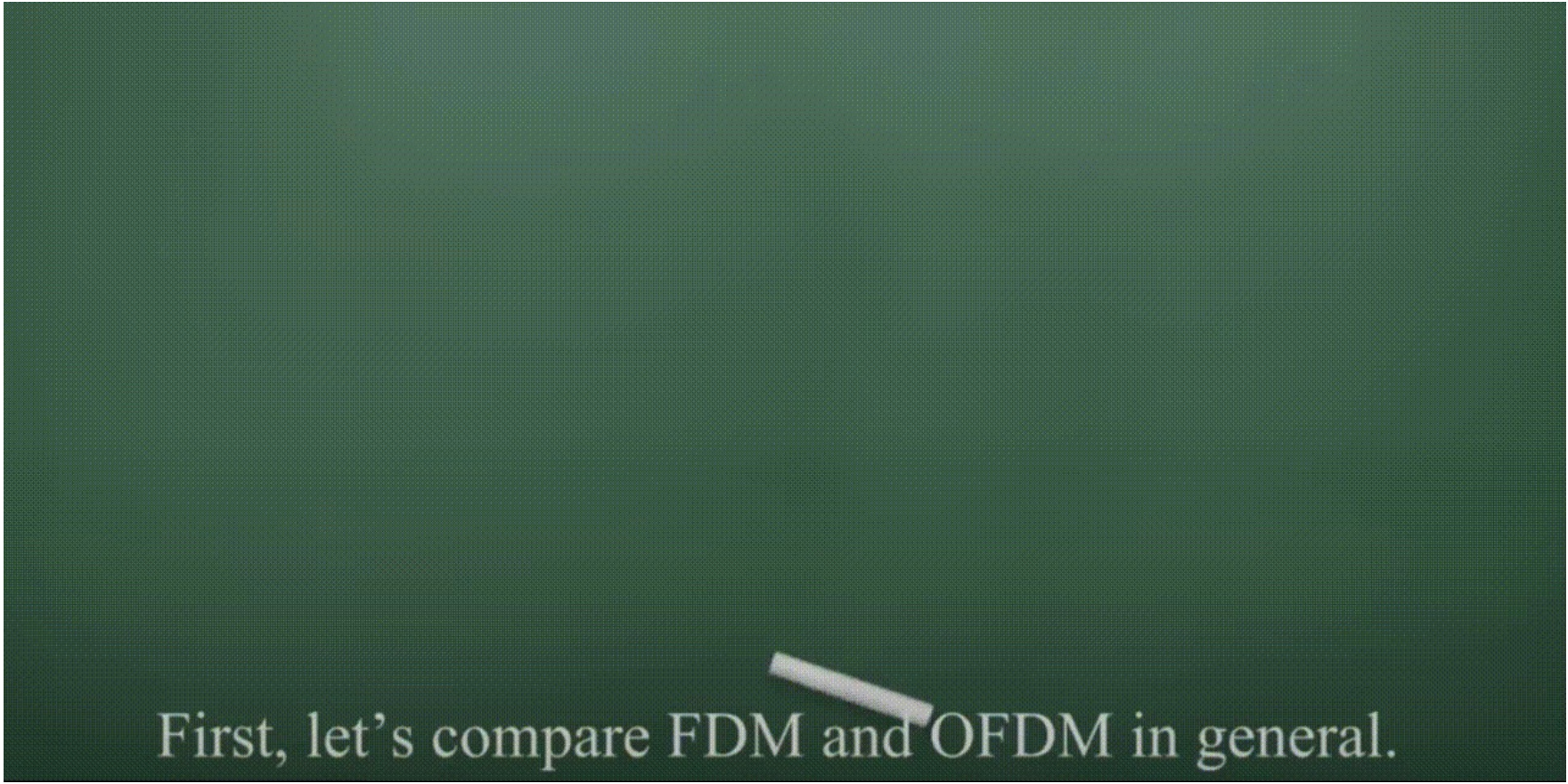


OSNOVNI PRINCIPI OFDM TEHNOLOGIJE



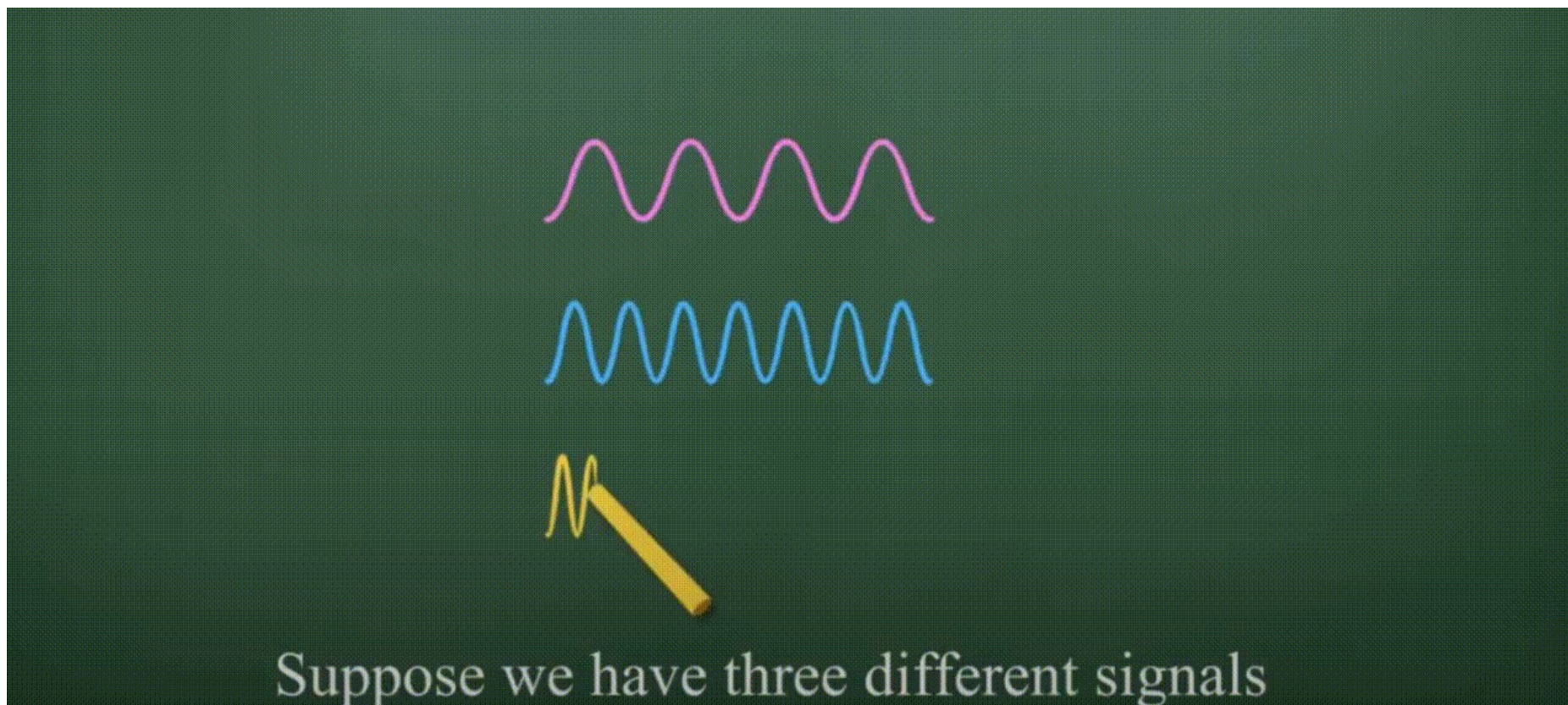


OFDM (*Orthogonal Frequency Division Multiplexing*).



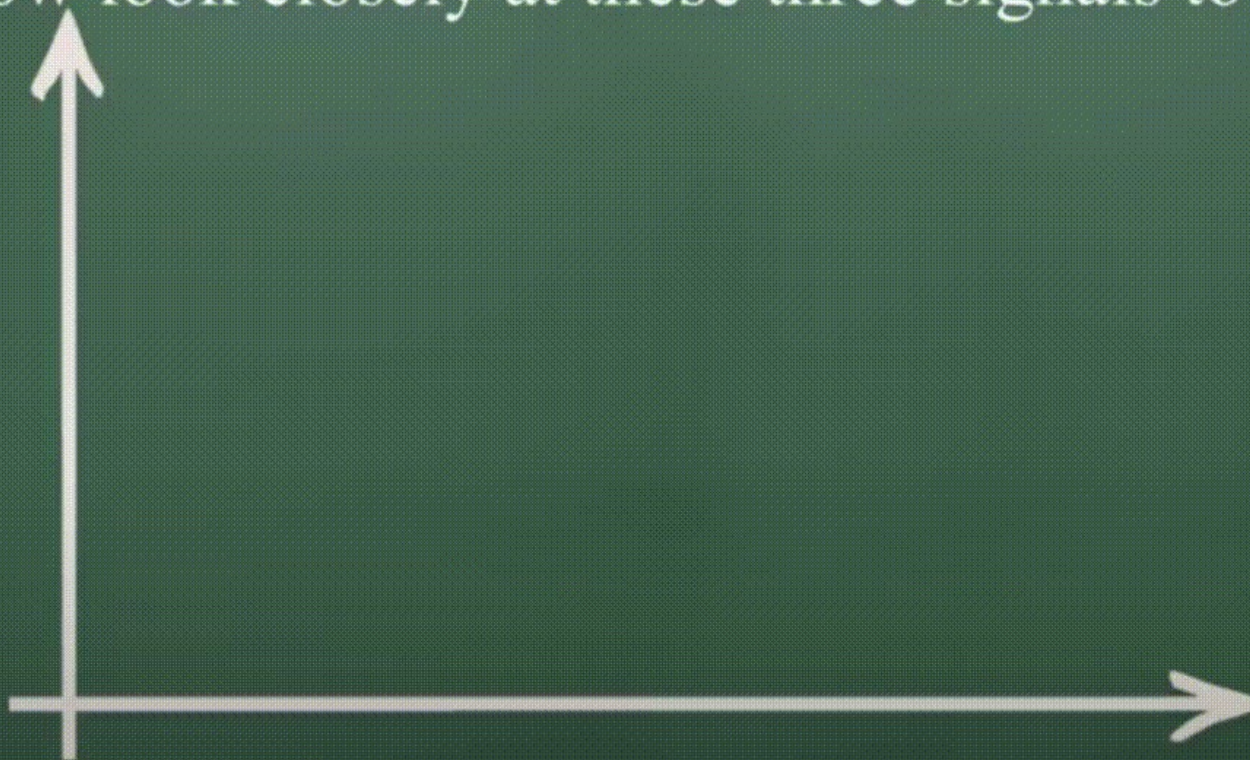
First, let's compare FDM and OFDM in general.

OFDM (*Orthogonal Frequency Division Multiplexing*).

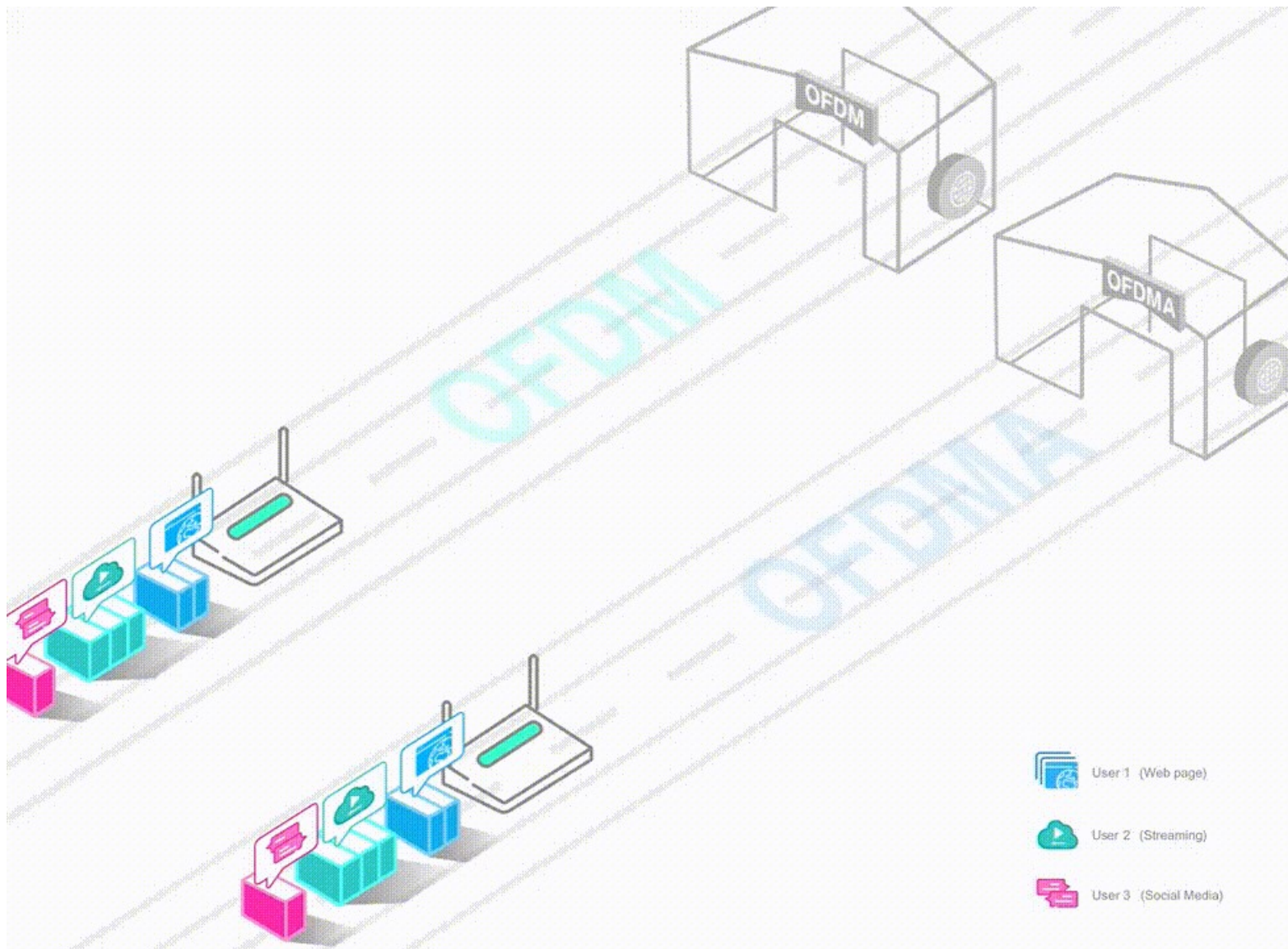


OFDM (*Orthogonal Frequency Division Multiplexing*).

Now look closely at these three signals to see



OFDM (*Orthogonal Frequency Division Multiplexing*).



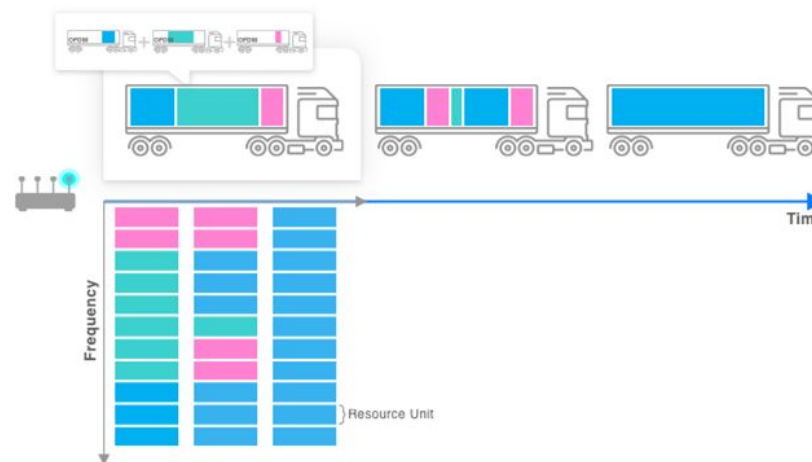
OFDM (*Orthogonal Frequency Division Multiplexing*).

 User 1 (Web page)
  User 2 (Streaming)
  User 3 (Social Media)

OFDM



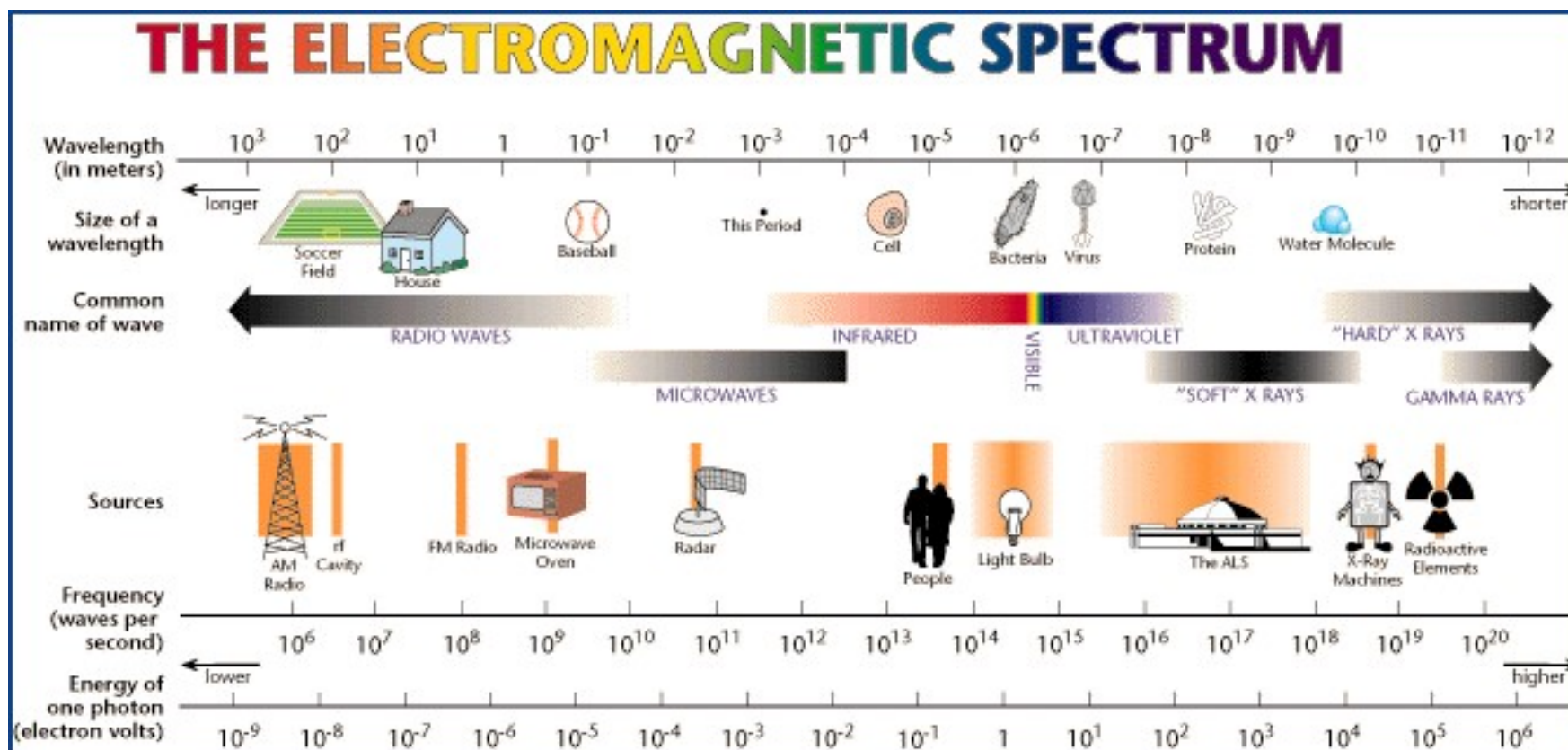
OFDMA



UVOD U BEŽIČNE RAČUNARSKE MREŽE

Elektromagnetni spektar

U celom elektromagnetskom spektru, zona od interesa za bežične komunikacije je između 10^6 i 10^{11} Hz.



Elektromagnetni spektar

Tipovi spektralne alokacije

Na osnovu tipa alokacije, spektar se deli na:

- rezervisani
- otvoreni.

Ministarstvo za telekomunikacije Srbije je zaduženo za dodelu frekvencija i njihovo korišćenje, i koordinisano je sa međunarodnim institucijama (UN ITU-R, EU, US FCC...).

Rezervisani spektar

Rezervisani spektar je ekskluzivno dodeljen korisnicima koji za njegovo korišćenje obično plaćaju državi. Opsezi su tačno određeni i strogo se definiše kolika je maksimalna predajna snaga i nivo interferencije u susednim opsezima. Primeri rezervisanog spektra i korisnika su :

- Celularna mreže: 400, 700, 800, 900, 1800, 1900, 2100 MHz (Telenor, MTS...).
- TV kanali: L-VHF 50 do 88 MHz, H-VHF 174 do 216 MHz, UHF 470 do 806 MHz.
- Komunikacione veze (PTT, Telekom...).
- Vojska i policija.
- Satelitski veze.
- Civilni i vojni radari.
- GPS: 1575,42 MHz i 1227,60 MHz.

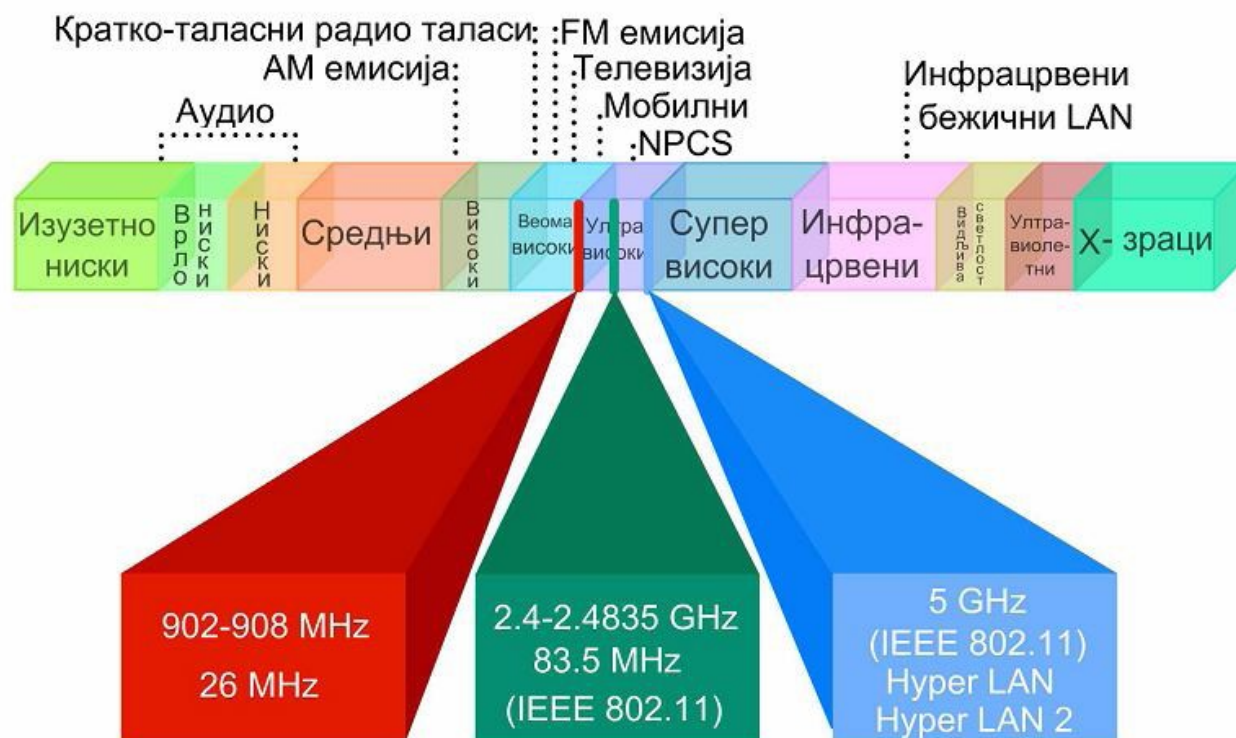
Elektromagnetni spektar

Otvoreni spektar

Ovaj spektar je otvoren za sve korisnike koji moraju da poštuju propisane maksimalne nivoe predajne snage i interferencije u susednim frekvencijskim opsezima. Opsezi radio-frekvencijskog spektra bez posebnih dozvola za potrebe industrije, naučnih istraživanja i medicine (ISM- Industrial Scientific Medical) obuhvataju tri grupe frekvencija:

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

WiFi (802.11), Bluetooth, Zigbee, igračke na daljinsko upravljanje i mikrotalasne pećnice koriste ove opsege.



Bežične mreže: istorija

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 100kb/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)

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. Iskristalisalo se je nekoliko topologija.

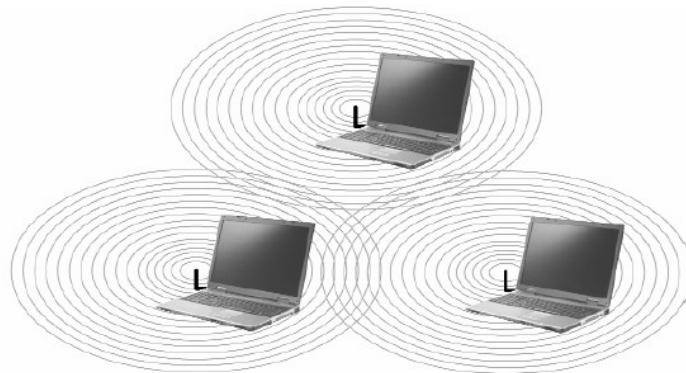
WLAN topologije

Postoje tri tipa WLAN topologije:

- Nezavisni skupovi servisa (IBSS – Independent basic service sets)
- Osnovni skupovi servisa (BSS - Basic service sets)
- Prošireni skupovi servisa (ESS – Extended service sets)

Takodje kao poseban slucaj postoji i topologija **tipa tačka-tačka (point to point)**. Izraz skup servisa (service set) se odnosi na logičku grupu uređaja.

IBSS se sastoji od grupe 802.11 stanica koje komuniciraju direktno jedna sa drugom, što se još naziva i ad-hoc mrežom, pošto ona i jeste peer-to peer WLAN mreža.

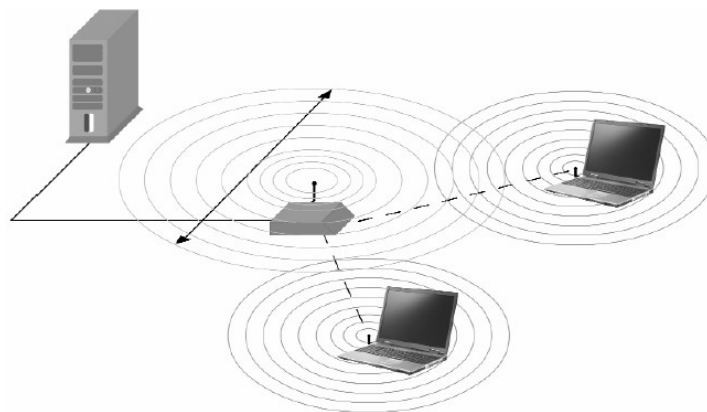


Slika. Ad-hoc

WLAN topologije

Ad hoc 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.

BSS predstavlja grupu 802.11 stanica koje komunikaciju ostvaruju preko specijalizovane stanice koja se naziva **tačka pristupa (AP – access point)**. Ovaj tip predstavlja tzv. **infrastrukturu** (infrastrukturni mod).



Infrastrukturni način povezivanja

WLAN topologije

Ukoliko stanice nisu u stanju da komuniciraju samostalno u tzv. ad - hoc mreži i bez posredstva uređaja za pristup AP (Access Point) onda se primenjuje način rada koji zahteva odgovarajuću infrastrukturu. Sve stanice koje se nalaze u zoni pokrivanja uređaja za pristup međusobno komuniciraju preko njega.

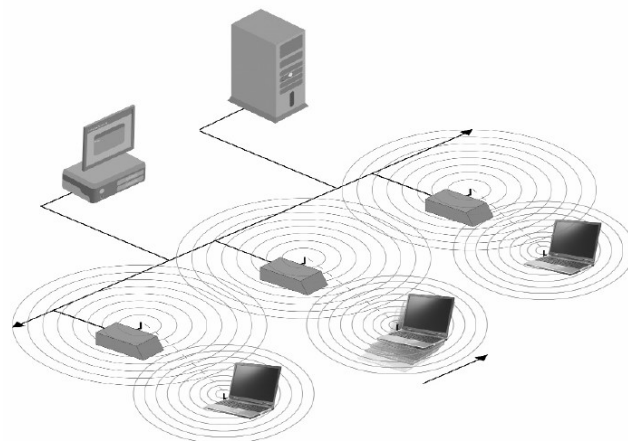
Domet jednog uređaja za pristup (AP) zavisi od primene i kreće se od 100m u zatvorenim prostorima do 300m na otvorenom.

Broj korisnika koje može da opsluži jedan uređaj za pristup zavisi od proizvođača i kreće se od 15 do 50 u wi-fi 5 i ranijim standardima a maksimalno je 74 u wi-fi 6 standardu prvenstveno zahvaljujući OFDMA implementaciji.

WLAN topologije

ESS predstavlja više BSS infrastruktura povezanih preko uplinka u distribucionni sistem (DS). ESS predstavlja skup više pristupnih tačaka sa svojim okruženjem.

Ovo se primenjuje u slučaju da se želi povećati pokrivenost kada se instalira više AP uređaja i formira ćelijska (celularna) mreža.



Ćelijski način povezivanja

U takvoj mreži stanice ne mogu da komuniciraju direktno među sobom već isključivo posredstvom uređaja za pristup (AP), međusobno povezanih kablovima u računarsku mrežu. Određenim brojem AP - ova može se pokriti određeno područje, pri čemu se zone pokrivanja pojedinih stanica, tzv. ćelije, mogu međusobno delimično i preklapati.

WLAN topologije

U slučaju da je u određenoj ćeliji velika gustina saobraćaja moguće je istu površinu pokriti sa više AP - a (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 (AP) 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 (point o point)**, 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 fiksno karaktera, odnosno njihovi korisnici ne mogu biti mobilne stanice.

TEHNIKE PRENOSA U BEŽIČNIM MREŽAMA

Bežične lokalne računarske mreže 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

TEHNIKE PRENOSA U BEŽIČNIM MREŽAMA

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.

Performanse

Udruženje za Infracrveni prenos podataka (Infrared Data Association - IrDA) definiše tri kategorije:

- IrDA-SIR: Infracrvena veza male brzine koja podržava brzine prenosa podataka do 115 Kbps.
- IrDA-MIR: Infracrvena veza srednje brzine koja podržava brzine prenosa podataka do 1,15 Mbps.
- IrDA-FIR: Infracrveni signal velike brzine koji podržava brzine prenosa podataka do 4 Mbps.

TEHNIKE PRENOSA U BEŽIČNIM MREŽAMA

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.
- infracrveni talasi ne prodiru kroz čvrste objekte, tako da su sigurniji od neovlašćenog prisluškivanja spolja.
- na infracrvene talase ne utiče radio interferenca.

Nedostaci infracrvene veze:

- Potrebna je opticka vidljivost, teško je kontrolisati stvari koje nisu u vidokrugu predajnog IC kontrolnog uređaja.
- komunicira jedan po jedan uređaj.
- maksimalna brzina prenosa podataka je oko 4 Mbps
- uređaj treba da bude nepokretan tokom režima prenosa podataka.
- fizičke prepreke (kao što su vrata, zidovi), jaka sunčeva svetlost, dim, prašina i magla utiču na infracrvenu komunikaciju.
- iako ne možemo da vidimo infracrvene talase, oni mogu oštetiti oči ako se prenose sa većom snagom signala.

TEHNIKE PRENOSA U BEŽIČNIM MREŽAMA

Sirokopojasni prenos

Kod upotrebe radio talasa za prenos signala 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 (CDMA).

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:

- 1.frequency-hopping spread spectrum (FHSS) i
- 2.directe-sequence sread spectrum (DSSS)

TEHNIKE PRENOSA U BEŽIČNIM MREŽAMA

Sirokopojasni prenos

FHSS (frequency-hopping spread spectrum)

se zasniva na sledećem principu: uređaj koji koristi FHSS definiše niz frekvencija f_1 , f_2 , f_3 , .. 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 pseudoslučajnog generatora brojeva. Prijemni uređaj koristi isti algoritam i generiše isti set frekvencija.

TEHNIKE PRENOSA U BEŽIČNIM MREŽAMA

Sirokopojasni prenos

FHSS komunikacije za bežične LAN mreže obično funkcionišu između 2,4 i 2,483 GHz i koriste do 79 zasebnih kanala, i koriste 22 različita šablona (redosleda frekvencija).

Učestalost sa kojom uređaj menja frekvencije menja se u skladu sa komunikacionim polisama uspostavljenim u konkretnoj zemlji.

Posmatrano u kratkom vremenskom intervalu FHSS koristi uskopojasne kanale, ali posmatrano u dužem vremenskom intervalu koristi široki propusni opseg.

TEHNIKE PRENOSA U BEŽIČNIM MREŽAMA

Sirokopojasni prenos

DSSS (direct-sequence spread spectrum)

tehnologija funkcioniše na nešto drugačiji način.

DSSS proširuje jedan bit podataka na više njih. Koraci DSSS-a:

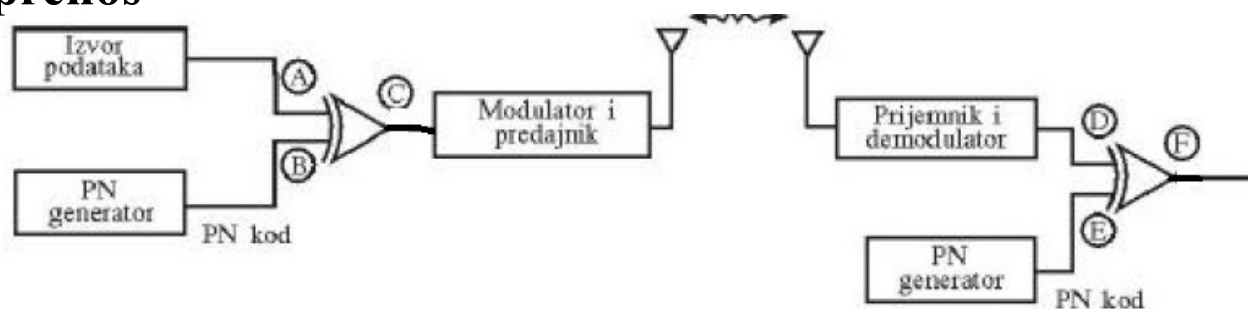
- Predajni uređaj startuje sa stringom podataka
- Za svaki bit podataka generiše pseudoslučajno izabrani niz bitova, nazvan chipping sekvenca, sa n bitova
- Kombinuje svaki bit podataka i odgovarajuću chipping sekvencu za kreiranje chip koda dužine n bitova
- Proces izvodi operaciju isključivo ILI (XOR)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

Primer (n=4):

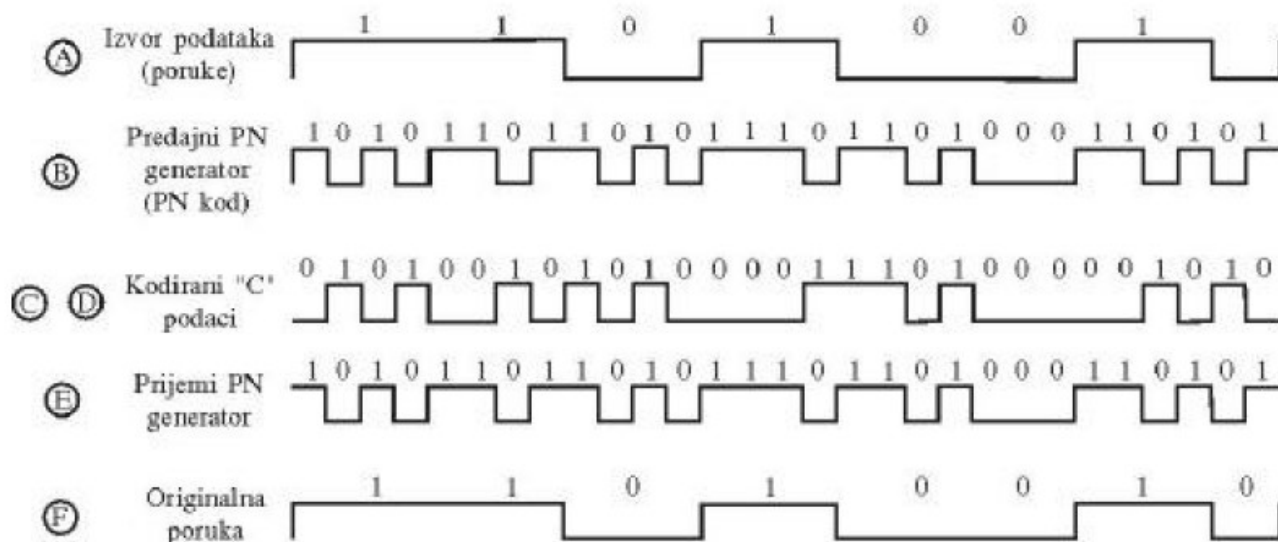
0	1	0	1	niz podataka
0010	1101	1000	1101	chipping sekvenca
0010	0010	1000	0010	rezultat nakon XOR operacije

TEHNIKE PRENOSA U BEŽIČNIM MREŽAMA

Sirokopojasni prenos



A	B	C
0	0	0
0	1	1
1	0	1
1	1	0



TEHNIKE PRENOSA U BEŽIČNIM MREŽAMA

Sirokopojasni prenos

802.11 standard koristi 11-bitnu chipping sekvencu koja se naziva **Barkerov kod** za generisanje chip kodova.) Ovde predajnik mora da prenese n (11) bitova za svaki bit podatka. Npr da bi se postigla brzina od 1Mbps, uređaj mora da ima mogućnost prenosa n Mbps.

Sa druge strane, veća bitska brzina zahteva veći propusni opseg. Tako da dolazi do rasipanje signala preko šireg opsega.

802.11 standard primenjuje BPSK binarnu faznu modulaciju za chip kod kako bi se postigla bitska brzina od 1 Mbps i QPSK kvadraturnu faznu modulaciju za postizanje bitske brzine od 2 Mbps. Signal se moduliše na nosećoj frekvenciji od 2,4 do 2,483 GHz pre prenosa.

TEHNIKE PRENOSA U BEŽIČNIM MREŽAMA

Uskopojasni prenos

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 prijemu odstranjuje sve signale osim željenog.

Prvi proizvođač koji je napravio uskopojasnu bežičnu računarsku mrežu u nelicenciranom frekvencijskom opsegu je RadioLAN 1995. godine.

- Koristi se za uskopojasni prenos pri maloj snazi 0,5 W ili manje
- Radi na 10 Mbps
- Opseg 5,8 GHz
- 50 m u poluotvorenoj kancelariji i 100 m u otvorenoj kancelariji
- Peer-to-peer konfiguracija
- Bira se jedan čvor kao “mastera” - dinamički izbor na osnovu lokacije, smetnji i jačine signala, tj. master se može automatski menjati kako se uslovi menjaju
- Stanice mogu da služe kao repetitori za stanice koje su van dometa mastera

Bežične mreže: IEEE 802.11 standard

Najuspešnija familija standarda, IEEE 802.11, za bežične lokalne komunikacione mreže je definisana od strane Institute of Electrical & Electronics Engineers (IEEE), u Sjedinjenim Američkim Državama.

U nameri da ubrzaju razvoj i interoperabilnost između uređaja proizvedenih od strane raznih proizvođača formirana je industrijska alijansa pod nazivom Wireless Fidelity (WiFi). Alijansu čine više od 300 kompanija.

Alijansa je razvila interoperabilne testove, procedure, i laboratorije za sertifikaciju. Svaki uređaj koji je sertifikovan nosi WiFi znak.

Alijansa je definisala podskup zahteva na osnovu šireg 802.11 standarda, i trenutno podržava 802.11a, b, g, n, ac, ax, be.

Pored IEEE 802.11 standarda, Evropski telekomunikacioni institut za standarde European Telecommunications Standards Institute (ETSI) je definisao ekvivalentni standard za bežične lokalne komunikacione mreže, HiperLAN. Taj standard nije doživeo komercijalni uspeh i dalji rad na ovom standardu je spojen sa IEEE 802.11.



WiFi sertifikacioni znak

Bežične mreže: IEEE 802.11 standard

WiFi i pristup bežičnom medijumu

Elementarna komunikaciona operacija u WiFi-u se sastoji od slanja podataka i prijema potvrde (ACK). Ukoliko potvrda izostane posle određenog vremenskog intervala, smatra se da operacija nije uspela. U WiFi-u ne postoji eksplicitna negativna potvrda prijema (ne postoji NACK).

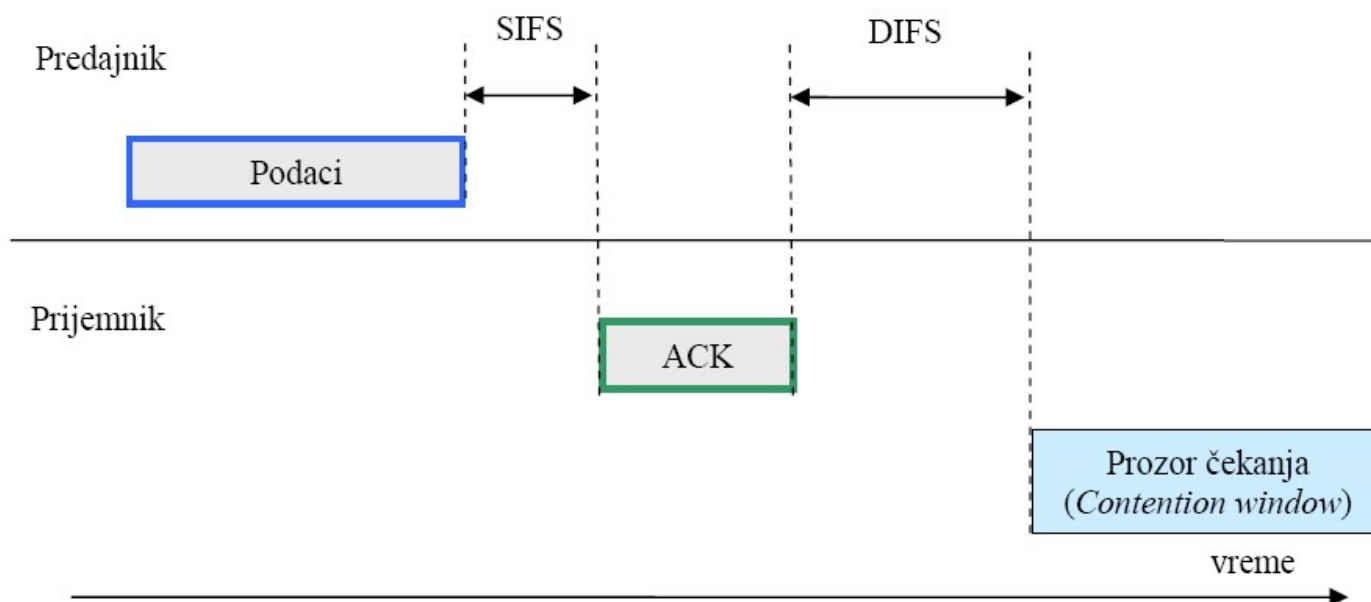
Osnovna funkcija MAC nivoa mreže je da odluči na koji će se način pristupiti medijumu, tj., bežičnom kanalu. Postoje dve metode pristupa bežičnom medijumu u WiFi-u:

1. Osnovni pristup medijumu je zasnovan na metodi detekcije nosioca i izbegavanja kolizije (Carrier Sensing Multiple Access/Collision Avoidance (CSMA/CA)). Ovaj metod je sličan onome u ethernetu, gde se primenjuje Carrier Sensing Multiple Access / Collision Detection (CSMA/CD). On predstavlja osnovu distribuirane koordinacione funkcije WiFi mreže (Distributed Coordination Function (DCF)).

2. Nešto komplikovaniji pristup je zasnovan na metodi zahteva za slanje i dozvoli za slanje (Request to Send / Clear to Send (RTS/CTS)). Ovom metodom se smanjuje broj mogućih kolizija što povećava efikasnost, ali u isto vreme povećavaju se i neefikasnosti zbog komplikovanijeg protokola u odnosu na CSMA/CA metodu.

Bežične mreže: IEEE 802.11 standard

Algoritam za detekciju nosioca i izbegavanje kolizije (CSMA/CA)



CSMA/CA je mehanizam za pristup prenosnom medijumu , koji u osnovi sadrži sledeće korake:

- Detekcija nosioca (Carrier Sense): pre prenosa, stanica prvo sluša deljeni medijum (detekcija signala u bežičnoj mreži) da bi utvrdio da li drugi čvor emituje ili ne. Moguce je da se javi tzv. problem sa skrivenim terminalom (znači da drugi terminal možda emituje), što u ovoj fazi ostaje neotkriveno.

Bežične mreže: IEEE 802.11 standard

Algoritam za detekciju nosioca i izbegavanje kolizije (CSMA/CA)

- Izbegavanje kolizije (Collision Avoidance): ako se “čuje” drugi terminal, stanica čeka jedan, slučajno odabrani, vremenski period (na osnovu Binary Exponential Backoff (BEB) algoritma) pre nego što ponovo krene da osluškuje da li je komunikacioni kanal slobodan.

Zahtev za slanje/dozvola za slanje (RTS/CTS) može opciono da se koristi u ovom trenutku za posredovanje u pristupu deljenom mediju. Ovo donekle pomaže u ublažavanju problema sa skrivenim terminalima jer u bežičnoj mreži, pristupna tačka (Ap - Access Point) u datom trenutku samo jednom terminalu izdaje dozvolu za slanje (Clear to Send). Međutim, implementacije bežičnog 802.11 obično ne koriste RTS/CTS za sve prenose; ova opcija može da bude potpuno isključena, ili barem da se ne koriste za male pakete (opterećenje RTS/CTS metode pristupa je preveliko za prenose tzv. malih paketa podataka i može izazvati zagusenje mreže).

Bežične mreže: IEEE 802.11 standard

Algoritam za detekciju nosioca i izbegavanje kolizije (CSMA/CA)

- Prenos: ako je medijum identifikovan kao slobodan stanica mora da čeka vremenski interval *DCF Interframe Spacing* (DIFS) koji je definisan standardom (50 mikrosekundi za 802.11b, 34 mikrosekunde za 802.11a, 29 mikrosekundi za 802.11g). Nakon isteka DIFS intervala, mrežna stanica slučajno izabere trenutak kada (na osnovu Binary Exponential Backoff (BEB) algoritma) da započne transmisiju u okviru prozora čekanja. Ukoliko je terminal primio CTS signal što je eksplicitna dozvola za slanje, stanica ne mora da čeka DIFS period već odmah šalje ceo frem podataka.

Za razliku od CSMA/CD, za bežični terminal je veoma tesko da “sluša” u isto vreme dok emituje (njegova emisija će maskirati slušanje). Tako da bežična stanica “ne zna” da li je istovremeno još neka stanica emitovala na istom kanalu. Zato nakon slanja terminal čeka na potvrdu o prijemu paketa od AP-a.

Short InterFrame Spacing (SIFS) je period vremena u mikrosekundama koji je potreban bežičnom interfejsu da obradi primljeni okvir i da odgovori okvirom odgovora. Ako takva potvrda ne stigne na vreme, pretpostavlja se da doslo do kolizije sa drugim terminalom, što dovodi do toga da terminal uđe u BEB (Binary Exponential Backoff) period čekanja pre pokušaja ponovnog prenosa.

Bežične mreže: IEEE 802.11 standard

Algoritam za detekciju nosioca i izbegavanje kolizije (CSMA/CA)

Sa svakom neuspehom transmisijom i odgovarajućom retransmisijom, maksimalna dužina čekanja, tj. dužina prozora će se povećati do neke granične vrednosti. Dužina prozora eksponencijalno raste sa svakom retransmisijom (funkcija oblika 2^N), dok ne dosegne 1023 vremenskih perioda (time slot, koji je 20 mikrosekundi za 802.11b i 9 mikrosekundi za 802.11a).

Kada prozor dostigne 1023 perioda, ostane na toj dužini do god se ne ostvari uspešan prenos podataka, ili dok se ne odustane od predaje. Maksimalna dužina čekanja, tj., prozor čekanja je poznat kao Contention Window.

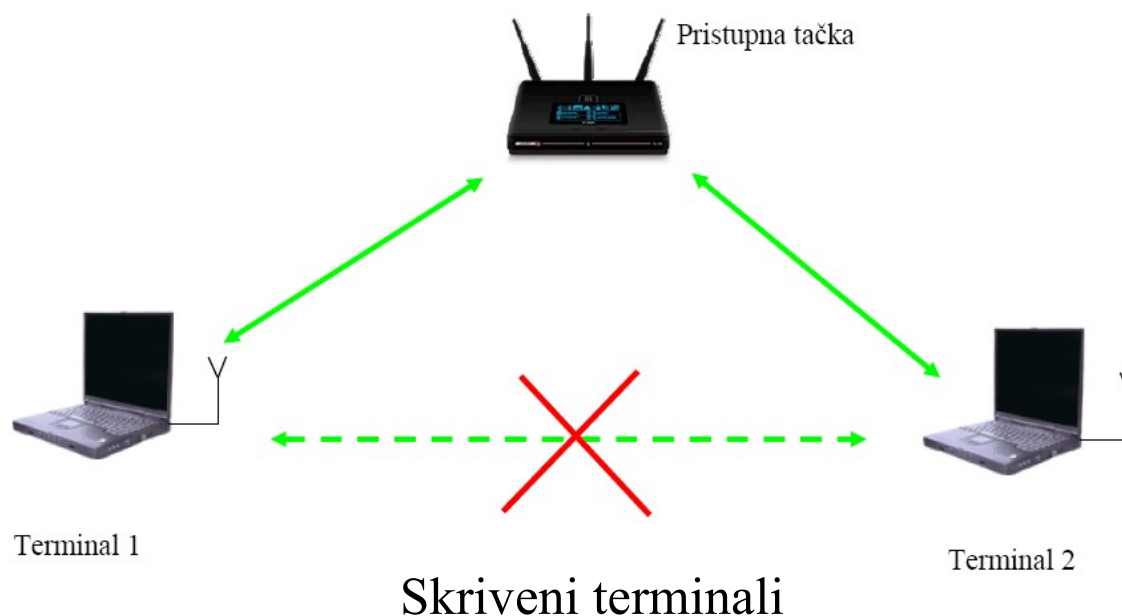
Ovaj algoritam omogućava stabilan prenos i pri velikom opterećenju mreže, tj., pri velikom broju korisnika.

Bežične mreže: IEEE 802.11 standard

Algoritam za detekciju nosioca i izbegavanje kolizije (CSMA/CA)

Problem skrivenog terminala (*hidden node problem*)

Ovaj problem se javlja zbog načina prostiranja radio talasa. U bežičnim mrežama može doći do situacije kada dva terminala mogu da komuniciraju sa AP - om, ali nemaju mogućnosti za međusobnu komunikaciju (bilo zbog udaljenosti, fizičke prepreke ili nekog drugog razloga koji sprečava prostiranje radio talasa između dva terminala). Situacija je prikazana na slici, gde je terminal 1 skriven, u radio domenu, od terminala 2, i obrnuto.

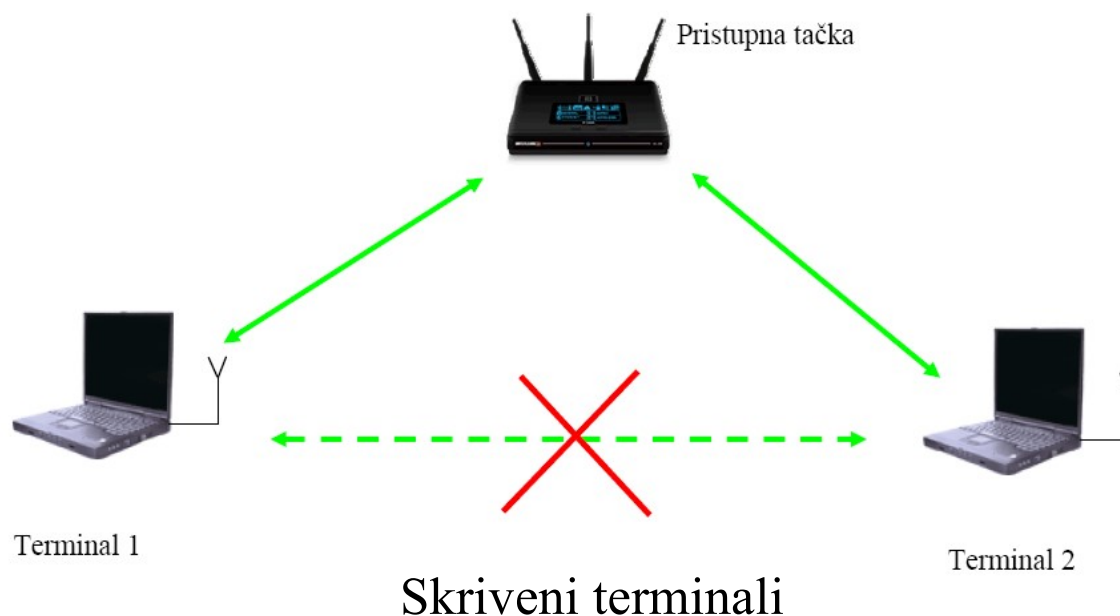


Bežične mreže: IEEE 802.11 standard

Algoritam za detekciju nosioca i izbegavanje kolizije (CSMA/CA)

Problem skrivenog terminala (*hidden node problem*)

Problem se javlja kada oba terminala istovremeno pristupaju bežičnom medijumu (započnu transmisiju prema AP - u). U tom slučaju dolazi do neželjene kolizije, što izaziva potrebu za retransmisijom paketa, što dalje dovodi do pada brzine prenosa podataka. Ovaj problem se ne može efikasno rešiti metodom detekcije nosioca i izbegavanje kolizije (CSMA/CA) i jedan je od razloga uvođenja metode zahteva za slanje i dozvole za slanje (RTS/CTS) pristupa



Bežične mreže: IEEE 802.11 standard

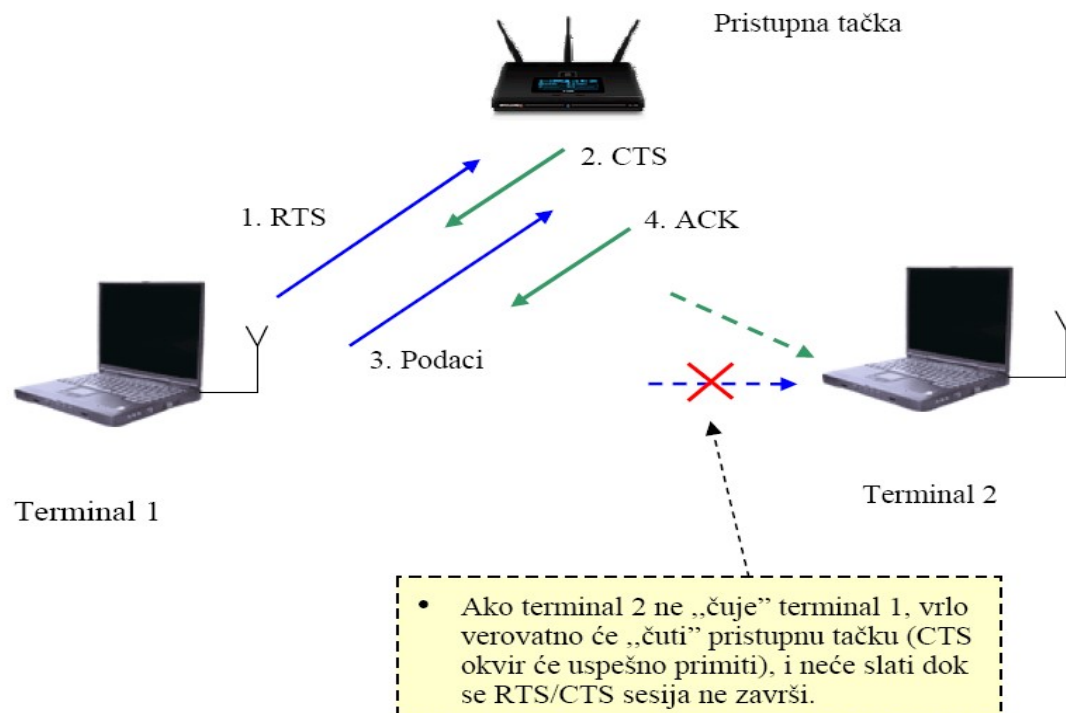
Metoda zahteva za slanje i dozvole za slanje (RTS/CTS)

- Terminal ili AP (pristupna stanica) koja započinje transmisiju šalje frejm zahtev za slanje (Request To Send (RTS)).
- Ako je transmisija uspešna, odredišni čvor odgovara sa frejmom dozvole za slanje (Clear To Send (CTS)).
- Svi mrežni čvorovi koji prime CTS frejm zaustavljaju pristup medijumu, osim čvora kome je CTS frejm bio namenjen.
- Taj čvor započinje slanje korisničkih podataka.
- Nakon završetka slanja podataka, odredišni čvor odgovara frejmom uspešnog prijema (ACK).
- Svi čvorovi koji prime ovaj frejm registruju da je bežični medijum slobodan i mogu da mu pristupe.
- Ukoliko čvor ne primi frejm uspešne transmisije u nekom zadatom vremenskom periodu, podrazumeva da je medijum slobodan.
- Kada se ispostavi da je medijum slobodan, može se započeti novi pristup CSMA/CA ili RTS/CTS metodom.

Primer RTS/CTS protokola je dat na slici, gde terminal započinje prenos.

Bežične mreže: IEEE 802.11 standard

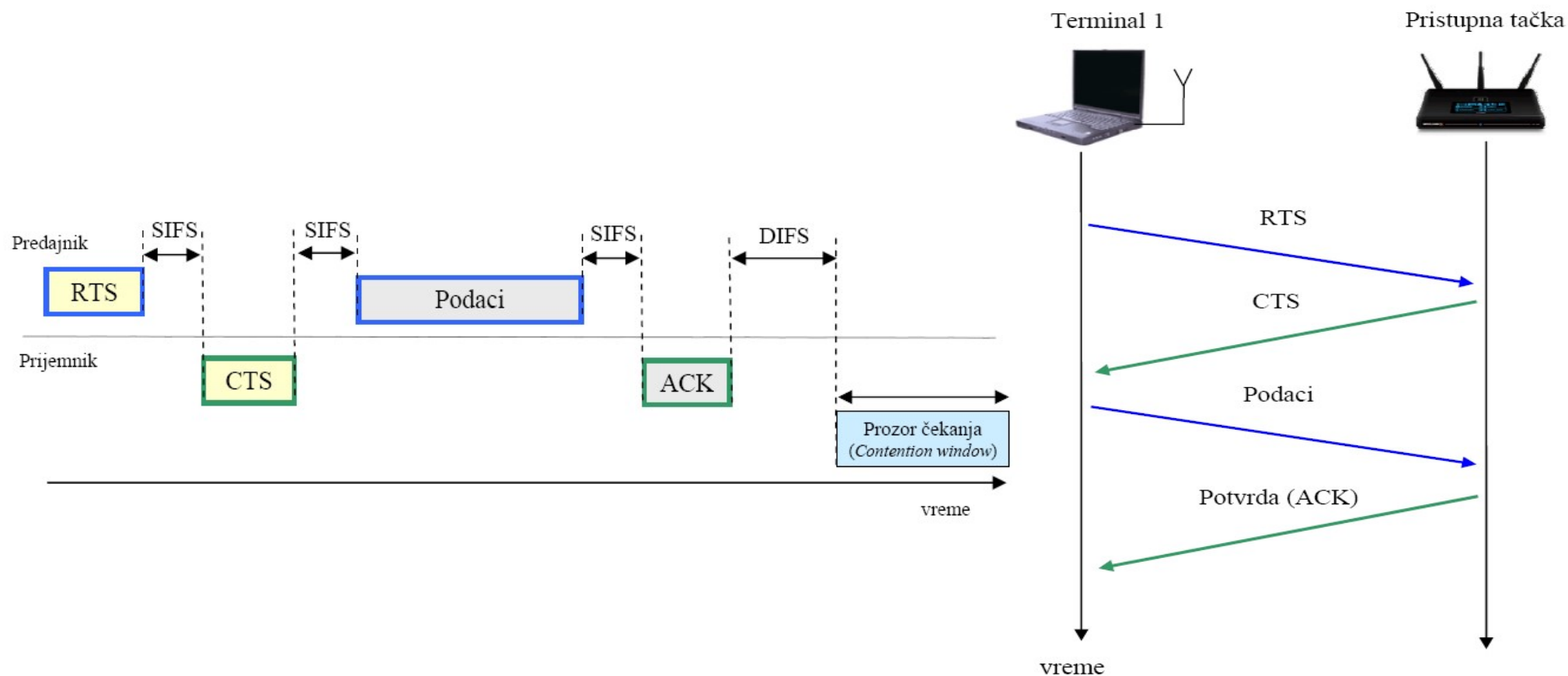
Metoda zahteva za slanje i dozvole za slanje (RTS/CTS)



Ako terminal 2 ne može da primi RTS okvir od terminala 1 (terminal 1 i 2 su skriveni jedan od drugoga), zahvaljujući prijemu CTS frejma koji je poslalo AP, terminal 2 će ipak biti obavešten o zauzeću medijuma. Ovim se znatno smanjuje verovatnoća kolizije usled pojave skrivenog terminala. Kolizija je i dalje moguća kada se terminal 2 pojavi u mreži u toku slanja podataka od strane terminala 1, te terminal 2 nije imao mogućnost da primi RTS ili CTS frejm i time nema informaciju o zauzeću medijuma.

Bežične mreže: IEEE 802.11 standard

Metoda zahteva za slanje i dozvole za slanje (RTS/CTS)



Vremenski dijagram RTS/CTS protokola je dat na slici.

Bežične mreže: IEEE 802.11 standard

Metoda zahteva za slanje i dozvole za slanje (RTS/CTS)

Short InterFrame Spacing (SIFS) je vremenski interval između frejmova u RTS/CTS sesiji. Treba uočiti da je SIFS kraći od DIFS. Osnovni razlog za to je da terminal koji primenjuje metodu detekcije nosioca i izbegavanje kolizije i prati zauzeće medijuma, ne započne predaju dok god čitava RTS/CTS sesija ne bude završena. Drugi razlog je da se poveća efikasnost pristupa medijumu (tj., da se smanji protocol overhead) jer se u toku ovakve sesije tačno zna ko i kada šalje.

U odnosu na metodu detekcije nosioca i izbegavanje kolizije, ova metoda ima **prednosti**:

- ima mnogo manju verovatnoću kolizije i uspešno rešava problem skrivenog terminala.

Sa druge strane, nedostaci su:

- sto ona unosi dodatni kontrolni saobraćaj i čekanja (protocol overhead) u vidu kontrolnih frejmova (RTS i CTS) i perioda čekanja (SIFS i DIFS).

U slučaju prenosa dužih blokova korisničkih podataka, metoda zahteva za slanje i dozvole za slanje (RTS/CTS) postaje efikasnija pošto se smanjuje relativna dužina trajanja kontrolnih okvira i perioda čekanja. Stoga, ako je dužina bloka manja od definisanog praga, koristi se CSMA/CA, a ako je duža onda se primenjuje RTS/CTS metoda. Vrednost praga se obično postavlja u okviru drajvera bezicne kartice terminala ili AP - a.

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 zicana 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.

VARIJACIJE STANDARDA 802.11

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 modulirani 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 koja se koriste kao kodna sekvenca pri procesu širenja spektra DSSS tehnikom. Da li će protok biti 11 Mb/s ili 5,5 Mb/s zavisi od stanja u kanalu, a uređaj se sam tome prilagođava.

VARIJACIJE STANDARDA 802.11

Standard IEEE 802.11g

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

Standard IEEE 802.11e

U standardu IEEE 802.11e unapređene su koordinacione funkcije MAC podsloja tako da se definišu klase saobraćaja. Tako da se na primer e-pošti može dodeliti najniži prioritet, a govoru najviši. Stanica sa većim prioritetom u proseku čeka malo manje, pre nego što pošalje svoj frejm, 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 frejmova.

Kvalitet usluga (QoS) može se podešavati prema zahtevima korisnika. Na taj način su obezbeđeni uslovi za kvalitetan prenos govora i videa.

VARIJACIJE STANDARDA 802.11

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 šifriranje. 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

Bitske brzine veće od 100Mb/s (do 600 Mb/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).

VARIJACIJE STANDARDA 802.11

Standard IEEE 802.11ax

IEEE 802.11ax, koji Wi-Fi Alliance zvanično oznacio kao Wi-Fi 6 (2,4 GHz i 5 GHz) i Wi-Fi 6E (6 GHz). Četvorostruko povećanje ukupne propusnosti u odnosu na Wi-Fi 5 omogućeno je većom spektralnom efikasnošću. Ključna karakteristika koja ovo omogućava OFDM . Ostala poboljšanja u korišćenju spektra su bolje metode kontrole snage kako bi se izbegle smetnje sa susednim mrežama kao i QAM višeg reda 1024QAM

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.

VARIJACIJE STANDARDA 802.11

Generation	IEEE standard	Adopted	Maximum link rate (Mbit/s)	Radio frequency (GHz)
Wi-Fi 7	802.11be	(2024)	1376–46120	2.4, 5, 6
Wi-Fi 6E	802.11ax	2020	574–9608 ^[1]	6 ^[a]
Wi-Fi 6		2019		2.4, 5
Wi-Fi 5	802.11ac	2014	433–6933	5 ^[b]
Wi-Fi 4	802.11n	2008	72–600	2.4, 5
(Wi-Fi 3)*	802.11g	2003	6–54	2.4
(Wi-Fi 2)*	802.11a	1999		5
(Wi-Fi 1)*	802.11b	1999	1–11	2.4
(Wi-Fi 0)*	802.11	1997	1–2	2.4