

ZAVOD ZA ELEKTRONIKU, MIKROELEKTRONIKU, RAČUNALNE I INTELIGENTNE SUSTAVE
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
SVEUČILIŠTE U ZAGREBU

IEEE 802.16 Standard

ZORAN RUŠINOVIĆ
MREŽE RAČUNALA

Zagreb, 2002

1.UVOD	1
1.1 UVOD U IEEE 802.16 (WIRELESSMAN™) STANDARD	1
1.2 KVALITETA USLUGE (QOS) ZA BWA.....	2
1.3 REFERENTNI MODEL ZA BEIINI ŠIROKOPOJASNI PRISTUP	3
2. MAC SLOJ	4
2.1 MAC CS (CONVERGENCE SUBLAYER).....	5
2.1.1 ATM CS.....	5
2.1.2 Paketni CS.....	6
2.2. MAC CPS (COMMON PART SUBLAYER)	9
2.2.1 MAC usluge.....	10
2.2.2 MAC adrese i povezivanje	11
2.2.3 Mehanizmi dodijele uplinka.....	16
2.2.4 Mehanizmi alociranja propusnog pojasa	17
2.2.5 MAC potpora fizičkom sloju	18
2.3 MAC P (PRIVACY SUBLAYER)	20
2.3.1 Kriptiranje paketa podataka.....	20
2.3.1 Protokol za upravljanje ključevima (PKM protokol)	21
2.3.2 Sigurnosne asocijacije (SA).....	21
3. FIZIČKI SLOJ (PHY).....	23
3.1 FIZIČKI SLOJ ZA FREKVENCIJSKI OPSEG 10-66 GHZ	23
3.1.2 Downlink.....	24
3.1.2 Uplink.....	27
3.2 BRZINE I PROPUSNOST.....	28
4. PRAKTIČNE IZVEDBE 802.16 SUSTAVA.....	29
4.1 VRSTE IZVEDBI 802.16 SUSTAVA	29
4.1.1 PMP sustav	29
4.1.2 MP-MP sustavi (Mesh).....	29
4.2 SMETNJE (INTERFERENCIJE)	29
4.2.1 Smetnje baznoj stanici	31
4.2.2 Smetnje korisničkoj stanici	32
5. ZAKLJUČAK.....	34
6.LITERATURA	35

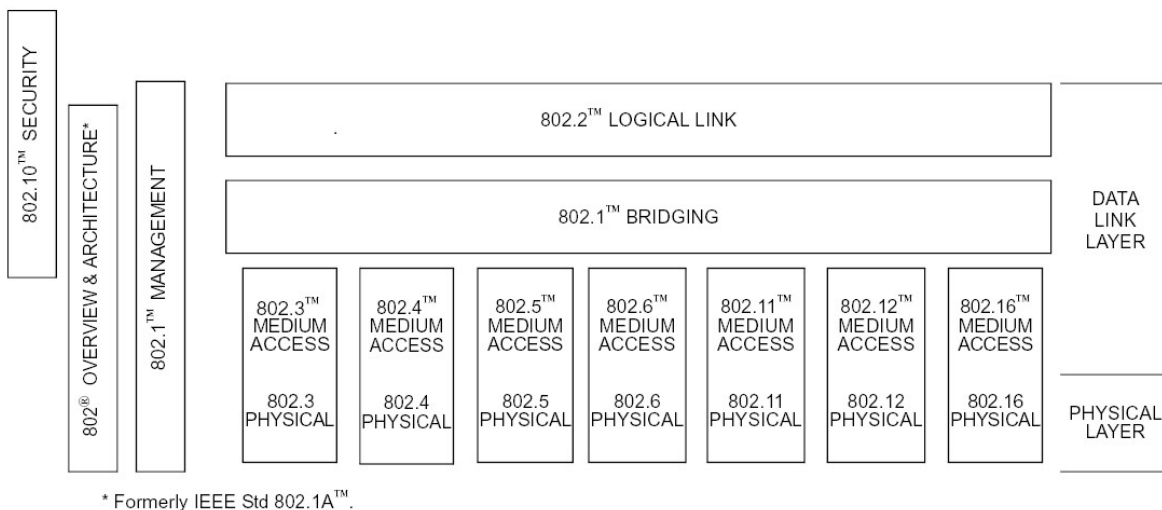
1. Uvod

Sve većim porastom potreba za brzim Internet vezama i višemedijskim prijenosom (integrirani prijenos podataka, digitaliziranog govora i videa) bežični širokopolasni pristup (BWA- *Broadband wireless access*) postao je vrlo pogodan način za ostvarenje takvih potreba. Takav pristup omogućuje proširenje postojećih mreža, uglavnom baziranih na optičkim vlaknima, i pružanje veće propusnosti od one dostupne širokopolasnim prijenosom preko kabelske mreže (*broadband transmission*) ili prijenosom preko DSLa (*Digital Subscriber lines*).

Pri tome, kao jedan od najznačajnijih aspekata ove tehnologije, je mogućnost izgradnje visokopropusnih mreža u vrlo kratkom vremenu postavljanjem tek malog broja baznih stanica.

1.1 Uvod u IEEE 802.16 (WirelessMAN™) standard

Da bi omogućili veću BWA dostupnost IEEE-SA (*The Institute of Electrical and Electronics Engineers Standards Association*) je izradio IEEE standard 802.16, koji definira sučelje za pristup bežičnim gradskim mrežama (*WirelessMAN Air Interface*). Taj standard dio je skupine standarda za lokalne i gradske mreže, a njegovo mjesto unutar te skupine prikazano je na slici 1.1. Svaki od standarda unutar te skupine definira metode pristupa mediju (*Medium Access*) te pripadajuće prijenosne medije (*Physical*) za određeni tip mreže, odnosno IEEE 802.X standardi definiraju usluge i protokole za fizički i podatkovni sloj unutar ISO OSI RMa (*International Organization for Standardization (ISO) Open Systems Interconnection Basic Reference Model*).



Slika 1.1 Skupina IEEE 802. standarda. Brojevi označavaju pripadajući IEEE standard.

IEEE 802.16 standard donesen je u travnju 2002. godine, a sam razvoj, pod predsjedanjem Dr. Rogera Marksa trajao je dvije godine. Kao što je u većem Standard definira sučelje za pristup bežičnim gradskim mrežama. Riječ je, dakle, o lokalnoj petlji (*first-mile/last-mile*), a glavni naglasak je na efikasnoj upotrebi frekvencijskog opsega između 10 i 66 GHz (u izradi je draft dodatka IEEE 802.16 standardu koji će koristiti frekvencijski opseg između 2 i 11 GHz) i definiranju MAC podsloja koji podržava specifikacije različitih fizičkih slojeva, u zavisnosti o frekvenciji koja se koristi.

Pri tome kad govorimo o IEEE 802.16 standardu važno je napomenuti da je riječ isključivo o fiksnom bežičnom širokopolasnom pristupu, dakle onom u kojem su tijekom rada i bazna i

korisnička stanica nepokretne. Za potrebe izrade IEEE standarda za mobilni bežični širokopojasni pristup osnovana je radna grupa u travnju 2002.

Danas je u svijetu za mala poduzeća i kućne korisnike uobičajen način povezivanja putem DSLa ili putem kabelaške veze. DSL je tip veze koji je baziran na bakrenoj parici i omogućuje veze tipično između 128 kbps i 1.5 Mbps, međutim ovaj tip veze nije svugdje dostupan zbog ograničenja postavljenih na maksimalnu dozvoljenu udaljenost između korisnika i lokalne centrale.

S druge strane kabelaške mreže grade se na postojećoj infrastrukturi kabelaških TV mreža i također nisu svugdje dostupne, naročito ne u poduzećima.

Drugi nedostatak ovakvih veza, kao i starijih bežičnih sustava, je vrlo mala propusnost u smjeru u kojem korisnik šalje podatke (*upstream bandwidth*).

IEEE 802.16 standard za bežični širokopojasni pristup osigurava mogućnost diferenciranog¹ širokopojasnog pristupa uz prihvatljivu cijenu, omogućuje pristup tisućama korisnika integriranom prometu podataka, digitaliziranog govora i videa te osigurava skalabilnost na način da se proširenje sustava može izvesti jednostavnim dodavanjem dodatnih kanala ili čelija.

1.2 Kvaliteta usluge (QoS) za BWA

Bežični širokopojasni pristup je pristup koji se odvija kroz slobodan prostor i koji zahtijeva neprekinutu vizualnu vezu (*line-of-sight*) i kao takav je podložan prigušenju i smetnjama iz različitih izvora kao što su npr. vremenske nepogode, prirodna vegetacija ili prolaz vozila. IEEE 802.16 standard ne razmatra sustave koji bi radili i bez izravne vizualne veze (*non line-of-sight transmission*), već će takvi sustavi biti razmotreni u već spomenutom dodatku za frekvencijski opseg između 2 i 11 GHz. Ono što, međutim, IEEE 802.16 standard osigurava su mehanizmi koji omogućuju robusne veze za PMP (*Point-to-Multipoint*) BWA sustave koji rade s neprekinutom vizualnom vezom. PMP u bežičnim mrežama označava takvu topologiju kod koje jedna bazna stanica opslužuje više korisničkih stanica koje su geografski udaljene, dok svaka korisnička stanica cijelo vrijeme ostaje vezana na samo jednu, i to uvijek istu, baznu stanicu.

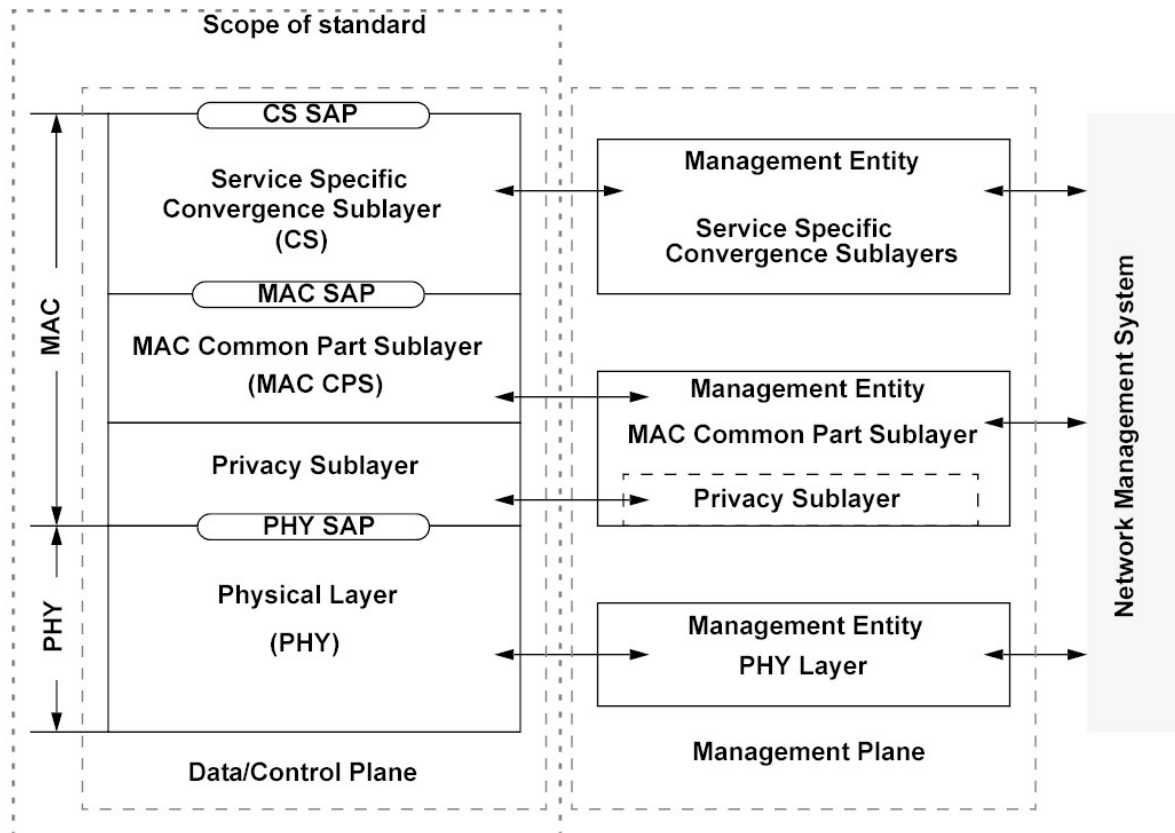
Mehanizmi pristupa prijenosnom mediju kod bežičnog širokopojasnog pristupa osiguravaju diferencirani QoS kao podršku različitim potrebama različitih primjena. Primjerice, digitalizirani glas i video zahtijevaju što manje kašnjenje, ali dopuštaju određenu pojavu pogrešaka pri prijenosu. S druge strane generičke programske aplikacije ne dopuštaju pojavu pogrešaka pri prijenosu, ali kašnjenje nije kritično. IEEE 802.16 standard opslužuje ovakve različite zahtjeve pri prijenosu podataka upotrebom odgovarajućih mehanizama unutar MAC podsloja, što je bitno efikasnije nego kad bi se to radilo upotrebom slojeva koji se nalaze iznad MACa, a što je uobičajeno u žičnim mrežama.

Brojni bežični sustavi u prošlosti koristili su fiksnu modulaciju. Modulacije viših redova u takvim sustavima omogućuju veću brzinu, ali zahtijevaju optimalne fizičke veze. Nasuprot njima modulacije nižih redova su znatno robusnije, ali omogućuju i znatno manje brzine. IEEE 802.16 standard podržava prilagodljivu modulaciju (*adaptive modulation*), čime se osigurava efikasno balansiranje između linija različitih kvaliteta i potreba za različitim brzinama. Standard također podržava frekvencijski i vremenski multipleks (i *dupleks* kao specijalni slučaj multipleksa, u kojem su vremenski ili frekvencijski multipleksirane samo dvije linije).

¹ Diferencirani pristup označava takav pristup u kojem je moguće svakom pojedinom korisniku pružiti određenu kvalitetu i vrstu usluge, neovisno o kvaliteti i vrsti usluge drugih korisnika.

1.3 Referentni model za bežični širokopojasni pristup

Slika 1.2. prikazuje referentni model za BWA i djelokrug standarda (*scope*).



Slika 1.2. Uslojavanje IEEE 802.16 standarda sa prikazanim točkama pristupa usluzi (SAP).

MAC sloj obuhvaća tri dodatna podsloja:

MAC CS (MAC C podsloj) pruža usluge pretvaranja podataka dobivenih iz mreže, preko CS pristupne točke (SAP), u MAC SDU (*Service Data Unit*) koje će biti predane MAC CPSu (MAC CP podsloj) preko MAC SAPa. To podrazumijeva klasificiranje SDUova dobivenih iz vanjske mreže i pridruživanje odgovarajućeg MAC CIDA (*Connection Identifier*) odnosno identifikatora veze.

MAC CPS (MAC CP podsloj) osigurava osnovnu funkcionalnost pristupa sustavu, alociranje potrebnog propusnog opsega kao i uspostavljanje i održavanje veze. MAC CPS prima podatke od različitih CSova preko MAC SAPova grupiranih prema odgovarajućim MAC vezama.

MAC Privacy Sublayer (MAC P podsloj) pruža uslugu autentifikacije² (*authentication*), sigurne razmjene ključeva (*secure key exchange*) i enkripcije (*encryption*).

Fizički sloj (PHY) može sadržavati višestruke specifikacije, karakteristične za pojedini frekvencijski opseg i pojedinu uslugu. Podržane specifikacije opisane su u poglavlju koje obrađuje fizički sloj.

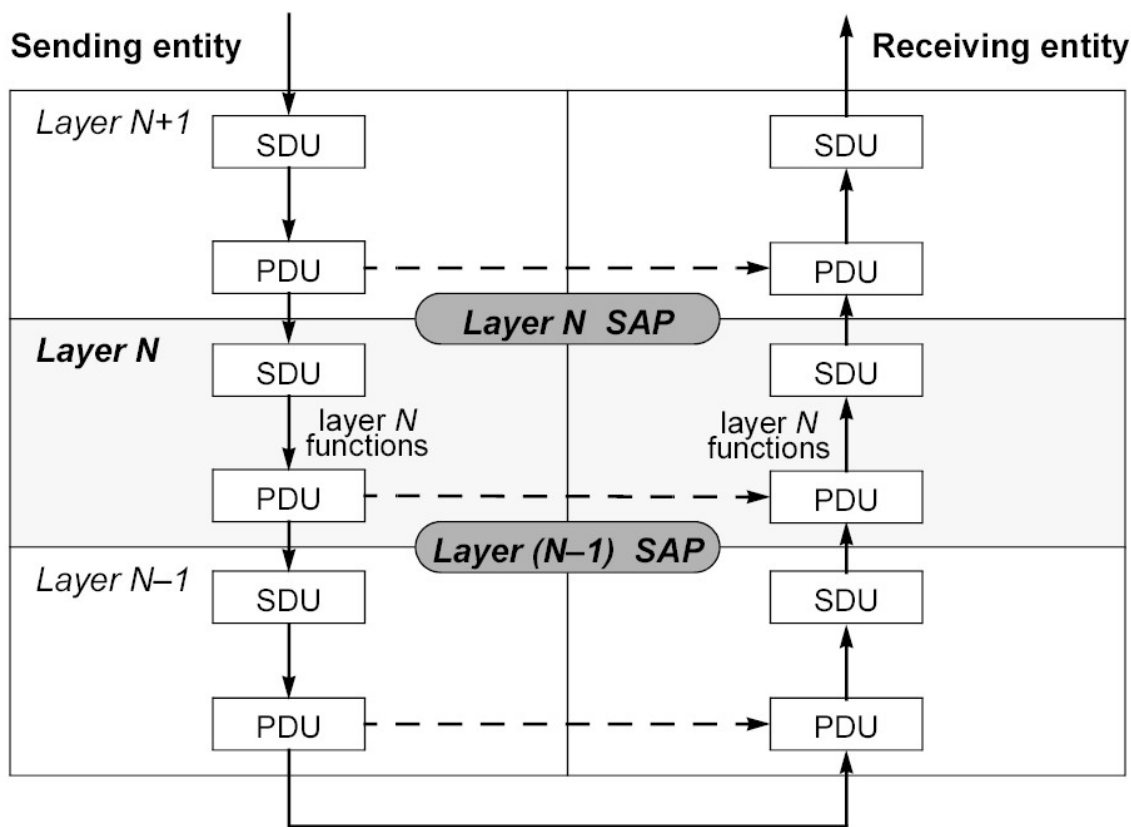
² U hrvatskom se jeziku upotrebljava i neposredan prijevod s engleskog – autentifikacija. Međutim, na osnovi tvorbe naziva identifikacija (od. lat. *idem* - isti i lat. *facio* – činiti) preciznije je koristiti naziv autentifikacija ([Budin02]).

2. MAC Sloj

Kao što je u uvodu prikazano MAC sloj sastoji se od tri podsloja: C podsloja (*Convergence Sublayer*), CP podsloja (*Common Part Sublayer*) i P podsloja (*Privacy Sublayer*). U nastavku će biti pojedinačno opisan svaki od tih podslojeva.

Radi lakšeg praćenja daljnjeg teksta, na ovom će mjestu, samo kratko, biti objašnjena razmjena jedinica podataka unutar OSI koncepta pružanja usluge (za detalje pogledati [Glavini02] ili [Tanennbaum96]).

Partnerski entiteti, odnosno entiteti u istom sloju ali na različitim strojevima, komuniciraju razmjenom PDU jedinica podataka. Kod entiteta koji šalje podatke, PDU je jedinica podataka³ koja se predaje prvom nižem sloju (u točki pružanja usluge) i dobivena je na način da se SDU jedinici podataka prije predaje nižem sloju doda zaglavlje. Kod entiteta koji prima podatke, PDU je jedinica podataka primljena od prvog nižeg sloja. SDU je jedinica podataka koja se razmjenjuje među susjednim slojevima. Kod entiteta koji šalje podatke to je jedinica podataka primljena od prvog višeg sloja, dok je kod entiteta koji prima podatke to jedinica podataka koja se predaje prvom višem sloju. Prema tome najjednostavnije možemo reći da (N)-PDU prelaskom u niži sloj postaje (N-1)-SDU i obrnuto, (N-1)-SDU prelaskom u viši sloj postaje (N)-PDU. Ovaj koncept prikazan je na slici 2.1.



Slika 2.1 Koncept pružanja usluge razmjenom PDU/SDU

³ Kako je PDU skraćenica od *Protocol Data Unit* nije jezično sasvim ispravno govoriti «PDU jedinica podataka», jer je to već sadržano u samoj skraćenici PDU, međutim radi jednostavnosti ovdje je to učinjeno.

2.1 MAC CS (Convergence Sublayer)

MAC CS (*Convergence Sublayer*) nalazi se na vrhu MAC sloja i iznad MAC CPS podsloja (slika 1.2) te koristi usluge MAC CPSa. MAC CS ima sljedeće funkcije :

- Prihvata PDUove iz višeg sloja
- Klasificira PDUove dobivene iz višeg sloja
- Prema potrebi vrši konverziju nad PDUovima iz višeg sloja
- Na osnovu klasifikacije predaje PDUove odgovarajućem MAC SAPu
- Prihvata CS PDUove iz partnerskih entiteta
- Uklanjanje i obnavljanje dijelova informacija iz zaglavlja poruke (PHS – *Payload Header Supression*)

Klasifikacija PDUova je proces u kojem se na osnovi određenih parametara (klasifikatora) određuje na koju će vezu, odnosno na koji će MAC SAP, određeni PDU biti predan. Trenutno postoje dvije CS specifikacije: asinhroni (ATM) CS i paketni CS.

2.1.1 ATM CS

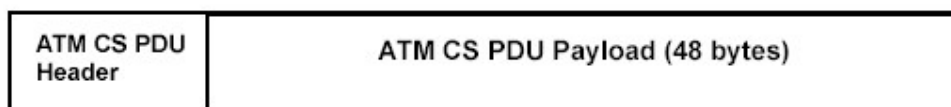
ATM CS je logičko sučelje koje povezuje različite ATM (*asynchronous transfer mode*) usluge sa MAC CPS pristupnom točkom. ATM CS prima ATM čelije od ATM sloja (OSI slojevi 2/3), vrši klasifikaciju, prema potrebi vrši PHS operaciju i zatim dostavlja CS PDUove odgovarajućoj MAC pristupnoj točki. PHS je proces u kojem se dijelovi zaglavlja poruke, koji se uzastopce ponavljaju, uklanjaju (sažimlju) na strani pošiljatelja a obnavljaju na strani primatelja. U ovom se slučaju na strani pošiljatelja uklanjaju dijelovi zaglavlja informacijskog polja iz CS SDUa koji se uzastopce ponavljaju, a obnavljaju se na strani primatelja. U slučaju *downlinka* pošiljatelj je ATM CS na baznoj stanici, a primatelj je ATM CS na korisničkoj stanici, dok je u slučaju *uplinka* situacija obrnuta.

ATM veza jednoznačno je određena parametrima VPI (*Virtual Path Identifier*) i VCI (*Virtual Channel Identifier*). ATM CS podržava poslovanje i virtualnim vezama (*Virtual Path switched*) i virtualnim kanalima (*Virtual Channel switched*), i pri tome PHS vrši uklanjanje informacija iz zaglavlja sukladno modu rada.

Klasifikacija ATM čelija koje dolaze do MAC CSa vrši se na osnovi VPI, VCI i CID klasifikatora. Ako ATM čelija zadovoljava kriterij klasifikacije zadan navedenim klasifikatorima, tada se ona dostavlja na odgovarajući MAC SAP.

Da bi se još dodatno uštedilo na propusnom opsegu više ATM čelija (sa ili bez primjene PHSa) koje imaju isti CID mogu biti zapakirane i prenesene unutar jednog MAC CPS PDUa.

Format ATM CS PDUa prikazan je na slici 2.2.



Slika 2.2 ATM CS PDU format

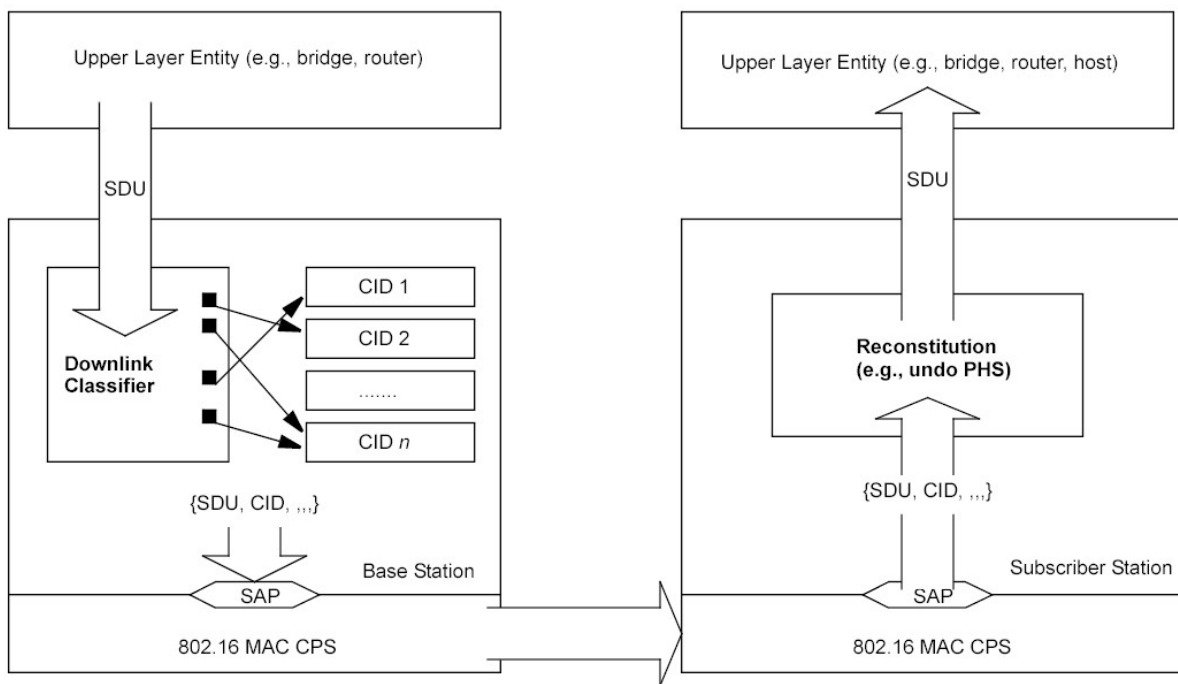
ATM CS PDU sastoji se od ATM CS PDU zaglavlja i ATM CS PDU informacijskog polja (*payload*) koje je identično sa primljenom ATM čelijom (SDU).

2.1.2 Paketni CS

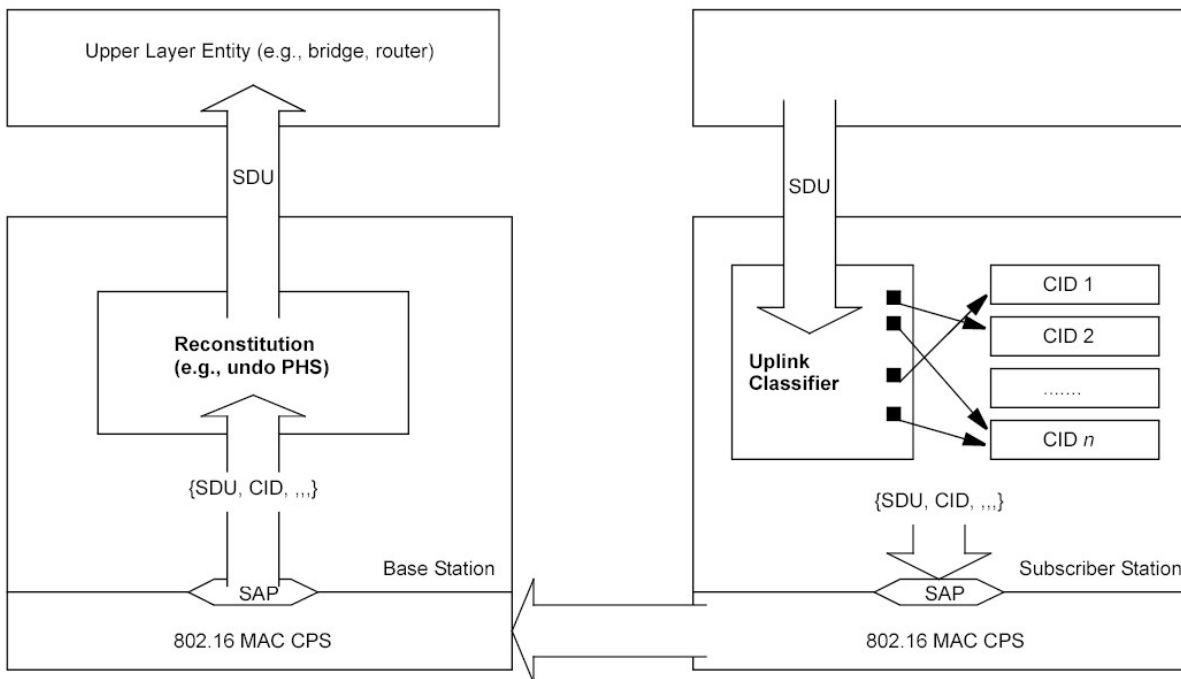
Paketni CS je logičko sučelje koje se koristi za prijenos prema MAC CPSu za sve paketne protokole, kao što su internet protokoli (IPv4 i IPv6), PPP protokol (*point-to-point*) i IEEE 802.3 standard (Ethernet).

U ovom se slučaju klasifikacija paketa koji dolaze do MAC CSa IEEE 802.16 mreže vrši na osnovu određenih klasifikatora karakterističnih za određeni protokol (primjerice IP adresa), na osnovi prioriteta i na osnovi reference na određeni CID (*Connection Identifier*). Ako paket zadovoljava kriterij klasifikacije zadan nekim od navedenih klasifikatora tada se on dostavlja do pristupne točke (SAP) za dostavu na vezu definiranu CIDom. Karakteristike upravljanja protokom za svaku pojedinačnu vezu pružaju određenu kvalitetu usluge (QoS) tom paketu. Budući da uvjet klasifikacije može biti zadan korištenjem nekoliko klasifikatora, svaki klasifikator ima svoj prioritet kako bi se izbjegla nejednoznačnost. Moguće je da određeni paket ne zadovolji uvijete klasifikacije u kojem slučaju CS može, zavisno od izvedbe, ili odbaciti paket ili ga poslati na unaprijed određeni CID.

Klasifikatori za downlink zadaju se od strane bazne stanice, dok se klasifikatori za uplink zadaju od strane korisničke stanice. Na slikama 2.3 i 2.4 prikazani su postupci klasificiranja za downlink i uplink.



Slika 2.3 Klasifikacija i CID mapiranje za downlink



Slika 2.4 Klasifikacija i CID mapiranje za uplink

Bazna stanica i korisnička stanica mogu prema potrebi realizirati PHS na slobodan način pod uvjetom da se poštuju pravila definirana protokolom.

Svaki MAC SDU dobiva PHSI (*payload header suppression index*) prefiks koji se odnosi na pojedini PHSF (*payload header suppression field*). PHSF predstavlja niz bajtova koji čine zaglavlje PDUa i u kojem je jedan ili više bajtova biti sažeti (to je u osnovi slika zaglavlja PDUa prije kompresije PHS metodom). PHSI je 8 bitni prefiks koji određuje pripadajući PHSF.

PHS ima i PHSV opciju (*payload header suppression valid*) koja određuje dali li se zaglavlje provjeravati prije sažimanja (to je zapravo zastavica veličine jednog bajta), kao i PHSM opcija (*payload header suppression mask*) kojom se omogućuje da se definiraju bajtovi koji se neće sažimati jer se mijenjaju od paketa do paketa (primjerice kontrolni izražun i sl.).

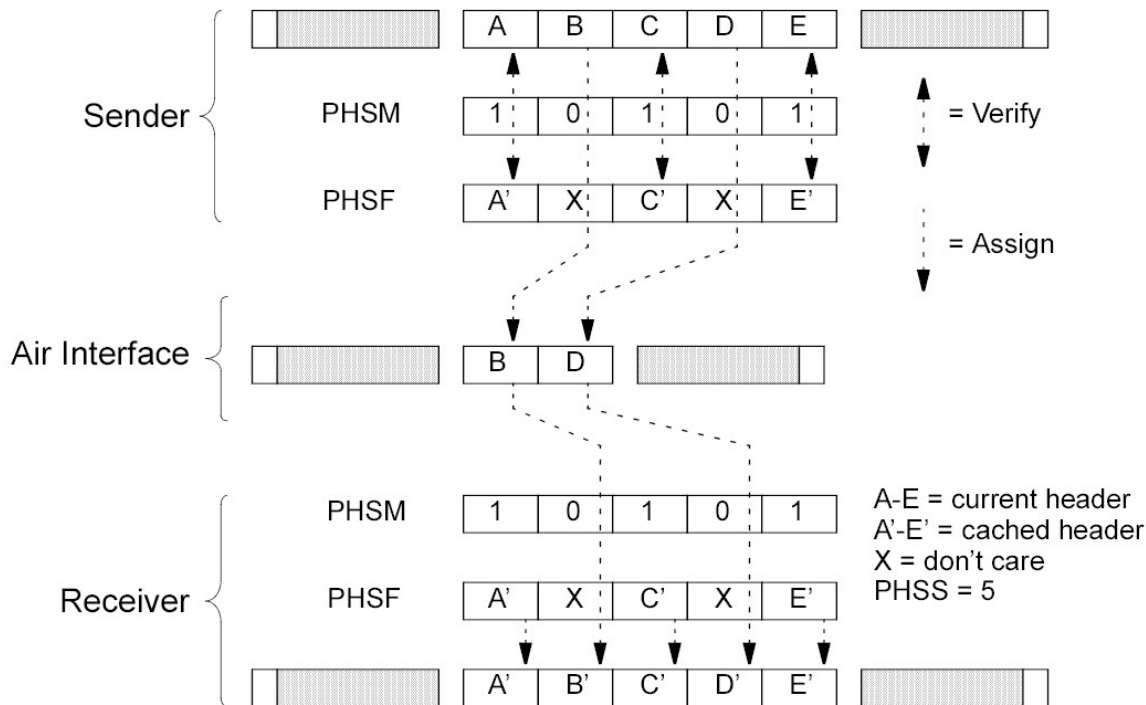
Na slici 2.5 zorno je prikazan jedan takav postupak sažimanja i obnavljanja bajtovnog niza primjenom PHS postupka i uz PHS maskiranje (odnosno uz definirane PHSM bitove, koji omogućuju da se definiraju bajtovi unutar izvornog paketa koji se neće sažimati jer se mijenjaju u svakom paketu).

Kod uplinka procedura propisana protokolom je slijedeća:

Nakon što je paket predan paketnom CSu korisničke stanice, CS primjenjuje listu klasifikatora. Kao rezultat toga dobije se *uplink tok*, odgovarajući skup CIDova i PHS pravila. PHS pravilo definira pripadni PHSF, PHSI, PHSM i PHSS. PHSS je kratica od *payload header suppression size* i predstavlja veličinu PHSFa u bajtovima tj. broj bajtova zaglavlja koje će se sažimati. Ako je postavljena PHSV opcija, korisnička stanica uspoređuje sve bajtove unutar zaglavlja primljenog paketa sa bajtovima unutar PHSFa koji će biti sažeti (što je definirano maskom PHSM). Ako se bajtovi poklapaju, korisnička stanica sažimlje sve bajtove iz PHSFa u poruci za uplink, osim onih definiranih PHSM maskom. Nakon toga korisnička stanica dodaje PHSI prefiks na PDU te predaje takav MAC SDU na MAC SAP za prijenos na uplink.

Kada bazna stanica (primatelj) primi paket pregledom generičkog MAC zaglavlja najprije odredi pripadajućim CID, te zatim pošalje primljeni PDU na odgovarajući MAC pristupnu točku (određenu pripadajućim CIDom). Nakon toga paketni CS u baznoj stanici, na osnovi CIDa i PHSIa, odredi ispravan PHSF, PHSM i PHSS.

Ako je bila postavljena opcija PHSV garantira se istovjetnost bajtova iz izvornog zaglavlja sa bajtovima u PHSFu. Ta opcija je inicijalno postavljena, aktivna je u logičkoj nuli, a njenim postavljanjem u logičku jedinicu traži se od pošiljatelja da vrši sažimanje zaglavlja poruka koje **alje bez** usporedbe sa PHSFom iz čega je jasno da ne postoji nikakva garancija da će paket sastavljen na suprotnoj stranici dodavanjem PHSFa biti identičan izvornom paketu.



Slika 2.5 PHS postupak sa PHS maskiranjem.
Kao što se vidi iz slike sažimlju se samo bajtovi koji u PHS maski imaju postavljen pripadajući bit na 1 (duljina tog polja je n bitova).

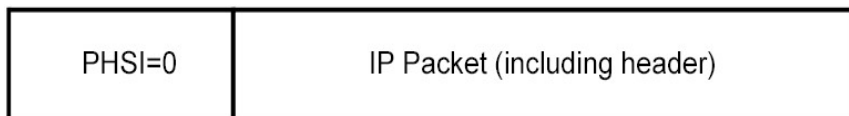
Procedura kod *downlinka* identična je gore opisanoj proceduri uz zamijenjene uloge bazne stanice (koja je sada pošiljatelj) i korisničke stanice (koja je sada primatelj).

Najprije bazna stanica primjeni svoj skup klasifikatora rezultat čega je *downlink tok*, sa skupom odgovarajućih CIDova i PHS pravila (koje definira pripadni PHSF, PHSI, PHSM i PHSS). Ako je postavljena opcija PHSV, bazna stanica uspoređuje zaglavlje poruke sa PHSF poljem i ako se podudaraju iz poruke se sažimlju svi PHSF bajtovi, te se na takav PDU se doda PHSI prefiks (koji određuje pripadni PHSF) i tako dobiveni SDU se predaje na MAC pristupnu točku.

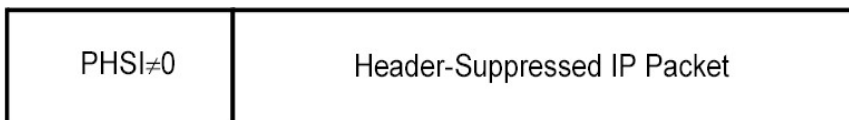
Kad korisnička stanica primi paket pregledom MAC zaglavlja određuje se MAC pristupna točka, a paketni CS u korisničkoj stanici na osnovu PHSI prefiksa određuje PHSF, PHSM i PHSS.

Samo određivanje PHS pravila koje jedinstveno određuje zamjenski niz bajtova (PHSF) unutar jednog opslužnog toka (*service flow*) zadaća je entiteta iz viših slojeva. Njihova je zadaća također i osigurati nepromjenjivost takvog bajtovnog niza koji se sažimlje za vrijeme trajanja svakog opslužnog tok.

Formati IP CP PDU paketa prikazani su na slikama 2.6 i 2.7.



Slika 2.6 IP CS PDU format bez sažimanja zaglavlja



Slika 2.7 IP CS PDU format sa sažimanjem zaglavlja

2.2. MAC CPS (Common Part Sublayer)

Svaka mreža koja koristi dijeljenje prijenosnog medija zahtijeva mehanizme za efikasno ostvarenje dodijele tog prijenosnog medija. Dobar primjer dijeljenja prijenosnog medija je dvosmjerna *point-to-multipoint* bežična mreža gdje je dijeljeni medij prostor kroz koji se šire radio-valovi. *Downlink*, od bazne do korisničke stanice, takve mreže radi na *point-to-multipoint* principu odnosno na principu mreže s difuzijom. Svaka bazna stanica ima sektorizirane antene koje su u mogućnosti simultano pokrivati nekoliko nezavisnih sektora, a unutar određenog sektora (i određene frekvencije) sve korisničke stanice primaju iste podatke ili njihove dijelove (princip tzv. promiskuitetnih mreža gdje korisnička stanica provjerava adresu primatelja u primljenoj poruci i zadržava samo poruke upućene njoj). U suprotnom smjeru sve stanice dijele *uplink*, na principu pojedinačne potreba. Unutar sektora sve korisničke stanice pridržavaju se MAC protokola koji nadgleda dodjelu prijenosnog medija i osigurava potreban propusni opseg uz dopustljivo kašnjenje svake stanice. To se postiže kroz implementaciju mehanizma za dodjelu *uplinka* baziranih na cikličkoj dodjeli, dodjeli prozivkom i dodjeli sukobom u zavisnosti od potreba pojedine stanice. Primjerice dodjela sukobom može se koristiti da se izbjegne prozivka stanica koje su dugo neaktivne, dok s druge strane prozivka osigurava determinističku dodjelu prijenosnog medija, ako je to potrebno.

Bazna stanica može dodjeljivati propusni opseg na bazi pojedine veze (spoja) ili na bazi sveukupno akumuliranih zahtjeva unutar određenog vremenskog intervala.

Jednom ostvarena veza može zahtijevati aktivnu brigu oko njenog održavanja tijekom trajanja te veze. Primjerice IP usluga može zahtijevati značajne prilagodbe tijekom veze, zbog velike vjerojatnosti fragmentiranja kao i čestih pojava usnopljenog prometa

MAC sloj je spojno orijentiran (*connection-oriented*), odnosno cjelokupna razmjena podataka odvija se u kontekstu pojedine veze a u svrhu pridruživanja pojedinih usluga i njihove kvalitete (QoS) pojedinim korisničkim stanicama. Odmah po uključenju pojedine korisničke stanice u sustav, opslužnom toku te korisničke stanice pridružuje se odgovarajuća veza (jedna veza po jednom opslužnom toku). Dodatno nove veze mogu biti uspostavljene, ako korisnička stanica treba nove usluge. Svaka veza definira opslužni tok i način mapiranja partnerskih procesa koji koriste MAC uslugu. Sam opslužni tok definira parametre kvalitete usluge (*QoS parameters*) za pojedine PDUove koji se izmjenjuju na pojedinoj vezi. Koncept opslužnog toka na pojedinoj vezi (spoju) bitan je za efikasan rad MAC protokola, jer opslužni tok osigurava mehanizme za upravljanje kvalitetom usluge na *uplinku* i *downlinku* i ključan je u postupku alociranja potrebnog propusnog

opseg (*bandwidth allocation process*). Svaka korisnička stanica može tražiti potreban propusni opseg na osnovi pojedine veze, čime je implicitno definiran i opslužni tok.

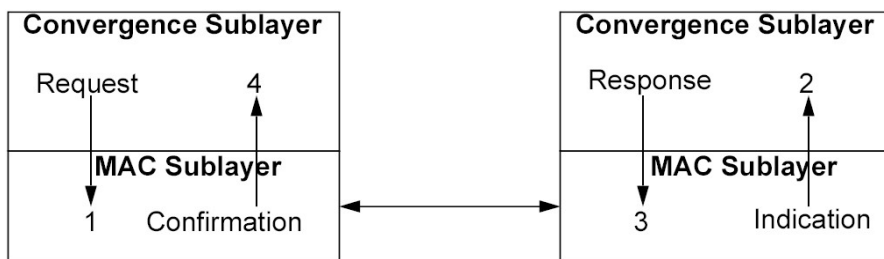
2.2.1 MAC usluge

U protokolima koji su organizirani po slojevima podaci koje se razmjenjuju na granici slojeva mogu biti opisane primitivima koji predstavljaju određeni podatak koji izaziva određenu radnju i služe da bi pojasnili odnose između pojedinih slojeva.

IEEE 802.16 standard podržava slijedeće primitive (dostupne u MAC točkama pristupa usluzi):⁴

MAC_CREATE_CONNECTION.request
MAC_CREATE_CONNECTION.indication
MAC_CREATE_CONNECTION.response
MAC_CREATE_CONNECTION.confirmation
MAC_CHANGE_CONNECTION.request
MAC_CHANGE_CONNECTION.indication
MAC_CHANGE_CONNECTION.response
MAC_CHANGE_CONNECTION.confirmation
MAC_TERMINATE_CONNECTION.request
MAC_TERMINATE_CONNECTION.indication
MAC_TERMINATE_CONNECTION.response
MAC_TERMINATE_CONNECTION.confirmation
MAC_DATA.request
MAC_DATA.indication

Na slici 2.8 prikazana je upotreba ovih primitiva na primjeru ostvarenja komunikacije između dva partnerska entiteta. Inicijalni zahtjev za ostvarenjem veze dolazi od CS sloja primjenom *request* primitiva (1). Taj zahtjev prima MAC CPS i šalje ga zračnom vezom (*air link*) do partnerskog MAC CPS podsloja (na slici označen kao **MAC Sublayer**). Partnerski MAC CPS generira *indicate* primitiv (2) kojim obavještava CS (partnerski entitet CSa koji je generirao *request*) o zahtjevu. CS odgovara *response* primitivom (3) koji se opet zračnom vezom šalje na stranu podnositelja zahtjeva, gdje MAC CPS šalje *confirm* primitiv (4) entitetu koji je podnio zahtjev.



Slika 2.8 Upotreba primitiva za uspostavu veze između partnerskih entiteta

⁴ Ovi primitivi dostupni su u MAC SAPovima, prema tome to su usluge dostupne na *logičkom sučelju* između MACa i CSa pa su zato i podržani primitivi samo informativni. Njihova je svrha da prikažu koji se podaci moraju razmijeniti između MACa i CSa da bi svaki od njih mogao obavljati svoju funkciju. IEEE 802.16 standard ne nameće formate za te primitive niti automate stanja za njihovo korištenje.

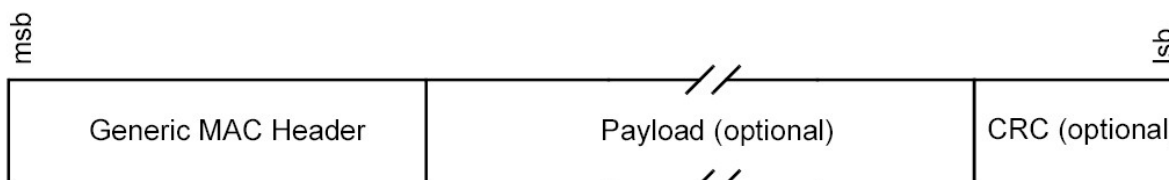
2.2.2 MAC adrese i povezivanje

Svaka korisnička stanica ima univerzalnu 48 bitnu MAC adresu, kako je to definirano u IEEE 802 standardu. Ova adresa jedinstveno određuje korisničku stanicu unutar skupa svih mogućih proizvođača i tipova opreme. Ta adresa koristi se u procesu registracije kojim se stvara odgovarajuća korisnička veza, kao i u procesu autentifikacije kojim bazna i korisnička stanica utvrđuju međusobne identitete. Svaka veza određena je 16-bitnim CIDom (*Connection ID*), čime je omogućena upotreba do 64K veza u svakom smjeru (uplink i donwlink).

Za vrijeme uspostave veze (inicijalizacije) za pojedinu korisničku stanicu stvaraju se tri upravljačke veze u svakom smjeru, tako da inherentno postoje tri različite kvalitete usluga za upravljanje prometom između bazne i korisničke stanice. Osnovna veza (*basic connection*) između MAC slojeva korisničke i bazne stanice koristi se za izmjenu hitnih i kratkih poruka.

Primarna upravljačka veza (*primary management connection*) koristi se za razmjenu dužih poruka, koje nisu hitne. Konačno, sekundarna upravljačka veza (*secondary management connection*) koristi se za razmjenu poruka koje nisu hitne, i oblikovane su u standardne pakete (DHCP, SNMP; TFTP itd.).

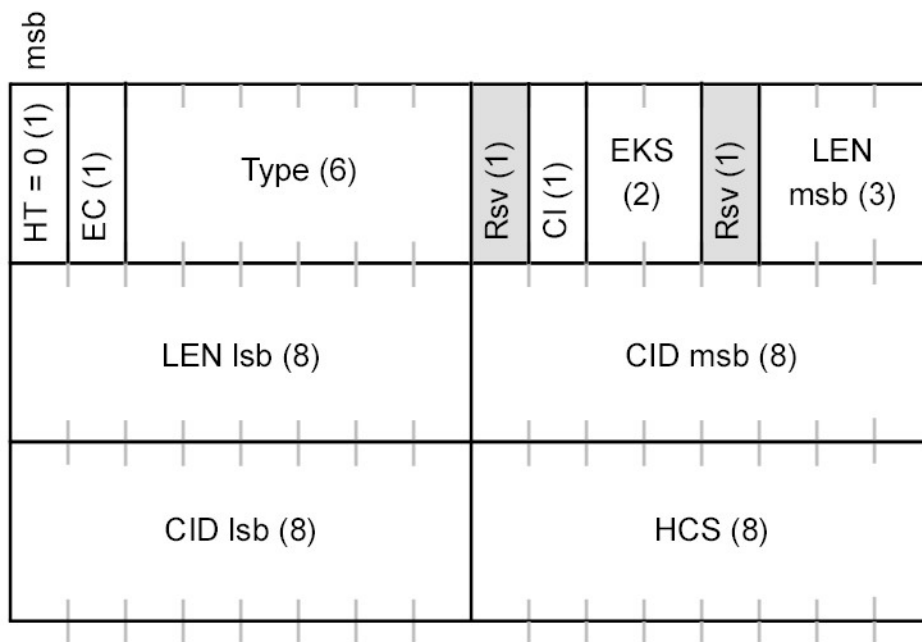
Na slici 2.9 prikazan je format MAC PDUa. Svaki PDU započinje sa generičkim MAC zaglavljem fiksne duljine. Iza njega slijedi informacijsko polje varijabilne duljine tako da i MAC PDU može biti varijabilne duljine, a prema potrebi informacijsko polje se do željene duljine popunjava nulama. To omogućuje jednostavno tuneliranje MAC PDUa unutar različitih pod mreža, ako je to potrebno. Na kraju MAC PDUa opcionalno se nalazi zaštitna riječ (CRC) koja pokriva MAC zaglavljem i informacijsko polje, a u slučaju da je prisutno i kriptiranje tada se zaštitna riječ rađuna posljednja.



Slika 2.9 MAC PDU format

Osim generičkog MAC zaglavlja kojim započinje svaki MAC PDU, a koji sadrži informacije potrebne za MAC upravljanje, postoji još jedan oblik MAC zaglavlja, a to je MAC zaglavljem zahtjeva za propusnim opsegom (*Bandwidth Request Header*) koje se koristi za zahtijevanje dodatnog propusnog opsega (to su takozvani *request MAC PDUovi* ili *Bandwidth request PDUovi*). O kojem se tipu zaglavlja radi određuje se na osnovi HT (*Header Type*) bita iz MAC zaglavlja. Ako je bit postavljen (HT=1) radi se o zaglavljem zahtijeva za dodatnim propusnim opsegom i takvi PDUovi nemaju CRC izračun.

Format MAC zaglavlja prikazan je na slici 2.10, dok je na slici 2.11 dano značenje pojedinih polja unutar zaglavlja.



Slika 2.10 format generičkog (HT=0) MAC zaglavlja

Name	Length (bits)	Description
CI	1	CRC Indicator 1 = CRC is appended to the PDU 0 = No CRC is appended
CID	16	Connection Identifier
EC	1	Encryption Control 0 = Payload is not encrypted 1 = Payload is encrypted
EKS	2	Encryption Key Sequence The index of the Traffic Encryption Key and Initialization Vector used to encrypt the payload. This field is only meaningful if the Encryption Control field is set to 1.
HCS	8	Header Check Sequence An 8-bit field used to detect errors in the header. The generator polynomial is $g(D)=D^8 + D^2 + D + 1$.
HT	1	Header Type. Shall be set to zero.
LEN	11	Length The length in bytes of the MAC PDU including the MAC header.
Type	6	This field indicates the payload type, including presence of subheaders.

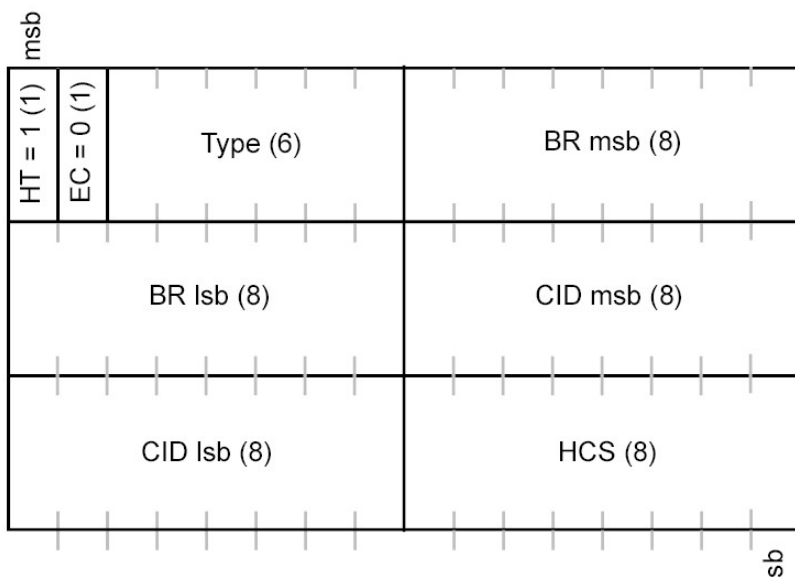
Slika 2.11 značenje pojedinih polja unutar generičkog MAC zaglavlja

Oznaka *Rsv* na slici 2.10 označava da se to polje (taj bajt) ne koristi, odnosno da je rezerviran za eventualnu buduću primjenu.

Zaglavlje na slici 2.10 je generičko jer nema postavljen HT bit (HT=0). Zaglavlje zahtijeva za propusnim opsegom (*Bandwidth Request Header*) ima postavljen HT bit (HT=1) a pripadajućim PDU-ovima (*Bandwidth Request PDU*) se sastoji samo od MAC zaglavlja, bez informacijskog polja i bez CRC izračuna. Format zahtijeva za dodatnim propusnim opsegom prikazan je na slici 2.12 i ima slijedeća svojstva:

- Zaglavlje je dugačko 6 bajtova
- EC polje nije postavljeno (EC=0) čim se signalizira da nema enkripcije

- CID određuje opslužni tok za koji se traži dodatni propusni opseg
- BR (*bandwidth request*) polje sadrži broj traženih bajtova za povećanje propusnog opsega
- Polje *Type* definira dali se traži povećanje (000000) opsega za iznos BR ili BR sadrži cjelokupni iznos potrebno opsega (000001)



Slika 2.12 Format MAC zaglavlja zahtijeva za dodatnim propusnim opsegom

Name	Length (bits)	Description
BR	16	Bandwidth Request The number of bytes of uplink bandwidth requested by the SS. The bandwidth request is for the CID. The request shall not include any PHY overhead.
CID	16	Connection Identifier
EC	1	Always set to zero.
HCS	8	Header Check Sequence An 8-bit field used to detect errors in the header. The generator polynomial is $g(D)=D^8 + D^2 + D + 1$.
HT	1	Header Type = 1
Type	6	Indicates the type of bandwidth request header

Slika 2.13 Značenje pojedinih polja unutar MAC zaglavlja zahtijeva za dodatnim propusnim opsegom

Budući da propusni opseg dodjeljuje bazna stanica, razumljivo je da zahtjevi za dodatnom propusnošću mogu ići samo od korisničke stanice prema baznoj stanici. U slučaju da korisnička stanica primi PDU traženja dodatnog opsega, ona ga zanemaruje.

Pored ova dva tipa MAC zaglavlja postoje još i tri tipa podzaglavlja (*Subheader*) čija prisutnost se naznačuje postavljanjem odgovarajućih bitova u *Type* polju MAC zaglavlja. Dva od njih su PDU podzaglavlja jer se odnose na PDU i ona se umetnu u MAC PDU neposredno iza generičkog MAC zaglavlja. To su *Fragmentation subheader* i *Grant Management subheader*. Podzaglavlje za fragmentaciju (*fragmentation subheader*) dugačko je 1 bajt i služi pri fragmentaciji PDUova. Podzaglavlje upravljanja dodjelom (*Grant Management subheader*) dugačko je 4 bajta i definira

određene postavke pri zahtjevima za propusnim opsegom. Primjerice tu se postavlja PM (*Poll Me*) bit o kojem će biti kasnije riječ.

Formati i značenja pojedinih polja dana su na slikama 2.14- 2.17

Syntax	Size	Notes
Fragmentation subheader () {		
FC	2 bits	
FSN	3 bits	
<i>reserved for CS use</i>	3 bits	
}		

Slika 2.14 Format podzaglavja za fragmentaciju

Name	Length (bits)	Description
FC	2	Fragmentation Control Indicates the fragmentation state of the payload: 00 = no fragmentation 01 = last fragment 10 = first fragment 11 = continuing (middle) fragment
FSN	3	Fragmentation Sequence Number Defines the sequence number of the current SDU fragment. This field increments by one (modulo 8) for each fragment, including unfragmented SDUs.

Slika 2.15 Značenje pojedinih bitova u podzaglavju za fragmentaciju

Syntax	Size	Notes
Grant Management subheader() {		
if (scheduling service type == UGS) {		
SI	1 bit	
PM	1 bit	
<i>reserved</i>	14 bits	Set to 0
}		
else {		
PiggyBack Request	16 bits	
}		
}		

Slika 2.16 Format podzaglavja upravljanja dodjelom prijenosnog medija

Name	Length (bits)	Description
PBR	16	PiggyBack Request The number of bytes of uplink bandwidth requested by the SS. The bandwidth request is for the CID. The request shall not include any PHY overhead.
PM	1	Poll-Me 0 = No action 1 = Used by the SS to request a bandwidth poll.
SI	1	Slip Indicator 0 = No action 1 = Used by the SS to indicate a slip of uplink grants relative to the uplink queue depth.

Slika 2.17 Značenje pojedinih bitova u podzaglavju za upravljanje dodjelom

Jedino SDU podzaglavje je podzaglavje pakiranja (*Packing subheader*). Ono se umetne ispred svakog MAC SDUa, ako je tako naznačeno u *Type* polju. Podzaglavja pakiranja i fragmentacije su međusobno isključiva i ne smiju biti prisutna unutar istog MAC PDUa. Isto tako, ako je prisutno, PDU podzaglavje mora doći prije SDU podzaglavja.

Zaglavje pakiranja koristi se za pakiranje više SDUova unutar jednog novog MAC SDUa, a MAC označava svaki takav 'zapakirani' SDU sa podzaglavljem pakiranja.

Oblik podzaglavja pakiranja prikazan je na slikama 2.18 i 2.19.

Syntax	Size	Notes
Packing sub-header () {		
FC	2 bits	
FSN	3 bits	
Length	11 bits	
}		

Slika 2.18 Format podzaglavja pakiranja

Name	Length (bits)	Description
FC	2	Fragmentation Control Indicates the fragmentation state of the payload: 00 = no fragmentation 01 = last fragment 10 = first fragment 11 = continuing (middle) fragment
FSN	3	Fragmentation Sequence Number Defines the sequence number of the current SDU fragment. This field increments by one (modulo 8) for each fragment, including unfragmented SDUs.
Length	11	The length in bytes of the MAC SDU or SDU fragment, including the two-byte packing subheader.

Slika 2.19 Značenje pojedinih bitova u podzaglavju pakiranja

2.2.3 Mehanizmi dodijele uplinka

Kako bi se povećala efikasnost dodijele prijenosnog medija i mehanizma prozivke, definirani su mehanizmi dodjele uplinka i pripadajućih QoS parametara.

Osnovne mehanizmi su: Dobrovoljno pružanje usluge (UGS), Prozivka u stvarnom vremenu (rtPS), Prozivka izvan stvarnog vremena (nrtPS) i Metoda najboljeg nastojanja (BE). Opis ovih mehanizama dan je u nastavku.

1. Dobrovoljno pružanje usluge (UGS – Unsolicited Grant Service)

Dobrovoljno pružanje usluge oblikovano je za podržavanje protoka podataka u stvarnom vremenu u kojem se generiraju paketi fiksne duljine u poznatim, periodičkim intervalima. Primjer takvog prometa je prijenos glasa preko interneta (*VoIP Voice over IP*). Ova usluga pruža propusni opseg fiksne veličine u periodičkim intervalima, čime se eliminira potreba korisničke stanice da traži prijenosni medij, a time se smanjuje kašnjenje i troškovi a omogućuje usluga u stvarnom vremenu. Korisnička stanica koja ima ostvarenu UGS vezu ne može tražiti dodatni propusni opseg (*bandwidth stealing*) ali može biti prozivana na nekoj drugoj vezi koja nije UGS.

2. Prozivka u stvarnom vremenu (rtPS – Real Time Polling Service)

Mehanizam prozivke u stvarnom vremenu oblikovan je za podržavanje prometa u stvarnom vremenu u kojem se generiraju paketi *varijabilne* duljine u poznatim, periodičkim intervalima vremena (npr. MPEG video). Ovakva usluga periodično pruža korisničkoj stanici mogućnost dodijele prijenosnog opsega tražene veličine. Time se zadovoljava potreba za prijenosom u stvarnom vremenu uz dodjelu optimalnog iznosa prijenosnog pojasa. Vrijeme između prozivki naziva se *Nominal Polling Interval*. Niti kod ovog mehanizma dodijele prijenosnog medija nije dozvoljena *krađa* dodatnog propusnog opsega od strane rtPS ostvarene veze, međutim kako unutar jedne korisničke stanice može biti ostvareno nekoliko veza, dopušteno je alociranje dodatnog propusnog opsega na GPSS (*Grant Per Subscriber Station*) principu. GPSS je metodu podnošenja zahtjeva za dodatnim propusnim opsegom kod koje se zahtjevi svih veza unutar jedne stanice skupljaju te se podnosi zajednički zahtjev za dodjeljivanjem propusnog opsega.

3. Prozivka izvan stvarnog vremena (nrtPS – Non Real Time Pooling Service)

Mehanizam prozivke izvan stvarnog vremena oblikovan je za podržavanje prometa koji ne zahtijeva odvijanje u stvarnom vremenu, a koristi pakete različitih duljina (npr. FTP promet). Prozivka ne mora biti periodična, ali se garantira da će svaki CID sa ostvarenom nrtPS vezom biti prozvan u nekom određenom intervalu (tipično veličine jedne sekunde ili manje), čime se osigurava svakoj vezi mogućnost dodijele prijenosnog medija i u slučajevima zagušenja mreže. Dodatni propusni opseg može se alocirati na GPSS principu.

4. Metoda najboljeg nastojanja (BE – Best Effort service)

Mehanizam dodijele prijenosnog medija metodom najboljeg nastojanja pruža podršku prometu koji se odvija prema 'najboljim nastojanjima' te se dodjela vrši sukobom (*contetion*). Kada korisnička stanica zatraži prijenosni medij (odnosno dio propusnog opsega na prijenosnom mediju) na vezi koja koristi metodu najboljeg nastojanja zahtjev stiže do bazne stanice koja pruža DAMA uslugu (*Demand Assigned Multiple Access*) i koja vrši dodjelu medija.

2.2.4 Mehanizmi alociranja propusnog pojasa

Kao što je već spomenuto, pri inicijalizaciji svakoj korisničkoj stanici pridružene su tri namjenske veze (CIDA) sa svrhom slanja i primanja kontrolnih poruka. To omogućuje primjenu različitih nivoa kvaliteta usluge na kanale koji prenose kontrolne poruke. Svi mehanizmi pristupa prijenosnom mediju, osim USGa kod kojeg je propusni opseg konstantan od trenutka uspostave veze pa do prekida, zahtijevaju promjene alocirano propusnog pojasa. Postoje brojni mehanizmi kojima korisnička stanica može poslati zahtjev baznoj stanici da treba alokaciju propusnog opsega na uplinku.

Zahtjev za dodjelom propusnog pojasa može biti poslat kao samostalni zahtjev (već spomenuti *Bandwidth Request Header*) ili može doći unutar paketa s odgovorom (takav mehanizam gdje kontrolni i podatkovni paketi putuju istim linkom općenito se naziva *Piggybacking*). Zahtjev može biti inkrementirajući ili agregatni. Kada bazna stanica primi inkrementirajući zahtjev ona će pridodati traženi propusni opseg već postojećem. Ako je zahtjev agregatni, tada se cjelokupni dotadašnji propusni opseg zamjenjuje sa traženim. Vrsta zahtjeva određuje se na temelju polja *Type* u MAC zaglavlju za traženje propusnog opsega. Zahtjevi dostavljeni *Piggybackingom* imaju generičko MAC zaglavlje, pa oni mogu biti samo inkrementirajući, odnosno agregatni zahtjevi mogu biti postavljeni isključivo upotrebom MAC zaglavlja zahtjeva za propusnim opsegom. Da bi se optimizirala upotreba propusnog opsega, mehanizam dodijele medija može zahtijevati periodičke agregatne zahtjeve za propusnim opsegom (vremenski intervali između takvih zahtjeva funkcija su kvalitete pružene usluge).

Postoje dva moda rada kojima korisnička stanica može tražiti *bandwidth*: dodjela po vezi (*GPC – Grant per Connection mode*) i već spomenuta dodjela po korisničkoj stanici (*GPSS – Grant per Subscriber Station*). Kao što je već objašnjeno u drugom slučaju *bandwidth* se dodjeljuje svim vezama koje su ostvarene unutar jedne korisničke stanice, dok se u prvom slučaju propusni opseg dodjeljuje isključivo točno određenoj vezi. GPSS mod dopušta manji broj UL (uplink) zahtjeva i korisničkim stanicama daje mogućnost da u zadnji čas eventualno drugačije preraspodjele zatraženi propusni opseg, što može biti korisno za aplikacije koje rade u stvarnom vremenu i koje zahtijevaju brzo reagiranje sustava. Prema IEEE 802.16 preporukama sustavi koji rade u frekventijskom opsegu između 10 i 66 GHz trebali bi koristiti GPSS mod. Treba primijetiti da i u GPSS modu zahtjevi za određenim propusnim opsegom dolaze isključivo od strane pojedinih veza (CIDova) unutar korisničke stanice, ali se pristup daje osnovnom CIDu (*Basic CID* koji pripada već spomenutoj osnovnoj vezi) a ne eksplicitno pojedinim CIDovima, dok raspodjelu dodijeljenog propusnog opsega pojedinim vezama vrši sama korisnička stanica.

Posebna vrsta dodijele prijenosnog medija je prozivka (*polling*). Prozivka je proces u kojem bazna stanica samostalno alokira propusni opseg isključivo da omogućiti korisničkoj stanici podnošenje zahtjeva za alociranjem propusnog opsega. Prozivati se može ili pojedina korisnička stanica ili grupa korisničkih stanica ili samo pojedina veza. Pri tome se u uplinku odgovarajuće stanice alokira dovoljni propusni opseg da stanica pošalje zahtjev za dodjelom prijenosnog medija. Ako korisnička stanica ne treba prijenosni medij, onda vraća baznoj stanici *popunjene bajtove* (*stuff bytes - 0xFF*). Ako korisnička stanica ima ostvarenu UGS vezu i radi u GPSS modu, tada ona neće biti prozivana, osim ako ima postavljen PM (*Poll Me*) bit u zaglavlju paketa na UGS vezi.

Ako nema dovoljno propusnog opsega za prozivku pojedinih stanica, moguća je prozivka difuzijom, ili difuzijom u grupu. U tu svrhu rezervirani su određeni CIDovi, kao što je to vidljivo na slici 2.20. Razlika između individualne prozivke i prozivke difuzijom (u grupu) je ta što se u potonjem slučaju alocirani propusni opseg daje CIDu za difuziju (*broadcast CID*), a ne osnovnim CIDovima pojedine korisničke stanice. Da bi se smanjila mogućnost kolizija, samo korisničke

stanice koje zahtijevaju dodatni propusni opseg odgovaraju baznoj stanici (odnosno one koje ne trebaju propusni opseg ne šalju popunjene bajtove 0xFF). dodjela propusnog opsega u ovom slučaju vrši se sukobom (*contention resolution*) pri čemu se za određivanje slučajnog vremena čekanja koristi algoritam binarnog eksponencijalnog odustajanja (*binary exponential backoff*).

CID	Value	Description
Initial Ranging	0x0000	Used by an SS during initial ranging as part of network entry process.
Basic CID	0x0001— m	
Primary Management CIDs	$m+1$ — $2m$	
Transport CIDs and Secondary Management CIDs	$2m+1$ —0xFEFF	
Multicast Polling CIDs	0xFF00—0xFFFE	An SS may be included in one or more multicast groups for the purposes of obtaining bandwidth via polling. These connections have no associated service flow.
Broadcast CID	0xFFFF	Used for broadcast information that is transmitted on a downlink to all SS.

Slika 2.20 Prikaz rezerviranih (*well known*) CID adresa

Korisnička stanica koja ima ostvarenu UGS vezu može postaviti PM bit u MAC podzaglavljju paketa na UGS vezi, čime informira baznu stanicu da izvršava prozivku ovakve korisničke stanice kako bi ona mogla zahtijevati propusni opseg za neku drugu vezu koja nije UGS. Taj bit se postavlja u posebnom podzaglavljju *Grant Managment Subheader*, koje se umetne neposredno iza generičkog MAC zaglavlja, a čija se prisutnost evidentira postavljanjem odgovarajućih bitova u *Type* polju generičkog MAC zaglavlja. Kako bi se uštedio *bandwidth* takva prozivka vrši se samo ako je postavljen PM bit (ili ako je trajanje UGS veze predugo da bi se zadovoljili QoS zahtjevi traženi na drugim vezama te iste korisničke stanice). Nakon što bazna stanica detektira postavljanje zahtijeva za prozivkom, ista se vrši pojedinačnom prozivkom.

2.2.5 MAC potpora fizičkom sloju

MAC protokol podržava nekoliko tehnika dupleksa. Izbor tehnike, može utjecati na određene parametre fizičke veze, kao i na određene usluge koje su podržane.

1. Neokvireni frekvencijski dupleks⁵ (*Unframed FDD*)

U neokvirenom dupleksu u frekvencijskoj domeni kanali za *uplink* i *downlink* nalaze se na različitim frekvencijama i svaka korisnička stanica može istovremeno i slati i primiti podatke. Pored toga niti *uplink* niti *downlink* prijenos ne koriste okvire fiksnog trajanja. U ovoj vrsti sustava *downlink* kanal je uvijek 'uključen' (aktivan) i sve korisničke stanice ga osluškiju, odnosno *downlinkom* se promet odvija difuzijom korištenjem vremenskog multipleksa (TDM). Kanal za *uplink* dijeli se između korisničkih stanica korištenjem TDM pristupa (*time division multiple access*), u kojem postoji centralizirana dodjela propusnog opsega na uplinku.

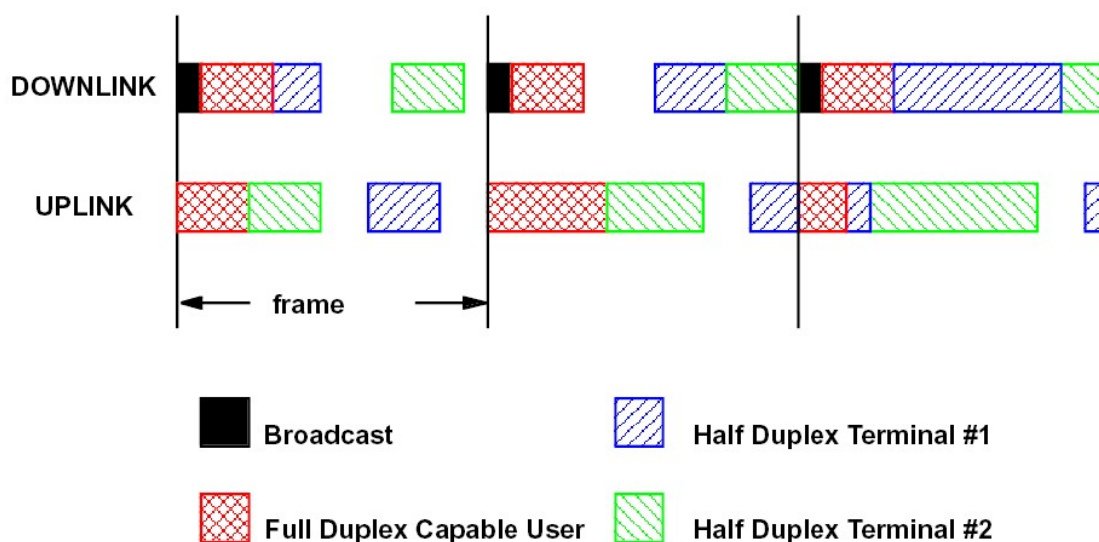
Trenutnim važećim standardom nije predviđeno da fizički sloj koristi neokvireni FDD.

⁵ Koristi se izraz dupleks jer je riječ o multipleksiranju dva kanala, onoga za uplink i onoga za downlink

2. Uokvireni frekvencijski dupleks (Framed FDD)

U uokvirenom duplesku u frekvencijskoj domeni kanali za *uplink* i *downlink* nalaze se na različitim frekvencijama. I za *uplink* i za *downlink* koriste se okviri *fiksne duljine trajanja*, što omogućuje upotrebu različitih tehnika modulacije, kao i istovremenu upotrebu i dvosmjernih i obosmjernih korisničkih stanica. Ako se koriste obosmjerne korisničke stanice, dodijeljiva propusnog opsega ne može alocirati propusni opseg za *uplink* takve stanice ako ona otkuže podatke na *downlinku*.

Na slici 2.21 prikazan je osnovni model rada uokvirenog frekvencijskog dupleksa. činjenica da se koriste okviri fiksne duljine trajanja pojednostavljuje postupak alociranja propusnog opsega. Dvosmjerne korisničke stanice mogu cijelo vrijeme osluškivati *downlink* dok obosmjerne stanice mogu osluškivati *downlink* samo dok ne šalju podatke *uplinkom*.



Slika 2.21 Primjer alociranja *bandwidtha* kod uokvirenog FDDa

3. Vremenski dupleks (TDD)

U slučaju vremenskog dupleksa prijenos *uplinkom* i prijenos *downlinkom* odvija se u različitom vremenu i na istoj frekvenciji. Okviri pri prijenosu u vremenskom duplesku također imaju fiksno trajanje i podijeljeni su na dva dijela – jedan dio za *downlink* i drugi dio za *uplink*. Jedan takav okvir podijeljen je na cjelobrojni broj fizičkih slotova (*PSova – physical slot*) čime je olakšano dodjeljivanje potrebnog propusnog opsega. Uokviravanje u vremenskom duplesku je prilagodljivo na način da se granica između dijela okvira alociranog za *downlink* i dijela okvira alociranog za *uplink* može pomicati. Granica između ta dva dijela sistemski je parametar i nadziru ga viši slojevi unutar sustava.

Na slici 2.22 prikazana je struktura TDD okvira.

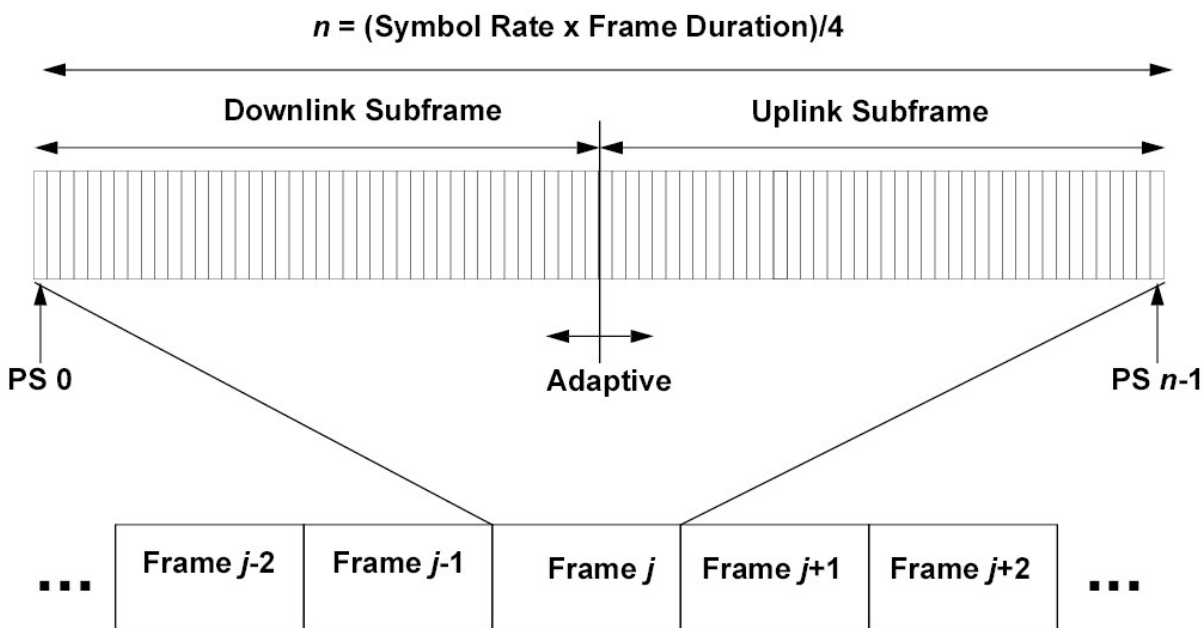


Figure 38—TDD frame structure

Slika 2.22 format TDD okvira

2.3 MAC P (*Privacy Sublayer*)

Ovaj podloj zadužen je za tajnost razmijene podataka unutar širokopojasne bežične mreže, a osnovna svrha mu je da vrši kriptiranje prometa između bazne i korisničke stanice. Pored toga on služi i za zaštitu samih operatera (pružatelja usluge) od krađe usluge na način da sprečava pristup uslugama bežične mreže neovlaštenim osobama. Tajnost se ostvaruje protokolom distribucije ključeva unutar kojeg bazna stanica vrši distribuciju ključa klijentskoj korisničkoj stanici. Pored toga, osnovni mehanizam zašтите tajnosti pojačan je mogućnošću dodavanja autentifikacije, bazirane na digitalnim certifikatima i protokolu distribucije ključeva.

MAC P podsloj ima dvije osnovne komponente:

Prva komponenta je enkapsulacijski protokol koji vrši kriptiranje podataka unutar bežične širokopojasne mreže. Taj protokol definira skup kriptografskih usluga (algoritama za autentifikaciju i kriptiranje) i pravila za primjenu tih usluga na MAC PDU.

Druga komponenta ovog podsloja je protokol za distribuciju ključeva (PKM – *Privacy Key Management*) koji omogućuje sigurnu distribuciju ključeva od bazne do korisničke stanice. Taj protokol također služi i za sprečavanje neovlaštenog pristupa mreži.

2.3.1 Kriptiranje paketa podataka

Informacije vezane za kriptiranje paketa pohranjuju se u za to predviđenom polju unutar generičkog MAC zaglavlja. Uvijek se kriptira samo informacijsko polje unutar MAC PDUa, odnosno samo MAC zaglavlje se nikad ne kriptira, jer bi se time onemogućilo ispravno funkcioniranje MAC podsloja.

Kada korisnička i bazna stanica žele komunicirati preko sigurne veze, tada pošiljatelj mora vršiti kriptiranje podataka, a primatelj dekriptiranje podataka. U MAC zaglavljju nalaze se svi potrebni podaci nužni da bi primatelj uspješno izvršio dekriptiranje (EC, EKS i CID).

Postavljeni bit EC signalizira da je sadržaj kriptiran, dok 2 bita EKS polja (*Encryption Key Sequence*) sadrže redni broj ključa koji se koristi. Taj podatak je nužan zato jer bazna stanica periodički prilagođuje parametre sigurne veze pa i pojedini ključ ima ograničeno trajanje. Na taj način korisnička stanica zna dali koristi ispravan ključ jer usporedbom rednog broja ključa zapisanog u MAC zaglavljju i rednog broja za koji korisnička stanica misli da se (još uvijek) koristi, može lagano otkriti nesinkroniziranost trenutnog ključa sa stvarnim ključem.

2.3.1 Protokol za upravljanje ključevima (PKM protokol)

Korisnička stanica koristi ovaj protokol da bi ostvarila autorizaciju (dozvolu pristupa) i dobila potrebne parametre za ostvarivanje sigurne veze. Također ovim protokolom se ostvaruje periodička provjera identiteta (reautorizacija) i spomenuta periodička promjena ključa za kriptiranje. Protokol za upravljanje ključevima koristi X.509 digitalne certifikate, RSA asimetrični postupak kriptiranja i nekoliko algoritama za simetrično kriptiranje (DES, 3DES). PKM protokol zasniva se na modelu poslužitelj-klijent, gdje korisnička stanica (PKM klijent) traži ključ (ili nekakav drugi kriptografski materijal), a bazna stanica (PKM poslužitelj) odgovara na zahtjev, osiguravajući da samo točno određena korisnička stanica dobije traženi ključ.

Bazna stanica vrši autorizaciju korisničke stanice na osnovi jedinstvenog X.509 digitalnog certifikata kojeg je izdao proizvođač (ili neki drugi izdavač certifikata). Takav digitalni certifikat sadrži javni ključ (*Public Key*) i MAC adresu korisničke stanice. Korisnička stanica koja traži autorizaciju mora baznoj stanici poslati svoj X.509 certifikat i listu algoritama za kriptiranje koje korisnička stanica podržava. Bazna stanica određuje koji algoritam kriptiranja joj je zajednički sa korisničkom stanicom, koristi javni ključ korisničke stanice za kriptiranje tajnog ključa koji će se koristiti za kriptiranje prometa između bazne i korisničke stanice, i šalje tako kriptiran tajni ključ korisničkoj stanici. Pored razmijene ključeva, bazna stanica nakon provjere identiteta na osnovi digitalnog certifikata, dopušta pristup korisničkoj stanici samo onim uslugama kojima je korisnička stanica ovlaštena pristupati, odnosno onim uslugama koje su plaćene pružatelju usluge.

Svaka korisnička stanica mora imati tvornički ugrađen X.509 certifikat i RSA asimetrični par javnog i tajnog ključa ili imati ugrađeni algoritam kojim će takav par ključeva generirati prije prve razmijene simetričnih ključeva za kriptiranje prometa.

Postupak autorizacije korisničke stanice nadzire konačni automat bazne stanice. Nakon inicijalne autorizacije, korisnička stanica mora se povremeno reautorizirati, što također nadzire konačni automat.

2.3.2 Sigurnosne asocijacije (SA)

Sigurnosna asocijacija je skup informacija koji dijele bazna i jedna ili više njenih korisničkih stanica kako bi mogle ostvariti sigurnu vezu unutar bežične mreže. Postoje tri vrste sigurnosnih asocijacija: Primarna SA, Statička SA i Dinamička SA. Svaka korisnička stanica uspostavlja sa baznom stanicom Primarnu sigurnosnu asocijaciju tijekom procesa inicijalizacije. Statička SA je određena samom baznom stanicom, dok se Dinamičke sigurnosne asocijacije uspostavljaju i prekidaju tijekom rada, u zavisnosti od uspostave i prekida određenih usluga. I dinamičke i statičke SA-ove može dijeliti istovremeno više korisničkih stanica. Pojedina sigurnosna asocijacija jedinstveno je određena pripadajućim identifikatorom SAID (*Security Association Identifier*), kojeg dijele bazna stanica i pripadajuća korisnička stanice. Svaka korisnička stanica ima svoju jedinstvenu primarnu sigurnosnu asocijaciju sa odgovarajućom baznom stanicom, i njen SAID jednak je osnovnom CIDu te korisničke stanice. Kada upotrebom PKM protokola korisnička stanica zatraži od bazne stanice simetrični ključ za kriptiranje prometa tada se on u pravilu dostavlja primarnom

sigurnosnom asocijacijom jer do nje nemaju pristup druge korisničke stanice. Kada bazna stanica dostavi korisničkoj stanici ključ za kriptiranje prometa, ona joj dostavlja i trajanje perioda unutar kojeg će taj ključ biti valjan. Sama korisnička stanica mora zatražiti dostavu novog ključa prije nego istekne valjanost trenutnog ključa u baznoj stanici. Ako se ipak dogodi da valjanost ključa istekne prije nego što je korisnička stanica zatražila i dobila novi ključ, tada više neće biti u mogućnosti izvršiti dekriptiranje sadržaja i u tom slučaju mora izvršiti reinicijalizaciju veze.

Kao što je već spomenuto kao dio postupka autorizacije, korisnička stanica dostavlja baznoj stanici listu kriptografskih algoritama koje podržava. Bazna stanica iz liste izabire jedan algoritam koji će biti upotrebljen u primarnoj sigurnosnoj asocijaciji i šalje odgovor korisničkoj stanici. Ako bazna stanica zaključi da niti jedan od ponuđenih algoritama kriptiranja ne zadovoljava, biti će odbijen zahtjev korisničke stanice za autorizacijom. Odgovor na zahtjev za autorizaciju sadrži također i opcionalnu listu statičkih SAova i algoritama unutar pojedinog statičkog SA, bez obzira dali korisnička stanica podržava te algoritme. Međutim ako ih podržava, korisnička stanica može koristiti i komunikaciju definiranu nekom od takvih statičkih asocijacija.

3. Fizički sloj (PHY)

Kao što je prikazano u uvodu na slici 1.2 usluge fizičkog sloja dostupne su MAC entitetima u PHY tokama pristupa usluzi. Općenito se usluge fizičkog sloja obično opisuju skupom primitiva. U slučaju bežične širokopojasne mreže skup primitiva za komunikaciju između MAC sloja i PHY sloja može se grupirati u tri osnovne kategorije.

1. Primitivi koji podržavaju prijenos podataka. To su dakle primitivi koji djeluju kao posrednici u partnerskoj komunikaciji između partnerskih MAC entiteta. Oni čine skupinu **PHY_MACPDU** primitiva.
2. Primitivi koji imaju samo lokalno značenje i podržavaju komunikaciju između pojedinih podslojeva, a vezanu za upravljanje samim slojem. Oni čine skupinu **PHY_TXSTART** primitiva.
3. Primitivi koji služe za realizaciju usluga pojedinog sloja. Primitive oblika **PHY_*.request** generira MAC sloj i šalje PHY sloju da bi zatražio od njega neku uslugu. Primitive oblika **PHY_*.confirmation** generira PHY sloj i šalje MAC sloju kao potvrdu primitka zahtjeva. Primitive oblika **PHY_*.indication** generira PHY sloj i šalje MAC sloju kao rezultat izvođenja neke usluge.

3.1 Fizički sloj za frekvencijski opseg 10-66 Ghz

Specifikacije fizičkog sloja ciljanog za rad u frekvencijskom opsegu između 10 i 66 Ghz odlikuju se visokim stupnjem fleksibilnosti ostvarene s ciljem da se pružateljima usluge omogući optimizacija sustava obzirom na broj baznih stanica, cijenu, kvalitetu usluge i kapacitet. U svrhu maksimalne iskoristivosti frekvencijskog pojasa, podržan je i vremenski dupleks (TDD) i frekvencijski dupleks (FDD). U oba slučaja moguće je prilagodljivi usnopljen prijenos u kojem se parametri veze (uključujući modulacije i sheme kodiranja) mogu prilagođavati individualno za svaku korisničku stanicu i to na principu prilagodbe svakog pojedinačnog okvira (*frame-by-frame basis*). Frekvencijski dupleks podržava i dvosmjerni (full-duplex) i obosmjerni (half-duplex) prijenos.

Fizički sloj za uplink baziran je na kombinaciji višestrukog pristupa u vremenskoj domeni (*TDMA time division multiple access*) i višestrukog pristupa na zahtjev (*DAMA demand assigned multiple access*). U oba slučaja uplink je podijeljen u vremenske odsječke fiksnog trajanja. Broj dodijeljenih odsječaka različit je za različite namijene a nadzire se od strane MAC sloja u baznoj stanici i može biti različit u različito vrijeme kako bi se postigla optimalna usluga.

Kanal za downlink je vremenski multipleksiran, a podaci za pojedinu korisničku stanicu koji su multipleksirani unutar jednog vremenskog odsjeka dostupni su svim korisničkim stanicama unutar sektora (naravno ako je promet kriptiran niti jedna druga stanica, osim one kojoj su podaci namijenjeni, ne bi mogla čak i ako bi htjela, dešifrirati podatke).

Fizički sloj također ima svoj C podsloj (*Convergence Sublayer*) a koji u downlinku stavlja pokazivački bajt (*pointer byte*) na početak informacijskog polja da bi pomogao primatelju da prepozna početak MAC PDUa.

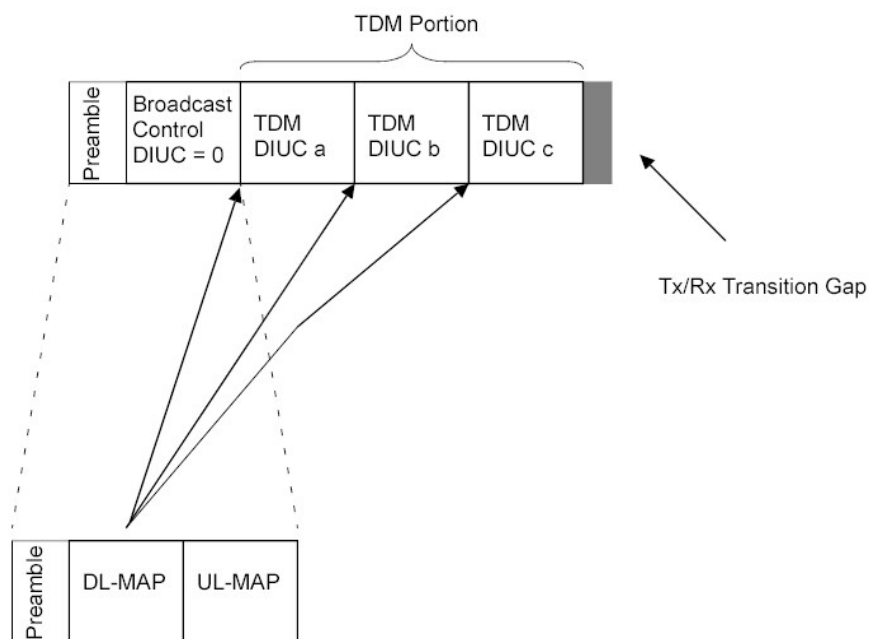
Fizički sloj po IEEE 802.16 specifikaciji radi sa okvirima (*framed format*). Unutar svakog okvira nalazi se podokvir (*subframe*) za downlink i za uplink. Downlink podokvir započinje informacijama nužnim za sinhronizaciju okvira. U slučaju vremenskog dupleksa, prvo dolazi podokvir za downlink, a zatim podokvir za uplink (pogledati sliku 2.22). U slučaju frekvencijskog dupleksa istovremeno se odvija prijenos i uplinkom i downlinkom

3.1.2 Downlink

Dostupni propusni opseg u smjeru downlinka određen je veličinom fizičkog slota PS (*Physical Slot*). Fizički slot je jedinica vremena, zavisna od specifikacija fizičkog sloja, koja služi kao osnovna mjera za alociranje (odnosno trajanje alociranog) propusnog pojasa.

Broj fizičkih slotova unutar jednog okvira je funkcija broja promjena simbola fizičkog sloja (*symbol rate*), koji se odabire tako da se dobije cjelobrojni broj fizičkih slotova unutar jednog okvira.

Izgled podokvira (*subframe*) za downlink prikazan je na slici 3.1

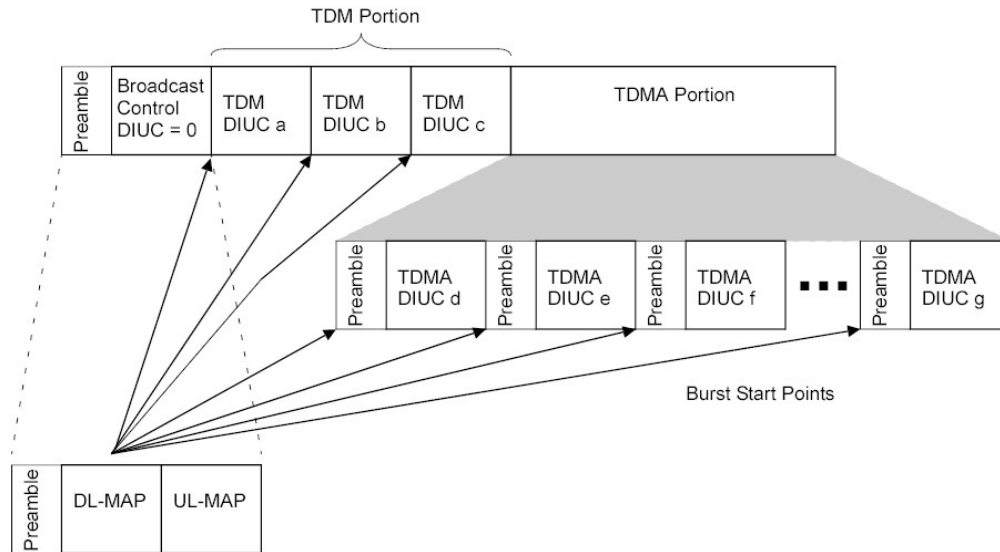


Slika 3.1 Format podokvira za downlink uz TDD

Struktura podokvira za downlink, pri korištenju vremenskog dupleksa, prikazana je na slici 3.1. Podokvir započinje sa *Frame Start* preambulom koju koriste fizički sloj za sinhronizaciju. Nakon toga slijedi dio za kontrolu okvira koji sadrži downlink i uplink mapu (DL-MAP i UL-MAP). Dio za kontrolu okvira ne smije biti kriptiran. DL-MAP i UL-MAP sadrže informaciju gdje počinje usnopljen prijenos izražen u terminima fizičkih slotova (odnosno nakon koliko fizičkih slotova počinje usnopljen prijenos) pri čemu je prvom fizičkom sloju dana oznaka 0. Nakon toga slijedi TDM dio (*time division multiplex*) koji sadrži same podatke organizirane u snopove. Pri tome svaki snop može imati drugačija svojstva (na slici označeno sa DIUC a DIUC b i DIUC c). DIUC je skraćenica od *Downlink Interval Usage Code* i označava određeni tip usnopljenog prijensa unutar jednog intervala.

Sve korisničke stanice unutar jednog sektora dekodiraju kontrolne informacije i zatim traže MAC zaglavlje koje bi ukazalo na prisutnost podataka za tu korisničku stanicu u ostatku downlink podokvira.

Struktura podokvira za downlink, pri korištenju frekvencijskog dupleksa, prikazana je na slici 3.2



Slika 3.2 Format podokvira za downlink uz FDD

Kao i u slučaju TDDa, podokvir započinje sa 'Frame Start' preambulom, iza koje slijede dio za kontrolu okvira i TDM dio. TDM dio downlink podokvira sadrži podatke koje se prenose :

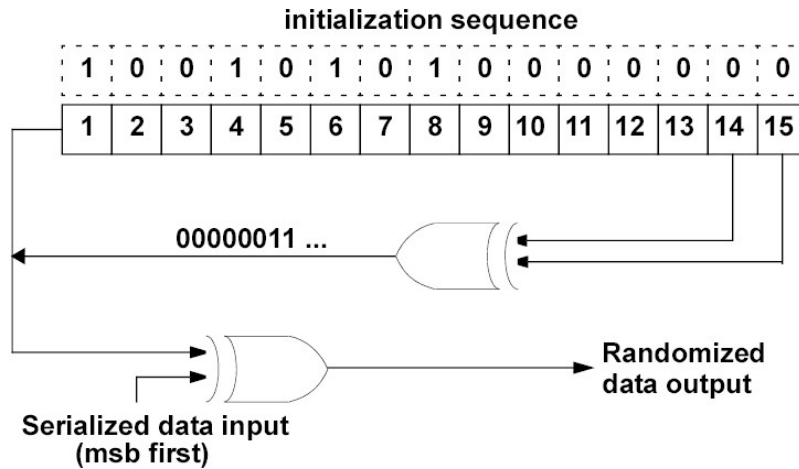
- Dvosmjernim korisničkim stanicama
- Obosmjernim korisničkim stanicama koje prvo primaju podatke, a nakon toga šalju
- Obosmjernim korisničkim stanicama koje ne šalju podatke za vrijeme trajanja trenutnog okvira

Iza TDM dijela slijedi TDMA dio koji sadrži informacije koje se mogu prenijeti bilo kojoj obosmjernoj korisničkoj stanici koja prvo šalje a onda prima podatke. To omogućuje pojedinoj korisničkoj stanici da ne mora dekodirati čitav podokvir. Unutar TDMA svaki snop podataka označen je sa TDMA preambulom za resinhronizaciju.

Oba tipa preambula (za početak podokvira i TDMA preambule) koriste QPSK modulaciju. Preambula za početak podokvira sastoji se od 32 znaka generirana ponavljanjem CAZAC (*constant amplitude zero auto-correlation*) sekvence od 16 znakova.

TDMA preambula sastoji se od 16 znakova generiranih ponavljanjem CAZAC sekvence od 8 znakova.

Da bi se spriječila mogućnost pojave periodičkih nizova simbola ili pojave duljih nizova bez promijene simbola što bi moglo dovesti do ispada iz sinkronizacije (TDM okviri nemaju svoju preambulu za sinkronizaciju) informacijski bitovi se prethodno kodiraju pseudoslučajnim nizom ($\sum \text{mod } 2$) primjenom posmatnog registra s povratnim vezama. Slika takvog generatora pseudoslučajnih brojeva dana je na slici 2.4.



Slika 3.4 Generator pseudoslučajnih brojeva

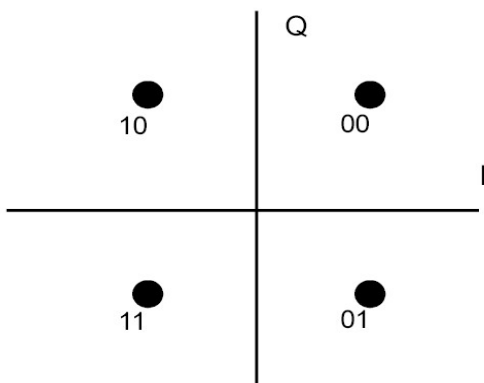
Na početku svakog snopa u generator se upiše početna vrijednost 100101010000000. Preambule se ne kodiraju pseudoslučajnim nizom.

Da bi se maksimizirala upotreba propusnog pojasa, fizički sloja koristi kombinaciju više modulatorskih postupaka. Dijagram stanja (*constellation pattern*) može biti odabran za svaku korisničku stanicu, ovisno o kvaliteti RF kanala. Ako je stanje na vezi dobro, mogu biti izabrane složenije sheme modulacije kojim će se maksimalno iskoristiti propusnost veze, uz još uvijek zadovoljavajuću pouzdanost. Ako se kvaliteta veze smanji, primjerice zbog vremenskih uvjeta, sustav može izvesti promjenu dijagrama stanja kako bi poboljšao pouzdanost prijenosa.

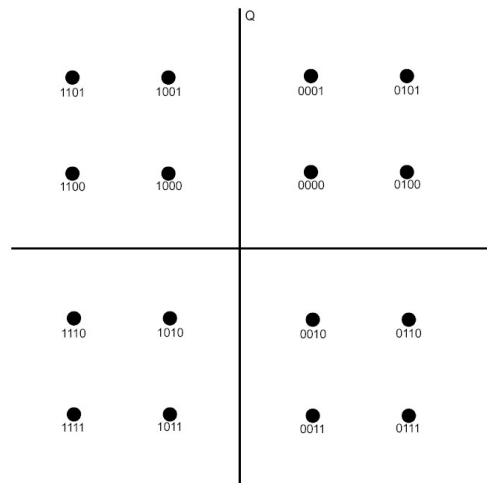
U downlink prijenosu, bazna stanica mora podržavati QPSK ($n=2$) i 16-QAM ($n=4$) modulacije i opcionalno 64-QAM modulaciju ($n=6$).

Pri promijeni vrste modulacije, koriste se dva načina prilagodbe jačine signala. Prvi način je taj da se srednja vrijednost signala zadrži istom bez obzira na vrstu modulacije, dok je drugi način da se vršna vrijednost signala zadrži istom bez obzira na vrstu modulacije. Ako se dogodi da zadnji dio modulirane poruke ne završi točno na granici fizičkog slota, tada se ostatak slota do početka novog slota popunjava nulama.

Na slici 2.5 prikazan je dijagram stanja za QPSK modulaciju, a na slici 2.6 dijagram stanja za 16-QAM modulaciju.



Slika 2.5 QPSK modulacija



Slika 2.6 16-QAM modulacija

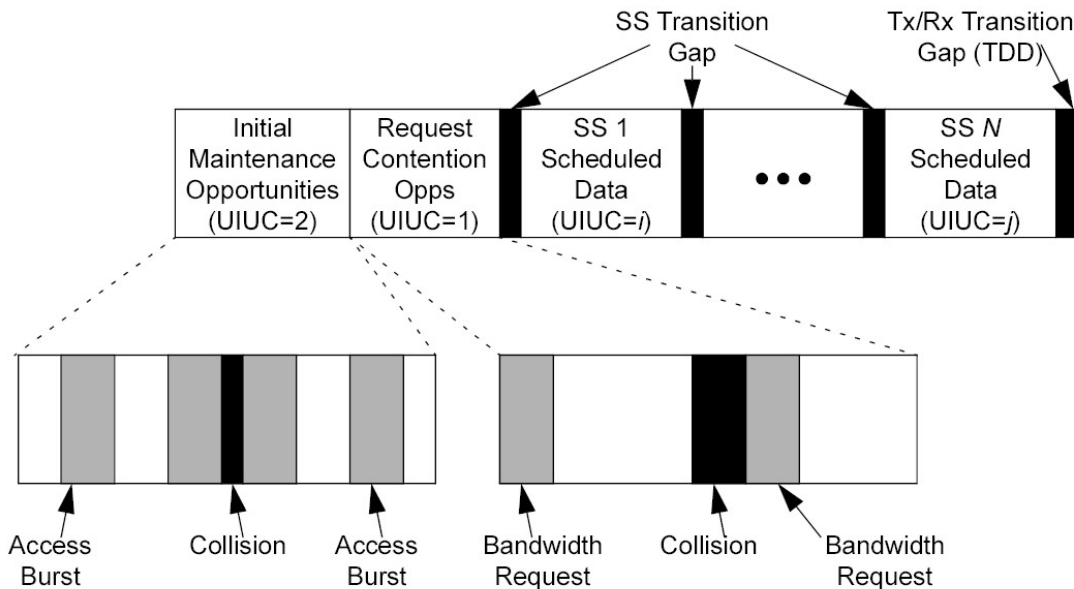
3.1.2 Uplink

Na slici 2.7 prikazan je format podokvira za slanje podataka u smjeru od korisničke prema baznoj stanici (*uplink*). Podaci poslani od korisničke stanice mogu biti grupirani u tri kategorije:

1. Podaci koji su poslani za vrijeme uspostave veze.
2. Podaci koji su poslani nakon što je bazna stanica dobila dio propusnog opsega u postupku dodjele sukobom.
3. Podaci koji su poslani za vrijeme u kojem bazna stanica periodički dobiva dio propusnog opsega na ostvarenoj UGS vezi.

Podaci iz bilo koje kategorije se mogu pojaviti slobodnim poretkom (odnosno podaci iz kategorija se mogu međusobno mijenjati) i u slobodnoj količini (ograničenoj samo brojem slobodnih fizičkih slotova). O kojoj je kategoriji podataka riječ određuje parametar UIUC (*Uplink Interval Usage Code*), a podaci koji stižu od različitih korisničkih stanica odvojene su prijenosnim prazninama (*SS Transition Gap*). One omogućuju da bazna stranica obradi pristigle podatke te da se sinhronizira sa slijedećom korisničkom stanicom.

Kodiranje pseudoslučajnim nizom vrši se, kao i kod uplinka, primjenom posmaćnog registra s povratnim vezama uz početnu vrijednost 100101010000000 zapisanu u registru.



Slika 2.7 Format podokvira za uplink

Preambula kojom započinje slanje snopa podataka dobije se ponavljanjem CAZAC sekvence zarotirane za +45 stupnjeva (IEEE Std 802.16.2-200 [I1]). Kao i kod uplinka u zavisnosti o tome dali je preambula dugačka 16 ili 32 znaka, ponavlja se 8 bitna ili 16 bitna CAZAC sekvenca. Bazna stanica mora podržavati QPSK modulaciju, a opcionalno i 16-QAM i 64-QAM modulacije. Pri

promijeni modulacija koristi se jedno od već spomenutih pravila za prilagodbu snage (konstantna srednja vrijednost ili konstantna vrhna vrijednost).

3.2 Brzine i propusnost

Unutar frekvencijskog opsega između 10 i 66 GHz moguće je koristiti vrlo različite frekvencije, zavisno od zakonskih propisa za određeno područje. Iz tog razloga IEEE802.16 standardom nije propisan frekvencijski plan za širokopojasni bežični pristup. Kao primjer u Europi je frekvencijski pojas između 24.5 GHz i 26.5 GHz rezerviran od strane CEPTAe (*European Conference of Postal and Telecommunications Administrations*) dok je u Sjevernoj Americi isti taj frekvencijski opseg slobodan.

Na slici 2.8 prikazana je tabela s ostvarivim brzinama u zavisnosti od primijenjene modulacije i širine upotrijebljenog frekvencijskog opsega (broj promjena simbola fizičkog sloja u 1 sec. je odabran tako da broj fizičkih slotova u jednom okviru bude cjelobrojan).

Channel size (MHz)	Symbol rate (MBaud)	Bit rate (Mbit/s) QPSK	Bit rate (Mbit/s) 16-QAM	Bit rate (Mbit/s) 64-QAM	Recommended Frame Duration (ms)	Number of PSS/frame
20	16	32	64	96	1	4000
25	20	40	80	120	1	5000
28	22.4	44.8	89.6	134.4	1	5600

4. Praktične izvedbe 802.16 sustava

Nepokretni širokopojasni bežični pristup ostvaruje se prvenstveno između korisničkih stanica i bazne stanice koja pruža pristup jezgri mreže. Termin *širokopojasni* u IT terminologiji obično označava mogućnost prijenosa podataka brzinama većima od 1.5 Mbit/s iako, kao što je prikazano na slici 2.8, 802.16 mreže podržavaju značajno veće brzine.

4.1 Vrste izvedbi 802.16 sustava

Fiksne širokopojasne bežične mreže najčešće se zasnivaju na MP (*multipoint*) arhitekturi. MP je izraz koji označava vrstu topologije bežičnih mreža kod koje sustav istovremeno pruža uslugu za nekoliko, geografski udaljenih, korisničkih stanica i obuhvaća PMP sustave (*point-to-multipoint*) i MP-MP (*multipoint-to-multipoint* ili *mesh*) sustave. PMP topologija je objašnjena u poglavlju 1.2 u kojem se govori o kvaliteti usluge, dok je MP-MP takva topologija kod koje su korisničke stanice, koje su također geografski udaljene, međusobno povezane te mogu vršiti ulogu prijenosnika (*repeatera*). Na taj način kod MP-MP topologije mogući su različiti putovi od same jezgre mreže do korisničke stanice i u takvim mrežama ne postoji bazna stanica u smislu u kojem postoji kod PMP mreža.

4.1.1 PMP sustav

PMP sustav sastoji se od baznih stanica, korisničkih stanica i od, ako je potrebno, prijenosnika. Bazne stanice imaju širokokutne antene i omogućuju pokrivenost od 360 stupnjeva često i sa samo jednom antenom. Veze između samih baznih stanica nisu dio protokola za bežični širokopojasni pristup i mogu biti ostvarene radio-vezom, optikom ili nekim drugim sredstvom. Ako su bazne stanice povezane radio-vezom, moguće je realizirati da koriste iste frekvencije koje se koriste unutar same bežične mreže (odnosno na istim onim frekvencijama koje se koriste za vezu između bazne stanice i korisničkih stanica).

Korisničke stanice imaju uskokutne direkcione antene usmjerene prema baznoj stanici.

4.1.2 MP-MP sustavi (*Mesh*)

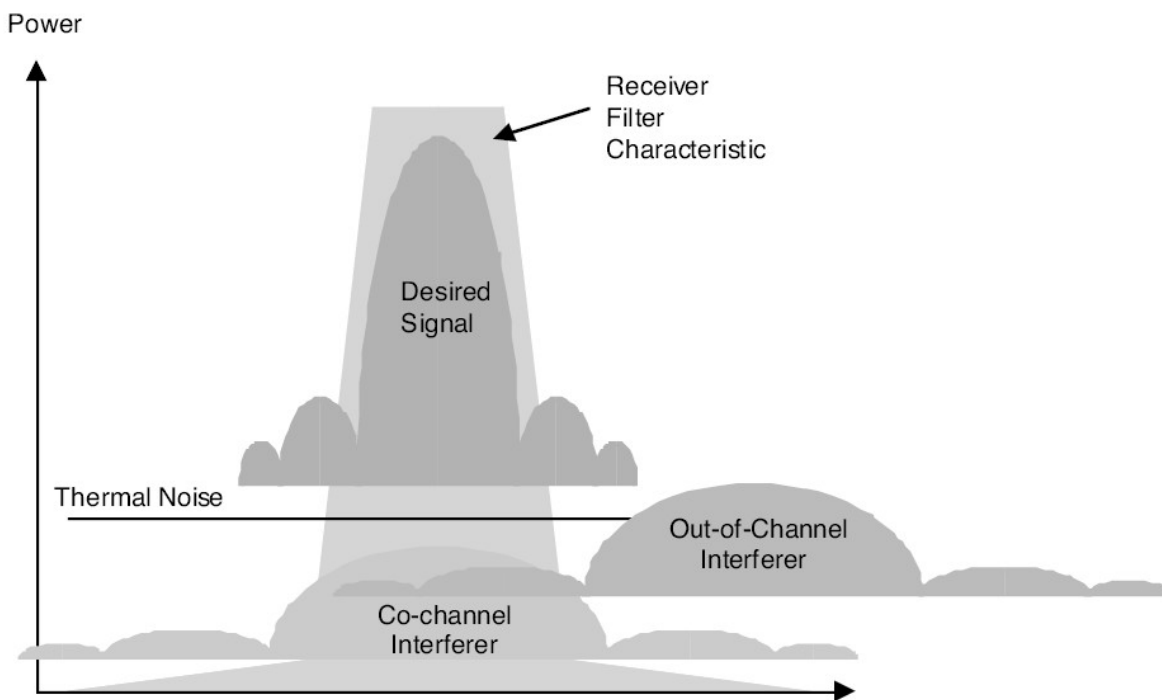
MP-MP mreže pružaju istu funkcionalnost kao i PMP mreže. Bazne stanice su na jednoj strani povezane sa jezgrom mreže na koju pružaju uslugu pristupa, dok su na drugoj strani vezane na korisničke stanice, koje mogu biti terminalne ili prijenosne. Promet do krajnje korisničke stanice može stoga ići preko jedne ili više takvih prijenosnih stanica.

4.2 Smetnje (interferencije)

Širenje signala iz frekventijskog opsega 10 – 66 GHz je relativno nedisperzivno, ali sa snažnim pojedinačnim prigušenjima (primjerice zbog oborina) koja se javljaju posebice pri višim frekvencijama. Apsorpcija radio valova od okolnih objekata ili prirodnih prepreka je u ovom području vrlo velika, pa je zato potrebna vizualna veza između predajnika i prijemnika da bi se dobili zadovoljavajući rezultati. Iz tih razloga je i maksimalna udaljenost između prijemnika i predajnika ograničena na nekoliko kilometara, čime se osigurava da će i u slučaju npr. oborina jačina signala biti dovoljna. Istovremeno upotreba modulacija višeg reda zahtijeva što veći omjer

signala i smetnje (*C/I Carrier-to-Noise Ratio*). Iz tih razloga su ovakve mreže (i bežične mreže općenito) osjetljive na smetnje koje mogu dolaziti i iz izvora koji se nalazi izvan područja rada same mreže. Osim toga i činjenica da oborine mogu na određenom području dodatno prigušiti korisni signal (*desire signal*) a da pri tome, zbog nejednolike raspodjele oborina, žetni signal nije uopće prigušen.

Na slici 4.1 prikazana su dva osnovna oblika smetnji: smetnje unutar kanala (*co-channel interference*) i smetnje izvan kanala (*out-of-channel interference*).

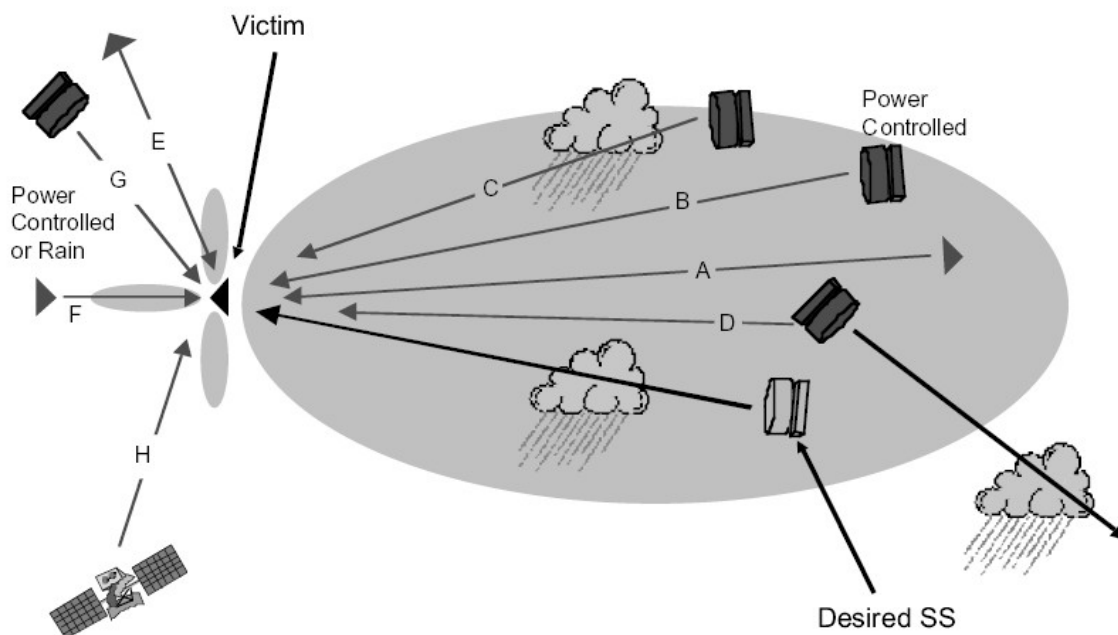


Slika 4.1 Vrste smetnji

Širina spektra od signala smetnje unutar kanala može biti šira ili uža od širine spektra korisnog signala. Na slici je prikazan slučaj kad je ta širina veća, i samo dio spektra signala smetnje pada unutar širine spektra korisnog signala (odnosno preciznije unutar širine propusnog pojasa frekvencijskog filtra na prijemniku). U ovom slučaju prijemnik može procijeniti jačinu smetnje množenjem snage signala koji prima sa veličinom dobivenom kao omjer širine spektra propusnog pojasa prijemnog filtra i širine spektra primljenog signala.

Kod smetnji izvan kanala, dio spektra koji nije dominantan, može se preklapati sa širinom spektra korisnog signala i taj dio smetnje može se promatrati kao da je riječ o smetnji unutar kanala. Međutim kako niti jedan filter nije idealan, dominantna frekvencija od smetnje koja dolazi izvan kanala neće biti potpuno uklonjena na filteru prijemnika i predstavljat će dodatak na smetnju unutar kanala. Razina ove smetnje ovisi o sposobnosti prijemnika da odbaci sve signale izvan frekvencijskog opsega kanala (mjera te sposobnosti naziva se *blocking performance*).

4.2.1 Smetnje baznoj stanici



Slika 4.2 Moguće smetnje baznoj stanici⁶

Na slici 4.2 prikazani su mogući oblici smetnji za baznu stanicu:

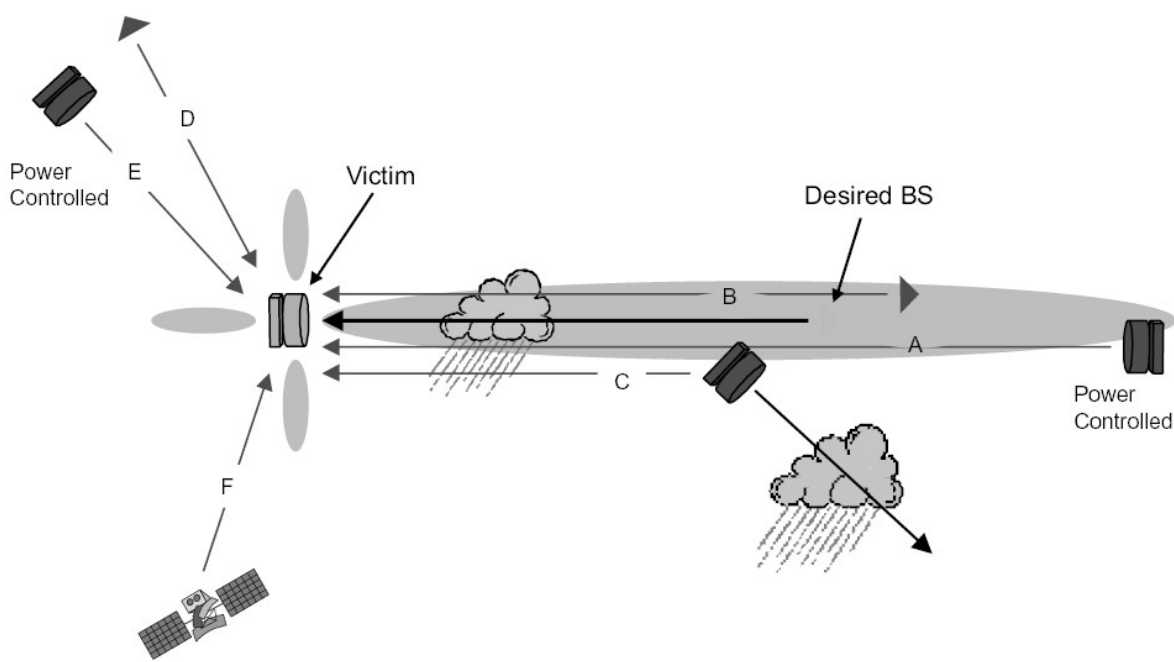
- Slučaj A pokazuje interferenciju između dvije bazne stanice u kojoj se jedna bazna stanica nalazi unutar emisije druge bazne stanice. Ovakav slučaj se može često pojaviti zato jer su pojedini sektori, unutar 360 stupnjeva djelovanja antene, dosta široki, čak do 90 stupnjeva. Zbog toga ometana stanica može čak primati kumulirani signal od nekoliko drugih baznih stanica. Mogućnost ovakvih smetnji može biti smanjena ako se osigura da jedna bazna stanica ne šalje podatke na frekvenciji na kojoj druga bazna stanica prima podatke (barem ne unutar jednog sektora).
- Slučaj B pokazuje interferenciju u kojem antena korisničke stanice šalje smetnju baznoj stanici. U ovom slučaju bazna stanica nema uspostavljenu vezu sa korisničkom stanicom nego joj od korisničke stanice dolazi samo signal smetnje. Ovakav slučaj je za baznu stanicu gori od slučaja A zato jer korisnička stanica ima direkcionu antenu koja će značajnije ometati baznu stanicu, međutim upravo zbog uskog kuta koji pokriva korisnička stanica vjerojatnost pojave ovakve smetnje je mnogo manja nego u slučaju A. Pod pretpostavkom da nema prepreka između (ometajuće) korisničke stanice i bazne stanice, korisnička stanica će smanjiti jačinu svog signala do razine na kojoj neće smetati baznoj stanici. Naravno takva kontrola snage nije savršena pa je moguće da korisnička stanica nedovoljno priguši signal.
- Slučaj C sličan je slučaju B, ali je pretpostavljeno da oborine prigušuju signal smetnje koji dolazi od korisničke stanice. Zbog toga je ovo povoljniji slučaj od slučaja B, jer će

⁶ Oznaka *Power Controlled* uz korisničke stanice označava svojstvo MP sustava da bazna stanica može upravljati signalom mijenjati jačinu signala koji dolazi od korisničke stanice. Osim za eliminaciju smetnji to svojstvo bazna stanica koristi da bi izjednačila razinu signala koju prima od bliskih i onih udaljenih stanica.

korisnička stanica nakon reakcije bazne stanice prigušiti signal isto kao i u slučaju B, ali će ga oborine još dodatno prigušiti.

- Slučaj **D** sličan je slučajevima B i C, ali je ovdje pretpostavljeno da signal smetnje dolazi od korisničke stanice kao raštrkano ili refleksirano zračenje, a ne kao primarni signal. Ovaj slučaj je u pravilu također povoljniji od slučaja B jer je takav signal obično već toliko prigušen da je smetnja od njega manja nego od **prigušenog** signala iz slučaja B. Iznimka od toga je ako reflektirani signal ne dolazi od korisničke stanice nego iz nekog drugog izvora kao npr. sa satelitske veze.
- Slučaj **E** sličan je slučaju A i predstavlja interferenciju od druge bazne stanice, ali signal od druge bazne stanice (nije prikazana) dolazi kao raštrkano ili refleksirano zračenje. Kako je takav signal znatno prigušen, ovaj slučaj je povoljniji od slučaja A. Ova interferencija može se riješiti istom metodom kao i u slučaju A
- Slučaj **F** predstavlja interferenciju dva raštrkana signala od dvije bazne stanice. Zbog malih snaga tih signala ovaj slučaj ne predstavlja smetnju na toj baznoj stanici iz primjera (*Victim*), ali bi ovakav signal mogao biti smetnja za neke druge uređaje, ako su prisutni. Ovaj slučaj se može riješiti (kao i sve ostale interferencije između baznih stanica) kao u slučaju A i E.
- Slučaj **G** predstavlja interferenciju između primarnog signala sa korisničke stanice i raštrkanog signala sa bazne stanice. Ovaj slučaj je povoljniji nego slučaj B i C, a također se rješava smanjenjem snage korisničke stanice.
- Slučaj **H** predstavlja interferenciju sa satelitske veze i na tu smetnju bazna stanica ne može djelovati, pa se stoga u IEEE802.16 preporukama za implementaciju niti ne razmatra.

4.2.2 Smetnje korisničkoj stanici



Slika 4.3 Moguće smetnje korisničkoj stanici

Na slici 4.2 prikazani su mogući oblici smetnji za korisničku stanicu:

- Slučaj **A** predstavlja interferenciju između dvije korisničke stanice koje imaju kolinearnu emisiju signala (odnosno nalaze se jedna nasuprot druge, što je u praksi vrlo rijetko). Za pretpostaviti je da će udaljenost između tih dvaju stanica biti prilično velika, tako da će signal koji dolazi do ometane stanice (*Victim*) biti prilično prigušen. Ovakva interferencija, ako se javi, obično će biti prekinuta na način da će neka od baznih stanica tražiti od ometajuće korisničke stanice da smanji snagu svog signal (kako ne bi smetala toj baznoj stanici).
- Slučaj **B** predstavlja interferenciju smetnju zbog oborina na putu između bazne i korisničke stanice.
- Slučaj **C** predstavlja interferenciju raspršenog ili refleksiranog signala sa druge stanice (ili primjerice sa neke satelitske veze). Ovaj slučaj je vjerojatniji od slučaja A, ali kako korisničke stanice imaju uskokutne antene, smetnja na drugu korisničku stanicu od ovako raspršenog signala je manja nego u slučaju A. Isto kao i kod slučaja A ometajuća korisnička stanica obično biva prigušena na zahtjev neke bazne stanice.
- Slučaj **D** predstavlja interferenciju između raspršenog signala sa korisničke stanice i primarnog signala sa neke bazne stanice (ne one sa kojom nađ ometana stanica ima uspostavljenu vezu). Ovaj slučaj je vrlo vjerojatan jer bazne stanice pokrivaju široka područja, ali ne predstavlja posebnu smetnju promatranoj korisničkoj stanici.
- Slučaj **E** predstavlja interferenciju između raspršenog signala sa promatrane korisničke stanice i primarnog signala sa neke druge korisničke stanice. Kao i kod interferencija na baznu stanicu ovaj slučaj ne predstavlja veliku smetnju ometanoj stanici, a kao i kod slučaja A i C ometajuća stanica bit će prigušena na zahtjev neke bazne stanice.
- Slučaj **F** predstavlja interferenciju sa neke satelitske veze i IEEE802.16 preporuke ne razmatraju ni ovaj slučaj.

5. Zaključak

Područje primjene bežičnog širokopolasnog pristupa izuzetno je veliko i obuhvaća bežični prijenos podataka, glasa i vrlo različitih multimedijских sadržaja (u nekim zemljama se stoga ovakav pristup naziva i MWS – *Multimedia Wireless Systems*). Ovakve mreže rade transparentno, omogućuju pružanje točno određene kvalitete usluge pojedinom korisniku, podržavaju obosmjerni i dvosmjerni promet, te korisnik uopće nije svjestan toga da se promet odvija radio valovima. Primjena bežičnih tehnologija ima brojne prednosti, među kojima je jedna od najznačajnijih mogućnost brze izgradnje širokopropusnih mreža tamo gdje je ožičenje nemoguće ili je preskupo.

Kao što je već spomenuto u Uvodu IEEE 802.16 radna grupa trenutno radi na razvoju standarda za pokretni širokopolasni bežični pristup i čini se da taj razvoj trenutno ide u dva smjera. Prvi je proširenje postojećeg 802.16 standarda na mogućnost pružanja određene, iako vrlo ograničene, pokretnosti unutar već izgrađenih mreža. Drugi smjer u kojem se projekt razvija je izrada novog standarda koji će omogućiti širokopolasni bežični pristup i pri vrlo velikim brzinama (primjerice iz vozila).

Istodobno se radi i na poboljšanju trenutnih mogućnosti fiksnih širokopolasnih bežičnih mreža, pa se tako dovraća dodatak standardu za područje između 2 i 11 GHz, a radi se i na povećanju prosječne brzine veze sa 45 Mbit/s na 144 Mbit/s [Hadad00].

Pa ipak fiksni širokopolasni bežični pristup još uvijek relativno sporo širi i trenutno se nalazi tek na trećem mjestu po broju korisnika koji na ovaj način ostvaruju širokopolasni pristup (na prvom mjestu su kabelaške veze, a na drugom DSL). Neke od prepreka za brže širenje ovakvih mreža svakako je i standardizacija. Zato je važnost donošenja ovakvih standarda podjednako značajna za razvijene zemlje, kao i za nerazvijene zemlje u kojima postoji vrlo slaba žičana infrastruktura pa je potreba za bežičnim mrežama velika.

6.Literatura

[Beyer02] IEEE 802.16 Session #18 – Dave Beyer, Carl Eklund, Mika Kasslin, Nico van Waes: "802.16 MAC Layer Mesh Extensions Overview". *Tutorial Open Forum on 12. March 2002*

[Budin02] Prod.dr.sc. Leo Budin, predavanja iz predmeta "Operacijski Sustavi 2". *Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave, FER, 2002.*

[Glavini02] Prof.dr.sc. Vlado Glavini: "Mreže računala". *Radni materijali za predavanje iz predmeta RA0907. Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave, FER, 2002.*

[Hadad00] IEEE 802.16 Session #7 – Zion Hadad: "Coded Orthogonal Frequency Division Multiple Access". *Tutorial Open Forum on 2 May 2000*

[I1] IEEE Std 802.16.2-200 - "Recommended Practice for Local and metropolitan area networks". *The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA*

[I2] IEEE Std 802.16.2-200 - IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems. *The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA*

[Tanenbaum96] Andrew S. Tanenbaum: "Computer Networks". *Third Edition. Prentice-Hall International, Inc. 1996.*