

13. Бежичне мреже

Бежичне мреже су према домету категоризоване у четири групе: бежичне личне мреже (WPAN¹), бежичне локалне рачунарске мреже (WLAN²), бежичне рачунарске мреже градских подручја (WMAN³) и бежичне рачунарске мреже ширих географских подручја (WWAN⁴).

13.1 Бежичне локалне рачунарске мреже

Први експеримент бежичног повезивања рачунара реализован је 1970. године у лабораторијама IBM-а у Швајцарској.

Прва бежична рачунарска мрежа ALOHA⁵ пуштена је у рад 1971. године. Мрежа се састојала од седам рачунара постављених на четири острва и сервера са којим су рачунари комуницирали бежичном везом. Ова мрежа представља први јавно представљени рад бежичне пакетске мреже за пренос података.

Развој бежичних мрежа наставља се 1985. године пошто је Федерална комисија за комуникације (FCC⁶) одобрила коришћење опсега радиофреквенцијског спектра без посебних дозвола за потребе индустрије, научних истраживања и медицине (ISM⁷ опсег). Овај фреквенцијски опсег обухвата три групе фреквенција: 902 - 928MHz; 2,4 - 2,4835GHz и 5,725 - 5,875GHz (слика 13.1).

Модуларност и флексибилност бежичних локалних рачунарских мрежа чини их добрим решењем за поједине објекте као на пример: повезивање рачунара на сајмовима, у болницама, библиотекама,

¹ *Wireless Personal Area Network*

² *Wireless Local Area Network*

³ *Wireless Metropolitan Area Network*

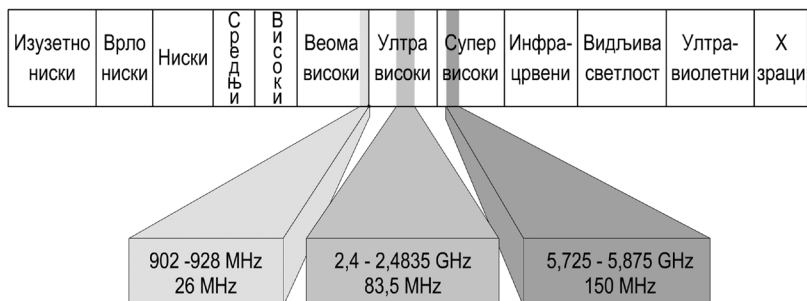
⁴ *Wireless Wide Area Network*

⁵ ALOHA значи здраво на хавајском. Назив се користи и за метод приступа трансмисионом медијуму.

⁶ *Federal Communications Commission*, тело у САД које регулише коришћење радио спектра

⁷ *Industrial Scientific Medical*

13. Бежичне мреже



Слика 13.1 ISM опсега који се користи за бежичне локалне рачунарске мреже повезивање зграда које су раздвојене прометним саобраћајницама или реком, у зградама од историјске вредности у којима није дозвољена промена изгледа зграде, али и као допуна или проширење кабловских мрежа.

13.2 Топологије бежичних локалних рачунарских мрежа

Бежичне мреже пружају велику флексибилност и могућност комбиновања различитих начина повезивања. Искристалисале су се следеће топологије: само за ову прилику (*ad hoc*), инфраструктурна, ћелијска, испреплетана¹ и тачка-тачка.

13.2.1 Топологија само за ову прилику

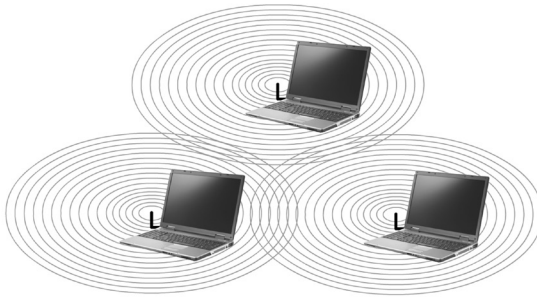
Топологија само за ову прилику (*ad hoc*) локалне рачунарске мреже (слика 13.2) омогућава корисницима успостављање везе „свако са сваким“ без уређаја за приступ (AP²). Као такве погодне су за комуникацију између мањих група корисника на малом растојању и углавном се примењују тамо где је потребно брзо успоставити привремену мрежу³.

Да би могла да се оствари међусобна комуникација потребно је да сваки рачунар буде у домету свих осталих рачунара, што ограничава покретљивост корисника на релативно мали простор.

¹ Mesh

² Access Point

³ Нпр. састанци, скупови, сајмови.

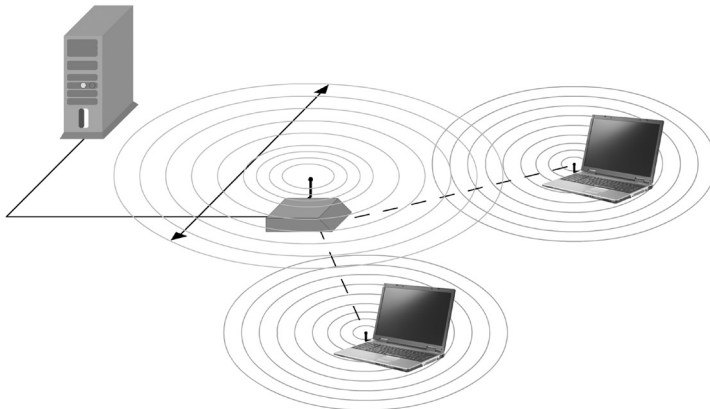
Слика 13.2 *Ad hoc* начин међусобног повезивања рачунара

13.2.2 Инфраструктурна топологија

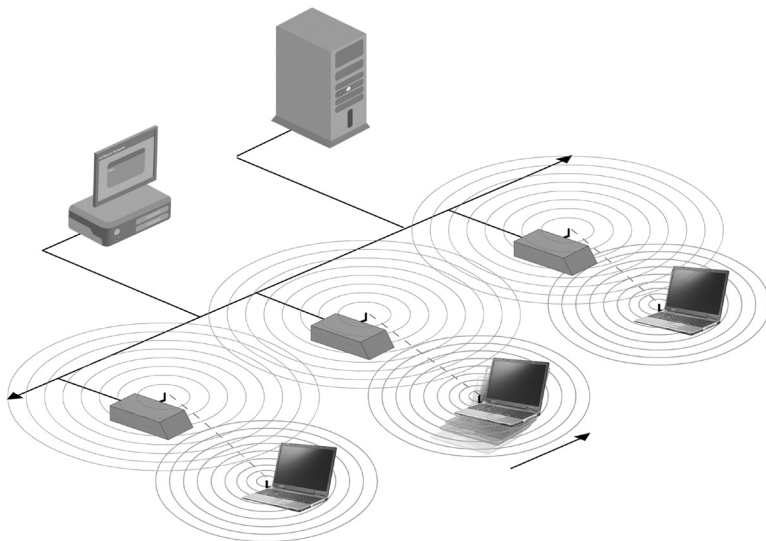
Уколико станице нису у стању да комуницирају без посредства уређаја за приступ (AP) онда се примењује начин рада који захтева одговарајућу инфраструктуру (слика 13.3). Све станице које се налазе у зони покривања уређаја за приступ међусобно комуницирају преко њега.

13.2.3 Ћелијска мрежа

У случају да се жели повећати покривеност може се инсталирати више уређаја за приступ и формирати ћелијска (целуларна) мрежа (слика 13.4). У таквој мрежи станице не могу да комуницирају директно међу собом већ искључиво посредством уређаја за приступ који могу бити међусобно



Слика 13.3 Међусобно повезивање рачунара помоћу уређаја за приступ (инфраструктурна топологија)



Слика 13.4 Ћелијска мрежа са инфраструктурним повезивањем уређаја за приступ

повезани жично или бежично. Одређеним бројем приступних станица може се покрити одређено подручје, при чему се зоне покривања појединих станица, тзв. ћелије, могу међусобно делимично и преклапати. У случају да је у одређеној ћелији велика густина саобраћаја могуће је исту површину покрити са више приступних станица, које међусобно деле мрежни саобраћај и на тај начин омогућавају опслуживање већег броја корисника.

Карактеристика ћелијских мрежа је да корисници могу бити покретљиви у току рада, мењајући приступне станице преко којих комуницирају са остатком мреже. Уређаји за приступ (AP) везују се на ожичену мрежу¹.

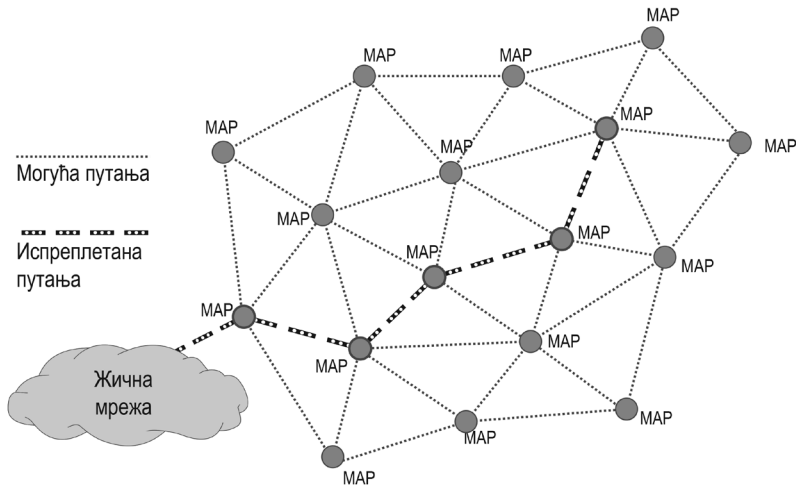
13.2.4 Испреплетана мрежа

Приступне тачке које се могу бежичним путем међусобно повезивати означавају се као испреплетане бежичне тачке (MAP²) и формирају испреплетану бежичну мрежу³ (слика 13.5).

¹ Кичму - Backbone

² Mesh Access Point

³ Прецизније би било: топологију бежичне испреплетане локалне мреже (*wireless local area network mesh topologies*) а према документу IEEE802.11s за испреплетане локалне мреже.



Слика 13.5 Испреплетана топологија

Са повећаном применом бежичних мрежа појавила се потреба да се обезбеди бежични приступ на местима где није могуће повезивање приступне тачке на комутаторе ожичене мреже. Дужина етернет кабла је ограничена на 100m што отежава постављање приступних тачака унутар пространих објеката. Ситуација је још сложенија код повезивања ван објеката код јавних услуга, општина или хитних служби.

Идеја да се бежичним линковима замене неки жични линкови (нпр. Етрнет¹) једнако је стара као и стандарди за бежичне локалне мреже. Замена каблова бежичним линковима доноси многе предности. Навешћемо неке од њих:

- Повећана флексибилност бежичних линкова над жичним. Неколико линкова између приступних тачака испреплетане мреже формирају преносни систем тако да се подаци могу пренети до жичне мреже.

¹ 1972. године Роберт Меткалф (*Robert Metcalfe*) и његове колеге из компаније Xerox PARC развиле су први експериментални етернет систем за повезивање Xerox Alto радну станицу са графичким интерфејсом. Назив ове експерименталне мреже *Alto Aloha Network* је Меткалф променио 1973. год. у Етернет (*Ethernet*) да би показао да систем може да обезбеди повезивање било ког рачунара, а не само Alto рачунара. Име потиче од речи етар (*ether*) која описује суштинску карактеристику система: физички медијум (нпр. кабл) преноси бите ка свим станицама практично на исти начин као што се некада сматрало да стари етар (енг. *Luminiferous ether/aether* - пренос светлости) преноси електромагнетске таласе кроз простор.

- Самоорганизовање¹. Уколико су алгоритми за детекцију најбоље путање ка жичној мрежи имплементирани у испреплетаним приступним тачкама онда је прављење или проширивање бежичне мреже веома једноставно.
- Могућност поновног самооправка². У случају отказа или искључења неке од приступних тачака аутоматски се проналази нова, најбоља путања.

13.3 Технологије бежичних локалних рачунарских мрежа

Бежичне локалне рачунарске мреже (WLAN) према технологији (техници) преноса генерално се могу поделити на следеће категорије:

- пренос у инфрацрвеном делу спектра (IR³),
- пренос проширивањем спектра сигнала (SS⁴),
- ортогонални фреквенцијски мултиплекс (OFDM⁵),
- пренос са више антена и више праваца пропагације таласа (MIMO⁶) и
- ускопојасне микроталасне технике⁷.

Нежељена преслушавања између канала избегавају се фреквенцијским планирањем, а сигурност и избегавање интерференције постижу се употребом посебних радио-фреквенција. Филтар на пријемнику одстрањује све сигнале осим жељеног.

13.4 Преглед стандарда IEEE 802.11

Стандард IEEE802.11 је скуп стандарда (први објављен 1997. год.) за бежичне локалне рачунарске мреже за рад у три фреквенцијска опсега: 2,4GHz; 3,6GHz и 5GHz.

Стандард је поставио основу за производе за бежичне локалне

¹ Self forming

² Self-healing

³ Infrared Technology

⁴ Spread Spectrum

⁵ Orthogonal Frequency Division Multiplexing

⁶ Multiple Input - Multiple Output

⁷ Narrowband Microwave

рачунарске мреже који носе ознаку Wi-Fi¹. Ознака „Wi-Fi“ је заштићени знак² Wi-Fi Alliance и ознака производа који раде по стандарду IEEE802.11. Производи Wi-Fi који су успешно прошли све тестове за међусобни рад³ које је прописала организација Wi-Fi Alliance могу да користе ознаку „*WiFi certified*“.

Бежичне локалне рачунарске мреже могу да раде у једном од два режима: без базне станице (слика 13.2) и са базном станицом (слике 13.3 и 13.4). У овом одељку биће анализирани скуп протокола⁴ IEEE802.11, бежичне технике преноса физичког слоја, протоколи MAC подслоја, формат рама и понуђене услуге.

Организација IEEE је од 1997. године до данас издала многе стандарде⁵ за бежичне локалне рачунарске мреже. Стандарди који су до сада нашли широку примену су: IEEE802.11, IEEE802.11a, IEEE802.11b, IEEE802.11g и IEEE802.11n. Основна обележја ових стандарда дата су у табели 13.1

Остали стандарди из серије IEEE802.11 који су развијени или на којима се ради а који неће бити анализирани у овом уџбенику биће дати у табели 13.6 на крају овог поглавља.

13.4.1 Фреквенцијски опсези и канали IEEE 802.11 мрежа

Радна група IEEE802.11 предвидела је употребу три различита фреквенцијска опсега: 2,4 GHz; 3,6 GHz и 4,9/5,0 GHz. Сваки од опсега је подељен у мноштво канала. Држава примењује своја правила (регулативе) о томе који се канали користе и колика је максимална снага предајника у оквиру сваког од канала. У неким државама (нпр. САД) оператери аматерског радија могу да користе предајнике већих снага код бежичних система већег домета.

¹ *Wireless Fidelity*

² *Trademark*

³ *Interoperability*

⁴ *Protocol stack*

⁵ У табели 13.6 (на крају поглавља) дат је списак проширења IEEE802.11 стандарда. Један је стандард IEEE802.11 али се користи термин стандард и за проширење стандарда.

13. Бежичне мреже

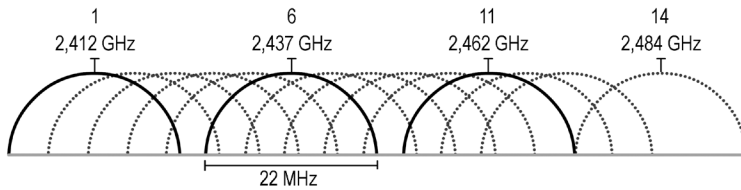
IEEE802.11	Објављен	Учестаност [GHz]	Опсег [MHz]	Брзина података по току [Mb/s]	Дозвољени број MIMO токова	Модулације	Домет у затвореном простору [m]	Домет у отвореном простору [m]
-	1997.	2,4	20	1, 2	1	DSSS, FHSS	20	100
a	1999.	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	120
		3,7 ¹					-	5000
b	1999.	2,4	20	5,5; 11	1	DSSS	38	140
g	2003	2,4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	140
n	2009.	2,4; 5	20	7,2; 14,4; 21,7; 28,9; 43,3; 57,8; 65; 72,2	4	OFDM	70	250
			40	15, 30, 45, 60, 90, 120, 135, 150			70	250
ad ²	2012.	2,4; 5; 60	7000-9000 ³	7000				
ac	~2014.	5	20	До 87,6	8	OFDM		
			40	До 200				
			80	До 433,3				
			160	До 866,7				

Табела 13.1 Основна обележја стандарда серије IEEE802.11

¹ IEEE802.11y-2008 проширио је опсег рада IEEE 802.11 на лиценцирани опсег 3,7GHz. Повећана предајна снага дозвољава опсег од 5km. Дозвољено само у САД.

² Означава се и као WiGig, покренут развој од конзорцијума *WiGig Alliance*. Постала је део WiFi групе. У будућности планирају се и веће брзине од 7Gb/s у нелиценцираном опсегу 60GHz.

³ Различито у различитим земљама



Слика 13.6 Графички приказ канала у опсегу 2,4GHz

Постоји 14 канала у опсегу 2,4GHz са међусобним растојањем од 5 MHz (слика 13.6). Изузетак је 14. канал који је 12MHz удаљен од 13. канала. У Европи се користи првих 13 канала. У Сједињеним Америчким Државама користе се првих 11 канала док канали 12 и 13 подлежу посебним ограничењима (нпр. мала снага). У Јапану дозвољено је и коришћење 14. канала али само за системе са директном секвенцом (DSSS), и CCK модулације што значи само стандард 802.11b.

Суседни канали међусобно се преклапају и могу да ометају један другог. Поред дефинисања централне учестаности канала IEEE802.11 стандард специфицира и спектралну маску којом је одређена дозвољена расподела снаге сигнала кроз канал.

Маска захтева да је сигнал ослабљен најмање 20dB (за OFDM системе¹) у односу на своју максималну вредност на одстојању ± 11 MHz од централне учестаности. Последица је да станице могу да користе сваки четврти или пети канал а да не дође до преклапања.

Да би се спречило међусобно ометање препоручује се коришћење 1, 6. и 11. канала у Северној Америци и 1, 5, 9. и 13. канала у Европи. Коришћење ових канала може се наћи у документу IEEE802.11-2012².

13.4.1 Компоненте IEEE802.11 мрежа

У општем случају мрежа IEEE802.11 састоји се од:

- станица (STA³) једне или више целина са основном (базном)

¹ За IEEE802.11b предвиђено је слабљење од 30dB.

² Године 2007. радна група је повезала сва дотадашња проширења стандарда IEEE802.11a, b, d, e, g, h, i, j у IEEE802.11-2007 а 2012. године десет проширења IEEE802.11k, r, y, n, w, p, z, v, u, s у стандард IEEE802.11-2012.

³ STAtion

услугом (BSS¹ целина, инфраструктурна BSS целина), које су повезане са дистрибуционим системом (DS²) (слика 13.7) и

- испреплетаних станица (MSTA³) које припадају целини са испреплетаном базном услугом (MBSS⁴ целина) и испреплетаног излазног уређаја (MG⁵ излаз) преко кога се MBSS целина повезује са дистрибуционим системом (слика 13.8).

Дистрибуциони систем има функцију окоснице и може да буде ожичена или било која друга комуникациона мрежа. Целина са основном услугом (BSS целина) основна је градивна целина архитектуре IEEE802.11. Група станица (STA⁶) која је под директним управљањем једне координационе функције формира целину са основном услугом (BSS).

Област коју покрива BSS целина означава се као област са основном услугом (BSA⁷ област) и одговара ћелији у целуларним комуникационим мрежама. Све станице у BSS целини могу међусобно да комуницирају. Може се десити да неке станице постану невидљиве због слабљења сигнала, као последице мултипутног фединга или због интерференције суседних станица.

Ad hoc мрежа представља груписање станица у једну целину са основном услугом (BSS). Стандард IEEE802.11 користи назив независна BSS целина (IBSS⁸). Било која станица у целини са основном услугом може да комуницира са било којом другом станицом без уређаја за приступ (AP).

Инфраструктурна мрежа

Када се за комуникацију између станица користи уређај за приступ (AP) онда стандард IEEE802.11 за такву мрежу користи термин инфраструктурна мрежа. Уређај за приступ омогућава проширење опсега

¹ Basic Service Sets

² Distribution System

³ Mesh STATION

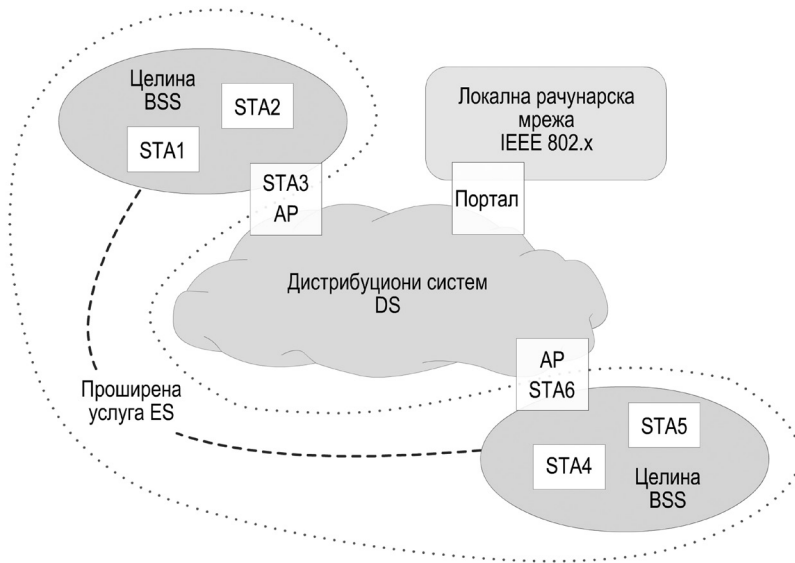
⁴ Mesh Basic Service Sets

⁵ Mesh Gate

⁶ Stations

⁷ Basic Service Area

⁸ Independent Basic Service Set



Слика 13.7 Компоненте IEEE802.11 инфраструктурне мрежа

и могућност комуникације више целина са основном услугом. Проширена услуга (ESS¹) састоји се од две или више целина са основном услугом, међусобно повезаних дистрибуционим системом. Проширена услуга појављује се као једна логичка локална рачунарска мрежа на подслоју слоја везе (LLC²).

На слици 13.7 уређај за приступ (AP) представљен је као део станице; представља логику у оквиру станице која омогућава и приступ дистрибуционом систему (DS) и саму станицу. Дистрибуциони систем (дефинисан стандардом IEEE802.11) је независан од имплементације. То значи да дистрибуциони систем може да буде жична IEEE802.3 локална рачунарска мрежа, или неки други медијум.

За интеграцију IEEE802.11 архитектуре са традиционалним локалним рачунарским мрежама са жичним трансмисионим медијумима³, или за повезивање на Интернет, користи се портал. Логика портала уграђује се

¹ Extended Service Set

² Logical Link Control

³ Користи се и термин не-IEEE802.11.

у уређаје као што су мостови или рутери који су део кабловске рачунарске мреже и који су прикључени на дистрибуциони систем (DS).

Испреплетана мрежа

Већ 2003. год. студијска група IEEE802.11 дефинисала је концепт бежичног дистрибуционог система (WDS¹) као механизам за бежичну комуникацију уз коришћење четири адресе у формату рама (слика 13.16). Студијска група није отишла ништа даље од дефиниције формата рама тј, није дала никакав опис како се тај механизам или формат рама користи. Постојала је велика потреба да се разјасни терминологија, дефинишу карактеристике и начин рада који се може интегрисати са IEEE802.11 стандардом. Радна група² је формирана 2004. године а стандард је објављен у јесен 2011. год. као IEEE 802.11s.

Стандард IEEE802.11s је предвидео унапређење MAC функција које обезбеђују бежичну испреплетану локалну топологију³. Испреплетана особеност је на располагању MSTA станицама које припадају целини са испреплетаном базном услугом (MBSS целина). Механизам који обезбеђује испреплетаност разликује се међу имплементацијама.

Способност да се реализује испреплетаност⁴ је скуп напредних функција, правила за приступање каналу, формат рамова, метода међусобне аутентификације, управљани објекти који се користе за пренос података између аутономних станица које не морају да буду у директној међусобној комуникацији преко једног бежичног линка.

Целина MBSS је IEEE 802.11 локална рачунарска мрежа која се састоји од аутономних станица (MSTA станица). Унутар MBSS целине станице успостављају бежичну везу са суседним станицама међусобно размењујући поруке. Даље, користећи способност за повезивање у више скокова⁵ поруке се могу пренети између MSTA станица које нису у међусобно директној вези. Са становишта испоруке порука изгледа као

¹ *Wireless Distribution System*. Обично се користи као колоквијални термин за механизам за бежичну комуникацију између станица које не подражавају функцију испреплетаности које користе четири адресе. Стандард IEEE802.11-2012 специфицира такав формат само за испреплетану базу целину (MBSS) и искључен је из даљих верзија.

² *Task group*

³ *Wireless LAN mesh topologies*

⁴ *Mesh facility*

⁵ *Multi-hop capability*

да су све станице у MBSS целини међусобно директно повезане на MAC слоју, иако оне нису све у домету једна другој.

Повезивањем у више скокова проширује се област покривања MSTA станице. У MBSS целини MSTA станица може да буде извориште, одредиште или да прослеђује саобраћај¹ (неким MSTA станицама то јесте једина функција). MBSS целина може да има интерфејсе ка спољашњим мрежама и да обавља функцију дистрибуционог медијума система (DSM² медијума) за инфраструктурну BSS целину.

Пример испреплетане базне целине (MBSS целина) приказан је на слици 13.8. Само MSTA станице могу да формирају MBSS целину, селектују путању и преусмеравају поруке. Стандрд IEEE802.11s каже да MSTA станица³ није део инфраструктурне базне целине и као последица тога она не може директно да комуницира са не-MSTA станицама⁴. Ово може да буде збуњујуће: како се испреплетана мрежа може повезивати са жичном мрежом другачије него преко IEEE802.11 уређаја. Разлог који стоји иза ове дефиниције је тај што у проширењу стандарда IEEE802.11s испреплетана станица представља функцију. У нашој свакодневной употреби станица је физички уређај али у терминологији IEEE802.11 термин станица је подскуп функција једног уређаја. Приступна тачка може у себи да интегрише функције испреплетане станице и комуницира са другим испреплетаним станицама а такође да интегрише и функције приступне тачке (AP) која обезбеђује асоцирање IEEE802.11 клијентских уређаја.

MBSS целина може се повезати са другим базним целинама (инфраструктурним или испреплетаним) преко дистрибуционог система (слика 13.8). MSTA станица може да комуницира са не-MSTA станицом преко дистрибуираног система.

Подаци се преносе између MBSS целине и дистрибуционог система преко једног или више излаза (MG⁵ излаз).

¹ *Propagators of traffic*

² *Distribution System Medium*. Трансмисиони медијум или скуп трансмисионих медијума које користи дистрибуциони систем (DS) за комуникацију између приступних тачака (AP), излаза из испреплетане целине MBSS (MG излаз) и портала проширеног скупа услуга (ESS).

³ Треба имати на уму да термин испреплетана станица у проширењу стандарда IEEE802.11s има значење функције а не уређаја.

⁴ *Non-mesh station*

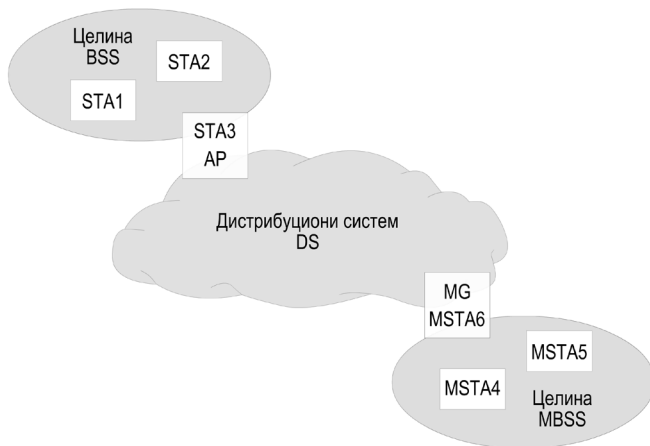
⁵ *Mesh gate*

Дистрибуциони систем „дистрибуира“ рамове са једног интерфејса на други. То може да буде дистрибуција рамова од клијента на 2,4GHz на клијента на 5GHz. У сваком случају битно је нагласити да је дистрибуциони систем логичка конструкција а не посебан трансмисиони медијум као што је то жични (нпр. Етернет).

Стандардом 802.11-2007 дефинисана је приступна тачка (AP) као станица која обезбеђује приступ дистрибуционом систему преко бежичног медијума станицама које су на њу повезане. Приступна тачка може да испоручује рамове другим станицама у ћелији или у ожиченој мрежи.

Функција приступне тачке која обавља превођење између бежичне мреже и жичне мреже назива се портал. Портал је функција. То је само логичка тачка где се бежична јединица података MAC слоја (MSDU¹ податак) преводи ка и из не-IEEE802.11 мреже. Приступна тачка уобичајено обавља функцију портала.

Када се превођење одвија између MBSS целине и неиспреплетаног IEEE802.11 дистрибуционог система функција се означава као излаз из испреплетане мреже (MG излаз). То је логичка тачка где се јединица



Слика 13.8 Пример повезивања станице (MSTA) у испреплетаној мрежи (MBSS) са станицама у инфраструктурној мрежи (BSS) помоћу MG излаза.

¹ MAC Service Data Unit

података испреплетаног MAC слоја (MMSDU¹ податак) преводи ка и од неиспреплетаног IEEE802.11 дистрибуционог система. Друге функције се обично захтевају да би се комплетирао превођење. На пример ако се рам који долази из MBSS целине шаље ка IEEE802.11 ћелији (инфраструктурној BSS ћелији) AP функција води рачуна о преусмеравању рамова ка жичној мрежи. Један уређај може да буде централна тачка ћелије (на тај начин је приступна тачка AP), повезује своје бежичне клијенте на жичну мрежу (на тај начин је портал) док истовремено учествује у испреплетаној базној станици (MBSS целини) и повезује испреплетане станице (MSTA станице) ка дистрибуционом систему (на тај начин је излаз испреплетане мреже).

Недостатак тачног дефинисања појмова и компонената испреплетаних мрежа је довео до различитих реализација произвођача. У време писања овог уџбеника међусобни рад уређаја различитих произвођача није могућ. Произвођачи користе специфичне своје термине, формате рамова и специфичне протоколе. Не може се са сигурношћу знати да ли су или у ком обиму произвођачи реализовали функције које су стандардом предвиђене.

13.4.2 Протоколи MAC подслоја IEEE 802.11

Протокол на MAC подслоју стандарда IEEE802.11 значајно се разликује од протокола на MAC подслоју стандарда IEEE802.3, због веће сложености бежичних у односу на жичне системе. Код IEEE802.3 система станица чека док се трансмисиони медијум не ослободи и тек онда започиње са слањем. Уколико не прими ометајући сигнал (који указује да је дошло до колизије) скоро је сигурно да је рам успешно испоручен одредишту. Код бежичних система ситуација је мало другачија.

Постоји проблем невидљиве станице²: све станице нису једна другој у радио-домету па се може десити да се предаја у једном делу ћелије не може детектовати у другом делу исте ћелије. У примеру на слици 2.3 станица C_1 шаље податке ка станици C_2 . Станица C_1 испитује канал и пошто је ван домета станице C_3 погрешно ће закључити да је канал слободан и да може да започне са слањем података ка станици C_2 .

¹ Mesh MAC Service Data Unit

² Одељак 2.2.1.

Постоји и други проблем – изложена станица¹: станица C_2 жели да пошаље податке станици C_4 и испитује канал. Кад открије да постоји неки сигнал погрешно ће закључити да не може да започне са слањем ка станици C_4 , пошто станица C_1 шаље податке ка станици C_3 . Многи радио-системи су полудуплексни што значи да не могу истовремено и да шаљу и да испитују (ослушкују) медијум на истој радио-учестаности. Последица тога је да IEEE802.11 системи не могу да користе CSMA/CD протокол који се користи код IEEE802.3 система.

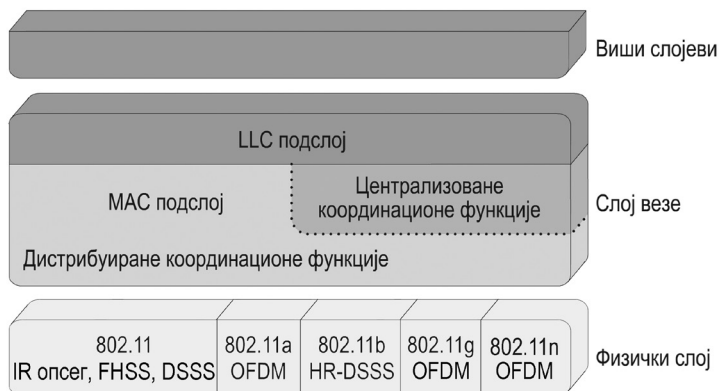
13.4.3 Слојевита архитектура протокола по стандарду IEEE 802.11

Слојевита архитектура протокола који се користе у првобитном IEEE802.11 стандарду има структуру као што је приказано на слици 13.9. Стандард се односи на прва два слоја OSI референтног модела: физички слој и слој везе. Подслој MAC (слоја везе) одређује начин доделе канала а подслој LLC (слоја везе) има задатак да заштити више слојеве од различитости техника IEEE802 серије.

У стандарду IEEE802.11 дефинисане су:

- дистрибуиране координационе функције (DCF²) и
- централизоване координационе функције (PCF) (слика 13.9).

Стандардом IEEE802.11-2012 обухваћене су и (слика 13.12):



Слика 13.9 Слојевита архитектура протокола у бежичним локалним рачунарским мрежама у оригиналном стандарду IEEE802.11

¹ Exposed node problem

² Distributed Coordination Function

- хибридне координационе функције (HCF¹) описане у документу IEEE802.11e и
- испреплетане координационе функције (MCF²) описане у документу IEEE802.11s.

Дистрибуирана координациона функција

Основни метод приступа трансмисионом медијуму IEEE802.11 система је дистрибуирана координациона функција (DCF) означена као вишеструки приступ са избегавањем колизије (CSMA/CA³). Метод DCF је имплементиран у свим станицама и може се описати на следећи начин (слика 13.10):

1. Станица која жели да шаље податке прво испитује трансмисиони медијум. Ако је слободан чека одређено време T_p да види да ли ће и даље бити слободан. Уколико је и по истеку T_p времена медијум и даље слободан започиње са слањем. CSMA/CA дистрибуирани алгоритам дефинише колики треба да буде минимални размак између суседних рамова;
2. Уколико је трансмисиони медијум заузет, било зато што је већ био заузет, било зато што је постао заузет после T_p времена, станица чека да се заврши слање и да се медијум ослободи;
3. Када се текуће слање заврши станица чека још T_p времена. Уколико је медијум и тада слободан станица чека још неко случајно време кашњења у слању⁴. Ово је период надметања (такмичења⁵) у коме станице могу да се такмиче (боре) за приступ медијуму. Трајање случајног времена одлагања слања одређује се за сваку станицу посебно као мултипл временских целина⁶. Ново, независно случајно време бира се за сваки нови покушај слања. Станица бира број временских целина по случајном

¹ Hybrid Coordination Function

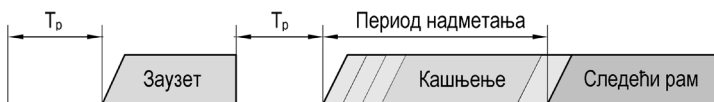
² Mesh Coordination Function

³ CSMA with Collision Avoidance - CSMA са избегавањем колизије

⁴ Random auck off time. Користи се исти алгоритам са бинарним експоненцијалним кашњењем као код IEEE802.3.

⁵ Contention time

⁶ Slot time Нпр. износи 9μsec за мреже по стандарду IEEE802.11a.



Слика 13.10 Протокол CSMA/CA

избору у опсегу од 0 до времена надметања (CW^1 - прозора надметања). Ово време се иницијално поставља на минималну вредност² CW_{min} . Све станице користе исто CW_{min} време али бирају случајно време кашњења у слању. Код система са дистрибуираним координационим функцијама (DCF) све станице раде са истим CW_{min} временом тако да имају исти приоритет у приступу трансмисионом медијуму. Резултат је да не постоји механизам који може да прави разлику између станица и њиховог саобраћаја а самим тим не може да се обезбеди квалитет услуге (QoS).

4. Ако по истеку случајног времена нико није заузео медијум станица може да започне са слањем података.

Одлагање слања (случајно време) које се користи је бинарно експоненцијално и користи се код саобраћаја великог интензитета. Понављање неуспелих покушаја слања података доводи до све дужих одлагања слања, што помаже да се саобраћај развуче у времену. Ако се не би користило случајно кашњење догодило би се следеће: две станице које покушају истовремено да шаљу податке дошле би у колизију. Уколико би без међусобно различитог кашњења покушале поново да шаљу поново би дошло до колизије.

Увек када IEEE802.11 бежична станица (извориште) пошаље рам само ка једном одредишту³ (директно упућеном) и ако је рам примљен без грешке одредиште ће одговорити са рамом потврде (ACK рам). Уколико изворишна станица добије ACK рам она зна да је пренос успешно реализован. Ако се ACK рам не добије изворишна бежична станица ће морати да поново пошаље рам. Значи: за сваки рам упућен

¹ Contention Window

² Нпр. износи 15μсес за мреже по стандарду IEEE802.11a.

³ Unicast frame

једној станици мора да постоју потврда - ACK рам. Не може се тачно утврдити да ли је дошло до колизије, тј. не постоји детекција колизије.

У сваком случају пренос је успешно окончан по пријему ACK рама од станице којој је директно упућен или када је комплетно послат рам ка групи станица.

Да би се додатно минимизирала могућност истовременог слања (колизија) две станице предајна и пријемна станица могу да размењују управљачке рамове¹ RTS и CTS. Рамови се размењују пошто станице установе да је медијум слободан и после одлагања преноса а пре слања података.

Постоје два начина испитивања канала: физички и виртуелни механизми. Начин који се користи код система са дистрибуираном координационом функцијом заснован на протоколу CSMA/CA је испитивање виртуелног канала као што је приказано на слици 13.11.

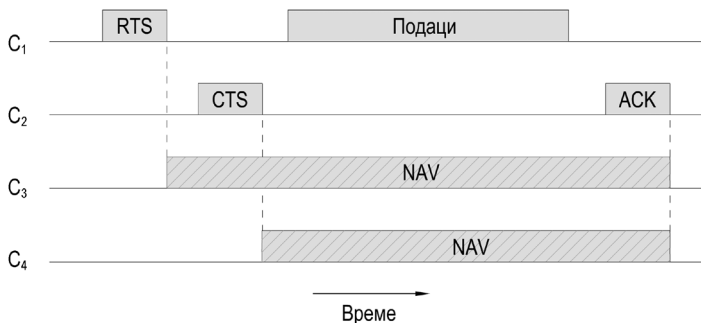
Размена RTS и CTS рамова је један од начина размене информација о резервацији трансмисионог медијума. Рамови RTS и CTS садрже информацију о трајању комуникације². Тако је дефинисан период времена у коме ће трансмисиони медијум бити резервисан за слање рамова и за пријем потврде (ACK рам). Станица која прима RTS рам (који је послала изворишна станица) или CTS рам (који је послала одредишна станица) ће реализовати процес резервације трансмисионог медијума. Може да се деси да станица није у стању да прими податке од изворишне станице али је ипак упозната са тим захтевом.

Анализирајмо пример (слика 2.3) станице C_1 која жели да пошаље податке станици C_2 . Станица C_1 прво шаље RTS рам којим тражи дозволу од станице C_2 да јој пошаље податке. Када станица C_2 добије захтев RTS станице C_1 , и ако жели да прими податке од ње, она шаље натраг дозволу - рам CTS. По пријему CTS рама станица C_1 шаље рам са подацима и поставља на одређено време часовник за потврду ACK. Када станица C_2 прими рам података она шаље рам потврде ACK и размена је окончана. Уколико време на које је часовник ACK постављен истекне пре него што стигне потврда (ACK) рама цела процедура се понавља.

¹ Детаљан опис може се наћи у одељку 2.1.2 овог уџбеника.

² *Duration field*

13. Бежичне мреже



Слика 13.11 Употреба испитивања виртуелног канала са протоколом CSMA/CA

Посматрајмо како размену података виде станице C₃ и C₄. Станица C₃ је у домету станице C₁, и може да прими RTS рам. Уколико га је примила она може на основу података из рама RTS да закључи да ће станица C₁ бити заузета одређено време. На основу тога станица C₃ поставља на одређену вредност ознаку (индикатор, вектор) заузетости канала (NAV¹). Рам RTS не може да допре до станице C₄ али може рам CTS, пошто је станица C₄ у домету станице C₂. Станица C₃ поставља на одређену вредност своју ознаку заузетости канала (NAV). Треба уочити да ознаке о заузетости канала (NAV) нису рамови који се шаљу, они су само интерни показатељи који указују колико дуго станица не треба ништа да шаље.

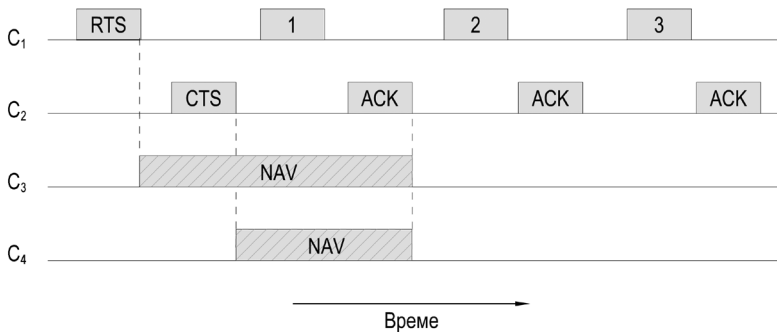
Други начин дистрибуирања информација о резервацији трансмисионог медијума је поље трајања² у рамовима који су адресирани ка појединачним станицама. Ово поље указује на колико је времена трансмисиони медијум резервисан.

За разлику од кабловских локалних рачунарских мрежа бежичне рачунарске мреже су непоуздане и са великим сметњама. Због тога је у IEEE802.11 рачунарским мрежама предвиђено дељење рамова у мање целине - фрагменте. Сваки фрагмент садржи свој контролни збир. Фрагменти су нумерисани и потврђују се помоћу протокола заустави се и чекај³. Фрагменти се шаљу један за другим (слика 13.12).

¹ Network Allocation Vector

² Duration/ID field

³ Детаљније објашњење може се наћи у 7. поглављу уџбеника Рачунарске мреже [1].



Слика 13.12 Слање фрагмената

Пошто је трајање батерија значајно за бежичне системе стандард IEEE802.11 је понудио решење које води рачуна о томе. Базна станица може да обавештава мобилну станицу да је у стању мировања¹ све док је она или корисник експлицитно не активирају. Ово има за последицу да базна станица преузима на себе смештање свих података који се упућују ка станици која је у стању мировања. Станица у мировању податке може да покупи касније.

Централизоване координационе функције

Други начин приступа медијуму код IEEE802.11 система је помоћу централизоване координационе функције² (PCF). Базна станица³ шаље пит (полира) другим станицама у ћелији да би видела да ли имају податке за слање.

Пошто редослед слања потпуно одређује базна станица до колизије не може да дође. Стандард прописује механизам полирања али не и учестаности, редослед или приоритете полирања.

Основни механизам састоји се у томе да базна станица шаље посебан рам⁴ периодично (10 до 100 пута у секунди). Посебан рам садржи параметре система као што су учестаност скакања и такт за синхронизацију. Такође се позивају нове станице да се пријаве.

¹ Стање успаваности

² У време писања овог уџбеника централизована координациона функција није део Wi-Fi спецификације.

³ Централизовани координатор

⁴ Beacon - фар

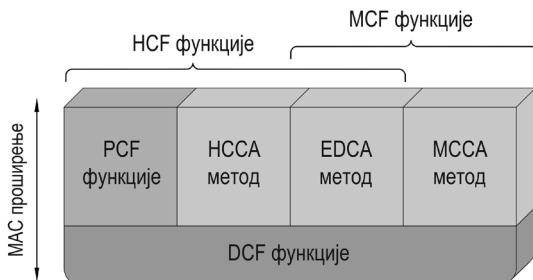
Хибридне координационе функције

Проширењем стандарда IEEE802.11е дефинисане су MAC методе потребне да се задовоље захтеви за квалитетом услуга (QoS¹) у преносу временски осетљивих апликација² бежичним локалним мрежама. У том циљу дефинисане су хибридне координационе функције (HCF³ функције) које обезбеђује два метода приступа (слика 13.13):

- унапређени дистрибуирани приступ каналу (EDCA⁴ метод) и
- хибридне координационе функције (HCF функције) за управљање приступом канала (HCCA⁵ метод).

Унапређена координациона функција је проширење дистрибуиране координационе функције (DCF функције). EDCA метод обезбеђује приступ трансмисионом медијуму (каналу) саобраћај са приоритетима коришћењем ознака о приоритетима дефинисаним у стандарду IEEE802.1D (табела .13.2).

Хибридна координациона функција (HCF функција) слична је централизованом координационој функцији (PCF функцији) и обезбеђује механизам за доделу приоритета користећи механизам упита помоћу хибридног координатора (HC⁶ координатора). Другим речима одређене станице могу да шаљу податке пре осталих.



Слика 13.13 MAC архитектура по стандарду IEEE802.11-2012 (укључена проширења IEEE802.11е и IEEE802.11s)

¹ Quality of Service

² Time-sensitive applications

³ Hybrid Coordination Function

⁴ Enhanced Distributed Channel Access

⁵ HCF Controlled Channel Access

⁶ Hybrid Coordinator

Приступна категорија ¹	Опис	Ознаке приоритета ²
Говор ³ (1. категорија)	Највећи приоритет. Дозвољава више VoIP позива уз минимално кашњење и прихватљив квалитет.	7, 6
Видео ⁴ (2. категорија)	Преносу видео садржаја даје се приоритет над преносом података ⁵ .	5, 4
Најбоља могућа ⁶ (3. категорија)	Саобраћај од апликација или уређаја који немају захтеве за квалитетом услуга (QoS) Овај саобраћај је мање осетљив на кашњења. Већина традиционалних итернет података подлеже овој врсти саобраћаја.	0, 3
У позадини ⁷ (4. категорија)	Саобраћај најнижег приоритета (скидање датотека, штампа) који нема стриктне захтеве у погледу кашњења и пропусног опсега.	2, 1

Табела 13.2 Врсте саобраћаја и категорије приоритети у бежичним локалним мрежама

Организација Wi-Fi Alliance објавила је WMM⁸ сертификат који делимично имплементира IEEE802.11е проширење. WMM сертификат ослоњен је на EDCA метод и обезбеђује четири категорије приоритета (табела 13.2).

Wi-Fi Alliance је објавила⁹ и WMM планирани приступ (SA¹⁰ приступ) који је заснован на HCCA методу. Код овог приступа нема надметања

¹ Access Categories

² Priority tags. Преузето из стандарда IEEE802.1D.

³ Voice

⁴ Video

⁵ Један IEEE802.11g или IEEE802.11а канал може да обезбеди пренос три до четири SDTV тока (Standard-definition television – телевизија стандардне резолуције) или један HDTV ток (High-definition television – телевизија високе дефиниције).

⁶ Best effort

⁷ Background

⁸ Wi-Fi Multimedia

⁹ The Wi-Fi Alliance је дефинисала WMM – PS (Power Save), што представља IEEE802.11е механизам за продужење века трајања батерија применом напредних метода штедње напајања.

¹⁰ Scheduled Access

између станица која од њих ће успети да приступи медијуму – унапред је испланирано (заказано). Планирани приступ (SA приступ) даје могућност апликацијама да резервишу мрежне ресурсе на основу карактеристика свог саобраћаја тако што клијент шаље захтев приступној тачки (AP). Овај приступ подржава тзв. параметаризовани, планирани приступ и одговара HCCA методу. Пошто је утицај случајног кашњења мањи SA приступ може да свеукупно смањи кашњење у мрежи употребом централизованог механизма управљања са планирањем времена¹.

Испреплетана координациона функција

Да би станице које су део MBSS целине биле у стању да детектују једна другу морају да раде на истом каналу. Приступ каналу је кључна компонента испреплетане инфраструктуре па је нова координациона функција направљена за испреплетане мреже: испреплетана координациона функција (MCF² функција). Она у приступу медијуму комбинује методе надметања³ и метод са временском расподелом⁴. MCF функција integriше елементе EDCA и HCCA метода стандарда IEEE802.11e и формира контролисани приступ испреплетаној мрежи (MCCA⁵ приступ).

Временски интервали између рамова

Стандард IEEE802.11-2012 је предвидео коегзистенцију начина рада: централизованих и дистрибуираних система у једној ћелији. Један од механизма су дефинисана времена између рамова. Пошто се један рам пошаље чека се одређени временски интервал пре него што било која станица може да пошаље следећи рам.

Дефинисано је шест временских интервала између рамова⁶ (слика 13.14):

1. Најкраћи интервал између рамова (SIFS⁷ време) користи се код станица које су већ у међусобној вези. То значи да ће по истеку

¹ Centralized scheduling control mechanism

² Mesh Coordination Function

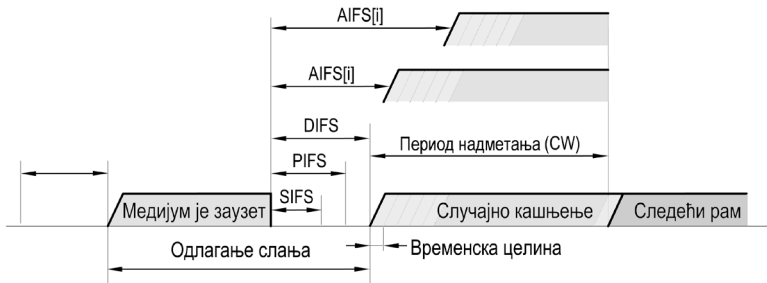
³ Contention-based

⁴ Scheduled access

⁵ Mesh controlled channel access

⁶ InterFrame Spacing

⁷ Short Interframe Spacing



Слика 13.14 Временски интервали између рамова по стандарду IEEE802.11-2012

SIFS времена: бити послат рам CTS као одговор на пријем рама RTS, или рам ACK као одговор на фрагмент или цео рам податка. Постоји само једна станица која би требало да шаље по истеку SIFS времена.

2. Редуковани интервал између рамова (RIFS¹ време) може се користити уместо SIFS времена када један предајник шаље више рамова и када се не очекује више одговора међусобно размакнутих SIFS временом. Не може се користити за различите одредишне адресе. RIFS време је време које протекне између последњег послатог симбола претходног рама и почетка преамбуле следећег рама који је присутан на радио интерфејсу.
3. Уколико станица не искористи канал у временском интервалу SIFS базна станица може да пошаље свој посебан рам или упит (PIFS² време). Овај механизам дозвољава да станица која шаље податке или секвенцу фрагмената заврши започето слање.
4. Уколико базна станица нема шта да пошаље по истеку временског интервала DIFS³ било која станица може да покуша да приступи каналу и пошаље нови рам. Примењује се уобичајен начин за приступање каналу и бинарни експоненцијални алгоритми за кашњења уколико дође до колизије.

¹ Reduced InterFrame Space

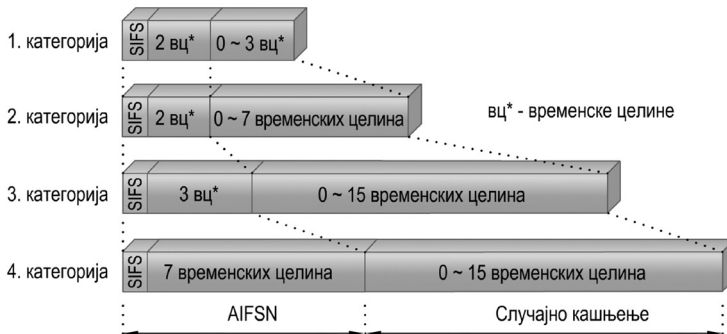
² Point Coordination Function Inter Frame Spacing - PCF размак између рамова

³ Distributed Coordination Function InterFrame Spacing - DCF размак између рамова

5. Временски интервал (EIFS¹ време) користи станица која је управо добила рам са грешком или рам који није очекивала². Она шаље обавештење о грешци. Идеја да се додели најнижи приоритет овом обавештењу произлази из чињенице да треба дати времена предајнику који не зна да је дошло до грешке и да се на тај начин спречи интерференција.
6. Арбитражни временски интервал (AIFS³ време) указује на број временских целина после којих станица треба да одложи слање пре него што активира алгоритам за поновно слање или започне процедуру слања. Минимална вредност AIFS времена је 2. AIFS време користе станице са имплементираном услугом квалитета (QoS) и које приступају медијуму користећи EDCA приступ за слање свих рамова података, рамова за надзор и услугу, рамова упита и управљачких рамова (RTS, CTS). Параметар „i“ у ознаци за арбитражни временски интервал AIFS[i] односи се на приступне категорије дефинисане у табели 13.2.

Уколико је медијум слободан прустапа се одмах по истеку времена DIFS и AIFS[i].

Алгоритам за разрешавање колизије који обезбеђује приоритете у приступу медијуму је пробабилистички и зависи од два временска



Слика 13.15 Арбитражни временски интервали у зависности од приступних категорија

¹ *Extended InterFrame Spacing* - проширени размак између рамова

² Изостављено са слике 13.13.

³ *Arbitration InterFrame Space*

Приступна категорија	CW_{min}	CW_{max}	AIFSN
Говор	15	1023	7
Видео	15	1023	3
Најбоља могућа	7	15	2
У позадини	3	7	2
Оригинални DCF	15	1023	2

Табела 13.3 Подразумевање вредности параметара EDCA метода за различите приступне категорије

параметра који се мењају у зависности од приступне категорије:

- минимално време између рамова (AIFSN¹),
- прозора надметања (CW) .

Обе вредности су мање за саобраћај већег приоритета. За сваку од приступних категорија вредност одлагања слања израчунава се (слика 13.15) као збир вредности минималног времена између рамова AIFSN и случајне вредности од 0 до вредности прозора надметања (CW). Вредност CW се мења у времену и иницијално се поставља на вредност која зависи од приступне категорије (табела 13.3).

После колизије прозор надметања (CW) се удвостручава све док не достигне максималну вредност. После завршеног успешног преноса CW се поставља на иницијалну вредност у зависности од приступне категорије. Приступна категорија са најмањим кашњењем стиче право да прва пошаље своје податке.

13.4.4 Структура рама стандарда IEEE 802.11

Стандард IEEE802.11 дефинише 3 различите класе рамова: податак, управљање и надзор. За сваки од ових рамова дефинисана су поља унутар MAC подслоја. Формат рама података приказан је на слици 13.16.

Прво поље за управљање рамом (FC²) садржи 11 потпоља:

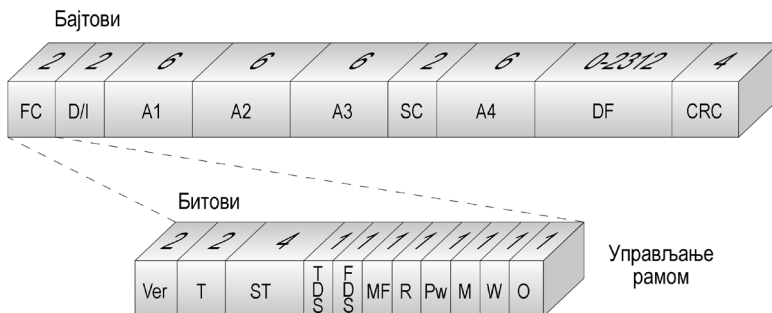
- верзија протокола Ver³ - дозвољава истовремени рад две верзије протокола у истој ћелији,

¹ Arbitrary InterFrame Space Number

² Frame Control field

³ Version

13. Бежичне мреже



Слика 13.16 Рам података IEEE802.11

- тип (T¹) - указује да ли је рам података, управљања или надзора,
- подтип (ST²) - указује да ли је рам RTS или CTS,
- ка DS (TDS³) и од DS (FDS⁴) - указује да ли рам одлази ка или долази од дистрибуционог система,
- бит MF⁵ - указује да постоји више фрагмената,
- бит поновни покушај (R⁶) - означава ретрансмисију рамова који су већ раније послати,
- бит управљање напајањем (Pw⁷) - користи базна станица за постављање мобилне станице у мирно или активно стање,
- бит M⁸ - указује да пошиљалац планира да пошаље још рамова примаоцу,
- бит W - указује да је садржај рама шифрован користећи WEP⁹ алгоритме,
- бит O¹⁰ - указује примаоцу да рамови са постављеним битом на 1 треба да буду обрађени редоследом којим су и примљени.

¹ Type field

² Subtype

³ To DS

⁴ From DS

⁵ More fragment

⁶ Retry

⁷ Power management

⁸ More

⁹ Wired Equivalent Privacy

¹⁰ Order

Поље трајања (D/I^1) указује на то колико ће дуго (изражено у микросекундама) рам и његова потврда заузимати канал. Ово поље постоји и у управљачким рамовима² тако да на основу њега станице могу да поставе своје индикаторе (NAV).

Заглавље рама садржи четири адресе ($A_1 - A_4$). Све адресе су стандардног IEEE802 формата. Две адресе су изворишна и одредишна адреса мобилних станица. Преостале две адресе су изворишна и одредишна адреса базних станица када се саобраћај одвија између ћелија³.

Поље за секвенцне бројеве (SC^4) користи се за обележавање фрагмената. Од 16 битова који су на располагању 12 битова се користи за обележавање рамова, а 4 бита за обележавање делова рама (фрагмената).

Поље података (DF^5) садржи корисне податке⁶ од 0 до 2312 бајтова.

Поље контролног збира (CRC^7) има уобичајену намену да открије грешке у преносу.

Рамови за надзор имају формат сличан формату рама података осим броја адреса. Пошто се рамови надзора размењују искључиво унутар једне ћелије адреса базне станице није потребна.

Управљачки рамови су краћи и имају само једну или две адресе. Не садрже поље за податке ни поље за секвенцне бројеве. Кључне информације у овим рамовима налазе се у потпољу подтип које указује да ли је рам захтев за успоставом везе (RTS), потврда о успостави везе (CTS) или потврда о успешном пријему рама података (ACK).

13.4.5 Услуге IEEE 802.11

Стандард IEEE802.11 дефинише девет услуга које треба да пружи бежична локална рачунарска мрежа да би обезбедила функционалност

¹ *Duration /Connection ID, Duration/ID*

² Поље трајања (*Duration/ID*) је дужине 16 битова. Садржај овог поља се мења у зависности од типа (и подтипа) рама. Зависи и од тога да ли се рам шаље за време CFP периода (*Contention Free Period*) када не може да дође до колизије (постављен NAV вектор). Мења се у зависности од квалитета услуге (QoS) изворишне станице.

³ Обично се користе само три адресе

⁴ *Sequence Control*

⁵ *Data Field*

⁶ *Payload*

⁷ 32-битни циклични кôд (*Cyclic Redundancy Check*)

13. Бежичне мреже

Услуга	Ко обезбеђује	За шта се користи
Приступање (<i>Association</i>)	Дистрибуциони систем	MSDU испорука
Одступање (<i>Dissassociation</i>)	Дистрибуциони систем	MSDU испорука
Дистрибуција (<i>Distribution</i>)	Дистрибуциони систем	MSDU испорука
Поновно приступање (<i>Reassociation</i>)	Дистрибуциони систем	MSDU испорука
Интеграција (<i>Integration</i>)	Дистрибуциони систем	MSDU испорука
Пријава (<i>Authentication</i>)	Станица	Приступ и безбедност локалне рачунарске мреже
Одјава (<i>Deauthentication</i>)	Станица	Приступ и безбедност локалне рачунарске мреже
Приватност (<i>Privacy</i>)	Станица	Приступ и безбедност локалне рачунарске мреже
Испорука јединица података MAC подслоја (<i>MSDU delivery</i>)	Станица	MSDU испорука

Табела 13. 4 Услуге IEEE802.11

еквивалентну оној која постоји у кабловским локалним рачунарским мрежама. Табела 13.4 приказује списак услуга и два начина на које оне могу да се систематизују¹.

На основу табеле може да се уочи следеће:

1. Услугу може да обезбеди или станица или дистрибуциони систем (DS). Услуге станице су примењене у свакој IEEE802.11 станици, укључујући приступне тачке (AP). Дистрибуционе услуге су обезбеђене између целина са основном услугом (BSS); ове услуге могу бити уграђене у приступне тачке (AP) или у друге уређаје са специјалним функцијама који су повезани на дистрибуциони систем.
2. Три услуге су употребљене за управљање приступом

¹ MAC Service Data Unit

поверљивошћу IEEE802.11 бежичних локалних мрежа. Од шест могућих услуга три се користе да би се обезбедила испорука MSDU јединица података између станица. MSDU јединица података је блок података који корисник MAC подслоја прослеђује MAC подслоју¹. Уколико је MSDU јединица података превише велика да би била послата користећи један MAC рам она се може поделити у делове (фрагменте) и послати користећи више MAC рамова.

За информације које се размењују бежичном мрежом користи се RC4² алгоритам за шифровање.

13.4.6 Физички слој стандарда IEEE 802.11

Као што се може видети из табеле 13.4 велика пажња поклања се побољшању свих карактеристика система са бежичним преносом. У овом одељку биће дата кратка анализа физичких слојева оригиналног стандарда IEEE802.11 и каснијих, побољшаних верзија IEEE802.11a, IEEE802.11b, IEEE802.11g и IEEE802.11n.

Оригинални стандард IEEE 802.11

Предвиђена су три начина реализације физичког слоја стандарда IEEE802.11. Први је користио пренос сигнала у инфрацрвеном опсегу спектра а друга два омогућавају радио-пренос података употребом техника проширеног спектра³, у фреквенцијском опсегу од 2,4GHz до 2,4835GHz. Подржан је пренос на брзинама од 1Mb/s и 2Mb/s.

Први начин реализације стандарда IEEE802.11 користи дифузну инфрацрвену технологију преноса. Може се користити на растојањима до 20m.

Други начин реализације стандарда IEEE802.11 користи пренос података техником проширеног спектра, употребом директне, Баркерове, секвенце. Број канала зависи од фреквенцијског опсега који одређују национална регулаторска тела. Примењују се диференцијалне фазне

¹ Обично је корисник LLC подслој и он прослеђује LLC PDU (*Logical Link Control Protocol Data Unit*) MAC подслоју.

² Аутор (1987. год.) RC4 (Rivest Cipher 4) је *Ron Rivest* један од оснивача компаније *RSA Security*. Име *RSA* је настало од иницијала проналазача *Ron Rivest*, *Adi Shamir* и *Len Adleman* по којима је *RSA* криптографски алгоритам јавних кључева (*RSA public key cryptography algorithm*) добио име.

³ Одељак 7.11 уџбеника Рачунарске мреже [1].

модулације и то: DBPSK¹ за проток од 1Mb/s и DQPSK² за проток од 2Mb/s.

Трећи начин реализације стандарда IEEE802.11 користи пренос података техником проширеног спектра са фреквенцијским скакањем. Сигнал носиоца мења учестаност у зависности од псеудослучајне секвенце. Дефинисано је 78 секвенци за скакање (у САД и Европи). Растојање између учестаности два узастопна скока је 6MHz у САД и већини европских земаља, а 5MHz у Јапану. Коришћени фреквенцијски опсег подељен је на 79 потканала (у САД и Европи) ширине 1MHz чиме је брзина ограничена на 2Mb/s.

Стандард IEEE 802.11a

Први у низу стандарда већих брзина у бежичним системима је IEEE802.11a. Користи се ISM фреквенцијски опсег 5,8GHz и ортогонални фреквенцијски мултиплекс (OFDM³). Не користи се техника проширивања спектра већ потканали са носиоцима на различитим међусобно ортогоналним учестаностима. Подаци се деле у више токова а сваки се преноси помоћу свог подносиоца, кроз свој потканал. Могуће брзине су: 6, 9, 12, 18, 24, 36, 48 и 54Mb/s. Користе се до 52 носиоца који су модулисани са BPSK, QPSK, 16QAM⁴, 64QAM у зависности од брзине која се захтева.

Стандард IEEE 802.11b

Циљ је био понудити стандард IEEE802.11b који подржава брзине преноса података као и (тадашњи) IEEE802.3 стандард. Понуђене су брзине 5,5Mb/s и 11 Mb/s и рад у ISM фреквенцијском опсегу од 2,400GHz до 2,4835GHz. Само повећање брзине преноса на 11Mb/s омогућено је употребом CCK⁵ модулације, или такозване модулације са комплементарним кодовима. Модулације CCK се користе као кодна секвенца при процесу ширења спектра DSSS техником. Да ли ће проток бити 11 Mb/s или 5,5Mb/s зависи од стања у каналу, а уређај се сам томе

¹ *Differential Binary Phase Shift Keying*

² *Differential Quaternary Phase Shift Keying*

³ *Orthogonal Frequency Division Multiplexing*. Среће се и под називом дискретна вишетононска DMT (*Discrete Multitone*) и модулација са више носиоца MCM (*MultiCarrier Modulation*).

⁴ *Quadrature Amplitude Modulation* - комбинација PSK и ASK (*Amplitude Shift Keying*).

⁵ *Complementary Code Keying*

прилагођава.

Стандард IEEE 802.11g

Стандард IEEE802.11g је побољшана верзија 802.11b. Користи OFDM модулацију али ради у 2,4GHz фреквенцијском опсегу. Теоретски може да достигне брзине од 54Mb/s.

Стандард IEEE 802.11n

Стандард IEEE 802.11n је проширење стандарда IEEE802.11-2007 који је издат 2009. године. Предвиђен је рад у оба опсега 2,4 GHz и мање коришћени 5GHz опсег. Планиране су брзине од 600Mb/s и коришћење ортогоналног фреквенцијског мултиплекса (OFDM) и MIMO¹ преноса.

Технологија MIMO користи више антена (просторно распоређених) и мултипутно простирање сигнала учетири одвојена тока података. Користи квадратурну амплитудску модулацију (QAM) са 64 и 256 констелационих тачака. Потканали су ширине 40MHz у односу на садашњих 20MHz (у државама у којима регулаторска тела то дозвољавају).

Пре него што је усвојена завршна верзија стандарда у бежичним мрежама већ су се користили сертификовани производи Wi-Fi Alliance (2007. године) направљени по предлогу стандарда који није био у потпуности усвојен².

13.5 Бежичне персоналне мреже

Под појмом персоналне мреже (PAN³) подразумева се повезивање рачунара, телефона и дигиталних персоналних уређаја (PDA⁴) које користи једна особа (лично). За повезивање ових уређаја могу се користити и радио или инфрацрвени таласи па је онда реч о бежичној персоналној мрежи (WPAN⁵). Велики број технологија и произвођача присутан је на тржишту бежичних персоналних мрежа. У овом поглављу биће анализирани стандарди организација *Bluetooth SIG* и *Zig Bee Alliance*.

¹ Multiple Input - Multiple Output

² Draft

³ Personal Area Network

⁴ Personal Digital Assistant

⁵ Wireless Personal Area Network

13.6 Стандард Bluetooth

Bluetooth¹ је стандард за бежичне везе, који је 1994. године промовисао Ericsson. Првобитно је био намењен за бежично повезивање мобилних телефона и уређаја, као нпр. дигитални персонални уређај (PDA), а тек касније за међусобно повезивање рачунара. Организација произвођача која развија и унапређује ову технологију позната је под називом *Bluetooth SIG*².

13.6.1 Архитектура Bluetooth мрежа

Основна јединица Bluetooth система је пиконет³ мрежа. Пиконет мрежа састоји се од две или више станица (уређаја) које користе исти физички канал, што значи да су синхронизоване на заједнички такт сигнал и да користе исту секвенцу скакања. Заједнички такт пиконета је идентичан такт сигналу главне станице (уређаја⁴). Све остале станице (уређаји) које се синхронизују са главном станицом су пратеће станице (уређаји⁵). Само једна станица може да буде главна, а све остале су пратеће. Комуникација се одвија само између главне и пратећих станица. Директна комуникација између пратећих станица није могућа у оквиру канала пиконета.

На једној локацији може да постоји више независних пиконет мрежа. Свака од тих пиконет мрежа ради на различитим физичким каналима (различита главна станица, независни такт пиконет мреже и секвенца скакања). Bluetooth станица може да буде главна само у једној пиконет мрежи.

Разлог је следећи: пошто је пиконет мрежа дефинисана преко синхронизације са главним Bluetooth тактом није могуће бити главна станица у више од једне пиконет мреже. Bluetooth станица може да буде пратећа станица у више независних пиконет мрежа користећи временски

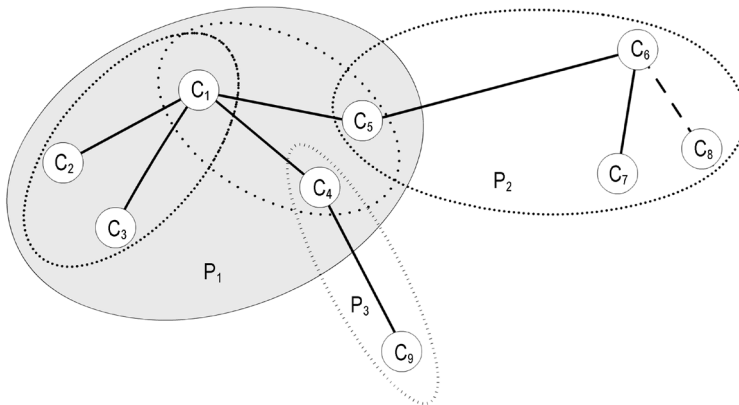
¹ Добила је име по викиншком краљу Харалду II Блатану (*Blatann Harald*), који је у X веку ујединио зараћена викиншка племена. Значење имена Блатан су плави зуби (*Bluetooth*).

² *Special Interest Group - Ericsson, IBM, Nokia, Toshiba и Intel*. Од када је 1998. године ова група издала проглас о званичном почетку развоја ове технологије преко 2000 компанија је потписало споразум који им даје за право да развијају, производе и продају Bluetooth уређаје.

³ *Piconet*

⁴ *Master*

⁵ *Slave*



Слика 13.17 Пример повезивања станица пиконет мрежа

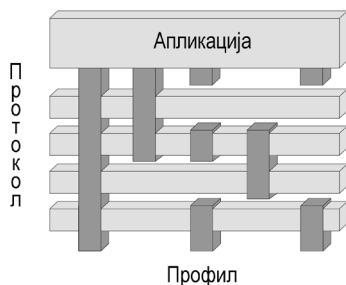
мултиплекс. Bluetooth станица која је члан више пиконет мрежа укључена је у разбацану мрежу¹. Укључење у разбацану мрежу не значи да је омогућено и преусмеравање саобраћаја. Језгро Bluetooth протокола не нуди такву опцију већ се сматра да је то у надлежности протокола виших слојева и ван је Bluetooth спецификације. На слици 13.17 приказан је пример топологије. Станица C_1 је главна станица у пиконету (осенчена област и означена као пиконет мрежа P_1) са станицама C_2 , C_3 , C_4 и C_5 као пратећим станицама. Пиконет мрежа P_1 за рад користи два канала: један за везу са станицама C_2 и C_3 и други за везу са станицама C_4 и C_5 . Приказане су и две друге пиконет мреже: једна са станицом C_6 као главном (означена као пиконет мрежа P_2) и станицама C_5 , C_7 и C_8 као пратећим и друга са станицом P_3 (означена као пиконет мрежа C_4) као главном и станицом C_9 као пратећом.

Поред активних станица (главне и пратеће) Bluetooth дефинише и неактивну станицу². Када пратећа станица нема потребе да ради (учествује у пиконет каналу), а још увек је синхронизована са тим каналом, она улази у неактивно стање. Повремено, када јој главна станица пошаље одговарајући сигнал (фар³) неактивна станица се због

¹ *Scatternet*

² *Parked*

³ *Beacon*



Слика 13.18 Веза апликације, протокола и профила код Bluetooth система синхронизације укључује. Неактивно стање омогућава уштеду напајања (батерије) и могућност да је у пиконет мрежи присутно више од седам пратећих станица.

Начин функционисања пратеће станице веома је једноставан, па су једноставна и ниских цена интегрисана кола које те функције реализују.

13.6.2 Примена Bluetooth мрежа

Да би станица користила Bluetooth мрежу мора бити у стању да интерпретира одређене дефинисане профиле. Профили представљају специфичне апликације од којих свака подржава различит скуп протокола (слика 13.18). У табели 13.5 приказано је 13 профила¹.

Профил за генерички приступ (GAP) у ствари није апликација већ основа на којој су све апликације направљене и од које зависе. Њен основни задатак је да обезбеди процедуре за откривање Bluetooth станица, успостављање и одржавање сигурне везе (канал) између станица.

Поред GAP профила и профили SPP, SDAP и GOEP сматрају се генеричким. Изнад профила за генерички приступ (GAP) налазе се серијски профил (SPP), профил за генеричку размену објеката (GOEP) и профил за синхронизацију (SP). Многи често коришћени профили су: приступ фиксној локалној мрежи (LAP), профил за везу слушалице и базне станице (HSP) и профил за факс (Fax Profile) који су изнад серијског профила (SPP). Навешћемо један пример: ако треба синхронизовати² дигитални лични уређај (PDA) и рачунар да би преко серијског порта

¹ За сада су дефинисана 33 профила.

² Користи се и термин *Bluetooth enabled*.

Ознака профила	Опис
GAP (<i>Generic Access Profile</i>)	Процедуре за надзор везе
SDAP (<i>Service Discovery Application Profile</i>)	Протокол за откривање понуђене услуге
CTP (<i>Cordeless Telephone Profile</i>)	Повезује слушалицу са локалном базном станицом
IP (<i>Intercom Profile</i>)	Дигитални воки-токи
SPP (<i>SerialPortProfile</i>)	Замена за кабл за серијски порт
HSP (<i>Headset Profile</i>)	Омогућава употребу телефона без држања апарата у руци
DUNP (<i>Dial Up Networking Profile</i>)	Омогућава да се преносиви рачунар повезује преко мобилног телефона
<i>Fax Profile</i>	Омогућава да се преносиви факс уређај повезује преко мобилног телефона
LAP (<i>LAN Access Profile</i>)	Протокол између мобилног рачунара и кабловске локалне рачунарске мреже
GOEP (<i>Generic Object Exchange Profile</i>)	Дефинише клијент-сервер релације између објеката у покрету
OPP (<i>Object Push Profile</i>)	Обезбеђује начин за размену једноставних објеката
FTP (<i>File Transfer Profile</i>)	Обезбеђује пренос датотека
SP (<i>Synchronization Profile</i>)	Дозвољава PDA уређају да се синхронизује са другим рачунаром

Табела 13.5 Неки од профила код Bluetooth мрежа

размењивали податке онда оба уређаја морају да подржавају профиле GAP, SPP, GOEP и SP. Остали профили нису потребни.

13.6.3 Скуп протокола код Bluetooth система

Језгро Bluetooth система обухвата четири најнижа слоја и одговарајуће протоколе који су део Bluetooth спецификације, као и заједнички протокол за откривање услуга (SDP¹) и свеобухватни генерички профил приступа (GAP²). Комплетна Bluetooth апликација захтева додатне услуге и протоколе виших слојева који су дефинисани али превазилазе обим овог уџбеника.

¹ *Service Discovery Protocol*

² *Generic Access Profile*

Детаљнија архитектура језгра Bluetooth система представљена је на слици 13.19. Најнижа три слоја груписана су у подсистем који се среће под називом Bluetooth контролер. Остатак система укључујући услугу L2CAP¹ и више слојеве означава се као Bluetooth хост.

Станице комуницирају користећи протоколе дефинисане Bluetooth спецификацијом. Језгро протокола чини: језгро система које нуди услуге преко бројних тачака приступа (SAP²). Услуге могу бити разврстане у две групе: управљачке, које се означавају као C³ раван, и корисничке које се означавају као U⁴ раван. Прва група води рачуна о успостављању и раскидању канала и веза, а друга о подацима који се том везом размењују.

Интерфејс услуга ка подсистему контролера дефинисана је на такав начин да се Bluetooth контролер може сматрати стандардним делом. У оваквој конфигурацији контролер ради на најнижа три слоја, а L2CAP слој садржи остатак апликације хост система. Стандардни интерфејс назива се интерфејс станица - контролер (HCI⁵). Његове приступне тачке означене су на горњој ивици контролера подсистема. Имплементација ових стандардних интерфејса ка услугама је опциона.

Слој основног опсега (BAB⁶) на неки начин је сличан MAC подслоју, али садржи и елементе физичког слоја. Води рачуна о томе како главна станица управља временским целинама и како су оне груписане у рамове.

Слој L2CAP може опционо да обезбеди додатну детекцију грешке и поновљено слање јединица протокола (L2CAP PDU⁷). Ова опција препоручује се апликацијама које у корисничким подацима захтевају малу вероватноћу неоткривених грешака. Следећа опција слоја L2CAP је контрола тока применом механизма клизајућег прозора⁸.

У тексту који следи биће укратко објашњена функција сваког од модула са слике:

¹ Logical Link Control and Adaptation Layer Protocol

² Service Access Point

³ Control

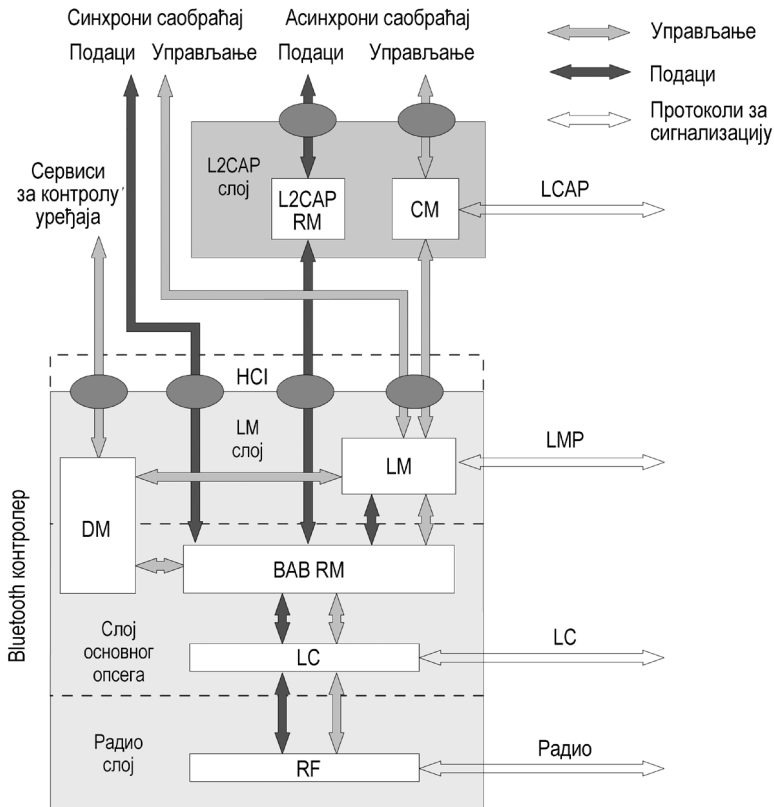
⁴ User

⁵ Host to Controller Interface

⁶ Baseband Layer

⁷ Protocol Data Unit - 1. поглавље овог уџбеника.

⁸ Детаљније у 5.4 одељку овог уџбеника.



Слика 13.19 Архитектура језгра Bluetooth система

- Модул за надзор канала (CM¹) задужен је за успостављање, управљање и раскидање L2CAP канала укључујући управљање напајањем, проверу идентитета и квалитет услуге. Протокол између парњак целина је L2CAP;
- Модул за управљање ресурсима (L2CAP_RM²) води рачуна о редоследу пријема сегмената. Такође води рачуна и о томе да ли апликације примају податке у складу са договореним квалитетом услуга QoS;

¹ Channel Manager

² L2CAP Resource Manager

- Модул за надзор станице (DM¹) управља општим радом Bluetooth станице. Задужен је за све операције које нису директно везане за пренос података као што су испитивање присуства суседних станица, повезивање са тим станицама итд.;
- Модул за надзор везе (LM²) задужен је за успостављање, модификовање, раскидање логичке везе и иновирање параметара везаних за физичку везу између уређаја. За комуникацију са модулом за управљање везом и удаљеном станицом користи се протокол за управљање везом (LMP³);
- Модул за управљање везом (LC⁴) задужен је за кодирање и декодирање Bluetooth корисних података као и параметара везаних за физички канал;
- Модул за управљање ресурсима основног опсега (BAB_RM⁵) одговоран је за приступ медијуму;
- Радио - модул (RF) задужен је за предају и пријем рамова на физичком каналу.

Радио-слој Bluetooth система

Радио-слој преноси битове од главне станице до пратеће и обрнуто. Систем ради у 2,4GHz фреквенцијском опсегу (ISM) као и IEEE802.11 (Wi-Fi) системи тако да се међусобно преклапају. Фреквенцијски опсег је подељен на 79 канала ширине 1MHz, а модулација је GFSK⁶ (верзија 1.2). Користи се фреквенцијско скакање са 1600 скокова у секунди. Време између два скока је 625µs.

Домет Bluetooth везе је 1m са предајником снаге 0dBm, 10m са предајником снаге 4dBm и 100m са предајником снаге 20dBm. Мору се достићи брзине од 1Mb/s (верзија 1.2), 3Mb/s (верзија 2.1+EDR⁷) и 24Mb/s (верзија 3.0+HS⁸).

¹ Device Manager

² Link Manager

³ Link Management Protocol

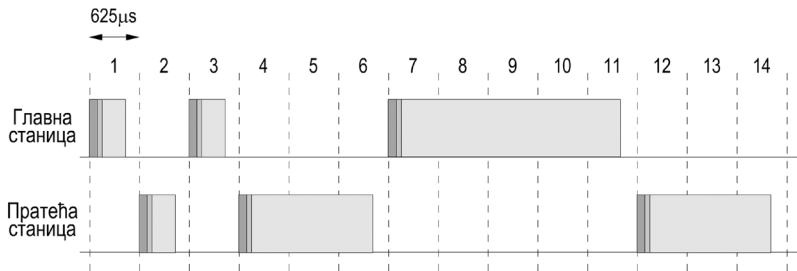
⁴ Link Contoller

⁵ Baseband Resource Manager

⁶ Gaussian Frequency Shift Keying

⁷ Enhanced Data Rate

⁸ High Speed



Слика 13.20 Размена пакета између главне и пратеће станице

Слој основног опсега Bluetooth система

Овај слој претвара ток битова у рамове и дефинише формате од значаја. У најједноставнијем облику главна станица у свакој пиконет мрежи дефинише серију временских целина величине 625μs. Главна станица шаље у непарним временским целинама, а пратећа станица у парним. Ово је традиционалан временски мултиплекс у коме је главној станици додељена половина временских целина а пратеће станице деле другу половину.

Рамови могу бити дугачки 1, 3 и 5 временских целина (слика 13.20).

Сваки од рамова шаље се преко логичког канала - везе¹. Постоје две врсте везе:

- асинхрона без успоставе везе (ACL²), и
- синхрона са успоставом везе (SCO³).

Код ACL врсте користи се пакетска комутација и примењује се на податке који пристижу у неравномерним временским интервалима. Подаци пристижу са L2CAP слоја на предајној страни и предају се L2CAP слоју на пријемној страни. Саобраћај се испоручује на најбољи могући⁴ начин али не постоји гаранција да су подаци успешно стигли на одредиште. Пратећа станица може са главном станицом да успостави само једну ACL везу.

¹ Лунк

² Asynchronous ConnectionLess

³ Synchronous Connection Oriented

⁴ Best effort - термин који се користи код система без успоставе везе као што су Интернет слој, Етернет и сл.

Друга врста - SCO везе користи се за апликације у реалном времену, као што су телефонске везе. За овакав тип канала додељују се тачно одређене временске целине у оба правца. Због природе апликација у реалном времену - критична су временска кашњења - не користе се поновна слања већ механизам за корекцију грешака (FEC¹). Пратећа станица може да има до три SCO везе са главном станицом. Свака SCO веза може да пошаље 64000b/s кодирани PCM аудио сигнал.

Слој L2CAP

Слој L2CAP има три важне функције:

- Прво, прима пакете до величине од 64kB од виших слојева и дели их на рамове погодне за пренос. На одредишту рамови се поново повезују у пакете;
- Друго, води рачуна о мултиплексирању и демултиплексирању пакета из различитих извора. Када се пакети поново повезују L2CAP указује коме од виших слојева су упућени;
- Треће, L2CAP руководи захтевима за квалитет услуге и у фази успоставе везе и за време нормалног тока података. Такође води рачуна и о усаглашавању величине пакета између станица. Ово је важно пошто нису све станице у могућности да раде са пакетима величине 64kB.

13.6.4 Структура рама у Bluetooth системима

Постоји неколико формата рамова. Један од њих приказан је на слици 13.21 и чине га:

- приступни код који идентификује главну станицу тако да пратеће станице које
- се налазе у радио-опсегу две главне станице могу да одреде који од саобраћаја је за њих,
- заглавље дужине 54 бита које садржи поља типична за MAC подслој,
- поље корисничких података величине до 2744 бита. Ова величина одговара трајању пет временских целина.

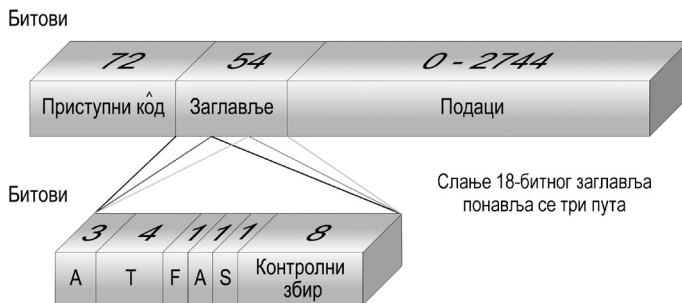
Заглавља сачињавају следећа поља:

¹ Forward Error Correction

- поље адресе A (дужине 3 бита) - указује којој од осам активних станица је рам упућен;
- поље типа T (дужине 4 бита) - указује на врсту рама (ACL, SCO...), врсту корекције грешке која се користи и на то колико временских целина је рам дугачак;
- поље тока F¹ (дужине 1 бит) - поставља пратећа станица када је њен меморијски простор попуњен и не може да прими више података;
- поље потврде A (дужине 1 бит) - користи се да се пошаље потврда преко рама података²;
- поље секвенце S³ (дужине 1 бит) - користи се за обележавање рамова. Пошто се користи протокол заустави се и чекај⁴ довољан је један бит;
- поље контролног збира⁵ (дужине 8 битова) - користи се за детекцију грешке.

Дужина заглавља од 54 бита постиже се троструким слањем 18-битне целине која се састоји од претходно описаних поља. Вишеструким слањем повећава се поузданост преноса у радио-медијуму.

Код ACL веза за поље података користе се различити формати. Формати рамова у SCO везама су једноставнији: поље података је увек



Слика 13.21 Карактеристичан рам података у Bluetooth системима

¹ Flow control

² Piggy back

³ Sequence

⁴ Stop and wait – детаљније се може наћи у 11. поглављу уџбеника [1].

⁵ CRC

дужине 240 битова. Постоје три верзије: 80,160 и 240 стварне дужине података. Остатак се користи за корекцију грешке. У најпоузданијој верзији (80 битова података) садржај се три пута шаље.

Пратећа станица може да користи само непарне временске целине, тј. 800 временских целина у секунди. Са 80-битним подацима капацитет канала пратеће и главне станице је по 64000b/s што одговара капацитету PCM¹ говорног канала. То и јесте био разлог да се одабере брзина скакања од 1600. Уколико се користи мање поуздана варијанта (без редундансе) могуће је реализовати истовремено три говорне везе што и представља максимум за SCO пратеће станице.

13.6.5 Унапређења новијих верзија Bluetooth стандарда

Верзија² 2.1+EDR, објављена 2007. године, компатибилна је са ранијим верзијама. Главна карактеристика је сигурно и једноставно упаривање (SSP³). Побољшања су везана и за размену додатних информација (EIR⁴) које се размењују у току успостављања веза са другим уређајима што доприноси бољем филтрирању уређаја са којим се повезује. Такође укључене су опције које смањују потрошњу у режиму мале енергетске потрошње. Брзина је 3Mb/s, домет 10m. Користи модулације DQPSK и 8DPSK.

Верзија⁵ 3.0+HS објављена је у априлу 2009. године. Подржава брзину преноса до 24Mb/s. У току успоставе везе и договора око параметара везе користи се Bluetooth веза (линк). Пренос података се реализује кроз IEEE802.11 линк. Нова, битна одлика је додатни MAC и физички слој (AMP⁶) реализован по стандарду IEEE802.11 који се користи за брзи пренос података⁷. Користи се Bluetooth радио-пренос у фази откривања уређаја, иницијализовања везе и конфигурисања профила. Али када треба пренети већу количину података биће употребљен

¹ Pulse Code Modulation - импулсна кодна модулација, детаљније објашњење може се наћи у 7. и 8. поглављу литературе [1].

² Bluetooth Core Specification Version 2.1 + EDR (Enhanced Data Rate)

³ Secure Simple Pairing

⁴ Extended inquiry response

⁵ Bluetooth Core Specification Version 3.0 + HS (High Speed)

⁶ Alternate MAC/PHY

⁷ Две технологије су биле предвиђене за AMP: 802.11 и UWB, али је UWB изостављена из спецификације.

други физички слој MAC/PHY по стандарду IEEE802.11. Када је систем неактиван користи се начин рада Bluetooth уређаја са малом потрошњом (потврђено у дугогодишњој примени). Домет је 10m.

Верзија¹ 4.0 објављена је у децембру 2009. године. Основно обележје ове верзије је изузетно мала потрошња уређаја малих димензија који користе батерије величине кованог новца². Сматра се да се на тај начин проширује тржиште на здравство, спорт, рекреацију. Као побољшање основне спецификације јесте могућност да се одаберу два режима: са два скупа протокола и са једним скупом протокола. У режиму рада са два скупа протокола особеност са малом потрошњом је интегрисана у стандардни Bluetooth контролер³. Резултујућа архитектура слична је стандардној архитектури (описаној у претходним одељцима) а резултује малим финансијским улагањима да би се добио нови систем. Произвођачи могу да користе интегрисана кола са постојећим верзијама (Bluetooth v2.1 + EDR или Bluetooth v3.0 + HS) и да додају нови скуп протокола који обезбеђује малу потрошњу.

13.7 Стандарди за персоналне мреже IEEE организације

Организација IEEE формирала је радне групе које се баве бежичним персоналним мрежама. Прва радна група радила је на прилагођавању стандарда Bluetooth SIG и издала 2002. године стандард IEEE802.15.1 (усаглашен са Bluetooth v1.1) који се односи само на физички слој и слој везе (слика 13.22). Иновирана верзија овог стандарда заснована на побољшањима која су укључена у верзију Bluetooth v1.2 издата⁴ је као стандард IEEE802.15.1-2005.

Као што смо видели у претходним поглављима Bluetooth⁵ спецификација обухвата цео систем, од физичког слоја до апликационог (слика 13.18). Без обзира што ове верзије нису идентичне оне конвергирају ка истом стандарду. Стандард IEEE802.15 односи се на

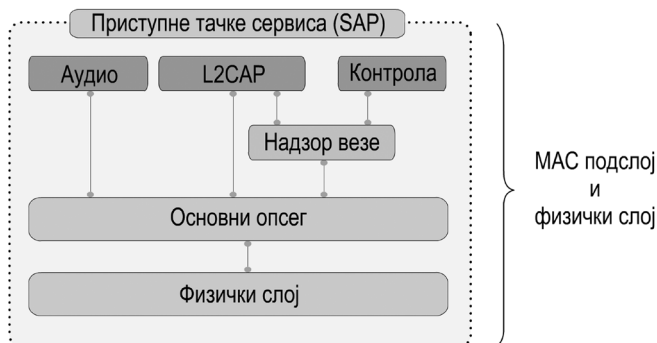
¹ *Bluetooth Core Specification Version 4.0*

² *Coin-cell batteries*

³ *Classic Bluetooth controller*

⁴ По доношењу овог документа радна група задужена за овај стандард донела је одлуку да нове верзије Bluetooth неће бити укључене у IEEE стандарде.

⁵ По верзији 1.1.



Слика 13.22 Стандард IEEE802.15.1

бежичну комуникацију уређаја малих димензија на релативно кратким растојањима као што су PDA, преносиви рачунари, мобилни телефони, MP3 уређаји...

Рад друге групе (IEEE802.15.2) односи се на могућност истовременог рада бежичних личних мрежа по стандардима серије IEEE802.15 и бежичних локалних рачунарских мрежа по стандардима серије IEEE802.11.

Генерално, пошто и бежичне персоналне мреже и бежичне локалне рачунарске мреже користе ISM фреквенцијски опсег 2,4GHz може да дође до интерференције у раду уређаја ових мрежа. Да би се разрешио овај проблем радна група је предложила механизам за истовремени рад¹.

Трећа радна група ради на стандарду IEEE802.15.3 за рад персоналних уређаја на релативно великим брзинама (већим од 20Mb/s) као и на дефинисању нових карактеристика као што су мала потрошња и квалитет услуга који одговара мултимедијалним апликацијама.

Постоји више радних група: IEEE802.15.3а бави се преносом у изузетно широком опсегу спектра (UWB²): опсег од 3,1GHz до 10,6GHz, ширине 500MHz, брзине до 480Mb/s. Стандард IEEE802.15.3b-2006 бави се применом и међусобним радом³ MAC подслоја. Стандард IEEE802.15.3c-2009 односи се на физичку спецификацију преноса са

¹ Coexistence Mechanism

² Multi-Band OFDM (MB-OFDM) подржава WiMedia Alliance, Direct Sequence - Ultra Wide Band подржава UWB Forum

³ Interoperability

милиметарским таласима (mmWaveWPAN). Користи се опсег од 57GHz до 64GHz а брзине преко 2Gb/s. Предвиђен је за брз приступ Интернету, скидање видео садржаја (стриминг¹) као што је видео по захтеву², телевизија високе резолуције (HDTV³), кућни биоскоп, итд.

Четврта радна група издала је стандард IEEE802.15.4-2006 за релативно мале брзине (LR-WPAN⁴), мање од 250kb/s. Стандардом су специфицирани физички слој и MAC подслој. У ову категорију спадају спецификације ZigBee, WirelessHART⁵ и MiWi⁶. Минимизирањем потрошње батерије у овим уређајима могу дуго да трају. Овај стандард развијен је за мреже са сензорима, за даљинско управљање и аутоматизацију у домаћинствима итд.

ZigBee Alliance има исту улогу у односу на стандард IEEE802.15.4 као Wi-Fi Alliance у односу на стандард IEEE802.11. У одељку који следи детаљније ће бити описана ZigBee технологија.

13.8 Сензорске мреже

Бежичне сензорске мреже (WSN⁷) састоје се од просторно дистрибуираних аутономних сензора који имају заједнички задатак да надгледају физичке услове или услове животне средине као што су температура, звук, вибрације, притисак, кретања или загађиваче. Мотив за развој сензорских мрежа везан је за војне пројекте у надзору бојних поља. Данас се користе у различитим индустријским и цивилним апликацијама као што су надгледање и управљање индустријских процеса, надгледање здравственог стања пацијената, надгледање животне средине, аутоматизација у домаћинствима и управљање саобраћајем.

Поред једног или више сензора, сваки чвор у бежичним сензорским мрежама обично има и радио-примопредајник, микроконтролер и извор

¹ Streaming

² Video on Demand

³ High Definition Television

⁴ Low Rate WPAN

⁵ WirelessHART је отворени стандард за технологију коју је развила HART Communication Foundation.

⁶ Произвођачка (proprietary) спецификација за бежични протокол коју је развила компанија Microchip Technology

⁷ Wireless Sensor Network

енергије. Сензор може да варира по величини: од величине кутије за ципеле до величине зрна прашине. Сензорска мрежа уобичајено формира бежичну *ad hoc* мрежу. Неколико стандарда везаних за бежичне сензорске мреже је за сада или усвојено или је у фази развоја. Поред ових постоје и бројне нестандартне произвођачке спецификације. Навешћемо неке од њих: 6LoWPAN¹, ISA100², WirelessHART и MiWi.

За сензорске мрежне апликације кључни захтеви у пројектовању крећу се око ограниченог трајања батерија, ниских цена, малих растојања између уређаја и концепта међусобно увезаних мрежа³ и комуникациона подршка за велики број међусобно повезаних уређаја у мултиапликационом окружењу. Ово су биле основе за IEEE 802.15.4 и ZigBee спецификације да обезбеде основ за релативно једноставну, прилагодљиву, великог обима бежичну мрежу са више скокова⁴ уз могућност да подржи велики број различитих апликација.

13.8.1 Концепција сертификавања Zig Bee производа

ZigBee Alliance је удружење састављено од великог броја компанија (чији се број стално повећава) које раде заједно на развоју јефтиних, поузданих, са малом потрошњом бежичних мрежа и врше контролу производа насталих на глобалном отвореном стандарду. Да би производ носио логотип ZigBee Alliance, прво мора успешно да прође ZigBee програм сертификације.

Постоје два програма за сертификацију производа (слика 13.23). Први је ZigBee усаглашена платформа (ZCP⁵) и односи се на модуле, или платформе које су намењене, као градивни блокови, за крајњи производ. ZigBee сертификовани производи односе се на крајње производе који су изграђени на ZigBee усаглашеној платформи.

Производи који користе јавне апликационе профиле⁶ тестирани су да

¹ Акроним за *IPv6 over Low power Wireless Personal Area Networks* на коме ради радна група у оквиру IETF (*Internet Engineering Task Force*).

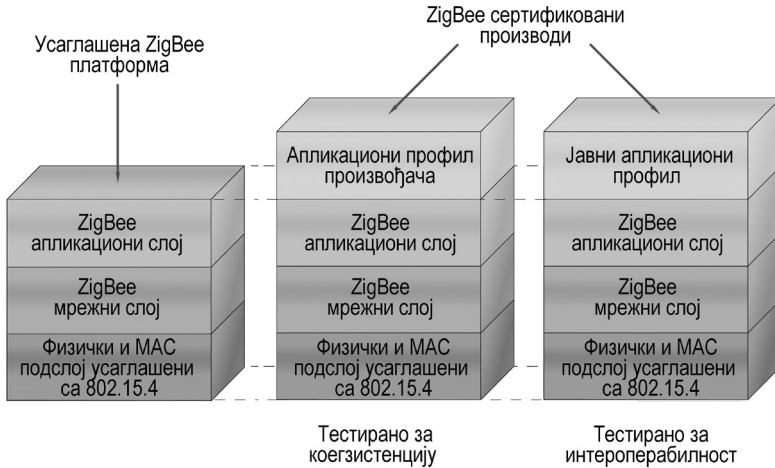
² Стандарде за бежично умрежавање намењено аутоматизацији у индустрији које развија организација ISA (*International Society of Automation*).

³ *Mesh*

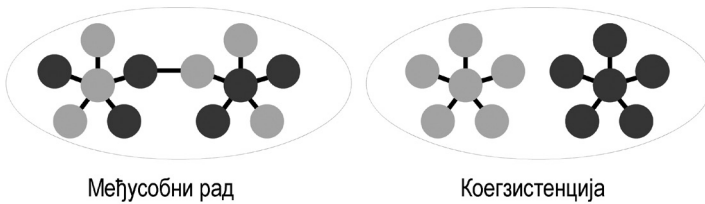
⁴ *Multi-hop*

⁵ *ZigBee Compliant Platform*

⁶ *Public application profiles*



Слика 13.23 Концепт сертификавања ZigBee производа



Слика 13.24 Међусобни рад и коегзистенција

би се обезбедио међусобни рад (интероперабилност) са другим ZigBee крајњим производима. Производи који користе од стране произвођача одређене профиле¹, који ће радити као затворени системи², тестирани су да би се обезбедио истовремени рад (коегзистенција) са другим ZigBee системима (слика 13.24).

13.8.2 Архитектура Zigbee протокола

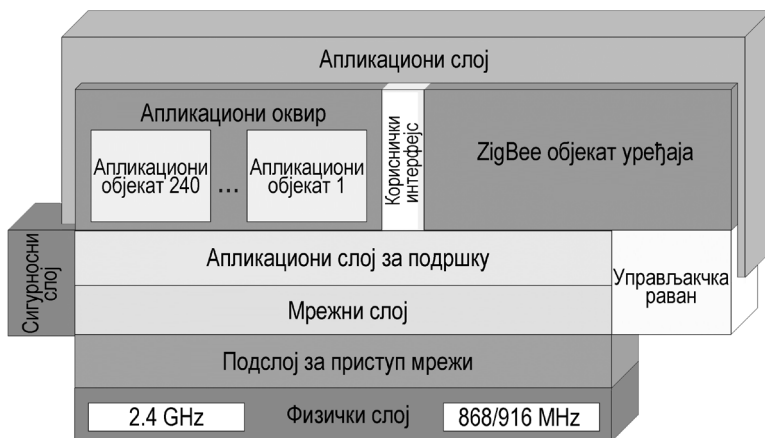
ZigBee спецификацијом дефинисани су слојеви архитектуре протокола изнад физичког слоја и MAC подслоја (слика 13.25).

Апликациони слој (APL³) представља највиши слој ZigBee скупа протокола. Састоји се од:

¹ *Manufacturer-specific profiles*

² *Embedded*

³ *Application*



Слика 13.25 ZigBee скуп протокола

- апликационог оквира (AF¹) чија је основна функција да обезбеди опис како да се направи профил ZigBee скупу протокола (како би се осигурало да профили могу бити генерисани на конзистентан начин);
- ZigBee објекта уређаја (ZDO²) који дефинише улогу уређаја у оквиру мреже, иницира и/или одговара на захтеве повезивања или откривања путање (руте) и успоставља сигурне релација између мрежних уређаја;
- апликационог подслоја за подршку (APS³) који нуди сличну подршку апликационим услугама као што то чини TCP протокол у TCP/IP мрежама. Разлика ипак постоји: овај подслој не обезбеђује контролу тока који нуди TCP протокол;
- апликационог објекта (APS⁴) који представља софтвер крајњих тачака које контролишу рад уређаја.

ZDO управљачка раван (MN⁵) омогућава комуникацију између апликационог и мрежног слоја са ZigBee објектима уређаја (ZDO).

¹ Application Framework

² ZigBee Device Object

³ Application Support Sublayer

⁴ Application Support Object

⁵ Management Plane

Сигурносни слој (SSP¹) обезбеђује сигурносне механизме за слојеве који користе шифровање (мрежни и апликациони).

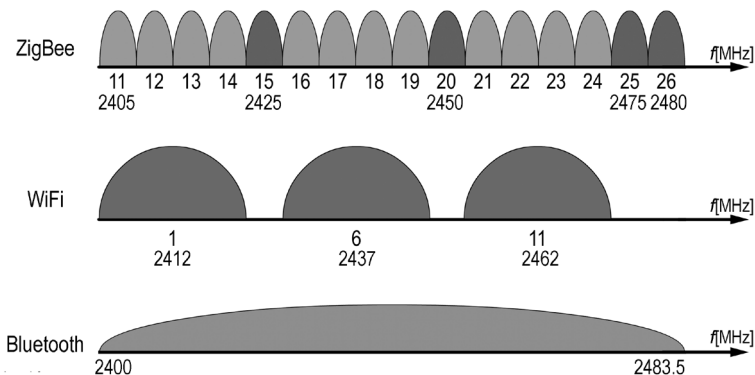
Мрежни слој (NWK²) води рачуна о мрежним адресама и рутирању. Задаци овог слоја су и покретање мрежног координатора, придруживање мрежних адреса, додавање и уклањање мрежних уређаја, откривање руте, прослеђивање рутирајућих порука и примена сигурносних мера.

IEEE802.15.4 MAC подслој одговоран је за пружање поуздане комуникације између уређаја и његовог непосредног суседа, имплементацијом CSMA/CA протокола. MAC подслој је такође одговоран за састављање и декомпоновање рамова података.

IEEE802.15.4 физички слој обезбеђује интерфејс за приступ физичком преносном медијуму.

Физички слој се састоји од два слоја која раде у два одвојена фреквенцијска опсега. Нижа учестаност физичког слоја покрива два опсега: 868MHz (Европа) и 915MHz (САД и Аустралија). Виши опсег учестаности (2,4GHz) користи се у готово целом свету. Радио фреквенцијски спектар и доступни канали за ZigBee (IEEE802.15.4) и Wi-Fi (IEEE802.11b/g/n) се преклапају. Канали су обележени (слика 13.26) тако да:

- канал 0 припада опсегу 868MHz,
- канали 1-10 припадају опсегу 915MHz а
- канали 11-26 припадају опсегу 2,4GHz.



Слика 13.26 Фреквенцијски спектар и канали: ZigBee, WiFi и Bluetooth

¹ Security Service Provider

² Network layer

Избором канала могу се избећи сметње за оне који користе слободни простор између два суседна IEEE802.11 канала плус канали 25 и 26.

Канали 1, 6 и 11 обично се користе код WiFi мрежа у САД. Друге земље препоручују друге канале. У том случају је за све ZigBee производе најбоље користити канале који се најмање преклапају са наведеним. Са слике 13.26 види се да су то канали 15, 20, 25. и 26. Користе се следеће модулације: проширивање спекта директном секвенцом (DSSS¹), квадратурна фазна модулација (QPSK²) и амплитудска модулација (ASK³).

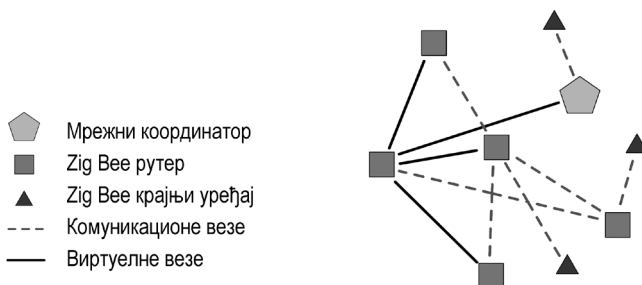
13.8.3 Врсте ZigBee уређаја

У ZigBee мрежи дефинисане су три врсте уређаја: координатор, рутер и крајњи уређај (слика 13.27).

Координатор је уређај који покреће и контролише мрежу. Координатор складишти информације о мрежи, које омогућују да делује као центар од поверења⁴ и као складиште за сигурносне кључеве.

Рутери проширују област покривања мреже, омогућују динамичке руте око препрека, као и резервне руте у случају загушења мреже или отказу уређаја. Они се могу повезати са координатором и другим рутерима, као и обезбедити подршку уређајима за које су задужени.

Крајњи уређаји могу да преносе или примају поруке, али не могу да обављају функције рутирања. Они морају бити повезани на координатор или рутер, а не могу пружити подршку уређају детету.



Слика 13.27 Врсте ZigBee уређаја и врсте њихових међусобних веза

¹ Direct Sequence Spread Spectrum

² Quadrature Phase Shift Keying

³ Amplitude Shift Keying

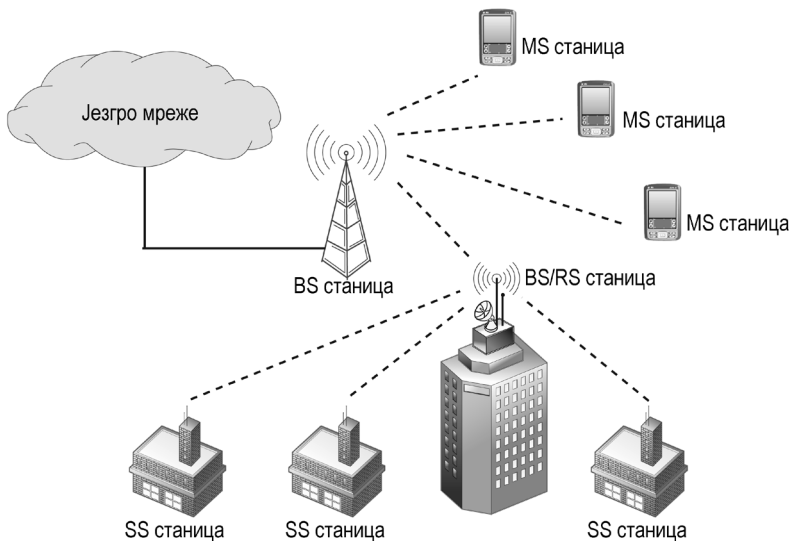
⁴ Trust Center

13.9 Бежичне мреже градског подручја

У овом одељку биће описане основе мрежне топологије бежичних мрежа градског подручја, архитектура протокола стандарда IEEE 802.16, као и разлике (где постоје) између различитих верзија стандарда.

13.9.1 Преглед IEEE 802.16 стандарда и начина повезивања

Архитектура мрежа реализованих по IEEE 802.16x стандарду (означавају се и као WiMAX мрежна топологија) је ћелијска. Мрежа је предвиђена да обезбеди приступ у великим градским или руралним областима. Као што је приказано на слици 13.28. WiMAX мрежна топологија састоји се од једне или више базних станица (BS¹ станица) скупа мобилних станица (MS² станица) и/или претплатничких станица (SS³ станица). У зависности од верзије стандарда IEEE 802.16 и учестаности које се користе станица корисника може али не мора да буде



Слика 13.28 Архитектура мреже реализоване по IEEE 802.16x (WiMAX мрежна топологија)

¹ Base Station

² Mobile Stations

³ Subscriber Stations

у линији видљивости (LoS¹) базне станице. Да би се мрежа проширила и повезала на преносни систем² користе се станице обнављивачи (RS³ станице).

Спецификација IEEE802.16 је еволуирала у протеклом периоду. Првобитна спецификација је прихваћена 2001. године као бежични стандард за мреже градског подручја (MAN⁴ стандард). Развијен је са намером да обезбеди велику брзину података и тачка-тачка комуникацију (PTP⁵) између фиксираних станица корисника. Стандард је предвидео коришћење лиценцираног опсега 10GHz до 66GHz, тако да је интерференција смањена. Пошто се користе радио-сигнали мале таласне дужине захтева се линија видљивости између станица. Уобичајена област примене је повезивање фиксираних тачака преносног система до локација које су повезане на жичну мрежу. Користе се усмерене антене на оба краја везе. Подржано је фреквенцијско дуплирање (FDD⁶) и временско дуплирање (TDD⁷).

Објављена су два проширења (амандмана⁸) стандарда. Прво је децембра 2002. год. усвојено проширење IEEE802.16с. У овој верзији стандарда додати су детаљни профили система или типична примена за опсег 10-66GHz и исправљене грешке претходне верзије стандарда. Друго проширење стандарда је IEEE802.16а. Оно је проширило употребу WiMAX система и на лиценцирани опсег учестаности испод 11GHz.

Уобичајено фреквенцијски опсег 2-11GHz садржи лиценциране и нелиценциране учестаности. Одговарајуће таласне дужине омогућавају сигнаlima да заобилазе препреке. Дозвољено је вишелинијско простирање и простирање ван линије видљивости (NLOS⁹). Поред подршке за тачка-тачка (PTP) пренос додата су два режима рада тј.

¹ Line-of-Sight

² Backhaul

³ Repeater Station

⁴ Metropolitan Area Network

⁵ Point To Point

⁶ Frequency Division Duplexing

⁷ Time Division Duplexing

⁸ Amendment/s

⁹ Non- Line-of-Sight

начина повезивања станица. Први је тачка-више тачака (P2MP¹) где скуп корисничких станица (SS станица) може да се повеже на једну базну станицу (BS станица). У другом начину - међусобно повезаних станица² корисничка станица не мора да буде повезана само на базну станицу већ може да шаље и суседној корисничкој станици. На тај начин се проширује област покривања мреже и умањује могућност отказа. Интернет посредницима погодује IEEE802.16а технологија пошто омогућава повезивање руралних области нарочито уколико жична инфраструктура не обезбеђује одговарајућу брзину приступа Интернету. Спецификација захтева коришћење омнидирекционих антена и динамичко бирање учестаности (DFS³). Ова техника дозвољава да се интерференција спречи динамичким пребацивањем на другу радио-учестаност (RF⁴) а на основу мерења неких параметара нпр. односа сигнала и шума. Ширина радио-канала који се користи је од 1,25MHz до 28MHz. Мреже реализоване по стандарду IEEE802.16а, које користе ортогонални фреквенцијски мултиплекс (OFDM⁵), омогућавају пренос података брзином до 75Mb/s. Величина ћелије може да буде и пречнику до 50km али је уобичајена величина 5km до 10km.

Стандарде који носи ознаку IEEE802.16-2004 замена је и унапређење проширења стандарда IEEE802.16, IEEE802.16а, IEEE802.16с и IEEE802.16d. Проширење стандарда IEEE802.16d, које се сматра првом верзијом WiMAX стандарда и основом за WiMAX компатибилност, довело је до употребе WiMAX система у фиксним мрежама. У овој верзији стандарда уведен је нов лиценцирани опсег учестаности. Користе се два опсега учестаности: 2GHz-11GHz и 10GHz-66GHz. Фреквенцијски опсег канала је променљив и креће се од 1,25MHz до 28MHz. Брзина преноса података је 75Mb/s ако се користи канал ширине 20MHz. Спецификација IEEE802.16-2004 предвиђа коришћење секторских омнидирекционих антена као замену за омнидирекционе антене. Уведен је двоструки механизам за аутентификацију између базе и корисничке станице.

¹ Point to Multi-Point

² Mesh

³ Dynamic Frequency Selection

⁴ Radio Frequency

⁵ Orthogonal Frequency Division Multiplexing

Све претходно описане верзије IEEE802.16 стандарда подразумевале су само рад са непокретним (стационарним) станицама и нису узимале у обзир механизме и функционалност која се захтева код покретних (мобилних) система. У ствари није подржан хендовер начин рада а модулационе шеме нису пројектоване тако да се „носе“ са мобилним окружењем и са променљивим карактеристикама канала. Најбитније проширење (амандман) WiMAX системима јесте подршка за мобилност корисника при брзини возила од 120 km/h. Основе овог система описане су стандарду IEEE802.16е који се среће и под ознаком IEEE802.16-2005. Стандард предвиђа: рад у фреквенцијском опсегу од 2GHz до 6GHz, примену протокола који дозвољавају мобилност у мрежи, и хендовер механизам подржан аутентификацијом. Са становишта сигурности подржана је сигурна размена кључева за време аутентификације и шифровања података коришћењем DES¹ или AES² алгоритама.

Да би се поправила рањивост мрежа по стандарду IEEE802.16-2004 уведени су нови механизми сигурности. Спецификација IEEE802.16е предвиђа неколико побољшања на физичком и MAC слоју, подржава ширину канала од 1.25MHz до 20MHz и обезбеђује брзине (нпр. <15Mb/s за канал од 5MHz) за мобилне и роминг³ кориснике. У поређењу са IEEE802.16d број корисника које мрежа може да подржи је повећан а и квалитет услуге је побољшан. Пречник ћелије је у опсегу од 2km до 5km. Стандард IEEE 802.16е омогућава приступ широкопојасном Интернету за преносиве уређаје са интегрисаним WiMAX адаптерима. Код мобилних WiMAX система неколико додатних мрежних механизма је подржано као што су: међусобна аутентификација између мобилног корисника и мрежа, трансфер квалитета услуга и сигурносних механизма за време хендовера.

Покренуто је неколико додатних стандардизационих пројеката: IEEE802.16f/1 за подршку мобилним MIB⁴ базама података, стандарди IEEE802.16j и IEEE802.16m за нови интерфејс. Детаљније о свим пројектима може се наћи у табели 13.4 која се налази на крају овог

¹ Data Encryption Standard

² Advanced Encryption Standard

³ Roaming

⁴ Management Information Base

поглавља.

13.10 Концепција WiMAX мрежа

Услуге које пружа WiMAX мрежа су различите. Мрежа може да подржи стационарне и мобилне кориснике у градским подручјима. Саобраћај може да буде уобичајено претраживање Интернета или саобраћај у реалном времену који захтева строга ограничења у квалитету услуга (QoS). Компоненте WiMAX мреже треба да са сигурношћу све захтеве испуне. Да би се достигао тај циљ захтева се имплементација и координација свих делова скупа протокола са циљем да се обезбеде сигурност, успостављање везе, брзи хендовер и одговарајући нивои квалитета.

Скуп IEEE802.16 стандарда усмерен је на радио и MAC слој и ни на који начин не указује како се управља вишим слојевима. Као што је познато WiMAX мрежа се може састојати од већег броја различитих елемената: мобилних станица, базних станица, међумрежних пролаза, сервера за аутентификацију који су потребни у мрежама са више корисника, више терминала и чак и више оператора.

У циљу дефинисања организације мреже где је обезбеђен међусобни рад свих компонената WiMAX Forum¹ је објавио скуп докумената који специфицирају мрежне елементе, организацију и конфигурацију која се мора применити у WiMAX мрежи².

13.10.1 Референтни модел WiMAX мреже

У циљу разумевања међусобних веза мрежних компоненти анализираћемо логичку презентацију WiMAX мреже. Ову шему објавио је WiMAX Forum и означена је као мрежни референтни модел (NRM³). На шеми (слика 13.29) могу се уочити логички домени⁴, функционалне целине⁵ и референтне тачке (RP⁶). Циљ је дозволити различита решења

¹ Може се наћи на адреси [20].

² Може се наћи у документима [21] и [22].

³ *Network Reference Model*

⁴ *Logical domains*

⁵ *Functional entities*

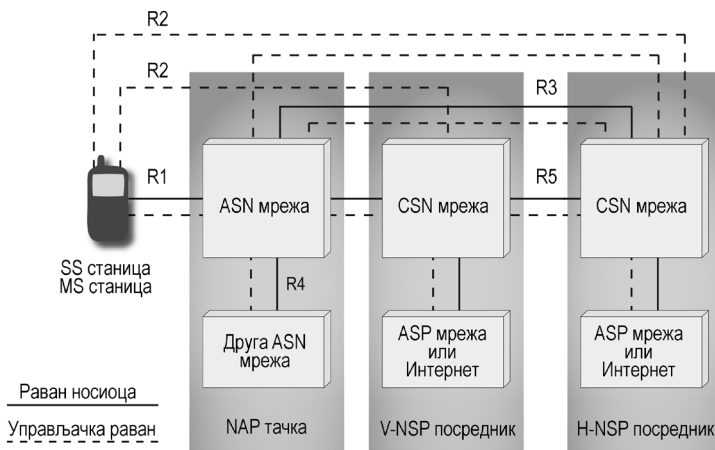
⁶ *Reference Points*

и истовремено одржавати свеобухватну интероперабилност између различитих реализација функционалних целина. Због тога никакве претпоставке нису направљене у имплементацији функционалних целина. За неке од њих одреднице су обезбеђене преко тзв. профила. У поглављу које следи биће описане релевантне компоненте мрежног референтног модела.

13.10.2 Функционалне целине

Главне функционалне целине скициране на слици 13.29 су:

- Мобилна станица (MS¹ станица). Мобилна станица је уређај који користи претплатник да би приступио WiMAX мрежи. Исти уређај може да користи један или више корисника и исти корисник може да приступи мрежи користећи више од једне мобилне станице.
- Мрежа за приступ услузи (ASN² мрежа). Представља границу функционалне интероперабилности WiMAX клијента са WiMAX услугом повезивања³. Она је највише одговорна за вођење

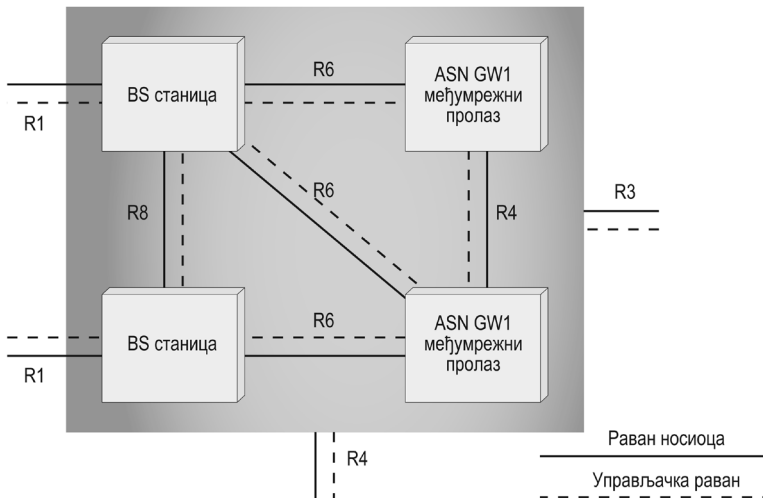


Слика 13.29 WiMAX референтни модел⁶

¹ Mobile Station

² Access Service Network

³ Connectivity services



Слика 13.30 WiMAX референтни модел, декомпозиција ASN мреже

рачуна о повезивању на слоју 2, преусмеравању свих AAA¹ порука ка матичном интернет посреднику (H-NSP² посредник), преусмеравање порука 3. слоја (нпр. порука DHCP протокола и мобилног IP протокола). Логичка декомпозиција ASN мреже приказана је на слици 13.30. Две најважније компоненте ASN мреже су радио базне станице (BS станица) и међумрежни пролаз ASN мреже (ASN-GW³). ASN-GW је међумрежни пролаз ка IP мрежи и крајњи терминал од RP3 референтне тачке што ће касније бити описано.

- Мрежа за пружање услуге повезивања је (CSN⁴ мрежа). CSN мрежа је целина (субјекат) која има право на управљање везом на IP слоју претплатничких терминала. Прецизније она обухвата следеће задатке:
 - обезбеђивање IP адреса,
 - међумрежни пролаз ка другим мрежама,

¹ Authentication, Authorization and Accounting

² Home Network Service Provider

³ Access Service Network Gateway

⁴ Connectivity Service Network

- реализацију AAA функција,
- вођење рачуна о мобилности у оквиру ASN мреже коришћењем мобилног IP протокола.

MS станица, ASN мрежа или CSN мрежа дефинисане су преко логичких функционалних целина које се могу реализовати у једној крајњој станици или се могу дистрибуирати на више крајњих станица.

13.10.3 Логички домени

Логички домени могу се посматрати као група функција које могу бити повезане у један домен. На слици 13.29 представљена су три логичка домена:

- Тачка приступа мрежи (NAP¹ тачка). Представља физичку тачку коју користи претплатнички терминал када приступа мрежи. Са логичке тачке гледишта ASN мрежа која опслужује MS станицу део је тачке приступа мрежи.
- Матични интернет посредник (H-NSP посредник). H-NSP посредник је WiMAX добављач интернет услуга са којим WiMAX претплатник има уговор о нивоу услуга². Пословна целина аутентификује и ауторизује претплатничке сесије и одговорна је за процедуре израчунавања и тарифирања чак и при преласку из сопствене (матичне) мреже у другу мрежу (роминг).
- Посећени интернет посредник (V-NSP³ посредник). V-NSP посредник је WiMAX добављач интернет услуга који претплатник користи да би приступио мрежи када је у ромингу без обзира што нема потписан уговор о нивоу услуга са V-NSP посредником. Опсег услуга који V-NSP посредник обезбеђује претплатнику зависи од роминг везе између V-NSP и H-NSP посредника.

13.10.4 Референтне тачке

Посматрајући слику 13.29 референтна тачка (Rx⁴ тачка) је крајња тачка комуникације између функционалних целина и чини стандардни интерфејс који се мора користити за постизање укупне

¹ Network Access Point

² Service Level Agreement

³ Visited Network Service Provider

⁴ Reference Point

интероперабилности између компонената различитих произвођача. Спецификација WiMAX Forum дефинише неколико референтних тачака у мрежном референтном моделу и такође обезбеђује три примера профила. Сваки профил укључује само подскуп ових референтних тачака. У даљем излагању биће описане најбитније референтне тачке које су дефинисане у мрежном референтном моделу. То су:

- Референтна тачка R1 - састоји се од протокола и процедура које се користе на ваздушном интерфејсу између MS станице ASN мреже. То је радио и MAC WiMAX интерфејс;
- Референтна тачка R3 - представља интерфејс између ASN мреже и CSN мреже (којом управља или H-NSP или V-NSP посредник). Ове две функционалне целине користе овај интерфејс за пренос AAA порука и порука везаних за управљање мобилним IP протоколом. У пракси овај интерфејс је линк са IP протоколом који даје подршку RADIUS¹ протоколу;
- Референтна тачка R4 - одговорна је за комуникацију између ASN мрежа којима управља иста CSN мрежа. На пример када MS станица обавља хендовер² између две ASN мреже у истој NSP мрежи AAA фаза може се избећи коришћењем комуникације преко овог интерфејса;
- Референтна тачка R5 - дефинише и обезбеђује међумрежне функције између CSN мрежа којима управљају H-NSP или V-NSP посредници. Овај интерфејс би у пракси била IP путања која би могла да се рутира кроз додељене³ или чак и јавне мреже;
- Референтна тачка R8 – користи се у оквиру ASN мреже са више базних станица (BS станица) R8 да подржи брз и неприметан хендовер мобилних станица.

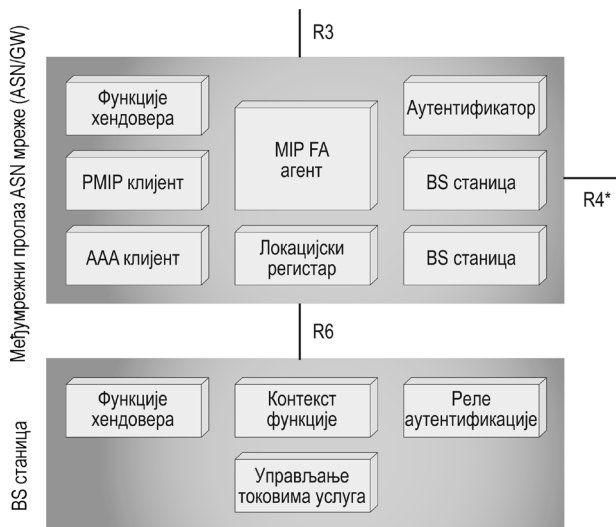
13.10.5 Профили ASN мреже

Посматрајући логичку архитектуру приказану на слици 13.30 могуће имплементације су предложене и описане у спецификацији организације

¹ RADIUS (*Remote Authentication Dial In User Service*) је мрежни протокол који обезбеђује централизовано управљање аутентификацијом, ауторизацијом и обрачунавањем (AAA - *Authentication, Authorization, Accounting*) за рачунаре који се повезују на мрежу и користе је.

² Handover

³ Dedicated



* Мобилност када је MS станица учвршћена за ASN мрежу могућа је преко R6 и R4 тачака.

* Подршка за ову функцију је опциона

Слика 13.31 WiMax профил за А имплементацију ASN мреже

WiMAX Forum. Ове опције називају се профили¹ и разликују се за различите референтне тачке. На сликама 13.31 и 13.32 представљена су два ASN профила (А и В) које је предложио WiMAX Forum са циљем да се усмери ASN имплементација ка двома најчешћим конфигурацијама.

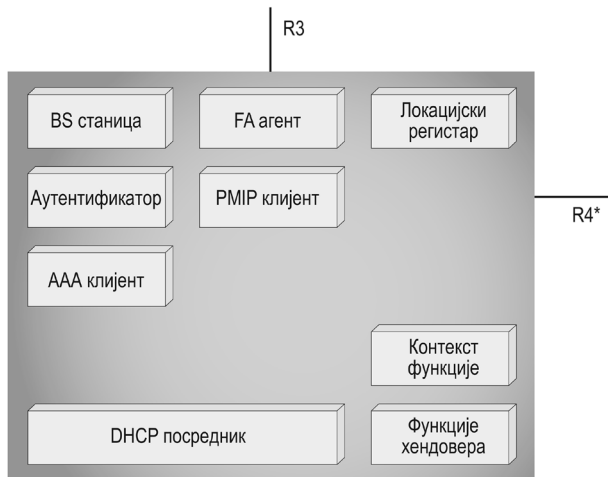
Профил А (слика 13.31) ће се користити у конфигурацији где један међумрежни пролаз ASN мреже (ASN-GW) управља са више базних станица. Оваква конфигурација је погодна када је потребно покрити већа пространства (области) или када се ради са великим бројем корисника. Мобилношћу потпуно руководи међумрежни пролаз ASN мреже (ASN-GW) који управља хендовером претплатника преко R4 референтне тачке².

Профил В приказан на слици 13.32 представља конфигурацију са физичком колокацијом³ међумрежног пролаза ASN мреже (ASN-GW) и базне станице (BS станица). Све функције ASN мреже укључене су у једну

¹ Profiles

² ASN-anchored mobility

³ Co-location



Слика 13.32 WiMax профил за В имплементацију ASN мреже

целину што као предност даје смањење комплексности. Недостатак овог решења је 1:1 однос између међумрежног пролаза ASN мреже (ASN-GW) и базне станице (BS). Због тога ово решење одговара само у случају малог броја корисника дислоцираних у локализованој области.

Функционална декомпозиција скицирана на сликама 13.31 и 13.32 указује да су ASN мрежи присутне целине потребне за подршку AAA процедурама, MIP¹ усаглашеној мобилности и DHCP² протоколу. Различита локација ових целина је најважнији елемент на који треба указати када се упоређују ова два профила.

Избор профила треба да буде у зависности од потреба за облашћу покривености и њеног утицаја на цену хардвера и софтвера потребног за то решење. На пример, када је примењен профил А може се користити хардвер и софтвер различитих произвођача што може довести до неконзистентности и некомпатибилности. Када је примењен профил В ови проблеми се избегавају (R1 и R4 су стандардни и широко примењени интерфејси) али је ограничена могућност проширења.

13.10.6 Хендовер процедура у WiMAX мрежи

¹ Mobile IP

² Dynamic Host Configuration Protocol

Мобилна станица у WiMAX мрежи може да мења тачке прикључивања на мрежу и реализује хендовер. Две различите врсте хендовера су могуће: када је мобилна станица учвршћена за ASN мрежу¹ или учвршћена за CSN мрежу². Посматрајући слику 13.29 у првом случају базне станице са којима се мобилна станица повезује при кретању налазе се у истој ASN мрежи. Међумержни пролаз (ASN-GW) са којим су базне станице повезане је исти, тако да не постоји потреба да се иновирају табеле рутирања или мрежне адресе. У овом случају хендовером управљају целине ASN мреже и немају никаквог утицаја на IP слој. У другом случају мобилна станица (MS станица) креће се из једне ASN мреже у другу. CSN мрежа на коју су повезане ASN мреже може да буде иста уколико нова ASN мрежа припада H-NSP посреднику или друга уколико нова ASN мрежа припада V-NSP посреднику.

У другом случају нова CSN мрежа ће се понашати као посредник и резултат је суштински исти. Подсетимо се да ASN мрежа није монолитна компонента већ се састоји од већег броја подмодула. Ови подмодули могу да буду физички смештени у истој крајњој станици (хосту) као што је то представљено на слици 13.32 или одвојени као што је представљено на слици 13.31. Промена тачке прикључивања мобилне станице значи промену базне станице али у зависности од изабране конфигурације може да значи промену других функционалних целина као што су аутентификатор или мобилни спољни агент (MIP FA³). У одељку који следи сматраћемо да је реч о мобилној станици учвршћеној за CSN мрежу пошто она директно утиче на мрежни слој. WiMAX мрежа требало би да обезбеди роинг корисницима који желе да задрже активне сесије у случају хендовера.

Два су предуслова да се сесија одржи активном: задржавање исте IP адресе код хендовера и иновирање реверзне руте од удаљеног одредишта у мобилној станици. Овај задатак се може одрадiti употребом мобилног IP протокола за мобилну станицу који подржава овај стандард. Уколико мобилна станица користи само DHCP протокол, онда се исти резултат може добити комбиновањем DHCP протокола за мобилну станицу и MIP

¹ *ASN anchored*

² *CSN anchored*

³ *Mobile IP Foreign Agent*

протокола који се користи само за крајње станице¹.

WiMAX Forum је обратио пажњу на неколико проблема умрежавања користећи структуру стандардних протокола прилагођених за специфичне проблеме WiMAX мрежа. Један од проблема је да не постоји стандард и уобичајени начин за пребацивање конфигурационих параметара са централизованог сервера у мобилну станицу. У принципу када мобилна станица улази у мрежу (по први пут или током хендовера) процедура аутентификације је једина фаза у којој су мобилни терминал, ASN мрежа и CSN мрежа присиљени да комуницирају. То је једини тренутак када се аутентификација, умрежавање и IP параметри могу пребацивати са позадинског управљања ка остатку мрежа. У пракси ово се дешава по следећој шеми:

- Параметри за одређени терминал или крајњег корисника чувају се у бази података којој RADIUS сервер има приступ;
- Ови параметри се премештају у аутентификатор користећи атрибуте RADIUS протокола преко референтних тачака R3 и R5;
- Од аутентификатора, користећи прилагођене протоколе, премештају се на друге елементе мреже. На пример QoS параметри су премештени у базну станицу заједно са MSK² кључем који је договорен у току аутентификације;
- Ако неки од њих морају да се преносе у мобилну станицу онда се они убацују у DHCP екстензију која ће бити коришћена за мобилну станицу преко R1 референтне тачке.

Треба уочити да је RADIUS протокол једини стандардни начин којим се премештају параметри из CSN мреже у ASN мрежу. У ASN мрежи крајња тачка која са њима управља је IEEE802.1x аутентификатор.

13.10.7 DHCP протокол и WiMAX мобилни системи

Мобилна станица која не подржава MIP протокол може да има статичку преконфигурисану IP адресу или може да користи DHCP протокол да добије нову IP адресу на сваком хендоверу (приликом сваког

¹ Back-end

² Master Session Key - привремени криптографски кључ из кога се изводе остали кључеви који служе за шифровање и дешифровање порука у току трајања једне сесије.

преузимања станице). Чак и у првом случају хендовер¹ не може да буде транспарентно за IP слој пошто је потребно остале мрежне параметре иновирати. Посебно на страни клијента мобилна станица ће морати да ажурира своју путању (руту) ка новом подразумеваном међумрежном пролазу или IP адреси неког DNS сервера присутног у новој мрежи. Не постоји други стандардни протокол који би могао да пребацује ове параметре ка мобилној станици осим DHCP протокола. Тако да ће мобилна станица, чак и ако има статички конфигурирану IP адресу, имати потребу да користи DHCP протокол.

На крају успешне аутентификације ASN мрежи још увек није познато да ли мобилна станица јесте MIP компатибилна или није. Разлика је заснована на активности мобилне станице. Ако је први пакет који шаље мобилна станица DHCP DISCOVER рам, ASN мрежа ће закључити да је DHCP компатибилна станица. Ако је рам MIP захтев за регистрацију ASN мрежа ће закључити да је реч о MIP компатибилној станици. У првом случају ће морати да активира DHCP процедуре а можда и PMIP² процедуру.

DHCP протокол може бити конфигурисан у WiMAX мрежи на два начина. Може се користити субјекат (целина³) који игра улогу DHCP агента за прослеђивање или DHCP посредника. У првом случају одговарајућа целина у ASN мрежи се не понаша као класичан DHCP сервер већ само прослеђује захтеве удаљеном серверу. У другом случају сам ASN је тај који одговара на DHCP REQUEST рам и додељује IP адресу мобилној станици. Треба имати на уму да, уколико желимо да сесија остане активна, IP адреса мора бити иста пре и после предаје мобилне станице.

Ако се DHCP сервер понаша као реле (агент за прослеђивање) његова улога биће да проследи DHCP REQUEST на други сервер који мора да буде исти онај који је користила мобилна станица у својој првој аутентификацији. DHCP реле (агент за прослеђивање) не може знати IP адресу овог сервера, тако да ова информација мора бити укључена, на неки начин, у информације које ASN мрежа прима на крају аутентификације, као RAIDUS атрибут. Овај параметар може

¹ Преузимање станице, прелазак станице, предаја станице

² Proxy-MIP

³ Entity

бити унапред конфигурисан (преконфигурисан) у ASN мрежи, али такав приступ није употребљив у мрежама са више оператера¹ у које клијент може да дође из спољне мреже².

Слично томе, ако је ASN мрежа конфигурисана да се понаша као DHCP посредник, она ће морати да одговори на DHCP DISCOVER поруку са истом IP адресом коју је користила мобилна станица пре хендовера (преузимање станице). Порука DHCP DISCOVER може да носи одређену опцију којом клијент тражи да му се додели IP адреса коју он већ користи. Из сигурносних разлога ова одлука не може бити заснована на IP адреси коју мобилна станица за себе захтева пошто су DHCP рамови неаутентификовани и мобилна станица можда покушава да добије туђу адресу. Опет, IP адреса која се додељује мобилној станици биће укључена у одређени RADIUS атрибут који је укључен у приступи/прихвати пакет који долази из CSN мреже.

13.10.8 Мобилни IP протокол и WiMAX мобилни системи

Мобилни IP протокол је стандардни комуникациони протокол³ организације IETF⁴ чија је основна намена да омогући кориснику да има сталну IP адресу док се креће и мења своју тачку приступа мрежи. Ова функција веома је корисна за све оне везе код којих је потребна стална веза током корисничког роминга кроз мрежу. У претходном одељку објаснили смо како је могуће користити DHCP да се задржи иста IP адреса за време хендовера. Ово је неопходно да се задржи сесија активном, али то није довољно. Други крај комуникационе везе ће примати IP пакете, али његови одговори ће бити усмерени ка сопственој мрежи чвора. Достављање пакета из сопствене мреже у гостујућу мрежу⁵ обезбеђује мобилни IP протокол.

Мобилни IP протокол решава проблем одржавања сесије помоћу две адресе за сваки терминал: сопствене адресе и заштитне адресе (COA⁶ адреса). Сопствена адреса је IP адреса чвора коју је добио од свог

¹ *Multi-operator networks*

² *Foreign network*

³ Описан у документима RFC5944 и RFC4721.

⁴ *Internet Engineering Task Force*

⁵ *Visited network*

⁶ *Care-of-Address*

сопственог агента (HA¹ агента) на својој сопственој мрежи. Ова IP адреса је она која ће остати непромењена (фиксна) за време роминга. COA² адреса је адреса коју је чвору дао спољни агент (FA³ агент), агент мобилности који је задужен да обезбеди IP адресе терминалима који су прикључени на V-NSP мрежу.

Начин на који мобилни IP (MIP) протокол ради може се укратко представити:

1. У време своје прве аутентификације мобилна станица добија IP адресу од свог HA агента у својој сопственој мрежи. Докле год је станица покривена овом мрежом пакети ка и од тог чвора усмеравају се једноставно користећи ову адресу и мобилни IP протокол се не користи.
2. Када се мобилни терминал помери изван своје сопствене (матичне) мреже ка другој мрежи он трага за FA агентом и добија COA адресу од њега.
3. Након доделе COA адресе мобилна станица започиње MIP регистрацију са HA агентом користећи стандардну процедуру слањем захтева за регистрацију (RRQ⁴). Ова регистрација има намеру да обавести HA агента о тренутној COA адреси која треба да се користи да би се дошло до терминала на посећеној (гостујућој) мрежи. Да би потврдио да је регистрацију добио HA агент шаље назад одговор (RRP⁵).
4. Пут до и од мобилне станице мора да се промени након регистрације у спољном домену. Када мобилна станица жели да комуницира са удаљеном станицом она користи директну путању из своје гостујуће мреже. Када удаљена станица жели да комуницира са мобилном станицом она мора да користи технику троугластог рутирања⁶. Удаљена станица шаље свој пакет (IP датаграм) на матичну адресу мобилне станице. HA

¹ Home Agent

² Care-of-Address

³ Foreign Agent

⁴ Registration Request

⁵ Registration Reply

⁶ Triangular routing

Стандард IEEE	Опис	Статус
802.16-2001	Бежични широкопојасни фиксни приступ (<i>Fixed Broadband Wireless Access</i>) 10 - 63 GHz	Замењен
802.16.2-2001	Препоручена пракса за коегзистенцију (<i>Recommended practice for coexistence</i>)	Замењен
802.16-2004	Ваздушни интерфејс за бежични широкопојасни фиксни приступ (<i>Air Interface for Fixed Broadband Wireless Access System</i>) Збирно 802.16 - 2001, 802.16a, 802.16c и P802.16d)	Замењен
802.16f-2005	MIB база података (<i>Management Information Base</i>) за 802.16-2004	Замењен
802.16e-2005	Мобилни бежични широкопојасни приступни систем (<i>Mobile Broadband Wireless Access System</i>)	Замењен
802.16k-2007	Премошћавање (<i>Bridging</i>) за 802.16 (проширење за IEEE802.1D)	Важећи
P802.16i	Мобилна MIB база (<i>Mobile Management Information Base</i>) Пројекат спојен са 802.16-2009	Припојен
802.16-2009	Ваздушни интерфејс за системе са фиксним и мобилним широкопојасним приступом (<i>Air Interface for Fixed and Mobile Broadband Wireless Access System</i>) Збирно: 802.16-2004, 802.16-2004/Cor 1, 802.16e, 802.16f, 802.16g и P802.16i.	Важећи
802.16j-2009	Преусмеравање у више скокова (<i>Multihop relay</i>)	Важећи
802.16h-2010	Механизам за унапређену коегзистенцију за рад код изузетих лиценци (<i>Improved Coexistence Mechanisms for License-Exempt Operation</i>)	Важећи
802.16m-2011	Унапређен ваздушни интерфејс са брзинама од 100Mb/s за мобилне и од 1Gb/s за фиксне кориснике. (<i>Advanced Air Interface with data rates of 100 Mbit/s mobile and 1Gbit/s fixed</i>) Познат као <i>Mobile WiMAX Release 2</i> или <i>WirelessMAN-Advanced</i> са циљем да испуни ITU-R IMT-Advanced захтеве за 4G системе.	Важећи
P802.16n	Мреже високе поузданости (<i>Higher Reliability Networks</i>)	У току је израда

Табела 13.6 Опис и статус стандарда IEEE802.16x

агент ће добити овај пакет, одредити тренутну COA адресу за мобилну станицу (на основу последњег поступка регистрације), послати пакет правом FA агенту који прослеђује IP датаграм мобилној станици.

13.11 Питања и задаци

1. Описати намену регулаторних тела за бежичне системе.
2. Које асоцијације произвођача бежичних система постоје?
3. Који се опсези без посебних дозвола користе код бежичних система?
4. Категоризовати бежичне рачунарске мреже по физичкој топологији?
5. Набројати предности испреплетаних мрежа.
6. На коликом су растојању носиоци и колика је ширина канала код IEEE 802.11?
7. Који непреклапајући канали могу истовремено да се користе у бежичним локалним рачунарским мрежама Европе а који у САД?
8. Описати основни принцип рада протокола CSMA/CA.
9. Описати проблем скривеног терминала и начин разрешавања.
10. Нацртати и описати архитектуру протокола по стандарду IEEE802.11-2012. Које су измене предложене проширењем IEEE802.11s?
11. Описати приступне категорије и њихову намену.
12. Описати времена дефинисана стандардом IEEE802.11-2012.
13. Нацртати и описати компоненте инфраструктурне IEEE802.11 мреже.
14. Како се повезују инфраструктурна и испреплетана мрежа?
15. Описати MIMO технологију и њену примену.
16. Која су основна обележја Bluetooth технологије.
17. Направити компаративну анализу Bluetooth верзија стандарда.
18. Која је намена Bluetooth профила? Навести један пример.
19. Нацртати и описати архитектуру протокола Bluetooth система.
20. Упоредити Bluetooth и IEEE802.15 архитектуре протокола?
21. Који IEEE се стандард односи на сензорске мреже?
22. Нацртати и описати ZigBee архитектуру протокола.
23. Које врсте чворова постоје у ZigBee мрежама?
24. Који фреквенцијски опсези се користе код сензорских мрежа?
25. Који се алгоритми за рутирање користе код сензорских мрежа?